Vraag 1 Structuur van active directory gegevens

1.a Bespreek de diverse namen die alle Active Directory gegevens identificeren.

Elk van onderstaande namen zijn uniek in het gehele forest.

De **Relative distinguished name** (RDN) identificeert het object uniek binnen een containerobject, maar niet noodzakelijk uniek binnen de gehele directory

De **Distinguished name** (DN) wordt afgeleid uit de RDN van het object zelf, en de DN's van alle bovenliggende containerobjecten waarvan het object hiërarchisch deel uitmaakt. Deze naamgeving is belangrijk voor de werking van het LDAP protocol. Iedere LDAP client kan queries op een object uit een willekeurige directory uitvoeren met behulp van URL's van de vorm *ldap://<server DN>/<object DN>*. De DN is belangrijk voor het maken van scriptcode die rechtstreeks AD objecten aanspreekt. De gebruikte conventie is **attributed naming** waarbij elke component van de naam als naam-waarde koppel wordt opgegeven. Deze namgeving is hiërarchisch, van beneden naar boven.

De **cannonieke naam** gebruikt dezelfde naamgeving als de DN, maar met een eenvoudigere syntax. De componenten worden gescheiden door een duitse komma.

De **Global Unique ID** (GUID) is een 128 bit onwijzigbaar getal dat wordt aangemaakt bij de creatie van objecten. Het kan worden gebruikt voor verwijzingen naar objecten vanuit externe processen.

1.b Wat zijn SPN objecten? Bespreek de aanvullende naamgeving.

Security Principal objecten zijn AD objecten waaraan een **Security ID** (SID) werd toegewezen. Ze worden gebruikt voor het verlenen van toegang tot domeinbronnen. Ze zijn van toepassing op groepen, domeinen, gebruikersaccounts en computeraccounts. De SID wordt gebruikt in de plaats van de GUID om compatibiliteit met oudere NT versies te bewaren. De SID wordt meestal voorgesteld als een hiërarchische string, gescheiden door koppeltekens. De string bestaat uit een drieledige standaard prefix (S-1-5), 3 32 bit getallen die worden bepaald door het domein (de *domain subauthority identifier*) en een relative ID (500) die naar het object zelf verwijst. De GUID en SID worden bij creatie van het SPN object door AD gegenereerd. De SID, GUID, DN en CN zijn steeds uniek binnen het gehele forest.

Een GUID verandert nooit, zelfs niet bij verplaatsing van het object naar een ander domein. SID's daarintegen kunnen wel veranderen bij verplaatsing naar een ander domein. Om te vermijden dat een gebruiker bij verplaatsing van zijn object naar een ander domein toegang tot domeinbronnen zou verliezen, wordt ook een multivalued kenmerk *sIDHistory* bijgehouden. Dit kenmerk bevat een lijst van alle SID's die het SPN object in het verleden heeft gehad.

Om het gebruik van aanmeldingsnamen voor gebruikers te vereenvoudigen, wordt de **User Principal Name** (UPN) gebruikt. Deze is uniek binnen het gehele forest. De UPN is van de vorm *<RDN gebruiker>@<UPN Suffix>*. De *UPN Suffix* kan zijn: hetzij de volledige DNS naam van het domein (standaard), de DNS naam van het rootdomein, of een willekeurige naam geregistreerd door een beheerder m.b.v. de AD domains & Trusts Snap-In. Meer couranter gebruikt men de vorm *<Netbios name>\<Gebruiker SAM naam>*. De netbios naam zijn de hoogstens 15 eerste tekens van de meest linkse component van de DNS naam van het domein. De gebruikers SAM naam zijn de hoogstens eerste 20 bytes van de RDN.

Een **Computeraccount** heeft een **Service Principal Name** (SPN), een SAM accountnaam en een DNS hostname. De SAM account naam wordt geregistreerd op basis van de eerste 15 tekens van de RDN, en mag op elk ogenblik worden gewijzigd. De DNS naam bestaat uit de eerste 15 tekens van de RDN en de suffix voor de primaire DNS. De SPN is essentieel voor de verificatie tussen clientzijde en de server die een bepaalde dienst aanbiedt.

1.c In welke partities zijn AD gegevens verdeeld? Geef betekenis, onderlinge relaties en replicatiekaraktristieken.

De **domeingegevens** bevatten de eigenlijke informatie over de objecten in het domein. Wijzigingen aan objecten worden ook hierin opgeslagen. Er zijn evenveel partities met domeingegevens als er domeinen in het forest zijn. Domeingegevens hebben steeds slechts betrekking op één enkel domein, en worden bijgevolg ook nooit gerepliceerd naar andere domeinen. Een subset van alle kenmerken van alle domeinen wordt opgeslagen in de **Global Catalog**.

AD biedt vanaf Server 2003 de mogelijkheid om gegevens onder te brengen in een of meerdere gescheiden **applicatiepartities**. Zo kunnen bijvoorbeeld de DNS gegevens worden ondergebracht in een eigen applicatiepartitie. Ze kunnen géén SPN objecten bevatten. Objecten van een applicatiepartitie kunnen niet buiten die partitie worden verplaatst. Ze zijn nuttig als container voor dynamische objecten.

De **Configuratiegegevens** beschrijven de fysieke topologie van de directory. Ze bevatten een lijst van alle domeinstructuren, locaties van domeincontrollers en global catalog controllers alsook de replicatietopologie. Gemeenschappelijke configuratiegegevens die geldig zijn binnen het volledige forest, worden dikwijls vertaald als eigenschappen van objecten in de configuratiegegevens. De *partitions container* van de configuratiegegevens bevat *crossRef* objecten die verwijzen naar een van de directory partities van het forest. Voor elke partitie (ook voor elke applicatiepartitie) is er een *crossRef* object. De configuratiegegevens zijn geldig voor alle domeinen in het forest.

De **Schema Partitie** bevat de formele definitie van alle objecten en kenmerken die kunnen worden opgeslagen in de directory. Het schema is uniek voor alle domeinen in het forest.

Elke partitie in de directory is een **eenheid van replicatie** waarbij telkens een specifieke groep van controllers hoort. Het *schema* en de *configuratiegegevens* worden gerepliceerd naar alle controllers in het forest. De *domeingegevens* worden gerepliceerd tussen alle domeincontrollers van dat domein. *Applicatiepartities* worden enkel gerepliceerd tussen geconfigureerde controllers, onafhankelijk van de domeingrenzen. De koppeling tussen

applicatiepartities en replicerende domeincontrollers wordt bijgehouden in het overeenkomstige *crossRef* object van de applicatiepartitie. Dit object bevindt zich in de configuratiegegevens.

Een willekeurige domeincontroller zorgt voor opslag en replicatie van:

- Alle objecten en eigenschappen in de domeingegevens van het bijhorende domein.
- Configuratiegegevens en schema van het forest.
- Specifieke applicatiepartities.

Een subset van kenmerken van alle objecten in de domeingegevens van elk domein wordt gerepliceerd naar de **global catalog**.

Vraag 2 attributeSchema Objecten

2.a Bespreek het doel en de werking van attributeschema objecten.

Het doel van attributeSchema objecten is het beschrijven van de kenmerken die in de klassen kunnen worden opgenomen. De beschrijving bevat bijvoorbeeld het gegevenstype en beperkingen op de waarden. Elk kenmerk kan in meerdere klassen worden opgenomen, maar wordt slechts een keer beschreven. Dit verhoogt de consistentie.

De kenmerken worden zelf als objecten opgenomen in de schema container van de directory. Ze kunnen op dezelfde manier worden beheerd als andere objecten.

2.b Bespreek de diverse naamgevingen van attributeSchema objecten.

- *Common Name:* Dit is de RDN van het object in de schema container
- *GUID*: Dit is de GUID van het kenmerk, en is onafhankelijk van de GUID van het attributesSchema object dat het kenmerk voorstelt. Dit kan automatisch gegenereerd worden bij creatie van het object. In dit geval zal het kenmerk een andere GUID hebben in elk forest, daarom wordt het best op voorhand gegenereerd met *guidgen* of *uuidgen*.
- *LDAP Display Name*: Voor programmatorische toegang.
- *Object Identifier*: Geldt als interne representatie. X500 ID, wordt verleend door speciale authoriteiten. Worden genoteerd in *dotted decimal* formaat. Bedrijven worden een tak toegekend door een authoriteit (ITU, ANSI, ISO). Indien het bedrijf nog niet over een tak beschikt, kan het er een aanvragen of een OID in de microsoft tak genereren met *oidgen*.

2.c Bespreek de belangrijkste kenmerken van attributeSchema objecten en hoe die kunnen worden ingesteld.

- *attributeSyntax* en *oMSyntaxt:* bepalen het gegevenstype van het attribuut. De *attributeSyntax* is een standaard X500 syntax. *oMSyntax* is een aanvullend nummer nodig om bepaalde AD types te kunnen onderscheiden.
- *rangeUpper* en *rangeLower*: lengte of bereikbeperkingen van attributen
- *isSingleValued*: geeft aan of het om een enkele waarde of een tabel gaat.
- *searchFlags:* Binaire informatie, waarvan de respectievelijke bits bepalen of de waarden op een of andere manier worden geïndexeerd, voor versnelde zoekopdrachten. De belangrijkste indexeringen zijn: eenvoudige indexering op de waarde, *containerized index* (indexeren op combinatie containernaam en waarde van kenmoer), *Ambiguous Name Resolution* (laat toe om filters te vertalen tot atomaire waarden die sneller te vergelijken zijn) en *tuple indexen* voor versnelde *wildcard searches*.
- *systemFlags:* eveneens binair. Bits voor replicatie (al dan niet) en of het over een geconstrueerd attribuut gaat.
- *isMemberOfpartialAttributeSet*: Bepaalt of het object in de global catalog wordt opgenomen.

- *linkID*: *backLink* en *forwardLink* attributen nummer en in relatie brengen. (Opeenvolgende even en oneven nummers inbrengen)

Eigenschappen van *classSchema* objecten wijzigen kan in het schema, bijvoorbeeld met ADSIEdit.msc.

2.d Welke andere types objecten bevat het AD schema? Wat is hun doel?

Het enkele exemplaar van het *Aggregate* object van de klasse *subSchema*. Het heeft als doel om aan LDAP clients een vereenvoudigd schema ter beschikking te stellen. Biedt in combinatie met ADSI een toegang tot het schema. Objecten (*classSchema*, *attributeSchema*) in het abstracte schema hebben slechts een beperkt aantal attributen die min of meer overeenkomen met hun overeenkomstige reële schemaobjecten.

2.e Via welke attributen kan de klassen van een willekeurig AD object achterhalen? Hoe moet je op zoek gaan naar alle objecten van een willekeurige klasse? Illustreer aan de hand van relevante voorbeelden.

De attributen *objectClass* en *objectCategory*. Elke klasse beschikt over deze attributen, omdat ze *mandatory* zijn in te *top* klasse.

ObjectClass bevat de hele overervingshiërachie van de klasse. Ook de klasse van het object zelf is er als laatste in opgenomen. Het attribuut is echter niet geïndexeerd. Voor *user* is dit bijvoorbeeld *{user,organizationalPerson,person,top}*

ObjectCategory bevat de meest typische vertegenwoordiger uit de hiërarchie. Dit is niet noodzakelijk de klasse van het object. Voor *user* is dit bijvoorbeeld *person*. Dit kenmerk is wél geïndexeerd.

Om op zoek te gaan naar objecten van een specifieke klasse, gebruikt men best beide kenmerken. Om zo alle *user* objecten te achterhalen gaan we op zoen naar objecten waarvan het *ObjectCategory* kenmerk is ingesteld op *person* en de *ObjectClass* de waarde *user* bevat.

Vraag 3 classSchema Objecten

3.a Bespreek het doel en de werking van classSchema attributen.

Voor elke klasse in AD is er een *classSchema* object waarmee de klasse ingesteld wordt. De kenmerken van het *classSchema* object definiëren de klasse en bevatten twee soorten regels: *structuurregels* en *inhoudsregels*. De *structuurregels* leggen de hiërarchische relaties tussen klassen of objecten. De *inhoudsregels* bepalen de beschikbare kenmerken van de klasse.

3.b Hoe benadert AD het mechanisme van overerving?

Een klasse neemt alle kenmerken over van zijn directe bovenliggende klasse. Dit mechanisme werkt recursief, zodat een klasse alle kenmerken van elk van zijn bovenliggende klassen, op alle niveaus in de hiërarchie, overneemt. De rechtstreekse bovenklasse wordt aangeduid met het attribuut *subClassOf* van het *classSchemaObject*. Elke klasse is al dan niet rechtstreeks afgeleid van de klasse *top*.

Ook *meervoudige overerving* is mogelijk. Een klasse kan, naast zijn onmiddellijke ouder, echter enkel kenmerken overnemen van een zogeheten *hulpklasse*. Deze hulpklassen zijn abstract en kunnen niet worden geïnstantiëerd. De kenmerken *auxiliaryClass* en *systemAuxiliaryClass* van het *classSchema* object bevatten alle mogelijke hulpklassen waarvan de klasse erft. Een klasse wordt als hulpklasse aangeduid door het *objectClassCategory* kenmerk in te stellen op waarde 3. In een dynamische aanpak kunnen, bij creatie, ook individuele instanties van klassen (objecten) erven van een bepaalde hulpklassen.

3.c Bespreek de diverse naamgevingen van classSchema objecten.

Net zoals bij *attributeSchema* objecten is de naamgeving viervoudig:

- *Common Name*: Wordt vertolkt door het kenmerk *cn*. Dit is de RDN van het object in de schema container
- *GUID:* Kenmerk *schemaIDGUID*. Dit is de GUID van de klasse, en is onafhankelijk van de GUID van het *classSchema* object dat het kenmerk voorstelt. Dit kan automatisch gegenereerd worden bij creatie van het object. In dit geval zal de klasse een andere GUID hebben in elk forest, daarom wordt het best op voorhand gegenereerd met *guidgen* of *uuidgen*.
- *LDAP Display Name:* Voor programmatorische toegang
- *Object ID:* Kenmerk *governsID*. Geldt als interne representatie. X500 ID, wordt verleend door speciale authoriteiten. Wordt genoteerd in *dotted decimal* formaat. Bedrijven worden een tak toegekend door een authoriteit (ITU, ANSI, ISO). Indien het bedrijf nog niet over een tak beschikt, kan het er een aanvragen of een OID in de microsoft tak genereren met *oidgen*.

3.d Bespreek de belangrijkste kenmerken van classSchema objecten, en hoe die kunnen ingesteld worden.

Net zoals bij *attributeSchema* objecten zijn de kenmerken opgedeeld in *inhoudsregels* en *structuurregels.* De *inhoudsregels* bestaan uit volgende kenmerken:

- De kenmerken *mustContain* en *systemMustContain* beschrijven de *mandatory attributes* van de klasse. Elke instantie van de klasse moet deze kenmerken bezitten.
- De optionele attributen zijn opgesomd in *mayContain* en *systemMayContain*
- *rDNAttID* bepaalt welk kenmerk van de klasse wordt gebruikt om de RDN van de objecten te bepalen. Dit is meestal ingesteld op *cn*
- *DefaultSecurityDescriptor* bepaalt de expliciete machtigingen die gelden op alle objecten van deze klasse. Instellen van dit object kan nuttig zijn voor delegatie van beheer.
- *systemOnly* bepaalt of de inhouds- en structuurregels kunnen worden gewijzigd.

De *structuurregels* bestaan, naast de attributen voor overerving, uit de volgende attributen:

- *defaultObjectCategory*
- *possSuperiors* en *systemPossSuperiors*: hiërarchische relaties tussen objecten van bepaalde klassen. Beide kenmerken bepalen welke klassen van objecten als container voor de objecten kunnen optreden.

3.e Welke andere types objecten bevat het AD schema, en wat is hun bedoeling?

Het enkele exemplaar van het *Aggregate* object van de klasse *subSchema*. Het heeft als doel om aan LDAP clients een vereenvoudigd schema ter beschikking te stellen. Biedt in combinatie met ADSI een toegang tot het schema. Objecten (*classSchema*, *attributeSchema*) in het abstracte schema hebben slechts een beperkt aantal attributen die min of meer overeenkomen met hun overeenkomstige reële schemaobjecten.

3.f Hoe en met welke middelen kan het AD schema worden uitgebreid?

Uitbereidingen en wijzigingen van het schema zijn risicovol, gelden voor het hele forest en kunnen potentieel de hele infrastructuur onbruikbaar maken. Schema objecten worden daarom ook beveiligd met ACL's. Aanmaken van geheel nieuwe structurele klassen en wijzigen van attributen van bestaande klassen moeten zoveel mogelijk vermeden worden.

Kleinschalige wijzigingen kunnen gebeuren met de *Active Directory Schema snap-in*. Een veilige manier om attributen aan een klasse toe te voegen, maakt eerst de nodige *attributeSchema* objecten aan. Vervolgens wordt een nieuwe hulpklasse aangemaakt, waarin de lijst van optionele attributen wordt aangevuld met de nieuw aangemaakte attributen. Tenslotte wordt de nieuw aangemaakte hulpklasse geasscocieerd met de klasse waaraan we de attributen wouden toevoegen.

Grootschaligere uitbereidingen gebeuren best met *ldifde* of proggramatisch met *ADSI Interfaces*. Met *ldifde* kunnen bestanden die geformatteerd zijn in *LDAP Data Interchange Fotmat* worden toegepast op de directory. Om het schema aan te passen, stellen we alle nodige acties voor in het *LDIF* formaat. Het bestand wordt dan meegegeven aan *ldifde -i -f* .

Vraag 4 Active Directory functionele niveaus

4.a Geef de diverse functionele niveaus waarop Active Directory kan worden ingesteld. Bespreek van elk niveau alle eraan gekoppelde voordelen. Geef hierbij een korte verklaring van de ingevoerde begrippen.

Een functioneel niveau stelt eisen aan het besturingssysteem van de domeincontrollers. Het bepaalt eveneens welke faciliteiten er beschikbaar zijn. Er zijn zowel **domein functionele niveaus** als **forest functionele niveaus**.

Het eerste domein functioneel niveau is het **Windows 2000 Mixed** domein niveau. Zowel Windows 2000, 2003 als NT4 domeincontrollers zijn toegelaten in het domein. Server 2008 domeincontrollers kunnen geen deel uitmaken van het domein. Het is het niveau met de laagste functionaliteit. Dit is het standaard niveau bij de installatie van Active Directory.

Het volgende niveau, **Windows 2000 Native** laat een willekeurige NT5+ domeincontroller toe. Deze eis geldt enkel voor domeincontrollers, niet voor werkposten en lidservers. Dit niveau heeft een aantal voordelen:

- Slechts één enkele **global catalog server** volstaat voor het gehele forest.
- **Transitieve vertrouwensrelaties** tussen alle domeinen van het forest.
- Alle domeincontrollers kunnen zelfstandig een aantal **SPN objecten** aanmaken. (Hiervoor gedelegeerd door de **RID master**, in Windows 2000 Mixed door de **PDC master emulator**.)
- Ruimere mogelijkheden om gebruikers en computers te verzamelen in **groepen**, met minder beperkingen op conversie, zichtbaarheid en nesten van groepen.
- **SID's** die een SPN object in het verleden heeft gehad, worden vanaf nu bijgehouden in het *sidHistory* kenmerk.

Het **Windows 2003** niveau staat enkel Windows 2008 en Windows 2003 domeincontrollers toe. Het schema bevat aanvullende schemaklassen en –attributen. De naam van een domeincontroller kan worden veranderd zonder degradatie en promotie. Er zijn eveneens aanvullende opdrachten beschikbaar. **UPN suffices** worden op DC niveau gecached. Er is lidmaatschap van universele groepen mogelijk. De global catalog server hoeft dus niet meer beschikbaar te zijn tijdens het inloggen. Group policies kunnen nu ook worden gefilterd met behulp van WMI scripts, naast de mogelijkheid op basis van beveiligingsgroepen.

Een **Windows 2008** domein kan enkel domeincontrollers bevatten die voorzien zijn van het Windows Server 2008 besturingssysteem. Er zijn opnieuw enkele aanvullingen aan het schema beschikbaar. De kerberos encryptie geschiedt met langere sleutels. In dit niveau zijn er ook **fine grained password policies** mogelijk. Een wachtwoordbeleid is nu niet langer

geldig voor het gehele domein, maar kan ook worden toegepast op individuele gebruikers en groepen. Tot slot is er ook replicatie van **DFS Namespaces** en de **Sysvol Share** mogelijk. Dit is performanter dan de traditionele *File Replication Services*.

Analoog aan domein functionele niveau's zijn er ook **forest functionele niveau's**. Het **Windows 2000** forest functioneel niveau stelt geen eisen aan het functioneel niveau van de kindomeinen.

Het **Windows 2003** forest functioneel niveau dicteert dat het forest enkel domeinen kan bevatten die minimaal op het Windows 2003 domein functioneel niveau opereren. Het belangrijkste deel van de recente AD functionaliteit kan benut worden:

- Gedeactiveerde klassen en attributen kunnen worden hergebruikt.
- Dynamische hulpklassen
- Dynamische objecten, met een beperkte levensduur die na het verstrijken van de *entryTTL* waarde automatische uit AD worden verwijderd. (tenzij ze opgefrist worden.)
- Efficiëntere replicatie van de global catalog gegevens.
- Herstructureren en hernoemen van de domeinen in het forest.
- Transitieve vertrouwensrelaties tussen verschillende forests.
- Windows 2008 RODC's
- Efficiëntere KCC algoritmen voor het construeren van de replicatietopologie.
- Replicatie van individuele waarden van een multivalued attribuut.

Het **Windows 2008** forest functioneel niveau biedt geen aanvullende functionaliteit, maar wordt wel aanbevolen om veiligheidsredenen. Er zijn enkel domeinen met een Windows 2008 functioneel niveau mogelijk.

4.b Hoe kan men detecteren op welk functioneel niveau een AD omgeving bevindt?

In eerste instantie kan men het domein functioneel niveau te weten komen door twee attributen van het domeinobject te raadplegen. Het attribuut ***ntMixedDomain*** heeft de waarde 1 voor het *Windows 2000 Mixed domain functional level* en 0 voor alle andere functionele niveaus. Het attribuut ***ms-DS-Behavior-Version*** heeft de waarden 0, 2, 3 voor respectievelijk 2000 Native/Mixed, 2003 of 2008. Het forest functioneel niveau wordt aangegeven door het ***ms-DS-Behavior-Version*** attribuut van de partitions container in de configuratiegegevens.

Anderzijds kan men gebruik maken van de ***Domains And Trusts*** *snap-in*. In deze tool klikt men rechts op een domein, vraagt men de properties op. De functionele niveau's van zowel het domein als het forest zijn te zien in de *general* tabpagina.

4.c Op welke diverse manieren kan men het functioneel niveau verlagen of verhogen?

Enerzijds kan men de attributen uit het voorgaande deel rechtstreeks wijzigen.

Anderzijds kan men in de *Domains And Trusts snap-in* rechts klikken op een domein of root *container* en de optie *raise functionality level* gebruiken.

Om de wijzigingen door te voeren moeten alle domeincontrollers worden herstart.

Het verlagen van het functioneel niveau is met controllers Lager dan *Windows Server 2008 R2* niet rechtstreeks mogelijk. Indien deze functionaliteit gewenst is, dan moet het domein volledig worden herbouwd, of moet de toestand vanuit een backup worden hersteld.

Vraag 5 Active Directory Domeinstructuren

5.a Wat is de bedoeling van vertrouwensrelaties?

Gebruikers in het ene (*trusted*, vertrouwd) domein kunnen worden geverifieerd door een domein controller in het andere (*trusting*, vertrouwend) domein. Het trusted domein bevat de gebruikers, het trusting domein bevat de resources.

Vooraleer een gebruiker in een domein toegang kan krijgen tot een bron in het andere domein, moet er worden bepaald of het trusting domein een **vertrouwenspad** heeft met het trusted domein. Een vertrouwensrelatie wil niet zeggen dat de gebruikers automatisch toegang hebben tot alle bronnen in het trusting domein. Dit wordt geregeld door machtigingen.

5.b Bespreek de verschillende soorten vertrouwensrelaties.

Er zijn twee soorten **expliciete vertrouwensrelaties**: **Forest Trusts** en **Realm Trusts**. Een forest trust is een vertrouwensrelatie tussen de domeinen van verschillende forests. Deze vertrouwensrelatie is bidirectioneel en transitief. Een Realm Trust is een vertrouwenspad tussen een 2008 domein en een willekeurig Kerberos V5 realm. Realm Trusts kunnen zowel transitief als intransitief worden gedefinieerd, alsook bidirectioneel of enkelvoudig. Realm trusts zijn te zien als een uitbereiding van Forest Trusts.

Naast de expliciete vertrouwensrelaties zijn er ook nog **verkorte vertrouwensrelaties** en **externe vertrouwensrelaties**. Verkorte vertrouwensrelaties worden ook wel *cross-link* of *shortcut* trusts genoemd. Het zijn aanvullende transitieve vertrouwensrelaties tussen domeinen van hetzelfde forest. Ze worden gebruikt om het vertrouwenspad tussen domeinen te verkorten, zodat de poerformantie van de verfificatie wordt verbeterd. Ze kunnen enkelvoudig of bidirectioneel zijn. Ze worden pas als nuttig beschouwd als een vertrouwenspad vijf domeinen overspant.

Een **externe vertrouwensrelatie** is een unidirectionele niet-transitieve vertrouwensrelatie, waarbij een domein een ander vertrouwt. Verificatieaanvragen kunnen enkel vanuit het trusting domein naar het trusted domein worden doorgestuurd. Externe vertrouwensrelaties kunnen enkel worden opgezet tussen een domein en een ander individueel domein in een ander forest, of met een NT4 domein. Vertrouwensrelaties tussen een NT4 en een NT5+ domein zijn steeds unidirectionieel en intransitief.

Impliciete vertrouwensrelaties worden door Windows Server automatisch aangemaakt tussen domeinen en hun kinddomeinen. Dit gebeurt ook tussen de trees van eenzelfde forest. Deze relaties kunnen niet worden verbroken en zijn automatisch bidirectioneel en transitief.

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

In eerste instantie kan de *Active Directory Domains And Trusts Snap-in* worden gebruikt om expliciete vertrouwensrelaties te configureren. Door rechts te klikken op een domein kunnen de *properties* van het domein worden opgevraagd. De *trusts* tabpagina toont een overzicht van

de reeds geconfigureerde vertrouwensrelaties. Om een nieuwe vertrouwensrelatie aan te maken, wordt de *New Trust* wizard gebruikt. Deze kan worden geopend door op de gelijknamige knop te klikken. Om een nieuwe vertrouwensrelatie aan te maken, moet de beheerder beschikken over beide domeinnamen, en een gebruikersaccount met machtigingen om een vertrouwensrelatie in beide domeinen aan te maken. Elke vertrouwensrelatie krijgt een wachtwoord toegewezen dat gekend moet zijn door de beheerders van beide domeinen. Na afloop van de configuratie wordt dit wachtwoord niet meer gebruikt. Optioneel kan men ook *selective authentication* en *SID Filtering* configureren. Standaard worden alle gebruikers van het trusted domein opgenomen in de groep *Authenticated Users* van het trusting domein. Om dit te vermijden kan Selective Authentication worden gebruikt om expliciet aan te geven welke gebruikers uit het trusted domein gebruik mogen maken van de vertrouwensrelaties.

Met behulp van de *command line* kunnen we vertrouwensrelaies maken met de opdracht *netdom trust* en de opties *domain*, *twoway*, *transitive* en *add*. Een overzicht van de reeds bestaande relaties kan worden bekomen met de opdracht *netdom query trust*.

5.d Welke verschillen zijn er in praktijk tussen NT4.0 en Windows Server Domeinstructuren? Bespreek de alternatieve mogelijkheden bij de conversie van een NT4.0 domeinstructuur naar een Windows Server omgeving.

Een eerste verschil tussen NT4 en Windows Server is het conceptueel onderscheid tussen *master domeinen* en *resource domeinen*. Een master domein bevat gebruikers en groepen, terwijl een resource domein lidservers bevat die diensten aanbieden aan de gebruikers, en zelf nauwelijks gebruikers bevat. De NT4 domeinstructuren bestaan meestal uit één (of meerdere) master domeinen, en meerdere resource domeinen. Er worden bidirectionele vertrouwensrelaties aangemaakt tussen alle masterdomeinen onderling, en unidirectionele vertrouwensrelaties waarbij elk resourcedomein elk masterdomein vertrouwt.

De omschakeling van NT4 naar Windows Server moet geleidelijk en gefaseerd gebeuren. Het aantal domeinen moet hierbij dalen. De *organizational units* (OU's) van Active Directory vervangen het conceptuele onderscheid tussen resource- en masterdomeinen. De upgrade begint steeds bovenaan in de domeinhiërarchie: Het masterdomein krijgt als eerste een upgrade, daarna volgen de resource domeinen.

Bestaande domeinen kunnen worden gesimuleerd door OU's in het Windows Server Domein. We bekomen zo een getrouwe weerspiegeling van de oude structuur. Eventueel kunnen aanvullende structuren worden toegevoegd om een meer gedetailleerde ordening te verkrijgen. Op deze manier wordt het aantal domeinen en trusts gereduceerd.

Indien er bepaalde bedrijfseenheden als afzonderlijke organisaties moeten worden behandeld, is een forest met afzonderlijke trees een goede oplossing. De gebruikersaccounts worden dan verplaatst naar de domeinen met de bronnen die ze gebruiken, in plaats van het centrale root domein.

Indien de oude structuur meerdere NT4 master domeinen bevat, zijn er hiervoor een aantal mogelijke oorzaken. In eerste instantie kan het zijn dat een enkel master domein te veel gebruikers en groepen zou bevatten. Deze verzoorzaken immers instabiliteit van de SAM

databank. Dit probleem is meteen opgelost door AD, omdat het veel schaalbaarder is. Een andere mogelijke oorzaak is de geografische situering. Het is mogelijk dat de verschillende geografische locaties verbonden zijn door links met kleine bandbreedte. Dit probleem kan worden opgevangen door AD sites te configureren. Het replicatieverkeer kan nog verder worden beperkt door gebruikt te maken van RODC's. Een derde mogelijkheid is de noodzaak aan een verschillend wachtwoordbeleid voor bepaalde gebruikersgroepen. Dit kan worden opgevangen door het domein functioneel niveau te verheffen naar Windows Server 2008, en een *fine grained password policy* in te stellen. Als laatste oorzaak voor verschillende NT4 master domeinen kan het zijn dat bepaalde onderdelen van de organizatie controle moeten kunnen uitoefenen over eigen bronnen en gebruikers. Dit is bij de invoering van AD de enige reden om apparte domeinen te behouden in de verschillende sites. De migratie gebeurt op een van de volgende manieren:

1. Elk NT4 domein wordt geupgraded naar de root van een Windows Server tree in hetzelfde forest. Alle gemachtigde gebruikers krijgen hierdoor potentiële toegang tot alle bronnen in alle domeinen van het forest. Het forest kan een gemeenschappelijk schema, gemeenschappelijke configuratiegegevens en een gemeenschappelijke global catalog delen.

2. Als alternatief kan elk NT4 domein worden geupgraded naar een subdomein van een artificiëel root domein van dezelfde tree. Dit root domein heet een *structural* of *placeholder* domein omdat het resources noch accounts bevat. Het is echter wel een uitstekende plaats om de global catalog onder te brengen.

Als laatste mogelijkheid voor migratie kan er besloten worden om alle NT4 domeinen samen te voegen tot één groot Windows Server domein. Dit kan op twee manieren. In de eerste manier worden alle domein eerst samengevoegd, en vervolgens geupgraded naar Windows Server. De oorspronkelijke domeinen worden dan omgezet in OU's. Er zijn hiervoor geen hulpmiddelen. De migratie gebeurt volledig manueel met behulp van commandolijnopdrachten. Als alternatief worden de afzonderlijke domeinen eerst geupgraded naar Windows Server. Vervolgens wordt in elk van de masterdomeinen voor de resourcedomeinen een OU aangemaakt. De machines in de resourcedomeinen worden dan verplaatst naar de OU's in de masterdomeinen.

Vraag 6 Active Directory server rollen

6.a Welke vragen moet men zich stellen na de initiële installatie van een Windows Server toestel, in verband met de rollen die het zal vervullen met betrekking tot Active Directory? Formuleer voor zover relevant telkens een antwoord op volgende vragen: Hoe wordt bepaald welke servers een specifieke rol vervullen? Hoeveel zijn er nodig? Hoe gebeurt de instelling ervan? Bespreek eigenschappen zoals functie, inhoud, synchronisatie, ... De eventuele relatie tussen de verschillende rollen. Vermeld eventueel welke rollen samen kunnen worden vervuld en welke niet. Op welke diverse manieren kan men de configuratie van een rol vervullen?

De eerste vraag die men zich moet stellen is of de server al dan niet wordt opgenomen in het domein. Zelfstandige servers kunnen wel nog bronnen delen, maar kunnen niet profiteren van de voordelen die AD biedt. Meestal besluit men de server als lidserver op te nemen in het domein. Met lidserver wordt bedoeld dat hij wel degelijk deel uitmaakt van het domein, maar niet de functie van domeincontroller vervult.

Een lidserver handelt geen inlogverzoeken af, slaat geen beleidsinformatie over domeinbeveiliging op en is niet betrokken bij het replicatieproces. Deze configuratie is geschikt voor onder andere fileservers, toepassingsservers, databaseservers, websersvers, firewalls en routers. Functies van een server worden ingedeeld op drie niveaus. In eerste instantie zijn er de eigenlijke *server roles*. Dit zijn de primaire functies van de server. Vervolgens zijn er de *role services*: het zijn optionele componenenten. Tot slot zijn er nog de features, dit zijn ondersteunende functies. De configuratie gebeurt voor elk van de niveaus met de respectievelijke wizard van de *server manager*. Alternatief kan ook de *ServerManagerCmd* opdracht worden gebruikt. Beleidsinstellingen die geldig zijn voor het domein, blijven geldig op de lidserver. Lidservers blijven wel de lokale SAM database behouden. De volgende vraag is dan of de server ook de rol van domeincontroller zal vervullen. Men moet hierbij in gedachten houden dat de promotie tot domeincontroller een aanzienlijke belasting met zich meebrengt. Hier moet worden rekening met gehouden in verband met de belasting die de andere rollen van de server veroorzaken. Meestal wordt slechts een fractie van de servers gepromoveerd tot domeincontroller. Een server tot domeincontroller promoveren gebeurt door middel van de *dcpromo* opdracht, alsook het degraderen tot lidserver.

Indien ervoor wordt gekozen een lidserver tot domeincontroller te promoveren, stelt zich de vraag of de domeincontroller ook de rol van *Global Catalog Server* zal vervullen. Indien er slechts een domein in het forest is, mogen alle domeincontrollers tot global catalog server worden gepromoveerd. Om het replicatieverkeer te beperken, zorgt men er best voor dat er steeds een global catalog server per *site* aanwezig is. De promotie gebeurt door de *Global Catalog* optie aan te vinken in de *general* tabpagina van de *properties* van de *NTDS Settings* van een domeincontroller. Dit is terug te vinden in de *Active Directory Sites And Services Snap-in*. De global catalog server heeft een kopie van alle objecten van de domeingegevens van het domein waarin de global catalog server zich bevindt, en een kopie van een subset van de eigenschappen van alle objecten van het gehele forest. Deze subset wordt enkel gerepliceerd tussen GC servers. Verder bevat de GC nog een kopie van de

configuratiegegevens van alle domeinen in het forest, en het unieke schema van het forest. Eventueel worden ook nog specifieke applicatiepartities bijgehouden in de global catalog.

Verder is er nog de vraag welke domeincontrollers de *Operations Master* rollen vervullen. We maken hierbij het onderscheid tussen OM rollen die uniek zijn binnen het domein, en OM rollen die uniek zijn binnen het hele forest. De *domain-wide operations master roles* bestaan uit de ***operations master*** en de ***infrastructure master***. De operations master behelst twee functies die steeds door de zelfde DC moeten worden uitgevoerd: de ***RID master*** en de ***PDC emulator master***. De RID master wijst reeksen van uniek RID's toe aan domeincontrollers voor de aanmaak van SID's voor nieuwe SPN objecten. Objecten tussen domeinen verplaatsen gebeurt vanaf de RID master van het domein dat het object bevat. Het verlies van de RID master heeft geen gevolgen voor beheerders en eindgebruikers, tenzij er SPN objecten moeten worden gecreëerd, en de RID pool onvoldoende RID's bevat. De *PDC emulator master* emuleert in een Windows 2000 mixed domein met BDC's een NT4 PDC. De verificatie voor NT4 clients gebeurt transparant door AD. De PDC emulator master verwerkt wachtwoordwijzigingen en repliceert de aanpassingen naar de BDC's. Wijzigigen die op andere DC's worden uitgevoerd worden eerst gerepliceerd naar de PDC emulator master. Indien een aanmeldingsverzoek een verkeerd wachtwoord meegeeeft, wordt het verzoek eerst doorgestuurd naar de PDC emulator master alvorens het defenities negatief te beantwoorden. De PDC emulator master is eveneens de primaire bron voor **tijdssynchronisatie**. Het verlies van de PDC emulator master heeft gevolgen voor eindgebruikers en moet direct worden gecorrigeerd. De *infrastructure master* is verantwoordelijk voor het bijwerken van verwijzigingen van objecten uit het eigen domein, naar objecten van een ander domein. (*forwardLink, backLink, phantom objects*). De infrastructure master doet beroep op de global catalog server om de kenmerken van objecten te vergelijken. Tenzij alle DC's van het domein de rol van GC vervullen, moet er worden voor gezorgd dat de rol van infrastructure master nooit samen wordt vervuld met de rol van global catalog server. De global catalog server beschikt immers steeds over de meest recente informatie, en bijgevolg zou de infrastructure master nooit werken. In het eerste scenario echter beschikken alle DC's steeds over de juiste informatie omdat ze allen de rol van GC vervullen, en maakt het bijgevolg niet uit op welke DC de infrastructure master wordt geïnstalleerd. Het verlies van de infrastructure master heeft enkel gevolgen voor een beheerder die recent grote aantallen accounts heeft verplaatst of hernoemd.

Naast de domain-wide operations master rollen, zijn er ook nog de *forest-wide* operations master rollen. Deze bestaan uit de ***schema master*** en de ***domain naming master***. De *schema master* beheert alle bijgewerkte en gewijzigde gegevens van het schema. Het schema van een forest bijwerken gebeurt dan ook steeds exclusief via de schema master. Dit zorgt voor consistentie en vermijdt conflicten. Het verlies van de schema master heeft enkel gevolgen voor beheerders die het schema proberen te wijzigen, of een toepassing installeren die een wijziging in het schema veroorzaakt. De *domain naming master* staat in voor het toevoegen en verwijderen van domeinen in het forest. Het is tevens de enige domeincontroller die de partitions container kan wijzigen. AD vereist dat de domain naming master tevens een GC server is.

Om de eigenaar van de domain-wide rollen te raadplegen, moet het *fSMORoleOwner* kenmerk van een object in een bepaalde partitie worden geraadpleegd. Om te weten te komen welke DC de rol van RID manager vervult, zoekt men het object *RID Manager$* op dat zich in de *System Container* van de domeingegevens bevindt. De infrastructure master kan worden

gevonden in het *Infrastructure* object dat zich restreeks in de domeingegevens bevindt. De *PDC Emulator master* kan worden gevonden in de eigenschappen van de domeincontainer. Bijvoorbeeld:

```
  DC=members,DC=contoso,DC=local                                    CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Leuven,CN=Sites,CN=Configuration,DC=cont
oso,DC=local
  CN=Infrastructure,DC=members,DC=contoso,DC=local                  CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Leuven,CN=Sites,CN=Configuration,DC=cont
oso,DC=local
  CN=RID  Manager$,CN=System,DC=members,DC=contoso,DC=local         CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Leuven,CN=Sites,CN=Configuration,DC=cont
oso,DC=local
```

De *domain naming master* kan worden geraadpleegd in het *partitions* object van de configuratiegegevens. De *schema master* kan worden geraadpleegd in het *Schema* object van de schemapartitie. Beiden zijn containerobjecten.

Om de domain-wide operations master rollen over te dragen, moet worden gebruikt gemaakt van de *Active Directory Users And Computers Snap-in*. (*dsa.msc*) Dit kan door de optie *Operations Masters* aan te klikken in het contextmenu van een domeinobject. Om de schema master rol over te dragen, gebruiken we dezelfde optie van het contextmenu van het *Active Directory Schema* item in de *Active Directory Schema Snap-in*. (*schmmgmt.msc*).

Bij de installatie van AD worden alle mogelijke rollen toegewezen aan de eerste domeincontroller van het nieuwe domein in de nieuwe tree in een nieuw forest. Bij toevoegen van een nieuw domein worden de drie domain-wide operations masters rollen toegewezen aan de eerste domeincontroller van het nieuwe domein. Als er meerdere domeincontrollers worden aangemaakt, is het een goed idee om de *single master* functies zoveel mogelijk over verschillende domeincontrollers te spreiden. In sites waar een DC met een operations master rol is opgesteld wordt best nog een andere DC voorzien. Dit beperkt het risico op cruciaal gegevensverlies indien de operations master rol eenzijdig zou moeten worden overgenomen.

Tot slot moet men zich erover bezinnen welke DC's als *Read Only Domain Controller* (RODC) zullen worden geconfigureerd. Dit is goede praktijk als de fysieke beveiliging van het toestel niet kan worden gegarandeerd, of waar specifieke interactieve toepassingen enkel op een DC kunnen worden uitgevoerd. Een bijkomend voordeel is dat het replicatieverkeer in een enkele richting wordt beperkt. Er kan ook nog configuratie van een *filtered attribute set* (welke kenmerken worden gerepliceerd, en welke niet) en een *Password Replication Policy* worden geconfigureerd met *credential caching* voor specifieke gebruikers en computers. RODC's kunnen tevens de rol van GC en DNS server vervullen. In het geval van DNS gaat het over een ordinaire secundaire nameserver. Een RODC biedt ook ondersteuning voor de operations masters rollen. Er geldt wel de beperking dat een RODC enkel met Windows Server 2008 DC's gegevens kan repliceren.

Vraag 7 Gedeelde mappen en NTFS

7.a Op welke diverse manieren kunnen gedeelde mappen gecreëerd en geconfigureerd worden? Geef hierbij een korte verklaring van de ingevoerde begrippen en de alternatieve configuratie-instellingen.

Om shares aan te maken kunnen we enerzijds gebruik maken van de *Advanced Sharing* knop van de *sharing* tabpagina van de *folder properties* van de map die we wensen te delen. Hier zijn een aantal opties te configureren:

- *Share This Folder* geeft aan of de map gedeeld is of niet.

- Het veld *Share Name* dient om een share naam toe te voegen. Men kan de map delen onder zoveel namen als gewenst.

- De spinner met het bijschrift *Limit the number of simultaneous users* dient om het aantal gebruikers dat tegelijk verbinding kan maken te beperken.

- Het *Comments* veld wordt gebruikt om optioneel een opmerking toe te voegen die zichtbaar is voor gebruikers wanneer ze naar de share bladeren.

- De knop *Permissions* wordt gebruikt om de share machtigingen in te stellen. Deze machtigingen worden in Server 2008 *SMB* machtigingen genoemd. Ze hebben steeds de overhand op de NTFS machtigingen. Meestal wordt ervoor gekozen om op share niveau iedereen volledige toegang toe te staan, en een fijnkorrelig beleid op NTFS niveau in te stellen.

- De knop *Caching* ten slotte, wordt gebruikt om client-side *offline access* te configureren. Hierdoor kan een gebruiker toch nog beschikken over de bestanden als de fileserver of share onbeschikbaar is.

Een tweede mogelijkheid maakt gebruik van de *Share Folders Snap-in*. Deze is beschikbaar is de *Computer Mamagement* console (*compmgmt.msc*) of autonoom via *fsmgmt.msc*. In het context menu van *shares* subtak selecteren we *new share*. Er start een wizard op waarin dezelfde opties als het vorige alternatief kunnen worden geconfigureerd. Bijkomend moet hier ook eerst het pad van de te delen map worden ingegeven.

Fileservers voorzien van het Windows 2008 besturingssysteem kunnen ook gebruik maken van de taak *Provision New Share* in de *Server Manager*, onder *Roles, File Services, Share And Storage Management*. Ook hier start een wizard op, die iets meer configuratiemogelijkheden biedt. Achtereenvolgens wordt gevraagd om volgende aspecten te configureren:

- *Shared Folder Location*

- *NTFS Permissions*

- *SMB Permissions*
- *SMB Settings*: *Access Based Enumeration* en *Client-side caching*
- *Quota Policy* (zie verder)
- *Filescreen Policy* (zie verder)

Lokale shares kunnen met behulp van de commandolijn worden gecreëerd via de opdracht *net share*. Om op een remote toestel een share aan te maken kan de opdracht *rmtshare* worden gebruikt. De optie */grant:<identity>,<permission>* wordt gebruikt om een machtiging aan een bepaalde identiteit toe te kennen. De optie */delete* vernietigd de share.

Nadat een share aangemaakt is, kunnen nog een aantal aspecten worden geconfigureerd. Een eerste aspect is de **zichtbaarheid** van de share. Deze kunnen we beïnvloeden door eenvoudigweg een *$*-teken achter de naam van de share te plaatsen. Standaard zijn er een aantal beheershares aanwezig, die standaard verborgen zijn.

Een volgend configuratieaspect zijn de **machtigingen** op de share. Deze kunnen op twee niveau's worden ingesteld: **NTFS machtigingen** en **SMB machtigingen**. De machtigingen bepalen wie toegang heeft tot de gegevens, en wat ze er kunnen mee doen. Elk object waarop machtigingen kunnen worden ingesteld heeft een *security descriptor* die bestaat uit volgende onderdelen: *Access Control List* (ACL), *System Access Control List* (SACL, logging), *SID* van de eigenaar en de primaire groep (wegens POSIX compatibiliteit).

De ACL is een verzameling van machtigingen die gelden voor bepaalde groepen of gebruikers. Ook het type van de machtiging is opgenomen in de ACL. Welke types machtigingen er beschikbaar zijn is afhankelijk van het object dat wordt beveiligd. Elke toewijziging van een machtiging wordt een *machtigingsvermelding* of *Access Control Entity* (ACE) genoemd. Het geheel van ACE's vormt de ACL. Het is een goed idee om een ACE steeds aan te maken voor een groep, en nooit voor een individuele gebruiker. ACE kunnen worden aangemaakt voor gebruikers en groepen van het eigen domein, en alle trusted domeinen. De ACL van een object wordt steeds in *cannonieke volgorde* verwerkt. Dit wil zeggen dat eerst de ACE's worden toegepast die een machtiging ontzeggen, dan pas de ACE's die een machtiging toestaan. Een machtiging ontzeggen is dominant, eens een machtiging ontzegd is voor een bepaalde gebruiker of groep, worden eventuele volgende toezeggingen genegeerd. Dit geld ook indien een bepaalde machtiging werd ontzegd aan een groep waarvan de gebruiker lid is.

Er zijn twee soorten machtigingen: **expliciete** en **impliciete** machtigingen. Een explicitiete machtiging werd ingesteld door middel van de ACL, een impliciete machtiging werd overgeërfd van de container waarin het object zich bevindt. Een expliciete machtiging heeft steeds de voorrang.

Machtigingen op shareniveau hebben steeds de overhand op NTFS machtigingen. Meestal geeft men volledige toegang op shareniveau, en stelt men specifieke beperkingen in op NTFS niveau. De veroorzaakt het probleem dat een gebruiker alle inhoud van een gedeelde map kan

bekijken, ook al heeft hij er geen machtigingen op. Om dit euvel op te lossen gebruikt men *Acess Based Enumeration*: op deze manier zijn enkel de objecten zichtbaar waarop de gebruiker machtigingen heeft. Op shareniveau zijn er slechts 3 machtigingen: *Full Control*, *Read* en *Change*.

Naast de 13 atomaire machtigingen en 6 moleculaire machtigingen, kunnen op NTFS niveau ook nog *quota* worden ingesteld. Quota verhinderen dat bepaalde gebruikers de beschikbare schijfruimte op een fileserver zouden monopoliseren door de opslagcapaciteit afdwingbaar in te stellen. We onderscheiden twee soorten quota: **volumequota** en **mapquota**. Volumequota gelden voor een volledige NTFS volume en zijn gebaseerd op bestandseigendom (op basis van SID.). Indien het volume meerder mappen bevat, zijn de quota collectief van toepassing op alle mappen. Het is mogelijk om mapquota te simuleren met volumequota, door de NTFS volumes te koppelen aan een map, en dan quota in te stellen op het volume. Volumequota houden geen rekening met eventuele bestandscompressie. *Mapquota* gelden voor een gehele map en zijn collectief, onafhankelijk van de bestandseigendom. Ze zijn dus enkel zinvol indien te toegang tot een map beperkt is to een enkele gebruiker. Voor beide types wordt gebruik gemaakt van twee drempelwaarden: de *soft treshold* en de *hard treshold*. Indien de soft treshold wordt overschreden, krijgt de gebruiker een waarschuwing dat zijn quota bijna vervuld zijn. Indien de hard treshold wordt overschreden, kan de gebruiker geen bestanden meer opslaan. Merk op dat aan een beheerder nooit schijfruimte wordt geweigerd.

Een derde configuratieaspect zijn de *filescreens*. Deze instelling verhinderen bepaalde gebruikers ervan om bestanden met een bepaalde extensie op te slaan in de gedeelde map. Het is mogelijk om bepaalde reacties te triggeren bij overtreding van het beleid.

Het laatste configuratieaspect is de *client-side caching*. Dit houdt in dat de beheerder kan instellen dat van veelgebruikte bestanden een lokale kopie wordt bijgehouden. Wijzigingen worden zowel in de cache als op de share doorgevoerd. Indien het bestand wordt opgehaald, wordt enkel het bestand met de meest recente timestamp opgehaald. De cache blijft beschikbaar als de netwerkshare onbeschikbaar is, zodat de gebruiker kan doorwerken. Het *Sync Center* programma zorgt ervoor dat off-line wijzigingen worden doorgevoerd wanneer de share terug beschikbaar wordt. Indien een conflict wordt gedecteerd, wordt de gebruiker om een actie gevraagd. De beheerder kan bij de configuratie de bestanden vrijlaten aan de gebruiker, alle bestanden laten cachen (*optimize for performance*: *.exe* wordt steeds lokaal uitgevoerd) of de caching verhinderen.

7.b Op welke diverse manieren kan men gebruik maken van gedeelde mappen?

De eenvoudigste manier om van een gedeelde map gebruik te kunnen maken, is door rechtstreeks het *UNC pad* in te geven in de adresbalk van een explorer venster.

Indien de share veelvuldig wordt gebruikt, is het handiger om hem te monteren in het lokale filessyteem. De share krijgt dan een stationletter toegewezen, en kan dan worden benaderd alsof het een gewone schijf betrof. Om dit te bewerkstelligen, kan in het *Computer* venster de optie *Map Network Drive* van het menu *Extra* worden gebruikt. Er start een wizard op die vraagt om het UNC pad van de share op te geven, en een driveletter te kiezen. Optioneel kunnen ook alternatieve *credentials* worden opgegeven. Hetzelfde effect kan ook worden bereikt met de opdracht *net use*. Bijvoorbeeld:

```
Net use U: \\files.contoso.local\homes\john
```

Indien er geen voorkeur is voor de driveletter, mag deze worden vervangen door een asterisk. De optie */user:<gebruikersnaam>* staat toe om een gebruikersnaam op te geven. De optie */d* verbreekt de verbinding. Alternatief kunnen ook de opdrachten *pushd* en *popd* worden gebruikt. De eerste maakt een verbinding met de eerst beschikbare driveletter (omgekeerde alfabetische volgorde), de laatste verbreekt de laatst ingestelde verbinding.

7.c Geef een overzicht van de belangrijkste voordelen van de opeenvolgende versies van het NTFS bestandssysteem. Bespreek elk van deze aspecten kort, en geef aan hoe je er gebruik kan van maken, bij voorkeur vanuit de commandolijn.

NTFS versies zijn:

- V1.0, V1.1, V1.2: NT4 en voorlopers
- V3.0: Windows 2000
- V3.1: Windows XP en recenter

Features vanaf V1.2

- Beveiliging op bestandsniveau. Dit is vereist voor sommig functies van Windows Server, waaronder Active Directory.
- Auditing op objecttoegang.
- Bestandscompressie
- Spanning/Mirroring met verschillende schijven
- Schijfactiviteiten worden vastgelegd in logboekbestanden. Het volume kan zichzelf herstellen na een stroomonderbreking.
- Grotere partities.

Bijkomende features vanaf V3.0

- Bestandscodering
- Volumequota’s
- Volumekoppelpunten

- Sparse bestanden: het toewijzen van schijfruimte aan de delen van grote bestanden waarnaar effectief wordt geschreven. Dit kan met de opdracht *fsutil sparse setflag <bestandsnaam>*

- Hardlinks: *fsutil hardlink create <linknaam> <bronbestand>*

- *Junction points*, analoog aan symlinks naar mappen. *Linkd <linknaam> <bronmap>*. De optie */d* verwijdert de link. De opdracht *rm –r* verwijdert de link en de bronmap.

- In NT6: voor beide de opdracht *mklink* gebruiken. De optie */H* zorgt voor een hardlink, de optie */D* zorgt voor een symlink naar een directory. Indien er geen optie wordt meegegeven wordt er een symlink naar een bestand verondersteld. Deze opdracht kan ook worden gebruikt voor bestanden die zich op een share bevinden, of zelfs voor volledige shares.

De meeste nieuwe features worden gerealiseerd door reparse punten. Wanneer NT5+ een repasepunt detecteert, wordt de tag van het reparsepunt teruggestuurd naar de IO-stack, waar bij de reparsetag wordt onderzocht door extra bestandssysteemfilters, die NT5+ vertellen dat er een ander stuurprogramma moet worden gebruikt dan het standaard NTFS stuurprogramma. Dit mechanisme laat toe dat er extra functionaliteit wordt toegevoegd aan het bestandssysteem, door Microsoft en andere partijen, zonder dat het bestandssysteem telkens moet worden herzien. Voorbeelden in Windows Server 2008:

- *Self-Healing* van het volume: corrupties kunnen online worden opgespoord en gecorrigeerd.

- Ondersteuning van **transacties**.

- Mapquota

- *File Screens.*