1. Bespreek de diverse namen die alle Active Directory objecten identificeren. (§2.2.1)

* **Relative distinguished name**, RDN
  + Zorgt ervoor dat het object uniek kan geidentificeerd worden binnen een containerobject
  + Hoeft niet uniek te zijn op globale Active Directory Niveau
* **Distinguished name**, DN
  + Samenstelling van RDN van het object zelf en de RDNS van alle containerobjecten waarvan het object hierarchish deel uitmaakt.
  + DN is uniek en belangrijk voor de werking van LDAP protocol
  + Heeft als naamconventie attributed naming; elk opeenvolgend deel wordt geschreven als attribuut=waarde koppel en bevat een verwijzing naar de bovenliggende structuur. Heeft komma als scheidingsteken
* **Canonical name**
  + Samenstelling zelfde als DN, maar eenvoudigere notatie
  + Wordt het meest getoond in de Active Directory
* **Globaal unieke ID**, GUID
  + 128bit getal, onwijzigbaar

1. Wat zijn SPN objecten ? Bespreek de aanvullende naamgeving voor deze objecten. (§2.2.2)

**Security principal objects** zijn Active Directory objecten waaraan security ID’s zijn toegewezen (opgeslagen in objectSid). SPN objecten worden gebruikt voor het verlenen van toegang tot domeinbronnen. SIDs zijn uniek. De notatie van SID is prefix (revision level en Authority identifier) – domain identifier – relative id. Een nieuwe account kan nooit de rechten en machtigingen bezitten van een oude, omdat het SID niet hetzelfde is. Er wordt ook en sIDHistory bijgehouden die alle SIDs bijhoudt die een object ooit gehad heeft. Samen met de GUID, DN en Canonieke naam zorgt de SID voor een unieke idenificatie.

1. Enkele veel gebruikte klassen (hiermee worden attributeschema en classschema objecten niet bedoeld) vertonen nog meer identificerende attributen voor hun instanties. Bespreek deze klassen en attributen.

Gebruikersobjecten heeft een eenvoudige aanmeldingsnaam nodig. Hiervoor worden **User Principal Names** (UPN), aanmeldingsnamen bijgehouden. Deze worden bij het maken van het gebruikersaccount door de beheerder ingevoerd. Deze moet uniek zijn. Standaard is deze RDN@UPN Suffix waarbij de UPN suffix de DNS domeinnaam is waarin het gebruikersaccount zich bevindt, of de DNS Domeinnaam van het root domein of een willekeurige naam die geregistreerd is. Het kan ook een willekeurige alternatieve naam zijn (indien die op voorhand bij de beheerder is geregistreerd)

Computeraccounts hebben ook een

* Sam accountnaam die standaard bestaat uit de eerste 15bytes van RDN + $. Deze naam kan aangepast worden.
* DNS hostnaam die standaard uit eerst 15bytes van RDN + suffix voor primaire DNS bestaat. Er kunnen meer dan 15 bytes gebruikt worden en een suffix van een andere DNS.
* Server principal name wordt samengesteld op basis van de DNS hostnaam en eventuele SRV records. De SPN wordt gebruikt voor de wederzijdste verificatie van clients software en de server die een service biedt.

1. In welke partities is de Active Directory informatie verdeeld ? Geef de betekenis van elke partitie, hun onderlinge relatie (zowel fysiek als met betrekking tot hun naamgeving), en de replicatiekarakteristieken ervan. (laatste helft §2.2.3)

* **Domeingegevens**
  + Bevatten de eigenlijke informatie over objecten in het domein, zoals gedeelde bronnen.
  + Wanneer er wijzigingen gebeuren in de directory van de organisatie, wordt dit ook hier opgeslagen.
  + Er zijn evenveel partities met domeingegevens als dat er domeinen in het forest zijn, ook hebben domeingegevens betrekking op slecht 1 domein en worden ze niet gedistribueerd naar andere domeinen.
* **Applicatiepartities**
  + Kunnen geen SPN ojecten bevatten, ook kunnen zijn objecten niet buiten de partitie verplaatst worden.
  + Zijn interessant als container voor dynamische objecten
  + Niet altijd aanwezig
* **Configuratiegegevens**
  + Dit zijn de fysieke topologie van de directory, ze bevatten een lijst van alle domeinstructuren, locaties van domeincontrollers en global catalog controllers, de sites en replicatietopologie.
  + Veel van de voor het ganse forest gemeenschappelijke instellingen worden vertaald in kenmerken van objecten in de configuratiegegevens. Zo moet enkel de uPNSuffixes van de Partitions container aangepast worden om de mogelijke UPN Suffices van het forest in te stellen. De Partition container bevat ook crossRef objecten met een nCName kenmrk dat verwijst naar 1 van de directory partities in het forest
* **Schema** is de formele definitie van alle objecten en kenmerkgegevens die kunnen worden opgeslagen in de directory. Uniek voor alle domeinen in het forest

Schema, configuratiegegevens zijn containerobjecten in het root domein van het forest. Eventuele applicatiepartities zijn containerobjecten tov de overeenkomstige domeingegevens. Dit is een logische structurering. Fysiek zijn de schema en applicatie partitie een aparte entiteit die geen deel uitmaken van de configuratiegegevens.

Elke partitie in de directory vormt een aparte eenheid voor replicatie, waarbij telkens een specifieke groep controllers hoort. Schema en configuratiegegevens worden gerepliceerd naar alle domeincontrollers in het forest, de domeingegevens enkel naar eigen domein.

Een subset van alle objecten in de domeingegevens van elk domein in het forest worden gerepliceerd naar de globale catalogus.

1. Bespreek het doel en de werking van attributeSchema objecten. Hoe kunnen deze objecten het best geraadpleegd en gewijzigd worden ?

Ze zorgen ervoor dat elk kenmerk slechts eenmaal gedefinieerd moet worden en in meerdere klassen kan gebruikt worden. Voor elk kenmerk in het schema is er een atributeSchema waarmee het kenmerk kan worden ingesteld en beperkingen opgelegd worden.

Voor ontwikkelingsodeleinden kan je *adsiedit.msc* gebruiken, met de Active Directory Schema snap-in *schmmgmt.dll* die geinstalleerd kan worden met regsvr32 kan je echter eenvoudiger bekijken, wijzigen en creeeren. Verwijderen van schemaobjecten is niet mogelijk, deactiveren wel.

1. Bespreek de diverse naamgevingen, specifiek voor attributeSchema objecten.

Alle attributeSchema objecten hebben een viervoudige naamgeving, elk uniek en gestandaardiseerd

* **Common name**, de RDN van het attrbuteSchema object in het Schema
* **GUID** van het kenmerk (onafhankelijk van GUID van attributeSchema object), dat automatisch kan gegenereerd worden.
* **LDAP display name**, voor de progammatische toegang
* **Object identifier**, voor de interne representatie. X.500 Object IDs worden verleend door speciale autoriteiten. Het is een decimale reeks met punten, gegarandeerd over de hele wereld.

1. Bespreek de belangrijkste kenmerken van attributeSchema objecten, en op welke waarden die ingesteld kunnen worden.

* attributeSyntax en oMSyntax
  + Syntax van een kenmerk bepaalt het data type. Er zijn 26 mogelijkheden waarvan 18 effectief gebruikt
  + Het is niet mogelijk omeen nieuwe syntax te definieren
  + Geidentificeerd door een objectID van de vorm 2.5.5.x
  + De oMSyntax dient voor het diversifieren obv een Int waarde
* rangeLower en rangeUpper
  + Bereikbeperkingen
* isSingleValued
  + Kenmerken kunnen een of meer niet geordende waarden hebben.
* searchFlags
  + Bevat binaire informatie waarbij meeste bits bepalen of het kenmerk geindexeerd wordt en zijn gebruikers dus sneller te vinden zijn.
  + Indien ingesteld:
    - Laagste bit: bepaalt eenvoudige indexering van de waarde van het kenmerk, onafh waar het object zich bevindt
    - 2e laagste bit: waarde van het kenmerk gecombineerd met ID van de container waarin het object zich bevindt. Snel binnen containers zoeken
    - 3e laagste bit: Ambiguous Name Resolution, wanneer men wil zoeken waar minstens 1 kenmerk een specifieke waarde aanneemt.
    - 6e laagste bit: versnelt opzoekingen waarin kenmerken wildcards gebruiken. Dergelijke tuple indexen worden vermeden door hoog resourceverbruik.
    - 5e laagste bit: Bepaalt of de waarde van het attribuut behouden blijft indien gekopieerd
* systemFlags
  + Laagste bit bepaalt of het kenmerk gerepliceerd wordt naar andere domeincontrollers. Niet repliceren wordt vaak toegepast op dynamische kenmerken.
  + 3e laagste bit wijst op een geconstrueerd attribuut, dat niet opgeslagen wordt in Act. Dir. Maar telkens berekend wordt.
* isMemberOfPartialAttributeSet
  + Bepaalt of het kenmerk in de global catalog wordt opgenomen
* linkID
  + Somige kenmerken vormen koppels met forward-link en back-link kenmerken. Indien forward-link wijst naar en DN van een ander object, wordt de back-link van dat object automatisch ingevuld en vice versa.
  + Forward link kan door gebruikers met voldoende machtigingen gewijzigd worden, back link door Security Accounts Manager van WIndows Server

1. Welke andere types objecten bevat het Active Directory schema, en wat is hun bedoeling ? (o.a. §2.2.7)

Naast classSchema en attributeSchema het subSchema met RDN als aggregate. Aggregate bevat compacte representatie, abstracte schema genoemd. De bedoeling is om vereenvoudigde schema gegevens ter beschikking te stellen. Gecombineerd met Active Directory Service Interfaces (ADSI) biedt het abstracte schema een toegang naar het schema (meer high leel dan reele schema).

1. Via welke attributen kun je de klasse van een willekeurig Active Directory object achterhalen ? Hoe moet je op zoek gaan naar alle objecten van een bepaalde klasse ? Illustreer aan de hand van relevante voorbeelden. (laatste paragraaf §2.2.6)

Met objectClass krijg je de klasse + als zijn superklassen. Het is multi-valued en niet geindexeerd. Voor user object krijg je dan {user, superklasse, superklasse} voor computer krijg je {computer, user, superklasse, superklasse}

Met objectCategory kan je de meest typische vertegenwoordiger krijgen uit verzameling van klasse en alle superklassen. Voor user en computer krijg je person en computer.

Om te zoeken moet je slim kiezen tussen het ene of het andere of een combo. Bijvoorbeeld om een gebruikers te vinden kan je objectCategory proberen (je wil person voor gebruikers), maar dan ga je niet enkel users vinden maar ook bijvoorbeeld contact objecten. Als je met objectClass probeert objecten te vinden die user bevatten, ga je ook computers vinden. Je wil dus zowel person in objectCategory als uer in objectClass.

1. Bespreek het *doel* en de *werking* van classSchema objecten.

Ze beschrijven directory objecten die gemaakt kunnen worden. Elke klasse heeft een verzameling kenmerken die het object beschrijven. De kenmerken bevatten twee soorten regels; structuurregels die definieren wat de mogelijke hierarchische relaties zijn tussen klassen of objecten en inhoudsregels die kenmerken definieren die beschikbaar zijn voor de klasse.

1. Hoe benadert Active Directory het mechanisme van *overerving* ?

Door overname kan je uit een bestaande klasse een nieuwe maken. De bestaande wordt dan de superklasse van de nieuwe genoemd. Alle klassen erven over van Top. Een subklasse neemt de kenmerken van de superklasse over, inclusief zijn structuur- en inhoudsregels. Overname werkt recursief (dus alle kenmerken van alle superklassen overneemt). Een klasse kan enkel kenmerken overnemen van zijn onmiddellijke superklasse en hulpklassen. Het instellen van de kenmerken auxiliaryClass of systemAuxiliairyClass is de statische variant van het gebruik van hulpklassen; alle objecten die gecreerd worden op basis van de klasse die verwijst naar een hulpklasse kan zo over de kenmerken van de hulpklasse beschikken. Hulpklassen kunnen echter ook dynamisch gebruikt worden, door bij de creatie van een object het objectClass kenmerk aan te vullen met de naam van de hulpklasse erft enkel de representant de kenmerken van de hulpklasse.

1. Bespreek de diverse *naamgevingen*, specifiek voor classSchema objecten

Alle attributeSchema objecten hebben een viervoudige naamgeving, elk uniek en gestandaardiseerd

* **Common name**, de RDN van het attrbuteSchema object in het Schema
* **GUID** van het kenmerk (onafhankelijk van GUID van attributeSchema object), dat automatisch kan gegenereerd worden.
* **LDAP display name**, voor de progammatische toegang
* **Governs identifier**, voor de interne representatie. X.500 Object IDs worden verleend door speciale autoriteiten. Het is een decimale reeks met punten, gegarandeerd over de hele wereld.

1. Bespreek de belangrijkste *kenmerken* van classSchema objecten, en op welke waarden die ingesteld kunnen worden.

* objectClassCategory
  + Bevat een Integer waarde die de categorie van de klase bepaalt; structureel, abstract (gebruikt voor verzameling kenmerken) of hulpklasse
* possSuperiors en systemPossSuperiors
  + Definieren de hierarchische relaties tussen objecten van een klasse. Een structurele klasse kan containerobjecten genereren van zodra een andere structurele klasse ernaar verwijst in de possSuperiors of systemPossSuperiors kenmerken.
* rDNAttID
  + bepaalt welk kenmerk van en klasse gebruikt wordt om de RDM van objecten te bepalen
* defaultSecurityDescriptor
  + Bepaalt expliciete machtigingen die gelden voor objecten van deze klassen. Het biedt een eenvoudige oplossing om het beheer van specifieke objecten te delegeren.
* systemOnly
  + Structuur- en inhoudsregels kunnen niet gewijzigd worden indien een klasse dit kenmerk heeft.
* objectClass en objectCategory
  + Bevatten respectievelijk de klasse en zijn superklassen en de meeste typische vertegenwoordiger van de klasse bestaande uit de verzameling van de klasse zelf en zijn superklassen

Kenmerken die exampleren van een bepaalde klasse kunnen hebben,worden gedefinieerd door inhoudsregels. Er zijn mandatory attributes aangeduid door (system)mustContain en optional attributes (system)mayContain

1. Welke andere types objecten bevat het *Active Directory schema*, en wat is hun bedoeling ? (o.a. §2.2.7)

Naast classSchema en attributeSchema het subSchema met RDN als aggregate. Aggregate bevat compacte representatie, abstracte schema genoemd. De bedoeling is om vereenvoudigde schema gegevens ter beschikking te stellen. Gecombineerd met Active Directory Service Interfaces (ADSI) biedt het abstracte schema een toegang naar het schema (meer high leel dan reele schema).

1. Hoe en met welke middelen kan het Active Directory schema uitgebreid worden ? Waarom moet je en hoe kan je hierbij *voorzichtig* te werk gaan ? (§2.2.8, ldifde fractie §2.2.3)

Het uitbreiden van een schema is een risicovolle bewerking, verkeerde wijzigingen kunnen het hele netwerk beschadigen of uitschakelen. Wanneer je een schema uitbreidt geldt de uitbreiding voor het hele forest. Uitbreidingen bieden echter wel veel potentieel, en zijn zeer eenvoudig te realiseren.

Enkele richtlijnen:

* Ontwikkel in een geisoleerde omgeving
* Maak enkel nieuwe stucturele klassen indien geen enkele bestaande klasse enigszins aan de behoeftheden voldoet
* Vermijd wijzigingen aan attributen van bestaande klassen

De aanbevolen manier om het Active Directory Schema uit te breiden op grotere schaal is *ldifde* (LDAP Data Interchange Format). Het gaat ook met de AD schema snap-in

1. Wat is de bedoeling van *vertrouwensrelaties* ?

Wanneer er een vertrouwensrelatie is tussen twee domeinen kunnen gebruikers in het ene vertrouwd domein geverifieerd worden door de domeincontroller in het andere vertrouwend domein. Met een continue rij vertrouwensrelaties kan je een vetrouwenspad maken. Dat een gebruiker door een trusting domeincontroller is geverifieerd wil nog niet direct zeggen dat de gebruiker toegang heeft tot de bronnen in dat domein. Deze toegang wordt geregeld met gebruikersrechten en machtigingen die aan de gebruiker zijn toegekend door de domeinbeheerder van het trusting domain.

1. Bespreek de verschillende *soorten* vertrouwensrelaties.

* Expliciete vertrouwensrelaties
  + Trusts die je zelf maakt, in tegenstelling tot degene die automatisch gemaakt worden tussen domeinen van eenzelfde forest bij creatie van een domein
    - Forest trusts: vertrouwensrelaties tussen de root domeinen van forests
    - Realm trust: veralgemening van forest trust, die vertrouwenspaden leggen tussen domeinen en Kerberos Realms. Kan zowel bidirectioneel als enkelvoudig, transistief als niet-transistief zijn
    - Shortcut/cross-link trusts: verkorte vertrouwensrelaties die gebruikt kunnen worden om het vertrouwenspad in grote en complexe trees korter te maken. Zowel enkel als bi
    - Externe trusts: enkelvoudige vertrouwensrelatie waarbij 1 domein een ander vertrouwt. Ze zijn niet transistief.

1. Op welke diverse manieren kunnen vertrouwensrelaties *gecreëerd* en *gecontroleerd* worden ? Bespreek ook de *optionele configuratiemogelijkheden*.

Dit kan automatisch gebeuren, Windows Server maakt automatisch vertrouwensrelaties tussen domeinen en hun child domeinen. Ook maakt het automatisch vertrouwensrelaties tussen trees van eenzelfde forest.

Om expliciete vertrouwensrelaties te maken, moet je beschikken over domeinnamen en een gebruikersaccount met machtigingen om in beide domeinen vertrouwensrelaties te maken. Elke vertrouwensrelatie krijgt een wachtwoord toegewezen dat bekend moet zijn bij de beheerders van beide domeinen.   
Dit gebeurt via de Active Directory Domains and Trusts snap-in, domain.msc.   
Aanvullende configuratie houdt in selective authentication waar voor iedere gebruiker moet ingesteld worden of ze worden opgenomen in de Authenticated users van het trusting domein. Ook kan er SID Filtering gebruikt worden, hierbij wordt dan enkel rekening gehouden met de SID in objectSid van de objecten in het trusted domein. Als dit wordt uitgeschakeld dan wordt ook de sIDHistory gebruikt, malafide beheerders kunnen langs deze weg zich meer rechten geven.

1. Welke verschillen zijn er in praktijk tussen *NT 4.0* en *Windows Server* domeinstructuren ? Bespreek onder andere telkens de noodzaak om meerdere domeinen in te voeren. Bespreek de alternatieve mogelijkheden bij de *conversie van een NT 4.0 domeinstructuur* naar een Windows Server omgeving.

Een NT4.0 domeinstructuur gebruikt master en resource domeinen. Het verschil tussen deze twee is niet ingebouwd maar gebaseerd op gebruik in de praktijk. Een master bevat gebruikersaccounts en groepen terwijl resources gedeelde mappen en printers aanbieden.

De Active Directory is meer schaalbaar en ondersteunt het combineren van een groot aantal domeinen in 1. Noodzaak voor meerdere master domeinen bij NT4 was er vaak;

* Te groot netwerk
* Verschillende geografische locaties zorgen voor trage verbindingen waarover we liever geen replicatieverkeer hebben tussen domeincontrollers
* Specifiek wachtwoordbeleid voor diverse groepen
* Domeinmodel weerspiegelt organisatie

Alternatieve conversies

1. Oude NT4 domeinen samenvoegen  
   Vervolgens upgraden  
   OU’s maken voor oorspronkelijke domeinen
2. Individuele upgrade van master enresource domains

OU’s van master domain voor elk van de resource domains

Welke vragen moet men zich stellen na de initiële installatie van een Windows Server toestel, in verband met *bijzondere functies* die de server kan vervullen met betrekking tot Active Directory ? Formuleer bij het beantwoorden van deze vragen telkens (voor zover relevant):

* Hoe bepaald wordt *welke servers* een dergelijke specifieke functie vervullen ? *Hoeveel* zijn er nodig (in termen van: *minimaal/exact/maximaal #, in functie van ...*), en waarom ?
* *Eigenschappen* zoals bedoeling, noodzaak, kriticiteit, inhoud, synchronisatie, voor welke Windows versie(s) van toepassing, ... ?
* De *eventuele relatie* tussen de diverse functies. Vermeld bijvoorbeeld welke functies al dan niet door dezelfde server *kunnen* vervuld worden, of misschien wel juist wel door dezelfde server *moeten* vervuld worden.
* Hoe kan achterhaald worden welk(e) toestel(len) de bijzondere functie vervult, en op welke diverse manieren men de *toewijzing* ervan kan instellen, wijzigen en/of ongedaan maken ?

1. **Wordt de server al dan niet opgenomen in een domein?**

Een computer waarop Windows Server staat, maar die lid is van een werkgroep (en niet een domein) wordt een zelfstandige server genoemd. Ze kunnen bronnen delen met andere pcs in het netwerk maar profiteren niet van de voordelen van de Active Directory.

1. **Vervult de in een domein opgenomen server al dan niet de functie van domeincontroller?**

Wanneer hij dit niet doet, wordt het een lidserver genoemd. Deze handelt geen login van gebruikers af, slaat geen beleidsinfo over domeinbeveiliging op en is niet betrokken bij Active Directory replicatie. Ze fungeren meestal als fileserver, web servers, firewall,… Windows server groepeert dergelijke functies op drie niveaus

* Server roles  
  DHCP server, DNS server, Web server, Network Policy and Acces services implementeren de primaire serverfuncties.
* Role services  
  Sommige meer complexe server rollen bieden optionele componenten
* Features  
  zorgen voor meer ondersteunende functies

Te configureren via Add Roles, Add Role Services en Add Features van Server Manager. Om dit op grotere schaal of remote te doen kan je beroep doen op ServerManagerCmd.

Lidservers behouden een eigen lokale beveiligingsdatabank (de Security Account Manager). Zowel gebruikers van de Active Directory als die in de lokale SAM kunnen gebruik maken van de faciliteiten van de lidserver.

1. **Indien gekozen wordt voor een domeincontroller, moeten dan de functies van de globale catalogus ondersteund worden?**

In elke site tenimnste 1 domeincontroller en 1 domeincontroller als globale catalogus

Dankzij caching kan het inlogproces van een gebruiker afgewerkt worde nzonder een globale catalougus.

1. Een aantal specifieke Acitve Directory functies, operations master rollen genoemd , kunnen slechts door 1 enkele controller in het domein/forest vervuld worden. **Welke domeincontrollers vervullen deze operations master rollen.**

Sommige rollen moeten in elk domein van elk forest voorkomen, en moeten uniek zijn in elk domein.

* RID master  
  Als een domeincontroller een SPN object maakt, moet de domeincontroller een uniek SID (bestaat uit een Domain Subauthority Identifier, die hetzelfde is voor alle securitiy IDS in een bepaald domein, en een relatief ID dat uniek is voor elk SID dat in het domein is gemaakt) aan het object toekennen. In Windows 2000 native en + wijst de RID master reeksen relatieve IDs toe aan de domeincontrollers in het domein. Indien je een object tussen domeinen wil verplaatsen moet dit ook gebeuren via de RID master. Tijdelijk verlies van de RID master is niet merkbaar voor gebruikers.
* PDC emulator  
  In een Windows 2000 mixed domein met NT4 backup domeincontrollers fungeert de PDC emulator master als een volledige emulatie van een NT4 primaire domeincontroller. De NT4 domeinen kunnen services normaal blijven leveren zonder door te hebben dat het een emulator is. In alle domeinen krijgt de PDC emulator master een voorkeursbehandeling bij de replicatie van wachtwoordwijzigingen. Ook fungeert de PDC emulator als primaire bron voortijdssynchronisatie; werkposten en lidservers synchroniseren hun klok met de domeincontroller die hen geverifieerd heeft en deze synchroniseren met de PDC emulator master.

Je laat best de PDC emulator en RID master door dezelfde controller uitvoeren.

* Infrastructure master  
  Verantwoordelijk voor het bijwerken van verwijzingen vanuit objecten in het eigen domein naar objecten in andere domeinen. Indien een forward link kenmerk zou verwijzen naar een object in een ander domein, dan kan het corresponderend back link kenmerk van dat object niet rechtstreeks aangepast worden. Dit wordt opgelost door een phantom object te creeren, dat doorverwisjt naar de DN, GUID en SID van de respectievelijk objecten in de andere domeinen. De infrastructure vergelijk de kenmerken van de phantom objecten met de corresponderende objecten in externe domeinen en de kenmerken van phantom objecten in externe objecten die doorverwijzen naar eigen objecten met deze objecten. Hiervoor doet hij beroep op de globale catalogus. Indien gegevens verouderd zijn, worden de bijgewerkte gegevens opgevraagd uit de globale catalogus. De rol van infrastructure master mag niet op de domain controller draaien, aangezien deze objecten nooit verouderd kunnen zijn. Bij windows server 2008+ word je hiervoor gewaarschuwd, bij NT5 niet. Netwerkgebruikers en -beheerders ondervinden niet direct problemen indien deze infrastructure master even uitvalt.

Rollen die uniek moeten zijn in elk forest:

* Schema master  
  Beheert alle bijgewerkte en gewijzigde gegevens voor het schema. Als je het schema van een forest wil bijwerken moet je dit doen via de schema master. Dit vermijdt problemen die zouden kunnen optreden indien een zelfde schema object op twee verschilende domeincontrollers worden aangepast. Tijdelijk verlies is niet merkbaar voor netwerkgebruikers en enkel merkbaar voor netwerkbeheerders indien ze een schema willen wijzigen.
* De domain naming master  
  Beheert het toevoegen en verwijderen van domeinen en applicatiepartities in het forest.Het is de enige domeincontroller die de Partitions container van de configuratiegegevens kan wijzigen. Het moet een global catalog server zijn. Tijdelijk verlies is niet merkbaar bij gebruikers en beheerders enkel wanneer ze een domein/app part willen toevoegen.

De diverse operations master rollen worden bijgehouden in fSMORoleOwner attributen van vijf verschillende objecten. Een operations master rol kan overgedragen worden naar andere domeincontrollers binnen het domein/forest via Operations Master optie in dsa.msc, domain.msc en de Active Directory Schema snapin of de transfer opdracht van ntdsutil

In situaties waar de huidige operations master niet actief is, en nooit beschikbaar gaat zijn, moet je om een operations master rol eenzijdig over te nemen de opdacht seize van ntdsutil gebruiken.

Wanneer je een eerste domein in een forest maakt, worden alle single master rolle automatisch toegeweze aan de eerste domeincontroller in dat domein. Als je een domein bijmaakt krijgt de eerste domeincontroller de rollen van RID master, PDC emulator master en infrastructure master. In grote omgevingen spreid je deze beter.

5. Alle NT5 domeincontrollers beschikken over een equivalente wijzigbare kopie van alle Active Directory partitites. Een windows server 2008+ domeincontroller kan men tijdens de promotie tot domeincontroller configureren als Read Only Domain Controller. Welke domeincontrollers worden als RODC ingesteld? Deze zijn nodig waar men de fysieke beveiliging van het toestel niet kan waarborgen.

Het replicatieverkeer van RODC blijft beperkt tot 1 richting. Bovendien kan men dynamisch een RODC filtered attribute set configureren, de verzameling die niet naar RODC gerepliceerd worden. Standaard niet de login gegevens van SPN objecten. Men kan een Password Replication Policy configureren die credential caching toestaat voor speciefieke gebruikers en computers. Alle andee SPN objecten worden bij aanmelding door de RODC doorverwezen naar een reguliere domeincontroller.

Een RODC kan de functies vervullen van globale catalogus of DNS server. Bij DNS wordt dit dan een secundaire nameserver. Ondersteuning van een operations master rol is niet mogelijk. Kan enkel repliceren met een windows 2008+ controller

 Active Directory functionele niveaus (§2.4.3)

1. Geef de diverse functionele niveaus waarop Active Directory kan ingesteld worden, en welke beperkingen er het gevolg van zijn. Geef ook de voordelen per niveau.

8 domein functionele niveaus

Windows 2000 mixed domein

* + Kan zowel NT4, Windows 2000 Server als Windows 2003 Server domeincontrollers bevatten, Windows Server 2008+ niet mogelijk
  + Biedt de laagste Active Directory functionaliteit
  + Standaard instelling na initiele installatie van NT5 controllers, zelfs in een nieuw domein

Windows 2000 native domein

* + biedt de keuze tussen willekeurige NT5+ domeincontrollers.
  + Heeft voordelen op Windows 2000 mixed
    - 1 globale catalog voor het ganse forest bestaat
    - Automatische vertrouwensrelaties tussen alle domeinen van eenzelfde forest
    - De domeincontrollers kunnen zelfstanding een aantal SPN objecten aanmaken
    - Ruimere mogelijkheden voor configuratie van groepen
    - sIDHistory attribuut

Windows Server 2003

* Enkel windows 2003 + domeincontrollers
* Laat nog dingen bovenop Windows 2000 native toe
  + Aanvullende schema klassen en attributen
  + Veranderen van de naam van een domeincontroller zonder degradatie en promotie
  + Aanvullende opdrachten
  + Caching op domeincontrollers niveau van UPN suffices en het lidmaatschap van universele groepen
  + Filtering van group policies op basis van beveiligingsgroepen en WMI Scripts

Windows server 2008

* Enkel windows 2008+ domeincontrollers
* Nog extra Active Directory functionaliteit bovenop 2003
  + Aanvullende schema klassen en attributen
  + Encryptie van het Kerberos protocol
  + Fine gained password policies
  + Replicatie van DFS namespaces en van de SYSVOL share met DFS Replication, performanter dan File Replication Service (FRS)

Windows Servr 2008 R2, Windows Server 2012 (RL)

8 Forest functioneel niveau

Windows 2000

* Stelt geen enkele eis aan het functioneel niveau
* Geen extra functionaliteit
* Standaard instelling na initiele installatie

Windows Server 2003

* + Enkel domeinen die minimum windows server 2003 bevatten
  + Hier kan een belangrijke fractie van de Active Directory implementatie gebruikt worden
    - Hergebruiken van gedeactiveerde klassen
    - Dynamische hulpklassen en objecten (met beperkte levensduur), bij creatie van het object objectClass kenmerk in te vullen met de naam van de hulpklasse zorgt ervoor dat enkel deze representant de kenmerken erft
    - Efficientere replicatie van global catalog gegevens
    - Optimalisatie KCC (Knowledge Consistency Checker), die de replicatietopologie genereerd
    - Veranderen van domeinstructuur in een forest
    - Vetrouwesrelaties tussen verschillende forests
    - Read-only Windows Server 2008
    - Replicatie van de individuele waarden van multi valued attributen

Windows Server 2008

* Enkel domeinen met Windows Server 2008 domein functioneel niveau bevatten
* Beperken van beveiligingsprobleem bij credential caching van RODC filtered attirbuten
* Geen automatisch site covering probleem bij sites met enkel RODC’s
* Vertrouwens met Kerberos

Windows Server 2008 R2, 2012 (R2)

1. Hoe kan men detecteren op welk niveau een Active Directory omgeving zich bevindt ? Hoe kan je het verhogen of verlagen

Door de attributen op te vragen of door domain.msc te gebuiken kan je detecteren.

Voor domein Wordt opgeslagen in 2 attributen vh domein: ntMixedDomain en msDS-Behavior-Version. Beiden hebben integerwaarde.

Door de attributen van het domeinobject te manipuleren of via GUI memt behulp van Active Directory Domans and Trust snap-in, beschikbaar in domain.msc. In domain.msc zie je een lijst met alle domeinen in het forest. Door de properties te selecteren kan je de functionele niveaus van het domein en forest opvragen. Vervolgens kan je met Raise Domain/Forest functional level naar een hoger functioneel niveau indien alle noodzakelijke voorwaarden voldaan zijn. Hierna moet je alle domeincontrollers herstarten.

 Active Directory replicatie (§2.5)

1. Wat is de bedoeling van replicatie ?

Om gebruikers en services op elk moment vanaf elke computer in het forest toegang te geven tot actuele directory gegevens. Hierbij bevatten alle domeincontrollers in een domein een volledige kopie van alle directory gegevens van het eigen domein en nemen ze allemaal deel aan de replicatie. Door die replicatie worden alle gegevens gedistribueerd in het netwerk en blijft alle informatie up to date en consistent na nieuwe of gewijzigde gegevens. Door te werken met meerdere domeincontrollers in een domein hebben we ook een grotere fouttolerenatie en belastingsverdeling.

1. Hoe wordt dit in Windows Server (ondermeer ten opzichte van NT 4.0) gerealiseerd: bespreek de verschillende *technische kenmerken* en *concepten* van Windows Server replicatie, en hoe men specifieke problemen vermijdt of oplost.

NT werkt met een master-slave model; Nadat directory gegevens zijn gemaakt of gewijzigd op een domeincontroller, worden de nieuwe of gewijzigde gegevens naar alle andere domeincontrollers in het systeem gestuurd.

In Active Directory worden multi-master replicatie gebruikt, zodat de directory kan bijgewerkt worden vanaf elke domeincontroller. Alle Windows Server domeincontrollers zijn equivalent, behalve voor de operations master functies. Om het replicatieverkeer te beperken worden alleen gewijzigde directory gegevens gerepliceerd. Om te voorkomen dat dezelfde wijziging niet meermaals gestuurd wordt, wordt gebruik gemaakt van het Update Sequence Number. Combinatie van USN en GUID vorm Up-to-dateness vector (UTD) Elke domeincontroller increased dit nr bij verandering en meldt bij iedere verandering aan een object zijn huidge UTD vector mee aan andere domeinen.  
Indien 2 objecten tegelijk worden aangepast, gaat de domeincontroller die de conflicten detecteert enkel de in de tijd laatste gebruiken.  
Bij de verwijdering van een object vormt nog een probleem, men moet vermijden dat het object opnieuw gecreeerd wordt door replicatie vanuit een andere domeincontroller. Daarom wordt een object niet onmiddellijk uit de Active Directory verwijderd, maar als tombstone gemarkeerd en in een hidden container Delete items geplaatst.

Bij store and forward replicatie wordt elke verandering op een specieieke controller slechts uitgewisseld met enkele andere domeincontrollers die op hun beurt dit ook weer doen. De replicatietoplogie , de configuratie van verbindingsobjecten die gebruikt worden om directory gegevens te repliceren tussen domeincontrollers wordt gegenereed door de Knowledge Consistency Checker. Er worden individuele topologien gecreeerd voor domeingegevens en schema en configuratiegegevens.

Windows Server replicatie is pull mechanisme; elke domeincontroller brengt zijn intrasite replicapartners op de hoogte, maar stuurt gegevens zelf niet door. Die worden opgevraagd. Het is robuust, maar kan wel veel netwerkverkeer veroorzaken. Daarom wordt propagation damping toegepast. Hierdoor is wel niet constant alles in sync maar convergeert het hier wel naatoe.  
Loose consistency model: Op elk moment dat er een verandering wordt verstuurd, is er misschien ergens anders al een nieuwe. - Urgent replication: Op sommige attributen worden propagation damping uitgeschakeld omdat het belangrijke zijn, zoals bvb lockout kenmerken en wachtwoorden

Windows server replicatie is multi-threaded, een domeincontroller kan simultaan repliceren met diverse partners. Bij replicatie tussen controllers in dezelfde site worden gegevens niet gecomprimeerd.  
Laatste verschil met NT4 is kleinste replicatie entiteit: NT4 domein -> volledig object, in forest met W 2000 niveau is dit de waarde v/e attribuut, en forests met W 2003 de atomaire waarde v/e attribuut

1. Welke toestellen repliceren onderling in een forest ? Welke specifieke gegevens worden hierbij uitgewisseld ?

Tussen domeincontrollers, waarvan er slechts 1 een globale catalogus heeft gebeurt er replicatie van directory gegevens. Alle directory objecten met corresponderende kenmerken voor het domein, het schema en de configgegevens van het forest worden tussen de controllers gerepliceerd.

Wanneer er tussen twee domeinen gerepliceerd wordt, en slechts een van de twee een globale catalogus heeft, wordt een subset van de eigenschappen van de directory objecten van domein zonder catalogus naar domein met catalogus gerepliceerd. Ze wisselen ook schema en configgegevens uit.

Wanneer er tussen twee domeinen gerepliceerd wordt, en ze allebei een globale catalogus hebben wordt de subset in beide richtingen gerepliceerd

1. Welke impact hebben sites met betrekking tot de replicatie van Active Directory gegevens ? Welke andere Active Directory aspecten worden door sites beïnvloed ?. (§2.6.1)

Er wordt een evenwicht gezocht tussen behoefte aan actuele gegevens en beperkingen die door bandbreedte worden opgelegd.

* Replicatiepartners van verschillende sites laten standaard het meldingsmechanisme van gewijzigde UTD vectortabellen achterwege, er wordt enkel polling toegepast.
* Gegevensuitwisseling tussen sites worden gecomprimeerd
* Sitekoppelingen kunnen gebruikt worden om aan te geven hoe de verschillende sites onderling met rechtstreekse fysieke netwerkverbindingen verbonden zijn. De KCC’s genereren automatisch verbindingsobjecten tussen sites als er tussen beide sites een sitekoppeling bestaat. Er wordt gepoogd zoveel mogelijk efficiente replicatie en fouttolerantie is.
* Men duidt per site automatisch een enkele domeincontroller als inter site topology generator om te vermijden dar er meerdere verbindingsobjecten van dzelfde sitekoppeling zouden gebruik maken.
* De ISTG’s zorgen er voor om voor elke partitite hoogstens één verbindingsobject per sitekoppeling aan te maken. De domeincontrollers die van dit uniek verbindingsobject gebruik maken , worden bruggenhoofdservers genoemd. Invoering van bruggenhoofdservers en ISTG’s zorgen voor optimale replicatie in de siteconfiguratie

1. Hoe wordt bepaald tot welke site computers, servers in het bijzonder, behoren ? (laatste paragraaf §2.6.2 en fractie §2.6.3)

Computers worden toegewezen op basis van de locatie in en IP subnet. Subnetten bieden de eenvoudigste manier om site te vertegenwoordigen, omdat de computers erin meestal betere onderlinge verbindingen hebben. Sites worden in praktijk beschouwd als een verzameling computers in 1 of meer subnetten. Een computer met meerdere IP adressen kan slechts tot 1 site behoren. Alle sites moeten 1+ sitekoppeling hebben en met 1+ subnet geassocieerd zijn.

Elke site heeft een container met Servers die alle domeincontroller objecten bevatten die in deze site zijn geplatst. De site locatie van een werkpost wordt dynamisch bijgewerkt, via het netwerkadres in welke site deze zich bevindt, de site locatie van een domeincontroller wordt bepaald door de vraag tot welke site in de directory het server object van de domeincontroller behoort

3.

 Gedeelde mappen en NTFS

1. Welke configuratieinstellingen kun je maken tijdens of onmiddellijk na het creëren van gedeelde mappen ? Bespreek het doel van elk van deze diverse instellingen en de belangrijkste eigenschappen en mogelijkheden ervan. (§3.2.1, §3.2.2, fracties §3.3.1, §3.4.2, §3.4.3, §3.5 en §3.6)

* Comment veld: beschrijving zichtbaar voor gebruikers.
* Limit number of simultaneous users: max gebruikers tegelijk toegang tot share
* Permissions: machtigingen, de eerste beveiliginslaag. Er zijn er drie mogelijk
  + Full control: gebruiker kan alle bewerkingen op alle bestanden en mappen, bv eigenaar worden, NTFS machtigingen instellen
  + Read: gebruiker kan de volledige structuur zien, en lezen
  + Change: gebruiker kan bestanden wijzigen en verwijderen
* Caching: client side caching voor offline toegang
  + Maakt kopie op lokale harddisk van vaak gebruikte bestanden
  + Door vergelijke van timestamps is geweten of de cache up to date is, de cache kan gebruikt worden in goed geval en dit maakt het sneller voor gebruiker. Het geet ook betere betrouwbaardheid
  + Passieve of actieve caching
    - Passief: cachen van bestand wanneer je het gebruikt
    - Actief: bestanden anduiden die gecached moeten worden
* Access based enumeration: voorkomen dat gebruikers die enkel NTFS machtigingen hebben en full access op share niveau submappen van een map kunnen zien waartoe ze geen NTFS machtiging hebben om iets uit te voeren
* Quota policy en file screen policy
* Connect to another computer: beheer een share van een server op afstand
* NTFS Permissions: atomaire of moleculaire machtigingen

1. Waar wordt de definitie en (partiële) configuratie van gedeelde mappen opgeslagen ? Hoe kan men deze wijzigen vanuit een Command Prompt ?
2. Geef een overzicht van de belangrijkste voordelen van de opeenvolgende versies van het NTFS bestandssysteem. Bespreek elk van deze aspecten (ondermeer het doel, de voordelen en de beperkingen ervan), en geef aan hoe je er gebruik kan van maken, bij voorkeur vanuit een Command Prompt. (NTFS fractie §1.6, fracties §3.4.1, §3.4.2 en §3.4.4)

NTFS heeft meeste voordelen tov andere filesystems. Het is niet altijd de snelste maar de hardware speelt hier een grotere rol in.

NTFS 1.2

* Ingebouwd systeem voor beveiliging tot op bestandsniveau
* Auditing op objecttoegang
* Ondersteuning voor compressie
* Volumes uit te breiden over verschillende fysieke schijven
* Schijfactiviteiten vastgelegd in logboekbestanden
* Maximum stationgrootte tot 2TB

NTFS 3.0/3.1

* Nieuwe functies zoals bestandscodering (via bestandssysteemfilter) en volumequota’s
* Ondersteuning voor sparse bestanden (fsutil)
* Ondersteuning voor hard links en soft links (mklink)
* Meeste nieuwe functies worden mogelijk gemaakt door reparsepunten die kenmerktags bevatten. Wanneer een reparsepunt tegengekomen wordt tijdens het ontleden van padnamen wordt de tag teruggestuurd naar de I/O stack, hier wordt hij onderzocht door extra bestandssysteemfilters, die aangeven de verwerking door te geven aan een ander stuurprogramma. Volgende voorbeelden:
  + file markers
  + self-healing (corrupties worden online opgespoord en gecorrigeerd)
  + transacties (atomaire reeks opeenvolgende bewerkingen)
  + diskquotas (afdwingen van bepaalde hoeveelheid beschikbare opslagcapaciteit) op volume (SID-gebonden, op gans volume, niet per gebruiker, collectief van toepassing op alle mappen) en map (collectief, onafhankelijk van de eigenaar) niveau. Volume te gebruiken via fsutil quota en map via fsrm.msc
  + file screens (verhinderen dat bepaalde extenties in mappen worden opgeslaan) toe.

Ondersteunig voor public key encryption waarbij elk bestand een unieke willekeurige symmetrische codeersleutel heeft als bestandskenmerk. (cmd cipher)

1. Welke rol spelen machtigingen bij de beveiliging van bronnen ? Geef een gedetailleerd overzicht van het algemeen (op alle windows objecten toegepast) mechanisme van machtigingen.

Met machtigingen kan de eigenaar bepalen welke gebruikers en groepen toegangsrechten voor het object hebben. Ze bepalen ook het type toegang.

Een toewijzing van machtiging aan een gebruiker/groep wordt een Aces Control Entry (ACE) genoemd. De gebruiker wordt hierin geidentificeerd met zijn SID en de machtiging met een bitveld. Er zijn toekenende en ontzeggende ACE’s en alle ACE’s samen vormt het ACL (Access Control List). Het is verstandig van machtigingen toe te passen op groepen ipv gebruikers

De Security Reference Monitor (SRM) verwerkt de verschillnede ACEs in een ACL in canonieke volgorde (dit wordt bereikt door ze in canonieke volgende in een attribuut van het object op te slaan); eerste alle ACEs die ontzeggen, daarna die toekennen. De machtigingen zijn cumulatief; behoor je als gebruiker tot diverse groepen dan word je toegang ontzegd indien slechts 1 van de groepen ontzegd wordt. Indien 1 van de groepen toegekend wordt en nergens anders ontzegd krijg je toegan

1. Bespreek hoe het mechanisme van machtigingen specifiek (en op diverse niveaus) toegepast wordt op bestandstoegang. Geef de verschillende soorten machtigingen, hun onderlinge relaties, en hoe deze kunnen geanalyseerd en ingesteld worden. Toon hierbij aan dat je zelf met deze configuratietools geëxperimenteerd hebt.

Dit gebeurt met Share machtigingen, deze hebben de overhand op NTFS machtigingen. De meeste beperkende laag heeft de overhand. In de praktijk is er meestal enkel beperking op NTFS niveau.

Met de Permissions Editor kan je de machtigingen analyseren en instellen. Dit bekom je door bijvoorbeeld door in Explorer de properties van een gedeelde map te openen, en hier te navigeren naar sharing-advanced sharing-permissions.

Ook in het detailpaneel van de shares map van compmgmt.msc kan je de properties van een share vragen en hier te navigeren naar permissions-share permissions.

De laatste manier is via het detailpaneel in de Share en Storage Management map van Server Manager en dan hetzelfde als in compmgmt.msc

Het gaat echter ook via command prompt met net share en rmtshare

Er zijn 3 soorten machtigingen

* Full control: Een gebruiker of groep kan alle soorten bewerkingen uitvoeren op alle bestanden en mappen op de share. Bijvoorbeeld eigenaar worden, NTFS machtigingen instellen
* Read: laat toe om via de share de volledige structuur van de gedeelde map te zien, om bestanden en mappen te lezen en om toepassingen in de maphierarchie uit te voeren
* Change laat hier bovenop toe om bestanden te wijzigen en te verwijderen en er de bestandskenmerken van te wijzigen. Hij kan in tegenstelling tot full control de NTFS machtigingen niet aanpassen.

De standaard machtiging is Full Control voor Everyone op Win Server 2000 en Read voor Everyone op Win Serer 2003+

1. Wat gebeurt er met de machtigingen bij het verplaatsen van een bestand ? Wat gebeurt er met de machtigingen bij het kopiëren van een bestand ?

De gebruiker die verplaatst of kopieert wordt de nieuwe eigenaar van het bestand. Wanneer je verplaatst naar een ander volume of kopieert naar hetzelfde/ander volume dan vervallen de expliciete machtigingen die zijn toegewezen aan het object. Het object en zijn inhoud nemen de machtigingen over van de doelcontainer. Indien je ze toch wil bewaren, gebruik je roocopy en scopy

Als je verplaatst naar hetzelfde volume behoud je de machtigingen. De effectieve machtigingen wrden bepaald door de expliciete en de overgenomen van de doelcontainer.

1. Op welke andere objecten zijn machtigingen van toepassing ?

Active Director objecten (users,usergroepnen)  
NTFS objecten (mappen en bestanden)  
Registersleutels (user profielen)  
Processen  
Services

1. Wie is in principe verantwoordelijk voor het configureren van machtigingen ? Door welke instelling is dit zo vastgelegd ? Hoe kan ervoor gezorgd worden dat enkel administrators verantwoordelijk gesteld worden voor het configureren van machtigingen ?

De eigenaar van het bestand. ?

1. Bespreek in detail het onderscheid tussen de diverse soorten veiligheidsgroepen, ondermeer afhankelijk of het toestel al dan niet in een domein is opgenomen. Behandel hierbij vooral de mogelijkheden en beperkingen. Bespreek ondermeer:
   1. de zichtbaarheid van de diverse soorten groepen,
   2. welke objecten er lid van kunnen zijn,
   3. de onderlinge relaties en de regels voor het nesten van de diverse soorten groepen ? Stel deze relaties eveneens schematisch voor.

**Lokale groepen**

* + Kunnen leden uit elk domein van het forest of een ander trusted domain bevatten
  + Zijn enkel zichtbaar en geldig in het eigen domein, ieder domein heeft z’n eigen lokale groep en die wordt niet gekopieerd naar de globale catalogus.
  + Ze worden typisch gebruikt om rechten en machtigingen toe te kennen en bevatten eerdere andere groepen dan gebruikers.

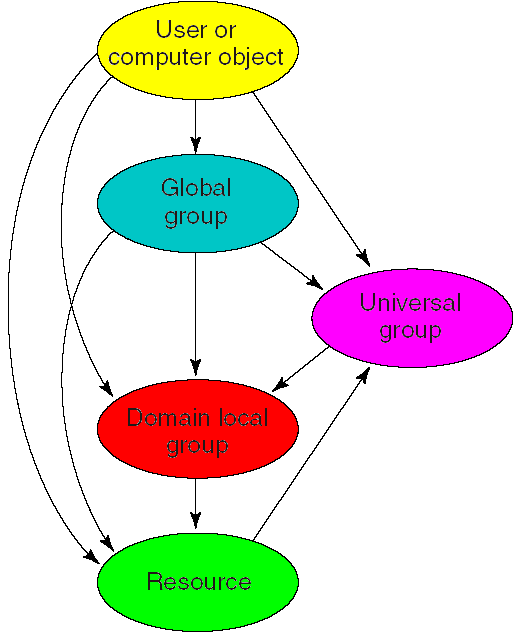
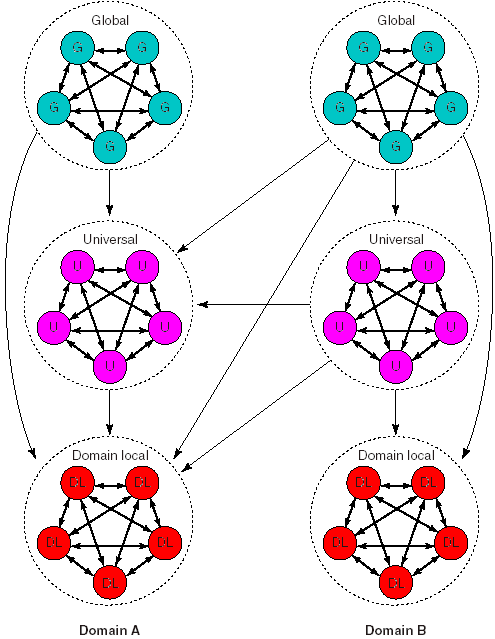
**Globale groepen**

* Kunnen alleen gebruikers en andere globale groepen uit hetzelfde domein omvatten.
* Zijn zichtbaar in elk domein van het forest, de naam van een globale groep wordt gekopieerd naar de global catalog maar niet de leden. Dit zorgt ervoor dat de groepen regelmatig gewijzigd kunnen worden zonder veel replicatieverkeer.
* Kunnen toegelaten worden tot de lokale groepen van werkstations en lidservers.
* Worden eerder gebruikt als containers voor gebruikers die dezelfde machtigingen of rechten nodig zullen hebben.

**Universele groepen**

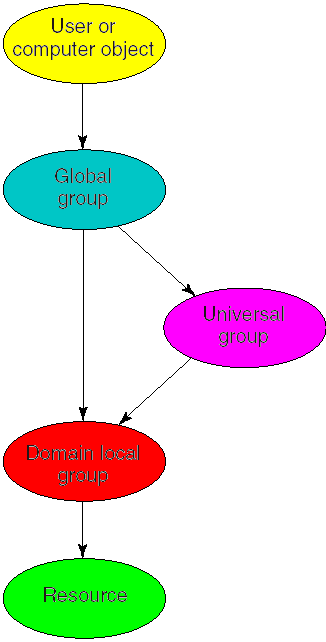
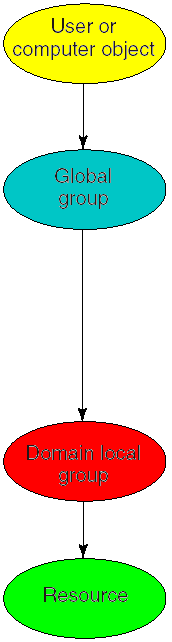
Nieuw voor Windows Server, minstens Windows 2000 native functioneel niveau nodig.

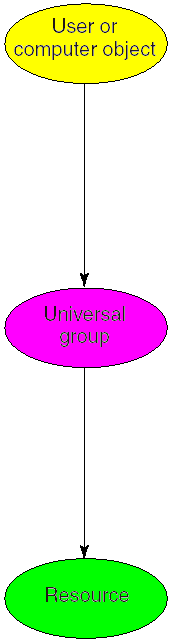
* Ze lijken de beste karakteristieken van lokale en globale groepen te hebben. Ze kunnen leden hebben uit elk domein van het forest (maar niet uit een ander trusted domain), en zijn zichtbaar in elk domein van het forest.
* Worden gebruikt om rechten en machtigingen toe te kennen
* Zijn in alle domeinen tegerlijkertijd geldig
* Zowel de namen als de leden worden in de global catalog bewaard (en enkel daar, niet in domeincontrollers) -> global catalog zou dus groot worden indien enkel universele groepen. Ook moeten ze dan statisch zijn aangezien er anders veel gesynced moeten worden.



Voor het nesten zijn er beperkende regels.

* Lokale groepen kunnen behalve gebruikers ook globale en universele groepen uit om het even welk domein van het forest omvatten, maar enkel lokale groepen uit hetzelfde domein
* Globale groepen kunnen enkel gebruikers en globale groepen uit het eigen domein bevatten. Ze kunnen dan ook maar naar groepen met een universel bereik geconverteerd worden zolang de groep geen lid is van een andere groep met een globaal bereik.
* Universele groepen kunnen andere universlee groepen, gebruikers en globale groepen uit alle domeinen van het forest bevatten, maar geen lokale groepen.

1. Hoe en waarom worden deze soorten groepen in de praktijk best gebruikt, al dan niet gecombineerd ? Van welke omstandigheden is dit afhankelijk ? Illustreer aan de hand van concrete voorbeelden.



* Standaard situatie: uniersele groepen vermijden door gebruikers te groeperen in globale groepen en deze lid te maken van een lokale groep.  
  Bv Een voorbeeld van lokaal en globaal combo. Indien 5 mensen op een printer moeten kunnen, maak je in elk domein een globale groep en voeg je de gebruikers daar aan toe. In het domein van de printer een lokale groep waaraan je al deze globale groepen toevoegd. Als er nu een printer wordt toegevoegd kan je de machtiging aan de lokale groep toekennen.
* Enkel universele groepen gebruiken om rechten en machtigingen toe te kennen. Dit is administratief veel eenvoudiger en het performantieverlies is verwaarloosbaar indien het forest slechts uit een enkel domein bestaat
* Een hybrideoplossing is aangewezen in grotere forests, waar ze alle drie in zitten.

1. Waar en hoe wordt het (volledige) lidmaatschap van een user object tot een groep bijgehouden ? Op welke diverse manieren kan men dit lidmaatschap configureren ? Op welke diverse manieren kan men de volledige verzameling van objecten, die deel uitmaken van een specifieke groep, of de volledige verzameling van groepen, waar een specifiek object deel van uitmaakt, achterhalen ? (partim §4.1.2 en §4.2.3)

Domeinaccounts worden opgeslagen in Active Directory, in de Users container. Het voornaamste hulpprogramma om gebruikersaccounts en groepen te beheren in een domeinstructuur is de Active Directory Users and Computers , beschikbaar in dsa.msc console.

Welke leden in een groep zitten wordt bewaard in de Members van een groep.

Met net group kan je groepsleden instellen manipuleren op Win Server 2003+ kan je ds(add/rm/get/mod) group uitvoeren.

1. Door wie wordt het lidmaatschap van de diverse groeptypes bij voorkeur ingesteld ?
2. Op welke diverse manieren kan men het beheer van Active Directory objecten, specifieke attributen van groepsobjecten in het bijzonder, delegeren aan niet-Administrators ? Bespreek een aantal technieken om dit delegeren zo eenvoudig mogelijk uit te voeren. (partim §4.1.2, en §4.4.2)

* Beheerstaken gedetailleerd instellen via de properties van de OU  
  Klik op de properties van de OU en dan kan je volledig analoog aan het instellen van NTFS machtigingen taken delegeren en de instelling voor reeds gedelegeerde taken wijzigen. Je kan op ieder moment de expliciete machtigingen van een object opnieuw initialiseren.
* Command prompt opdrachten  
  Gebruik van acldiag en dsacls en dsrevoke. Het member attribuut van groepsobjecten is nagenoeg het enige Active Directory item dat wordt gedelegeerd op niveau van de individuele objecten. Bij groepsobjecten kunnen er ook subscriptiegroepen geconfigureerd worden. Dit zijn groepen waar iedereen zich kan in- en uitschrijven
* Delegation of control wizard  
  Start dsa.msc en selecteer Delegate Control.  
  Hier kan je de groepen of gebruikers waaraan je beheersmachtigingen wil delegeren selecteren. Vervolgens kan je met Create a cusom task to delegate, hier kan je een aangepaste lijst samenstellen. Door delegwiz.inf aan te passen kan je de keuzes vergroten