Inhoudsopgave

Deel I

Mondeling

Hoofdstuk 1

Structuur van Active Directory gegevens

1.1 Bespreek de diverse namen die alle Active Directory objecten identificeren.

Relative Distinguished Name (RDN) zorgt voor de unieke identificatie binnen de container waar het object zich in bevindt. bv **cn=beelzebub** is RDN van computer beelzebub. De RDN wordt (meestal) opgeslagen in het kenmerk **cn** van het object.

Distinguished Name (DN) is opgebouwd uit de RDN van het object zelf en de RDNs van alle containerobjecten waarvan het object in de hiërarchische indeling deel van uitmaakt. Dit zorgt voor een unieke naamgeving voor elk object. Elk opeenvolgend deel van de DN heeft de vorm **attribuut=waarde**, staat bekend als *attributed naming*. De delen worden gescheiden door een komma. De DN naamgeving werkt van beneden (objectnaam) naar boven (root van AD). bv **cn=beelzebub,ou=iii,dc=hogent,dc=be** De DN is belangrijk voor de werking van het LDAP protocol, bv belangrijk bij het programmeren van scriptcode die AD rechtstreeks aanspreekt. Een LDAP-cliënt kan query's op willekeurige objecten uitvoeren door een LDAP URL te gebruiken met de vorm **LDAP://server DNS naam/object DN**. De DN wordt opgeslagen in het kenmerk **distinguishedName** van het object.

Canonical name wordt op dezelfde manier samengesteld als de DN, maar wordt op een eenvoudigere manier weergegeven: **hogent.be/iii/beelzebub**. De meeste hulpmiddelen in Active Directory tonen de canonieke naam, in plaats van de DN. Het wordt opgeslagen in het kenmerk **canonicalName** van het object. Dit is een geconstrueerd kenmerk.

Globaal Uniek ID (GUID) is een 128-bit getal dat niet kan gewijzigd worden. Het wordt

bepaald bij de creatie van het object. Ook als het object verplaatst of gewijzigd wordt zal de GUID niet veranderen. De GUID is beschikbaar voor verwijzing van externe processen en programmeerfuncties. Het wordt opgeslagen in het kenmerk **objectGUID** van het object.

1.2 Wat zijn SPN objecten? Bespreek de aanvullende naamgeving voor deze objecten.

Security Principal Objects (SPN) zijn AD-objecten waaraan Security ID's (SID) zijn toegewezen. De SID wordt opgeslagen in het **objectSid** kenmerk. SPN objecten worden, na aanmelding op het netwerk, gebruikt voor het verlenen van toegang tot domeinbronnen. Ze zijn van toepassing op gebruikeraccounts, computeraccounts, groepen en domeinen. SIDs zijn uniek, ook in de tijd: nieuw aangemaakte accounts kunnen zo nooit de rechten krijgen van een oude account.
SIDs worden meestal voorgesteld door een hiërarchische string getallen gescheiden door koppeltekens, bv **S-1-5-x-y-z-500**. S-1-5 is de standaard prefix, bestaande uit een *Revision Level* en een *Authority Identifier*. X, y en z zijn 32-bit getallen specifiek voor het domein (*Domain Subauthority Identifier*). 500 is een *relative ID* (RID), dat naar het feitelijke object verwijst. Bij verplaatsing binnen hetzelfde domein blijft de SID ongewijzigd. Bij verplaatsing naar een ander domein zal de SID we veranderen. De GUID blijft altijd ongewijzigd. Om te vermijden dat een gebruiker hierna zijn toegang tot domeinbronnen zou verliezen worden alle vorige SIDs van het object bijgehouden in het **sIDHistory** kenmerk.

1.2.1 Aanvullende naamgeving voor gebruikersaccounts

De RDN, DN en canonieke naam zijn ongeschikt als aanmeldingsnaam omdat ze bij verplaatsing veranderen. SID en GUID zijn mits hun numerieke karakter ook niet geschikt hiervoor. Elke gebruikersaccount heeft ook een *User Principal Name* (UPN), aka aanmeldingsnaam. Deze wordt bij het aanmaken van het account ingevoerd door de beheerder en opgeslagen in het *userPrincipalName* kenmerk. Dit moet uniek zijn binnen het forest. UPN bestaat standaard uit de RDN van de gebruiker en de UPN suffix, gekoppeld met het @-teken. Voor de UPN suffix zijn er een aantal alternatieven:

- Standaard wordt de DNS naam van het domein genomen
- Dikwijls kiest men voor: de DNS naam van het root domein van het forest
- Kan ook een willekeurige alternatieve naam zijn, als deze op voorhand geregistreerd is door een beheerder.

UPN is de meest geschikte aanmeldingsnaam maar wordt maar zelden gebruikt door compatibiliteit met vroegere NT versies. Meestal wordt als aanmeldingsnaam de NetBIOS naam

van het domein en de SAM accountnaam van de gebruiker, gekoppeld met \, genomen. De NetBIOS naam bestaat uit max 15 karakters, standaard de meest linkse component van de DNS naam. De SAM accountnaam bestaat uit max 20 karakters, standaard de eerste 20 bytes van de RDN. NetBIOS naam moet uniek zijn in het forest, SAM accountnaam uniek in het domein en wordt opgeslagen in het **sAMAccountName** kenmerk

1.2.2 Aanvullende naamgeving voor computeraccounts

Elke computeraccount in AD heeft behalve zijn RDN, DN, canonieke naam, GUID en SID ook een SAM accountnaam (ook NetBIOS computernaam genoemd), een DNS hostnaam en een *Service Principal Name* (SPN). SAM naam bestaat uit eerste 15 bytes van RDN, gevolgd door een $, en wordt opgeslagen in het sAMAccountName kenmerk. De DNS hostname wordt opgeslagen in het dnsHostName kenmerk en bestaat standaard uit de eerste 15 tekens van de RDN en de suffix van de primaire DNS. De SPN is essentieel tijdens de wederzijdse verificatie van client software en de server die een bepaalde service biedt: de client zoekt een computeraccount op aan de hand van de SPN naam van de service waarmee hij een verbinding tot stand wil brengen. De SPN wordt bepaald door het multi-valued *servicePrincipalName* kenmerk, oa samengesteld op basis van DNS naam en eventueel SRV records die naar het toestel verwijzen.

1.3 Enkele veel gebruikte klassen vertonen nog meer identificerende attributen voor hun instanties. Bespreek deze klassen en attributen

De klassen attributeSchema en classSchema zijn twee veelgebruikte klassen waarvan de objecten terug te vinden zijn in de schema partitie. Deze objecten beschrijven alle objecten in de AD: classSchema objecten beschrijven de klassen waarvan objecten kunnen aangemaakt worden. De attributen die een klasse kan bevatten worden apart beschreven door attributeSchema objecten, zo kunnen meerdere klassen dezelfde kenmerk-definitie gebruiken.
De objecten van deze klassen hebben een viervoudige naamgeving:

Common name is niets anders dan de RDN van het object in de schema container.

GUID van het kenmerk kan automatisch gegenereerd worden bij creatie van een nieuw kenmerk of kan op voorhand met guidgen worden gegeneerd zodat dezelfde kenmerken in verschillende forest dezelfde GUID kunnen krijgen.

LDAP display name wordt gebruikt voor programmatische toegang.

Object identifier (OID) dient voor interne representatie. Dit zijn X.500 Object IDs die worden verleend door speciale autoriteiten zoals ISO, en zijn gegarandeerd uniek in alle

netwerken over de hele wereld. Een bedrijf kan een eigen unieke subtak toegewezen krijgen of kan gebruik maken van een unieke subtak in een Microsoft subtak.

1.4 In welke partities is de Active Directory informatie verdeeld? Geef de betekenis van elke partitie, hun onderlinge relatie, en de replicatiekarakteristieken erven.

De directory wordt enkel opgeslagen op domeincontrollers. Op elke domeincontroller wordt een kopie opgeslagen van de directory voor het domein waarin de controller zich bevindt. De informatie die in de directory is opgeslagen, is fysiek verdeeld in minimaal drie categorieën: **directory partities**

Domeingegevens bevatten de eigenlijke informatie over objecten in het domein (zoals gedeelde bronnen, gebruiker- en computeraccounts). Bij de installatie worden een aantal standaard objecten geinstalleerd door het systeem, bv de beheerderaccount. Wordt gedeeld per domein, dus er zijn evenveel partities met domeingegevens als er domeinen zijn in het forest. De domeingegevens worden niet gedistribueerd naar andere domeinen. Er wordt wel een subset van alle kenmerken van alle domeinen bijgehouden in de globale catalogus.

Configuratiegegevens beschrijven de fysieke topologie van de directory. Dit bevat onder andere een lijst van alle domeinstructuren, de locaties van de domeincontrollers en de global catalog controllers, de sites en de replicatietopologie. De meeste gemeenschappelijke instellingen van het ganse forest worden hierin opgeslagen, als kenmerken van objecten. De configuratiegegevens gelden voor alle domeinen in het forest.

Het schema is de formele definitie van alle objecten en kenmerkgegevens die kunnen opgeslagen worden in de directory. Dit schema is uniek voor alle domeinen in het forest.

Applicatiepartities dit is een 4e vorm van partities die vanaf Windows server 2003 kan aangemaakt worden. Een deel van de AD gegevens kan in één of meerdere gescheiden applicatiepartities worden ondergebracht, dit is interessant voor dynamische objecten. Ze kunnen geen SPN objecten bevatten. Objecten binnen de applicatie partitie kunnen niet verplaatst worden buiten de partitie. bv voor DNS is er een aparte applicatiepartitie.

Het schema en de configuratiegegevens zijn containerobjecten in het root domein van het forest. Ook de eventuele applicatiepartities vormen containerobjecten ten opzichte van de overeenkomstige domeingegevens. Dit is een logische structurering, fysiek bestaat het wel uit meerdere bestanden.

AD servers wisselen continu gegevens uit. Elke partitie in de directory vormt een aparte eenheid voor replicatie, waarbij telkens een specifieke groep controllers hoort. Het schema en configuratiegegevens worden gerepliceerd naar alle domeincontrollers in het forest. De domeingegevens worden logischerwijs binnen het domein gerepliceerd. Applicatiepartities worden gerepliceerd tussen een eigen deelverzameling specifiek hiervoor geconfigureerde domeincontrollers van het forest. DNS partities kunnen zo bv enkel naar DNS nameservers gerepliceerd worden.
De koppeling tussen een partitie en zijn replicerende domeincontrollers wordt bijgehouden in het **msDS-NC-Replica-Locations** kenmerk van het overeenkomstige crossref object in de configuratiegegevens.
Een subset van de kenmerken van alle objecten in de domeingegevens van elk domein in het forest worden gerepliceerd naar de globale catalogus.

Hoofdstuk 2

attributeSchema objecten

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

Het AD schema is de formele definitie van alle objecten en kenmerkgegevens die kunnen opgeslagen worden in de directory. Het is een set regels waarmee de klassen van objecten en kenmerken in de directory, de beperkingen en limieten op exemplaren van deze objecten en de notatie van de namen van de objecten gedefinieerd worden. Deze definities zelf worden als objecten opgeslagen in de schema container, ze kunnen zo op eenzelfde manier beheerd worden als alle AD objecten. Er zijn twee types definities:

Kenmerken worden apart van klassen gedefinieerd.

Klassen beschrijven de directory objecten die gemaakt kunnen worden. Elke klasse heeft een verzameling kenmerken.

2.1.1 Doel en werking

Een attributeSchema object is een object waarmee een kenmerk wordt ingesteld en waarmee beperkingen opgelegd worden aan objecten die een exemplaar zijn van de klasse met dit kenmerk. Elk kenmerk moet zo maar eenmaal gedefinieerd worden, maar kan toch in meerdere klassen gebruikt worden.

2.1.2 Raadplegen en wijzigen

Voor ontwikkelings- en testdoeleinden kun je het AD schema bekijken en wijzigen met adsiedit.msc, of met een specifiek hiervoor ontwikkelde snap-in, Active Directory Schema. Er is geen standaard MMC console die deze snap-in bevat. Het wordt geimplementeerd door schmmgmt.dll, welke na installatie nog moet geregistreerd worden met regsvr32. De Schema

snap-in laat toe, op een meer eenvoudige wijze dan adsiedit.msc, om zowel kenmerken als klassen te bekijken, te wijzigen en te creëeren. AD ondersteunt geen verwijdering van schemaobjecten. Deactiveren is wel mogelijk, toch voor eigen ontwikkelde schemaobjecten, niet voor de standaard meegeleverde objecten.

2.2 Bespreek de diverse naamgevingen van attributeSchema objecten

Alle attributeSchema objecten in het schema hebben een viervoudige naamgeving, die alle vier uniek en gestandaardiseerd zijn:

common name (cn) is de RDN van het attributeSchema object in de Schema container. Opgeslagen in een kenmerk van het attributeSchema object met als LDAP display naam **cn**.

GUID van het kenmerk is onafhankelijk van de GUID van het attributeSchema object en kan automatisch gegenereerd worden bij creatie van een nieuw kenmerk. Hetzelfde kenmerk zal dan wel een ander GUID hebben in verschillende forests. Om dit te vermijden kan best op voorhand een GUID gegenereerd worden. Opgeslagen in een kenmerk van het attributeSchema object met als LDAP display naam **schemaIDGUID**.

LDAP display name is belangrijk voor programmatische toegang. Deze kan dikwijls, maar niet altijd, uit de common name afgeleid worden door alle streepjes te verwijderen, en de eerste letter niet in hoofdletters te vermelden. Opgeslagen in een kenmerk van het attributeSchema object met als LDAP display naam **lDAPDisplayName**.

Object identifier (OID) die geldt als interne representatie. X.500 IDs worden verleend door speciale autoriteiten, en zijn gegarandeerd uniek in alle netwerken wereldwijd. Het is een decimale reeks met punten, en worden hiërarchisch toegekend. Je kan een OID tak aanvragen bij de regionale ISO vertegenwoordiger of je kan een uniek OID laten genereren in een microsoft subtak met oidgen. Opgeslagen in een kenmerk van het attributeSchema object met als LDAP display naam **attributeID**.

2.3 Bespreek de belangrijste kenmerken van attributeSchema objecten, en hoe die ingesteld kunnen worden.

attributeSyntax en oMSyntax De syntax van het kenmerk bepaalt het data type, en zo het soort gegevens dat het kenmerk kan bevatten. Er zijn 26 mogelijkheden waarvan er maar 18 momenteel gebruikt worden in AD. Het is niet mogelijk om een nieuwe syntax te definiëren. Omdat men in AD bepaalde noodzakelijke data types niet van elkaar kan

onderscheiden op basis van louter de X.500 syntax is er een aanvullende integer waarde voorzien: OMSyntax.

rangeLower en rangeUpper Bepalen lengte- of bereikbeperkingen van kenmerken.

isSingleValued Kenmerken kunnen, afhankelijk van dit kenmerk, één waarde of meerdere niet-geordende waarden hebben. bv objectClass bevat de specifieke klasse van het object en de opeenvolgende klassen waarvan de klasse is afgeleid.

searchFlags Dit bevat binaire informatie, waarbij de meeste bits bepalen of het kenmerk op een of andere manier geïndexeerd wordt. Als je een kenmerk indexeert, kun je in Active Directory sneller objecten zoeken die dat kenmerk hebben. Alle exemplaren van het kenmerk worden dan toegevoegd aan de index, niet alleen de exemplaren die lid zijn van een bepaalde klasse.

- De laagste bit wordt meestal gezet en bepaalt eenvoudige indexering van de waarde van het kenmerk.
- De tweede laagste bit zorgt voor een containerized index en zorgt dat objecten snel kunnen gevonden worden binnen een specifieke container. De waarde van het kenmerk wordt hiervoor gecombineerd met de identificatie van de container.
- Het zetten van de derde laagste bit laat ambiguous name resolution (ANR) toe. Bij opzoekingen waar men op zoek gaat naar objecten waarbij minstens één kenmerk uit een verzameling kenmerken een specifieke waarde aanneemt. Bv voor displayName, givenName & name staat de ANR bit op 1.
- Instellen van de zesde laagste bit versnelt opzoekingen waarin kenmerken met jokertekens vermeld worden.

De vijfde laagste bit heeft niks met indexering te maken en bepaalt of de waarde van attribuut behouden blijft bij het kopieren van het object.

systemFlags is een binair informatieveld. De laagste bit bepaalt of het kenmerk gerepliceerd wordt naar andere domeincontrollers. Niet-gerepliceerde kenmerken worden dikwijls gebruikt om lokale caches te implementeren. Wordt ook gebruikt voor relatief dynamische kenmerken waarvan de waarde frequent wijzigt, zoals lastLogon en LastLogoff. LastLogonTimestamp wordt wel gerepliceerd. De derde laagste bit wijst op een geconstrueerd attribuut. Een geconstrueerd attribuut wordt niet opgeslagen in AD, maar wordt telkens opnieuw berekend. Bv canonicalName en parentGUID.

isMemberOfPartialAttributeSet bepaalt of het kenmerk in de global catalog opgenomen wordt of niet.

linkID Sommige kenmerken vormen koppels bestaande uit forward-link en back-link kenmerken. Indien de waarde van het forward-link kenmerk van een object verwijst naar de DN van een ander object, dan wordt het back-link kenmerk van dat object automatisch in- of aangevuld met de DN van het eerste object, en vice versa. Gebruikers met voldoende machtigingen kunnen enkel de waarde van forward-link kenmerken rechtstreeks wijzigen. Back-link kenmerken vallen volledig onder het beheer van de security accounts manager component van windows server. De forward-link kenmerken hebben een even waarde, de backward-link kenmerken hebben een oneven waarde, 1 hoger dan de forward-link waarde.

2.4 Welke andere types objecten bevat het Active Directory schema, en wat is hun bedoeling?

classSchema objecten Net zoals voor kenmerken bevindt zich voor alle klassen een classSchema object in het schema. De kenmerken van classSchema objecten definieren de klasse, en bevatten twee soorten regels: structuurregels definieren de hiërarchische relaties tussen hetzij klassen, hetzij tussen objecten, inhoudsregels kenmerken definiëren die beschikbaar zijn voor een exemplaar van die klasse.

Abstracte schema Naast classSchema en attributeSchema objecten bevat het schema nog één ander object: een subSchema object, het abstracte schema genoemd. Het heeft als RDN Aggregate en bevat een alternatieve, compacte voorstelling van het gehele schema. De bedoeling is om vereenvoudigde schema gegevens ter beschikking te stellen aan LDAP cliënts, zonder zich over veel implementatie details hoeven te bekommeren. Gecombineerd met de Active Directory Service Interfaces (ADSI) biedt het abstracte schema een toegang naar het schema, die veel meer high-level is dan via het reële schema.

2.5 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.

ObjectClass is multi-valued en niet geïndexeerd. het bevat niet alleen de klasse van het object zelf, maar ook alle hiërarchische superklassen (uitgezonderd de statische hulpklassen).

objectCategory is single-valued en is geïndexeerd. Het wordt echter niet noodzakelijk ingevuld met de klasse van het object, het bevat de meest typische vertegenwoordiger uit de verzameling bestaande uit de klasse zelf en alle hiërarchische superklassen.

2.5.1 voorbeelden

Voor het opzoeken van printers is de selectie van objecten, waarvoor de objectCategory ingesteld is op printQueue, duidelijk de beste keuze, aangezien dit de opzoeking toelaat om op indexering een beroep te doen.
Indien men analoog gebruikers zou willen opzoeken via objecten, waarvoor de objectCategory ingesteld is op person, dan is dit weliswaar een performante oplossing, maar zal dit niet alleen objecten van de klasse user opleveren, maar ook objecten van de klasse contact. Om deze uit te sluiten, zou men kunnen overwegen om objecten te selecteren, waarvoor user tot de objectClass behoort. Dit heeft echter het nadeel dat de zoekopdracht nu niet alleen objecten van de klasse user zal opleveren, maar ook objecten van de ervan afgeleide klasse computer. De enige juiste mogelijkheid in dit geval is om op zoek te gaan naar objecten waarvoor zowel de objectCatergory ingesteld is op person, als user tot de objectClass behoort.

Hoofdstuk 3

classSchema objecten

3.1 Bespreek het doel en de werking van classSchema objecten

Klassen zijn zelf ook objecten in het schema: voor elke klasse in het schema is er een classSchema object waarmee de klasse ingesteld wordt. Ze beschrijven de directory objecten die gemaakt kunnen worden. De kenmerken van classSchema objecten definiëren de klasse, en bevatten twee soorten regels: met structuurregels definieer je de mogelijke hiërarchische relaties tussen hetzij klassen, hetzij tussen objecten, terwijl inhoudsregels kenmerken definiëren die beschikbaar zijn voor een exemplaar van die klasse. Door middel van overname kunnen van bestaande klassen nieuwe klassen aangemaakt worden.

3.2 Hoe benadert Active Directory het mechanisme van overerving?

Door overerving kan je van bestaande klassen nieuwe klassen maken. De onmiddelijke superklasse van een klasse wordt bepaald door het kenmerk subClassOf van het classSchema object. Speciale superklasse Top waar alle klassen (onrechtstreeks) van worden afgeleid. Een subklasse neemt de kenmerken van de superklasse over, inclusief de structuurregels en de inhoudsregels. Overname werkt recursief. Een klasse kan enkel kenmerken overnemen van zijn onmiddelijke superklasse en van speciaal hiervoor bestemde hulpklassen. Hulpklassen zijn klassen die zelf geen objecten kunnen genereren. De kenmerken auxiliaryClass en systemAuxiliaryClass van elk classSchema object bevatten alle mogelijke klassen waarvan deze klasse kenmerken kan overnemen. Kenmerken met een LDAP display naam die beginnen met system zijn in tegenstelling tot de corresponderende kenmerken niet wijzigbaar door beheerders van het schema. Het gebruik van hulpklassen kan zowel statisch (met auxiliaryClass kenmerk) als dynamisch (hulpklasse opgeven bij creatie) gebeuren.

3.3 Bespreek de diverse naamgevingen van classSchema objecten

Alle classSchema objecten in het schema hebben een viervoudige naamgeving, die alle vier uniek en gestandaardiseerd zijn:

common name is de RDN van het classSchema object in de schema container. Opgeslagen in een kenmerk van het classSchema object met als LDAP display naam **cn**.

GUID van de klasse is onafhankelijk van de GUID van het classSchema object en kan automatisch gegenereerd worden bij creatie van een nieuwe klasse. Opgeslagen in een kenmerk van het classSchema object met als LDAP display naam **schemaIDGUID**.

LDAP display name is belangrijk voor programmatische toegang. Deze kan dikwijls, maar niet altijd, uit de common name afgeleid worden door alle streepjes te verwijderen, en de eerste letter niet in hoofdletter te vermelden. Opgeslagen in een kenmerd van het classSchema object met als LDAP display naam **lDAPDisplayName**.

Object ID die geldt als interne representatie. X.500 IDs worden verleend door speciale autoriteiten, en zijn gegarandeerd uniek in alle netwerken wereldwijd. Het is een decimale reeks met punten, en worden hiërarchisch toegekend. Je kan een OID tak aanvragen bij de regionale ISO vertegenwoordiger of je kan een uniek OID laten genereren in een microsoft subtak met oidgen. Opgeslagen in een kenmerk van het classSchema object met als LDAP display naam **governsID**.

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

De kenmerken van classSchema objecten definiëren de klasse, en bevatten twee soorten regels: met structuurregels definieer je de mogelijke hiërarchische relaties tussen hetzij klassen, hetzij tussen objecten, terwijl inhoudsregels kenmerken definiëren die beschikbaar zijn voor een exemplaar van die klasse.

3.4.1 Inhoudsregels

mustContain en systemMustContain kenmerken bevatten de lijst met kenmerken die verplicht zijn in elk exemplaar van de klasse. Een kenmerk is verplicht van zodra het verplicht is in één van de hiërarchische superklassen van de klasse, ook al is het voor de klasse zelf als optioneel gemarkeerd.

mayContain en systemMayContain kenmerken bevatten de lijst met kenmerken die optioneel zijn.

rDNAttID kenmerk bepaalt welk kenmerk van een klasse gebruikt wordt om de RDN van objecten te bepalen. Meestal staat dit kenmerk ingesteld op de waarde cn (common name).

defaultSecurityDescriptor kenmerk bepaalt de expliciete machtigingen die gelden voor objecten van deze klasse. Dit kan een eenvoudige oplossing bieden om het beheer van specifieke objecten te delegeren.

SystemOnly als dit de waarde True heeft, kunnen de structuurregels en de inhoudsregels van de klasse niet gewijzigd worden.

isDefunct hiermee kunnen schema objecten gedeactiveerd worden. Zo kunnen er geen nieuwe exemplaren van de klasse aangemaakt worden. AD ondersteunt geen verwijdering van schemaobjecten.

3.4.2 Structuurregels

objectClassCategory kenmerk heeft een integer waarde die de categorie van de klasse bepaalt: structurele klasse (1), abstracte klasse (0 of 2) of hulpklasse (3). Abstracte klassen zijn gelijkaardig aan structurele klassen, maar kunnen zelf geen objecten genereren.

defaultObjectCategory geeft de standaard objectCategory aan voor de klasse.

subClassOf kenmerk bepaald de onmiddelijke superklasse van een klasse.

auciliaryClass en systemAuxiliaryClass kenmerken bevatten alle mogelijke hulpklassen waarvan deze klasse kenmerken kunnen overnemen.

possSuperiors en systemPossSuperiors kenmerken van elk classSchema object definieren de mogelijke hiërarchische relaties tussen objecten van een klasse. Het feit of een klasse containerobjecten representeert, wordt niet bepaald door een kenmerk van de klasse zelf: een structurele klasse kan containerobjecten genereren van zodra een andere structurele klasse ernaar verwijst in zijn systemPossSuperiors of PossSuperiors kenmerken. De definitie van een klasse bepaalt voor zijn objecten bijgevolg niet van welke klasse het objecten kan bevatten als containerobject, maar wel van welke klasse de objecten als container kunnen optreden.

3.5 Welke andere types objecten bevat het Active Directory schema, en wat is hun bedoeling?

attributeSchema objecten zijn objecten waarmee een kenmerk wordt ingesteld en waarmee beperkingen opgelegd worden aan objecten die een exemplaar zijn van de klasse

met dit kenmerk. Elk kenmerk moet zo maar eenmaal gedefinieerd worden, maar kan toch in meerdere klassen gebruikt worden.

Abstracte schema Naast classSchema en attributeSchema objecten bevat het schema nog één ander object: een subSchema object, het abstracte schema genoemd. Het heeft als RDN Aggregate en bevat een alternatieve, compacte voorstelling van het gehele schema. De bedoeling is om vereenvoudigde schema gegevens ter beschikking te stellen aan LDAP cliënts, zonder zich over veel implementatie details hoeven te bekommeren. Gecombineerd met de Active Directory Service Interfaces (ADSI) biedt het abstracte schema een toegang naar het schema, die veel meer high-level is dan via het reële schema.

3.6 Hoe en met welke middelen kan het Active Directory schema uitgebreid worden?

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 veilge manier om attributen aan een klasse toe te voegen: maak 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 geassocieerd met de klasse waaraan we de attributen wouden toevoegen.
Grootschalige uitbereidingen gebeuren best met ldifde of programmatisch met ADSI interfaces. Met ldifde kunnen bestanden die geformatteerd zijn in LDAP Data Interchange Format 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.

Hoofdstuk 4

Active Directory functionele niveaus

4.1 Geef de diverse functionele niveaus waarop Active Directory kan ingesteld worden, en welke beperkingen er het gevolg van zijn.

Elk domein is gekenmerkt door een bepaald domein functioneel niveau. Dit domein functioneel niveau geeft aan welke minimum eis er gesteld wordt aan het besturingssysteem van de domeincontrollers, en bepaalt tegelijkertijd welke faciliteiten er beschikbaar zijn. Het wordt opgeslagen in twee kenmerken van het domeinobject: ntMixedDomain en msDS-Behavior-Version.

Windows 2000 mixed domein functioneel niveau kan zowel NT4, Windows 2000 Server als Windows server 2003 domeincontrollers bevatten, maar biedt de laagste AD functionaliteit. Het kan geen Windows Server 2008+ domeincontrollers bevatten. NT5 domeinen worden standaard op dit niveau gezet, omdat ze ervan uitgaan dat er nog NT4 domeincontrollers aanwezig kunnen zijn.

Windows 2000 native domein functioneel niveau biedt de keuze tussen willekeurige NT 5+ domeincontrollers. Stelt geen eisen aan lidservers en werkposten.

Windows Server 2003 domein functioneel niveau er zijn enkel Windows Server 2003+ domeincontrollers mogelijk. Stelt geen eisen aan lidservers en werkposten.

Windows Server 2008 domein functioneel niveau er zijn enkel Windows Server 2008+ domeincontrollers mogelijk. Stelt geen eisen aan lidservers en werkposten.

Analoog aan het domain functioneel niveau, is er ook een forest functioneel niveau. Dit wordt opgeslagen in het msDS-Behavior-Version kenmerk van het partitions containerobject van de

configuratie gegevens.

Windows 2000 forest functioneel niveau stelt geen enkele eis aan het functioneel niveau van de liddomeinen en is de standaard instelling.

Windows 2003 forest functioneel niveau kan enkel domeinen bevatten die minimaal op Windows Server 2003 domein functioneel niveau staan.

Windows 2008 forest functioneel niveau kan enkel domeinen bevatten met Windows Server 2008 domein functioneel niveau.

4.2 Bespreek van elk niveau alle eraan gekoppelde voordelen. Geef hierbij telkens een korte bespreking van de ingevoerde begrippen.

4.2.1 Domein functioneel niveau

Windows 2000 mixed domein biedt het minst AD functionaliteit. We bespreken voor de opeenvolgende domein functioneel niveaus steeds welke functionaliteit er is bijgekomen tegen over het vorige niveau.

Windows 2000 native

De voordelen van dit niveau tov Windows 2000 mixed functioneel niveau:

- Eén enkele global catalog voor het ganse forest volstaat. De Global Catalog bevat een read-only en verkorte inhoudopgave van elk domein in het forest.
- Transitieve vertrouwensrelaties tussen verschillende domeinen van eenzelfde forest. Tussen twee domeinen kan een vertrouwensrelatie tot stand gebracht worden, zodat gebruikers in het ene, trusted (vertrouwd), domein kunnen geverifieerd worden door een domeincontroller in het andere, trusting (vertrouwend), domein.
- Alle domeincontrollers kunnen zelfstandig een aantal SPN objecten aanmaken. Aan SPN objecten moet een uniek SID toegekend worden. De RID master wijst hiervoor aan elke domeincontroller reeksen relatieve IDs toe. Hievoor (Windows 2000 mixed) moest men steeds een beroep doen op de PDC emulator master.
- Ruimere mogelijkheden om gebruikers en/of computers te verzamelen in groepen, met bovendien minder beperkingen op de conversie, de zichtbaarheid en het nesten van deze groepen. Een veiligheidsgroep kan bv omgevormd worden in een distributiegroep en vice versa. Veiligheidsgroepen zijn groepen waaraan je rechten en machtigingen kan toekennen. Distributiegroepen hebben geen enkele beveiligingsfunctie. Ook universele groepen (kunnen leden hebben uit elk domein van het forest) zijn nu mogelijk.

- Alle SIDs die een SPN object in het verleden gehad heeft, worden bijgehouden in het sIDHistory kenmerk.

Niveau 2: Windows Server 2003

De voordelen van dit niveau tov Windows Server 2000 Native functioneel niveau:

- Aanvullende schema klassen en attributen. Zoals bv lastLogonTimestamp, een over de domeincontrollers gesynchroniseerde versie van het tijdstip van laatste logon van UPN objecten. Schema klassen en attributen zijn een formele beschrijving van de objecten in AD en hun kenmerken.
- Laat toe om een domeincontroller van naam te veranderen zonder degradatie en promotie.
- Aanvullende opdrachten. Zoals bv redirusr en redircmp om de default AD container te wijzigen waarin respecievelijk nieuwe gebruikers en nieuwe computers terecht komen.
- Caching op domeincontroller niveau van UPN suffices en het lidmaatschap van universele groepen, zodat het niet meer strikt noodzakelijk is dat tijdens het inlogproces een global catalog bereikbaar is.
- Group policies filteren, op basis van beveiligingsgroepen, maar ook met behulp van WMI scripts. Filteren is verhinderen dat het GPO op specifieke groepen van gebruikers en computers toegepast wordt.

Niveau 3: Windows Server 2008

De voordelen van dit niveau tov Windows Server 2003 functioneel niveau:

- Aanvullende schema klassen en objecten. Waardoor ondermeer de werkpost, waarop een gebruik het laatst zich met succes aagemeld heeft, en het aantal mislukte pogingen sindsdien, opgevraagd kan worden.
- Encryptie van het Kerberos protocol met langere sleutels.
- Fijnkorrelig wachtwoordbeleid (fine-grained password policies), zodat wachtwoordenrestricties niet langer globaal zijn voor het gehele domein, maar specifiek ingesteld kunnen worden voor individuele gebruikers of gebruikersgroepen.
- Replicatie van DFS namespaces en van de SYSVOL share met behulp van DFS Replication, wat meer performanter is dan via de traditionele File Replication Service. Distributed File System (DFS) biedt een mechanisme voor het omleiden van shares, door ze te bundelen in één naamruimte. Als dezelfde share beschikbaar gesteld wordt

op verschillende servers, moet er replicatie hiertussen voorzien worden. DFS-R is ontworpen met de minimalisering van de netwerkbeslasting als voornaamste doel en is dus efficienter op vlak van netwerkverkeer. De SYSVOL share bevat de logon scripts (configuratie bij inloggen) en wordt mbv DFS-R gerepliceerd naar alle domeincontrollers.

4.2.2 Forest functioneel niveau

Windows 2000 forest functioneel niveau biedt het minst AD functionaliteit en is de standaard instelling voor nieuwe installaties. We bespreken voor de opeenvolgende forest functionele niveaus steeds welke functionaliteit er is bijgekomen tegen over het vorige niveau.

Niveau 2: Windows 2003

De voordelen van tov Windows 2000 forest functioneel niveau:

- Het hergebruiken van gedeactiveerde attributen en klassen.
- Dynamische hulpklassen. Bij creatie van een object kan er gekozen worden welke hulpklasse deze gebruikt.
- Dynamische objecten, met een beperkte levensduur, die na het verstrijken van de entryTTL waarde automatisch uit AD verwijderd worden, tenzij ze opgefrist worden.
- Efficiënte replicatie van de global catalog gegevens, waardoor ondermeer toevoeging van een nieuw kenmerk niet langer leidt tot een volledige synchronisatie van alle objectkenmerken.
- Veranderen van de naamgeving en de hiërarchische structuur van domeinen in een forest.
- Transitieve vertrouwensrelaties tussen verschillende forests.
- Read-only Windows Server 2008+ domeincontrollers. Ideaal voor locaties waar de domeincontroller fysiche niet beveiligd kan worden. Er kunnen geen aanpassingen van de AD gegevens gebeuren op deze domeincontroller.
- Efficiëntere KCC algoritmen voor het construeren van de replicatietopologie.
- Replicatie van de individuele waarden van multi-valued attributen.

Niveau 3: Windows 2008

Dit niveau biedt geen aanvullende functionaliteit tov Windows Server 2003 forest functioneel niveau. Toch is het om beveiligingsredenen van belang om op dit niveau over te schakelen, bijvoorbeeld indien met Read Only Domain Controllers (RODCs) met RODC filtered attribtue set introduceert. Dit laatste is een verzameling van kenmerken die niet naar een RODC gerepliceerd worden.

4.3 Hoe kan men detecteren op welk niveau een Active Directory omgeving zicht bevindt?

Het domein functioneel niveau wordt opgeslagen in twee kenmerken van het domeinobject: **ntMixedDomain** en **msDS-Behavior-Version**. Het ntMixedDomain kenmerk zal enkel bij Windows 2000 mixed domeinen op 1 staan, bij alle andere niveau's op 0. Het msDS-Behavior-Version kenmerk voor Windows 2000 mixed en Windows 2000 native op 0, voor Windows Server 2003 op 2 en voor Windows Server 2008 op 3. Dit kan bv met dsquery opgevraagd worden.
Het forest functioneel niveau wordt opgeslagen in een kenmerk van het partitions container-object van de configuratiegegevens: **msDS-Behavior-Version**. Voor Windows 2000 forest functioneel niveau staat dit op 0, voor Windows Server 2003 forest functioneel niveau op 2 en voor Windows Server 2008 forest functioneel niveau op 3.

4.4 Op welk diverse manieren kan men het functionele niveau verhogen of verlagen?

De omschakeling naar een bepaald domein of forest functioneel niveau moet manueel gebeuren, gebeurt niet automatisch van zodra de controllers of domeinen aan een minimum voorwaarde voldoen.

- Door zelf manueel de attributen te manipuleren
- Via de Active Directory Domains and Trust snap-in

Men kan enkel het functioneel niveau verhogen, niet verlagen. De wijzigingen worden pas effectief doorgevoerd na een heropstart van alle domeincontrollers. Achteraf geïnstalleerde domeincontrollers zullen automatisch functioneren op het huidige niveau.

Hoofdstuk 5

Active Directory domeinstructuren

5.1 Wat is de bedoeling van vertrouwensrelaties?

Tussen 2 domeinen kan een vertrouwensrelatie tot stand gebracht worden, zodat de gebruikers in het ene, trusted domein kunnen geverifieerd worden door de domeincontroller in het andere, trusting domein. Vertrouwensrelaties worden weergegeven met een pijl in de richting van het trusted domein. Een gebruiker kan pas toegang krijgen tot bronnen in een ander domein als er een vertrouwenspad is van het trusting domein naar het trusting domein. Een vertrouwenspad is een continue rij vertrouwensrelaties tussen domeinen. Dat een gebruiker door een trusting domeincontroller is geverifieerd, wil nog niet automatisch zeggen dat de gebruiker toegang heeft tot de bronnen in dat domein. Deze toegang wordt geregeld met gebruikersrechten en machtigingen die aan de gebruiker toegekend zijn door de domeinbeheerder van het trusting domein.

5.2 Bespreek de verschillende soorten vertrouwensrelaties.

5.2.1 Automatische vertrouwensrelaties

Windows Server maakt automatisch vertrouwensrelaties aan tussen domeinen en hun child domeinen. Deze vertrouwensrelaties kunnen niet verbroken worden en zijn automatisch bi-directioneel en transitief. Windows Server maakt ook automatisch vertrouwensrelaties aan tussen de trees van eenzelfde forest: de root domeinen van alle trees in het forest vormen transitieve vertrouwensrelaties met het forest root domein van het forest. Aangezien Windows Server vertrouwensrelaties bi-directioneel en transitief zijn, heeft een domein dat nieuw aangemaakt wordt in een tree of forest, automatisch vertrouwensrelaties met alle andere Windows Server domeinen in de tree of het forest. Om in NT 4 hetzelfde te bekomen, moet je als systeembeheerder zelf vertrouwensrelaties construeren, en dan nog in twee richtingen, dit met elk bestaand domein.

5.2.2 Expliciete vertrouwensrelaties

Transitieve vertrouwensrelaties kunnen alleen bestaan tussen Windows Server domeinen in hetzelfde forest, tenzij de diverse forests minimaal op Windows Server 2003 functioneel niveau staan. In dat geval kun je manueel tussen de root domeinen van de forests bi-directionele en transitieve forest trusts configureren, waardoor je een federatie of realm van forests krijgt. Elk koppel domeinen in een dergelijke realm vertrouwt elkaar wederzijds. Bij meerdere forests moet men forest trusts configureren tussen elk koppel forests. Realm trusts, zijn een veralgemening van forest trusts, die vertrouwenspaden leggen tussen Windows Server 2008 domeinen en willekeurige Kerberos v5 realms. Een realm trust kan zowel bi-directioneel als enkelvoudig, en zowel transitief als niet-transitief gedefinieerd worden. Forest en realm vertrouwensrelaties zijn expliciete vertrouwensrelaties: trusts die je zelf maakt, in tegenstelling tot de vertrouwensrelaties die automatisch gemaakt worden tijdens de creatie van het domein. Een verkorte vertrouwensrelatie is ook een expliciete vertrouwenrelatie en maakt het mogelijk om een vertrouwenspad tussen 2 domeinen, in grote en complexe trees, te verkorten. Dit moet het aanmeldingsproces versnellen.
Het laatste type expliciete vertrouwensrelatie is de externe vertrouwensrelatie. Dit is een enkelvoudige vertrouwingsrelatie waarbij één domein een ander domein vertrouwt. Deze zijn niet-transitief. Je kan geen externe relatie instellen tussen AD domeinen in hetzelfde forest (heeft al automatische relaties). Dit kan wel ingesteld worden tussen:

- individuele domeinen in een ander forest.
- met NT 4 domeinen

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

Enkel de expliciete vertrouwensrelaties moeten manueel geconfigureerd worden. Dit kan op twee verschillende manieren geconfigureerd worden. Als je een expliciete vertrouwenrelatie wil maken, moet je beschikken over de domeinnamen en een gebruikersaccount met machtiging om vertrouwensrelaties in beide domeinen te maken. Elke vertrouwensrelatie krijgt een wachtwoord toegewezen, dat bekend moet zijn bij de beheerders van beide domeinen van de vertrouwensrelatie. Na het opzetten van de vertrouwensrelatie wordt dit wachtwoord niet meer gebruikt.

5.3.1 Active Directory Domains en Trust snap-in

Deze snap-in is beschikbaar in domain.msc. Het aanmaken van de vertrouwensrelatie kan door met de rechmuisknop op een domein te klikken en achtereenvolgens Properties en de

Trusts tabpagina te selecteren, en daarna de New Trust wizard op te starten.

5.3.2 Via de command-line

In de command prompt kan je een vertrouwensrelatie configureren met de netdom trust opdracht. Met netdom query trust krijg je een overzicht van alle vertrouwensrelaties en hun toestand.

5.3.3 Optionele configuratiemogelijkheden

- Standaard worden alle gebruikers van het trusted domein opgenomen in de Authenticated Users impliciete groep van het trusting domein. Men kan echter ook voor selective authentication kiezen, waardoor dit per individuele gebruiker of gebruikersgroep expliciet moet ingesteld worden.
- Indien men gebruik maakt van SID Filtering, dan wordt enkel rekening gehouden met de SID opgeslagen in het objectSid attribuut van de objecten in het trusted domein. Indien men SID Filtering uitschakelt, dan verwerkt het trusting domein ook de SIDs opgeslagen in het sIDHistory attribuut. Malfide beheerders in het trusted domein kunnen langs deze weg zichzelf meer machtigingen en rechten toeeigenen in het trusting domein.

5.4 Welke verschillen zijn er in praktijk tussen NT 4.0 en Windows Server domeinstructuren? Bespreek de alternatieve mogelijkheden bij de conversie van een NT 4.0 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 (OUs) van AD 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 OUs in het Windows Server Domein. We bekomen zo een getrouwe weerspiegeling van de oude structuur. Eventueel kunnen aan-

vullende structuren worden toegevoegd om een meer gedetaileerde 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 veroorzaken immers instabiliteit van de SAM databank. Dit probleem is meteen opgelost door AD, omdat het veel schaalbaarder is. Een andere mogelijk 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 replicatie verkeer kan nog verder worden beperkt door gebruik te maken van RODC's. Een derde mogelijkheid is de noodzaak aan een verschillend wachwoordbeleid 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 aparte domeinen te behouden in de verschillende sites. De migratie gebeurt op één 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, gemeeschppelijke configuratiegegevens en een gemeenschappelijke global catalog delen.

2. Als alternatief kan elk NT4 domein worden geupgraded naar een subdomein van een artificieel 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 uistekende 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 domeinen eerst samgevoegd, en vervolgens geupgraded naar Windows Server. De oorspronkelijke domeinen worden dan omgezet in OUs. Er zijn hiervoor geen hulpmiddelen. De migratie gebeurt volledig manueel met behulp van commando lijn opdrachten. Als alternatief worden de afzonderlijkde 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 OUs in de masterdomeinen.

Hoofdstuk 6

Active Directory server rollen

Welke vragen moet men zich stellen na de initiële installatie van een Windows Server toestel, in veband 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 aantal, 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 juist wel door dezelfde server moeten vervuld worden.
- Op welke diverse manieren men de toewijzing van elke bijzondere functie kan instellen, wijzigen en/of ongedaan maken?

6.1 Wordt server al dan niet opgenomen in een domein?

Als een Windows Server toestel lid is van een werkgroep, niet van een domein, dan wordt het een zelfstandige server genoemd. Deze profiteren niet van de voordelen die AD biedt. Vooral indien er reeds een AD domeinstructuur aanwezig is, is de keuze snel gemaakt.

6.2 Vervult de in een domein opgenomen server al dan niet de functie van domeincontroller?

Een in een domein opgenomen server die de functie van domeincontroller niet vervult, wordt een lidserver (member server) genoemd. Meestal fungeren lidservers als file servers, toepas-

singsservers, database servers, web servers, firewalls, routers of een combinatie hiervan. In Windows Server 2008+ worden dergelijke functies gegroepeerd op drie niveau's:

Server rollen (DNS, DHCP, ...) en Web Server implementeren primaire serverfuncties.

Role services optionele, meer complexe, server rollen.

Features (Powershell, SNMP, backup, ...) zorgen voor meer ondersteunende functies.

Men kan aanvullende server rollen, rol services en features configureren via respectievelijk de Add Roles, Add Role Services en Add Features wizards van Server Manager. Dit kan ook met de ServerManagerCmd opdracht.
Zowel voor lidservers als voor domeincontrollers gelden groepsbeleidinstellingen die gedefinieerd zijn voor het domein, de OUs of de site. Lidservers behouden, in tegestelling tot domeincontrollers, een eigen lokale beveiligingsdatabank, de Security Account Manager (SAM). Doorgaans configureert men slechts een fractie van de Windows Server toestellen als domeincontroller. Minimaal 1 per domein.

6.3 Indien gekozen wordt voor domeincontroller, moet ook de functie van globale catalogus ondersteund worden?

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 NSDS settings van een domeincontroller. Dit is terug te vinden in de AD 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.

6.4 Welke domain controllers worden als RODC ingesteld?

Domeincontrollers configureren als Read Only Domain Controller 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 één 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.

6.5 Welke domeincontrollers vervullen de operations master rollen?

Een aantal specifieke AD functies kunnen slechts door één enkele controller in het domein of in het forest vervuld worden.

6.5.1 Rollen uniek in elk domein

RID master In domeinen met minimaal Windows 2000 native functioneel niveau wijst de RID master reeksen relatieve IDs toe aan alle domeincontrollers in het domein. Hiermee kunnen de domeincontrollers zelfstandig SPN objecten met een SID aanmaaken. Wanneer een domeincontroller 80% van zijn RID pool heeft opgebruikt, vraagt hij een nieuwe reeks aan bij de RID master. Een object tussen domeinen verplaatsen moet gebeuren vanop de RID master van het domein dat het object bevat.

PDC emulator master In een Windows 2000 mixed domein met NT4 back-up domeincontrollers fungeert de PDC emulator master als een volledige emulatie van een NT4 primaire domeincontroller. NT4 domeinen kunnen hierdoor services blijven verlenen zonder te weten dat hun PDC in feite door AD vervangen is. De PDC emulator master verwerkt wachtwoordwijzigingen van cliënts en repliceert bijgewerkte gegevens naar de NT4 back-up domeincontrollers. Hij krijgt ook een voorkeursbehandeling bij de replicatie van wachtwoordwijzigingen, uitgevoerd door andere domeincontrollers in het domein. De PDC emulator master fungeert ook als primaire bron van tijdssynchronisatie. Best RID master en PDC emulator master laten vervullen door dezelfde domeincontroller. Het verlies van de PDC emulator heeft gevolgen voor netwerkgebruikers.

infrastructure master is verantwoordelijk voor het bijwerken van verwijzingen vanuit objecten in het eigen domein naar objecten in andere domeinen. De infrastructure master van een domein vergelijkt continu de kenmerken van zijn phantom objecten met de kenmerken van de corresponderende objecten in externe domeinen, en de kenmerken van phantom objecten in externe domeinen die doorverwijzen naar eigen objecten met de kenmerken van deze objecten. Hij doet hiervoor een beroep op de global catalog. Omdat domeincontrollers die global catalog zijn geen phantom objecten aanmaken, doordat ze reeds beschikken over een kopie van de objecten van andere domeinen, moet de rol van

infrastructure master vervuld worden door een domeincontroller die geen global catalog is.

6.5.2 Rollen uniek in het forest

schema master beheert alle gewijzigde gegevens voor het schema. Als je het schema van een forest wil bijwerken, dan moet je dit doen via de schema master. Dit om conflicterende wijzigingen in het schema te vermijden.

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 configuratie gegevens kan wijzigen. Het moet een global catalog controller zijn.

Deel II

Schriftelijk

Hoofdstuk 7

Active Directory replicatie

7.1 Wat is de bedoeling van replicatie?

Gebruikers en services moeten op elk gewenst moment vanaf elke computer in het forest toegang kunnen krijgen tot de directory gegevens. Een domein zonder actieve domeincontroller functioneert niet langer naar gebruikers toe. Doordat in één domein met meerdere domeincontrollers kan gewerkt worden, kan men de fouttolerantie en de belastingsverdeling verbeteren. Bij aanpassingen (CRUD) aan de AD gegevens moeten deze aanpassingen doorgegeven worden aan andere domeincontrollers.
AD omvat een replicatieservice waarmee directory gegevens gedistribueerd worden in het netwerk. Alle domeincontrollers in een domein nemen deel aan de replicatie en bevatten een volledige kopie van alle directory gegevens voor het eigen domein. Analoog beschikken alle domeincontrollers in een forest over het directory schema en de configuratiegegevens, en wordt deze informatie gedistribueerd doorheen het hele forest. De replicatieservice zorgt ervoor dat directory gegevens altijd actueel zijn. Behalve voor wat de operations master functies betreft, zijn alle Windows Server domeincontrollers in een domein dan ook equivalent.

7.2 Hoe wordt dit in Windows Server (ondermeer te opzichte van NT4) gerealiseerd: Bespreek de verschillende technische kenmerken en concepten van Windows Server replicatie, en hoe men specifieke problemen vermijdt en oplost.

In AD wordt multi-master replicatie gebruikt, zodat de directory kan bijgewerkt worden vanaf elke domeincontroller. Dit is een evolutie van het in NT4 gebruikte master-slave model met primaire domeincontrollers en back-up controllers.
Het is belangrijk om ervoor te zorgen dat het replicatie verkeer relatief beperkt blijft. In AD worden daarom alleen gewijzigde directory gegevens gerepliceerd. Om ervoor te zorgen dat een

specifieke wijziging niet meerdere malen naar dezelfde domeincontroller wordt gerepliceerd, wordt er gebruik gemaakt van een 64-bits Update Sequence Number (USN). Samen met het GUID van een domeincontroller wordt dit de Up-to-Dateness Vector (UTD vector) genoemd. Elke domeincontroller houdt in een tabel bij wat de meest recente UTD vector is die hij van elke andere controller ontvangen heeft. Dit uitwisselingsprotocol is op te volgen voor elke individuele partitie met behulp van de repadmin opdracht.
De metadata van elk object houdt van elk kenmerk ondermeer een Property Version Number (PVN) bij, samen met de corresponderende UTD vector (van de domeincontroller die de wijziging uitgevoerd heeft, op het ogenblik van de wijziging). Op basis van de UTD vectortabel kan een controller alle wijzigingen met een bepaalde minimale USN aan een andere controller opvragen. Aan de hand van de metadata kan deze controller precies te weten komen welke wijzigingen hij moet opsturen.
Met het multi-master model is het mogelijk dat hetzelfde kenmerk op meer dan één domeincontroller tegelijkertijd gewijzigd wordt. Dit wordt opgelost door de wijziging op het oudste tijdstip te negeren. Bij exact dezelfde tijd wordt de wijziging van de domeincontroller met het hoogste GUID geaccepteerd. Voor sommige objecten (schema objecten) is dit niet goed genoeg en kunnen verzoeken tot wijzigingen enkel door 1 specifieke domeincontroller verwerkt worden.
Verwijdering van objecten biedt een bijkomend probleem: men moet vermijden dat het object opnieuw gecreëerd wordt door replicatie vanuit een andere domeincontroller. Een object wordt hiervoor niet onmiddelijk uit AD verwijderd, maar als tombstone object gemarkeerd, en in een hidden container (Deleted items) geplaatst. Pas echt verwijderd na tombstoneLifeTime (default 60 of 180) dagen.
Nog een belangrijk verschil met NT4 is de **store-and-forward** replicatie: elke verandering op een specifieke controller wordt slechts uitgewisseld met enkele andere domeincontrollers, die op hun beurt de wijzigingen communiceren met nog enkele andere domeincontrollers. De gebruikte replicatietopologie wordt automatisch gegenereerd door de Knowledge Consistency Checker (KCC) software op elke AD domeincontroller. Via de hierbij aangemaakte verbindingsobjecten zoekt AD zelf de meest optimale manier om het repliceren zo snel mogelijk uit te voeren. Er worden hierbij individuele topologieën gecreëerd voor de domeingegevens enerzijds, en voor de schema en configuratiegegevens anderzijds. Ook voor elke applicatiepartitie is er een aparte replicatietopologie.
Windows Server replicatie is een pull, en geen push mechanisme. De domeincontrollers brengen elkaar wel op de hoogte van de wijzigingen, maar het opvragen gebeurt op initiatief van de replicatiepartner. Wijzigingen worden ook opgespaard in tijdsintervallen van standaard vijf minuten en pas daarna verstuurd. Dit wordt propagation damping genoemd en wordt uitgeschakeld voor objecten die met beveiliging te maken hebben. Automatisch om het uur: polling als er geen meldingen van een domeincontroller zijn gekomen.
Windows Server replicatie is multi-threaded: een domeincontroller kan simultaan repliceren

met diverse partners. Een laatste verschil met NT4 is de kleinste replicatie entiteit: in NT4 was dit een volledig object, in windows 2000 domein functioneel niveau is dit een heel attribuut en vanaf windows server 2003 functioneel niveau is de atomaire waarde van een attribuut (1 veld in multi-valued attribuut).

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

Domeincontrollers in een domein repliceren de domeingegevens van dat domein met elkaar. Naar elke Global Catalog wordt een subset van de domeingegevens van elk domein gerepliceerd. Het schema en configuratiegegevens worden gerepliceerd naar alle domeincontrollers in het forest.

7.4 Welke impact hebben sites met betrekking tot de replicatie van Active Directory gegevens? Je hoeft het begrip site op zich niet verder te behandelen.

Tussen sites is er automatisch en continu replicatie. Het is de bedoeling een evenwicht te vinden tussen enerzijds behoefte aan actuele directory gegevens en anderzijds beperkingen die door beschikbare netwerk bandbreedte opgelegd worden.
Inter-site replicatie vertoont heel wat implementatie verschillen met intra-site replicatie:

- Enkel polling, urgent replication is bijgevolg niet mogelijk.
- Standaard compressie, kan uitgeschakeld worden, reduceert volume tot 40%
- Met behulp van sitekoppelingen aan te geven hoe verschillende sites onderling, met rechtstreekse fysieke netwerkverbindingen, verbonden zijn.
  - KCCs genereren automatisch enkel verbindingsobjecten tussen sites als er tussen beide sites een sitekoppeling bestaat.
  - Fouttolerantie: AD houdt zoveel mogelijk rekening met meerdere routes tussen sites om wijzigingen te repliceren.
  - Alternatieve sitekoppeling maken de replicatie betrouwbaarder, als backup voor een falende sitekoppeling/verbinding.

Hoofdstuk 8

Active Directory sites

8.1 Welke rol vervullen sites? Welke Active Directory aspecten worden erdoor beïnvloed? Bespreek hoe deze aspecten anders gerealiseerd worden indien de toestellen zich al dan niet in verschillende sites bevinden. (ondermeer verschil tussen intrasite en intersite replicatie)

Het repliceren tussen domeincontrollers kan veel bandbreedte opslorpen. In een LAN omgeving is dit niet direct een groot probleem, maar in WAN omgevingen moet er wel de nodige aandacht aan besteed worden. De oplossing hiervoor in Windows Server is het gebruik van sites.
Sites komen overeen met fysieke locaties: een verzameling subnetwerken die onderling aan LAN snelheden met elkaar kunnen communiceren. Zoals domeinen en OUs zorgen voor een logische opsplitsing van het internetwerk, zorgen sites voor een fysieke structurering van het netwerk. Logische en fysieke structuren zijn onafhankelijk van elkaar.
Het gebruik van sites heeft niet enkel voordelen bij replicatie. Voor een vlotte werking van AD is het belangrijk dat er een domeincontroller zo dicht mogelijk bij de gebruikers geplaatst wordt. Sites maken het mogelijk om bij AD raadplegingen eerst op zoek te gaan naar domeincontrollers die zich in dezelfde site bevinden als de client.
Binnen een site worden directory gegevens continu en automatisch gerepliceerd. Tussen sites moet er een evenwicht gevonden worden tussen enerzijds de behoefte aan actuele directory gegevens en anderzijds de bandbreedte beperkingen. Inter-site replicatie vertoont dan ook heel wat implementatie verschillen met intra-site replicatie:

- Het meldingsmechanisme wordt standaard achterwege gelaten, er wordt enkel gebruik gemaakt van polling. Urgent replication is dan ook niet mogelijk. Standaard polling om de 3 uur.

- Gegevensuitwisseling wordt standaard gecomprimeerd. Reduceert volume tot 40%.
- Beheerders kunnen met behulp van sitekoppelingen aangeven hoe de verschillende sites onderling, met rechtstreekse fysieke netwerkverbindingen, verbonden zijn. De KCC's genereren automatisch enkel verbindingsobjecten tussen sites als er tussen beide sites een sitekoppeling bestaan. Een site zonder sitekoppelingen is zinloos, want er worden dan geen verbindingsobjecten aangemaakt.

Om meerdere verbindingsobjecten te vermijden die dezelfde sitekoppeling gebruiken, wordt er automatisch (grootste GUID) per site een Inter-site Topology Generator (ISTG) ingesteld. Enkel de KCC's van de ISTGs gebruiken de informatie in de sitekoppelingen om verbindingsobjecten tussen controllers van verschillende sites te genereren. De domeincontrollers die van dit uniek verbindingsobject gebruik maken, worden bruggenhoofd (bridgehead) servers genoemd. Een bruggenhoofd server is het punt waar directory gegevens tussen sites uitgewisseld worden. Door de invoer van ISTGs en bridgehead servers wordt ervoor gezorgd dat KCCs zich optimaal aanpassen aan de siteconfiguratie.

8.2 Welke relaties bestaan er tussen sites, domeinen, domeincontrollers en global catalogs? Druk deze relaties ondermeer uit in termen zoals ... een X vereist minimaarl/exact/maximaarl Ys.... Geef een verantwoording voor elk van deze beweringen.

Er is geen enkel verband nodig tussen sites en domeinen. Meerdere sites in 1 domein of meerdere domeinen in 1 site zijn mogelijk.
Sites zijn enkel zinvol indien er minstens één domeincontroller in geconfigureerd is. Als alle domeincontrollers in een site tijdelijk onbeschikbaar zouden zijn, wordt dynamisch de dichtstbijzijnde domeincontroller van een andere site toegewezen (site covering). Alle domeincontrollers in een site mogen RODCs zijn, Windows Server 2003 past dan wel automatisch site covering toe, maar kan uitgeschakeld worden in het register van die controller.
Omdat het voor verificatie van gebruikers in een AD domein steeds nodig is om vooraf een global catalog gecontacteerd te hebben, doet men er best aan om in elke site van ten minste één domeincontroller ook een global catalog te maken. Indien het forest slechts uit één domein bestaat, is er geen enkel bezwaar om van alle domeincontrollers een global catalogus te maken. Dankzij caching kan het inlogproces van een gebruiker afgewerkt worden, zonder een global catalogus te contacteren. Hiervoor moet het forest minimaal op Windows Server 2003 forest functioneel niveau staan.

8.3 Hoe wordt bepaald tot welke site computers behoren?

Voor werkposten wordt dit dynamisch bepaalt, telkens de IP software van een werkpost wordt opgestart, bepaalt de werkpost via het netwerkadres in welke site het zich bevindt.
De site locatie van een domeincontroller wordt daarentegen bepaald door de vraag tot welke site in de directory het server object van de domeincontroller behoort. Elke site heeft een container met de naam Servers, die alle domeincontroller objecten bevatten die in deze site zijn geplaatst. Tijdens de promotie van server tot domeincontroller wordt de server automatisch toegevoegd aan de site waaraan het subnet, waartoe de server behoort, is gekoppeld. Er is ook een Default-First-Site container voor als het subnet niet tot een bestaande site behoort.

8.4 Bespreek de diverse noodzakelijke instellingen om de verschillende aspecten van sites te configureren, en vermeld hierbij telkens: waar en in welke gegroepeerde vorm ze opgeslagen worden, waarom ze noodzakelijk zijn (ondermeer welke andere aspecten er afhankelijk van zijn)

De meeste informatie in verband met sites wordt in Active Directory zelf bijgehouden, in de Sites container van de configuratiegegevens. Enkele default instellingen van KCC en van het replicatie mechanisme worden echter, afhankelijk van de Windows Server versie, niet in AD bewaard, maar in het register van elke individuele domeincontroller.
Alle wijzigbare parameters staan gegroepeerd in de Parameters subtak van de NTDS service. Zo houdt de parameter Repl topology update period (secs) de periode bij van het KCC proces, en Replicator notify pause after modify (secs) de latentieperiode voor propagation damping bij intra-site replicatie.
Meer elementaire configuratiebewerkingen met sites kunnen via de MMC snap-in: Active Directory Sites and Services. Deze wordt aangeboden in de standaard console sssite.msc. Wordt gebruikt om sites te creëren en om servers naar een andere site te verplaatsen. Ook kan met behulp van site koppelingen worden aangegeven hoe de verschillende sites onderling verbonden zijn. Welke protocol, het (gebruiks)schema, de bandbreedte en de frequentie kan hier ingesteld worden.

Hoofdstuk 9

Gedeelde mappen en NTFS

9.1 Welke manier om gedeelde mappen te creeren biedt de meeste configuratieinstellingen aan? Bespreek het doel van deze diverse instellingen en de belangrijkste eigenschappen en mogelijkheden ervan.

Om gedeelde mappen aan te kunnen maken, moet je over de juiste machtigingen beschikken. Er zijn in Windows Server 2008+ diverse manieren om shares te maken:

- In Explorer
- Shared folders snap-in
- Server Manager
- Command Prompt

De Server Manager biedt de meeste configuratie instellingen.
Je kan een nieuwe share maken door in Server Manager de Roles\File Services\Share and Storage Management map te selecteren en vervolgens de Provision Share taak uit te voeren. In de opeenvolgende dialogen kunnen volgende zaken geconfigureerd worden:

- Shared Folder Location is het pad tot de map die je wil delen
- NTFS Permissions
- SMB Permissions
- SMB Settings
- Quota Policy
- Filescreen Policy

- DFS Namespace publishing

9.1.1 NTFS Permissions

Na machtigingen op shares zijn NTFS machtigingen de tweede (beveiliging van mappen) en derde (beveiliging van bestanden) verdedigingsmuren voor het beveiligen van gegevens en netwerkbronnen. Er bestaan twee niveaus van NTFS machtigingen:

- Het laagste niveau bestaat uit 13 atomaire of speciale machtigingen, die de bouwstenen vormen voor het hogere niveau. Dit zijn de kleinst mogelijke machtigingen die je kan instellen. Bieden de mogelijkheid om zeer nauwkeuring het toegangsniveau te bepalen.
- Het hoogste niveau, moleculaire of standaard machtigingen, omvat 6 veel gebruikte combinaties van atomaire machtigingen.

9.1.2 SMB Permissions

Share/SMB machtigingen vormen een eerste beveiligingslaag. Hebben overhand op NTFS als ze meer beperkend zijn. Op share niveau kun je drie machtigingen definiëren:

- Full Control
- Read: bekijken en toepassingen uitvoeren
- Change: wijzigen, verwijderen. De eigenlijke share en NTFS machtigingen kunnen niet aangepast worden.

9.1.3 SMB Setting

User limit maximum aantal users die de share gezamelijk kunnen benutten

Acces based Enumeration bestanden en submappen waar je geen enkele NTFS machtiging op hebt niet weergeven.

Client side caching cachen van veel gebruikte netwerkbestanden.

9.1.4 Quota policy

Mogelijkheid om de hoeveelheid beschikbare ruimte voor gebruikers in te stellen.

Volumequota Gebaseerd op bestandseigendom en dus onmogelijk om per gebruikersgroep de som te laten controleren.

Mapquota Vanaf Windows Server 2008 kan men wel mapquota op mappen plaatsen, maar dit geldt voor alle gebruikers. Werkt met soft en hard treshold.

9.1.5 Filescreen Policy

Mogelijkheid tot verhindern van opslaan van bestanden met een bepaalde extensie. Er kunnen reacties getriggerd worden als iemand dit toch probeert.

9.1.6 DFS Namespace publishing

Distributed File System namespace is equivalent en fungeert zoals een share, met het verschil dat een DFS namespace kan bestaan uit DFS mappen (die verwijst naar een share, niet noodzakelijk op dezelfde server of zelf een DFS namespace), bestanden en gewone mappen. Dit geeft de mogelijkheid om transparant aan gebruikers bronnen van meerdere servers op 1 locatie aan te bieden. De DFS topologie wordt automatisch in AD gepubliceerd en is dus altijd zichtbaar voor gebruikers op alle servers in het domein.
DFS folder targets geven de mogelijkheid om identieke shares samen te nemen tot 1 DFS map. Een client zal dan bij het connecteren tot een DFS namespace elke folder target uitproberen tot een werkende gevonden wordt. Dit geeft een hogere fouttolerantie en een spreiding van de belasting. Synchronisatie van deze verschillende shares gaat met FRS of DFS-R.

9.2 Waar wordt de definitie en (partiële) configuratie van gedeelde mappen opgeslagen? Hoe kan men deze wijzigen vanuit de command prompt?

De configuratie wordt opgeslagen in het register van de server. Per share 1 multi-valued sleutel in de Shares subtak van de LanManServer service.

net file Bekijk en beheer bronnen die gedeeld worden over het netwerk. De server service moet draaien om dit commando te kunnen gebruiken.

net config Bekijk het maximum aantal gebruikers die een gedeelde bron kunnen raadplegen en de maximum aantal open files per sessie.

net use Verbind of verbreek de verbinding met een computer van een gedeelde bron.

net session Beheer server connecties.

net share Maak, verwijder, beheer en toon gedeelde bronnen.

net view Toon informatie over de domeinen, computers en bronnen die gedeeld zijn door de aangegeven computer, inclusief de offline client cache setting.

net help Bekijk de hulp pagina voor de netwerk commando's.

9.3 Op welke diverse manieren kan men gebruik maken van gedeelde mappen?

Eenvoudigste manier: rechtstreeks pad ingeven in de adresbalk van een Explorer. Als je een bepaalde netwerklocatie frequent gebruikt, is het aangewezen om deze locatie in het lokale filesysteem te mappen. De share krijgt dan een stationsletter toegewezen, en kan net als een lokaal station gebruikt worden. Dit is in te stellen door in explorer rechtermuisknop op Network of My network places, dan Map Netwrok Drive en klik op wizard. Kan ook met het command net use.

9.4 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.

9.4.1 Features vanaf v1.2

- Beveiliging op bestandsniveau
- Logging van schijfactiviteiten
- Dynamisch uitbreiden van partities/volumes
- Compressie
- Grotere partities, zonder performantiedegradatie
- Hardlinks
- Auditing op objecttoegang

9.4.2 Features vanaf v3.0

- Reparsepunten en bestandssysteemfilters
- Transparante encryptie en decodering
- Individuele diskquota op volumeniveau
- Volumekoppelpunten: mounten van volumes in NTFS mappen

- Sparse bestanden
- Junction points naar mappen (soft link)

Hoofdstuk 10

Machtigingen op bestandstoegang

10.1 Welke rol spelen machtigingen bij de beveiliging van bronnen? Geef een gedetaileerd algemeen overzicht van het mechanisme van machtigingen.

Met machtigingen bepaal je wie toegang heeft tot welke gegevens, en wat die er mee kan doen. Elk object in AD, elk object van een NTFS volume, elke registersleutel, elk proces en ook elke service heeft een security descriptor. Deze bevat ondermeer:

- Een machtigingsset of Discretionary Acces Control List (DACL).
- De System Access Control List (SACL) definieert welke acties van de gebruiker gelogd worden.
- De SID van de eigenaar van het object. Makers van objecten zijn standaard eigenaar, maar de eigendom kan worden overgedragen. De eigenaar of beheerder is verantwoordelijk voor het instellen van de ACL.
- De primaire group van de maker, enkel van belang voor POSIX toepassingen.

De ACL is een verzameling machtigingen die bepaalt welke gebruiker of welke groep welke toegangsrechten heeft voor het object. De specifieke machtigingen die kunnen worden toegekend is afhankelijk van het object waarop ze worden toegepast.
De ACL bestaat uit Access Control Entries (ACEs) of machtigingsvermeldingen. Een ACE kan zowel een machtiging toekennen als ontzeggen. Machtigingen worden best zo veel mogelijk op groepen toegepast om beheer te vereenvoudigen.
ACEs worden in canonieke volgorde verwerkt. Eerst komen de ACEs die machtigingen ontzeggen aan de beurt, daarna degene die toekennen. Ontzeggen is steeds het sterkste kenmerk, een toekenning van een machtiging wordt genegeerd als die eerder ontzegd werd. Afwijken van deze volgorde kan enkel programmatorisch.

Machtigingen zijn cumulatief. De machtigingen van een groep worden op zijn leden toegepast, tenzijn die machtiging elders (op de specifieke gebruiker of een andere groep) ontzegd werden. Machtigingen worden impliciet geweigerd.
Er zijn twee soorten machtigingen:

Expliciete machtigingen rechtstreeks aan het object gekoppeld.

Overgenomen machtigingen machtingen overgenomen van de container waartoe het object behoort. Dit vereenvoudigt het beheer van machtigingen sterk.

Expliciete machtigingen krijgen altijd voorrang op impliciete. Het ontbreken van een ACL is een ernstig risico. Immers objecten zonder ACL zijn voor iedereen toegankelijk, terwijl een lege ACL ervoor zorgt dat toegang impliciet wordt geweigerd.

10.2 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.

Er zijn twee niveau's van machtigingen voor bestandstoegang: Share/SMB machtigingen en NTFS machtigingen.
Share machtigingen krijgen de bovenhand als ze beperkender zijn dan de NTFS. Men zou dus de share machtigingen of FULL Control kunnen zetten voor iedereen en verdere vernauwing van de rechten aan de hand van NTFS machtigingen bekomen, dit heeft echter 2 problemen:

1. FAT bestandssystemen kennen geen NTFS machtigingen.
2. Gebruikers met volledige share machtigingen kunnen alle submappen zien ook al hebben ze 0 NTFS machtigingen hierop. Dit kan opgelost worden met Access Based Enumeration.

10.2.1 SMB machtigingen

Dit is de 1e beveiligingsmuur voor bestandstoegang. Ze kunnen op drie manieren ingesteld worden: in Explorer, in het detailpaneel van de Shares map van compmgmt.msc en in het detailpaneel van de Share and Storage Management map van Server Manager. Er zijn 3 machtigingen, instelbaar per gebruiker of groep:

Full Control Alle bewerkingen op alle bestanden/mappen. Ook de share zelf kan worden gewijzigd.

Read Kan de hele hiërarchie van de share bekijken, elke file lezen en toepassingen uitvoeren.

Change Bovenop alles van Read ook wijzigen en verwijderen. Ook bestandskenmerken. Share zelf en NTFS machtigingen kunnen niet gewijzigd worden.

10.2.2 NTFS machtigingen

Na machtigingen op shares zijn NTFS machtigingen de tweede (beveiliging van mappen) en derde (beveiliging van bestanden) verdedigingsmuren voor het beveiligen van gegevens en netwerkbronnen. Er bestaan twee niveaus van NTFS machtigingen:

- Het laagste niveau bestaat uit 13 atomaire of speciale machtigingen, die de bouwstenen vormen voor het hogere niveau. Dit zijn de kleinst mogelijke machtigingen die je kan instellen en bieden de mogelijkheid om zeer nauwkeuring het toegangsniveau te bepalen.
- Het hoogste niveau, moleculaire of standaard machtigingen, omvat 6 veel gebruikte combinaties van atomaire machtigingen.

Instellen van NTFS machtigingen

NTFS machtigingen toewijzen is niet moeilijk, maar in een grote omgeving met veel bronnen en gebruikers moet je zeer methodisch en consistent te werk gaan. De ACL editor, van een bestand of map, kan opgeroepen worden via de Security tabpagina van het object. Hier kunnen ACEs toegevoegd en verwijderd worden. De grijze selectievakjes duiden overgenomen machtigingen aan.
Deze inheritance of propagation is zeer handig om op een eenvoudige manier de toegang wil definiëren tot de volledige naamruimte van een grote maphiërarchie.
De advanced knop in Security tabpagina geeft toegang tot een volgende niveau bestaande uit 4 tabpagina's:

1. Permissions: Toont steeds de correcte weergave v/d werkelijke ACLs en laat aanvullende mogelijkheden toe: Allow inheritance permissions, Replace all existing inheritance permissions, Add/Edit/Delete ACEs.
2. Auditing: Laat toe om SACL van het object in te stellen.
3. Owner: Laat toe om het ownership over te nemen. Het eigenaarschap kan niet eenzijdig worden overgedragen.
4. Biedt de voor probleemdiagnose interessante mogelijk om voor een specifieke gebruiker het zelfde algoritme toe te passen dat de SRM gebruikt om de uiteindelijke machtigingen op een object na te gaan.

10.3 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 de actie onderneemt wordt eigenaar van de bestanden wanneer ze bij de bestemming aankomen.
Wanneer de bestemming een container is op een ander NTFS volume, of de bestanden met standaard tools worden gekopieerd, vervallen de expliciete machtigingen. De machtigingen van de doelcontainer worden overgenomen door het object zelf en al zijn onderliggende objecten.
Objecten die naar een niet NTFS volume worden gekopieerd, verliezen alle machtigingen.
Om de machtigingen tijdens een kopieeropdracht te behouden moeten speciale tools zoals robocopy en scopy gebruikt worden.
Wanneer bestanden of mappen worden verplaatst naar een container binnen hetzelfde volume, worden de expliciete machtigingen behouden, en worden de machtigingen van de container overgenomen.

10.4 Op welke andere objecten zijn machtigingen van toepassing?

Elk object in AD, elk object van een NTFS volume, elke registersleutel, elk proces, en elke service heeft een security descriptor, en dus de bijhorende machtigingen.
Het individueel instellen van de machtigingen van elk object zou heel wat werk veroorzaken. Gelukkig worden de meeste objecten op één of andere manier hiërarchisch gestructureerd en ken er gebruik gemaakt worden van overerving van machtigingen.

Hoofdstuk 11

Gebruikersgroepen

11.1 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:

- De zichtbaarheid van de diverse soorten groepen
- Welke objecten er lid van kunnen zijn
- De onderlinge relaties en de regels voor het nesten van de diverse soorten groepen? Stel deze relaties eveneens schematisch voor.

Er zijn drie soorten veiligheidsgroepen, bereiken of scopes genoemd: lokaal, globaal en universeel. Zowel het type als de scope van een groep worden bijgehouden in de individuele bits van het groepType attribuut van het groep object. Het bereik van een groep bepaalt zowel of een groep leden uit andere domeinen en forests kan hebben, als de domeinen waarin rechten en machtigingen aan de groep kunnen toegewezen worden.

11.1.1 Lokale veiligheidsgroepen

Lokale groepen kunnen leden uit elk domein van het forest of andere trusted domeinen bevatten. Lokale groepen zijn enkel zichtbaar en geldig in het eigen domein. Lokale groepen worden niet gekopieerd naar de global catalog. Ze zijn niet enkel zichtbaar voor domeincontrollers maar ook op alle werkposten en lidservers van het domein.
Lokale groepen worden typisch gebruikt om rechten en machtigingen toe te kennen, en bevatten eerder andere groepen dan gebruikers.

11.1.2 Globale veiligheisgroepen

Globale groepen kunnen alleen gebruikers en andere globale groepen uit hetzelfde domein omvatten. Ze zijn zichtbaar in elk domein van het forest of andere trusting domeinen. Globale groepen kunnen ook toegelaten worden tot de lokale groepen van werkposten en lidservers. De naam van de groep wordt gekopieerd naar de global catalog, maar niet de leden ervan.
Ze worden vooral gebruikt als container voor gebruikers die dezelfde machtigingen of rechten nodig zullen hebben.

11.1.3 Universele veiligheidsgroepen

Universele groepen zijn nieuw voor Windows Server en zijn enkel te gebruiken in domeinen met minstens Windows 2000 native functioneel niveau. Ze kunnen leden uit elk domein van het forest (niet van andere trusting domeinen) bevatten en zijn zichtbaar in elk domein van het forest (niet in andere trusting domeinen).
Universele groepen worden net als lokale groepen typisch gebruikt om rechten en machtigingen toe te kennen, maar bieden het voordeel dat ze in alle domeinen tegelijkertijd geldig zijn. Ze zijn belastend voor de global catalog. Bij voorkeur bevatten universele groepen dan ook enkel globale groepen.

11.2 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.

Lokale groepen worden typisch gebruikt om rechten en machtigingen toe te kennen, door voor elke bron of verzameling bronnen één of meerdere lokale groepen te creëren en de toegang tot die bron in te stellen door één keer toegang te verlenen aan de lokale groepen. De toegang tot de bron wordt nadien enkel gewijzigd door het lidmaatschap te manipuleren. Lokale groepen zijn niet alleen zichtbaar op domeincontrollers, maar ook op alle werkposten en lidservers. Dit neemt de noodzaak weg om uit veiligheidsoverwegingen alle lidservers te configureren als domeincontrollers.

Globale groepen worden eerder gebruikt als containers voor gebruikers die dezelfde machtigigen of rechten nodig zullen hebben en als leden van andere groepen, in het domein zelf of in een trusting domein. Als je een verzameling gebruikers, afkomstig uit een ander domein toegang wil verlenen tot een bepaalde bron, dan kun je deze verzameling best groeperen in een glogale groep (van het vreemde domein) en deze lid maken van een lokale groep, gekoppeld aan de bron.

Universele groepen verenigt op het eerste zicht de beste karakteristieken van zowel lokale als globale groepen. Universele groepen worden net als lokale groepen typisch gebruikt om rechten en machtigingen toe te kennen, maar bieden het voordeel dat ze in alle domeinen tegelijkertijd geldig zijn en dus slechts eenmaal moeten gedefinieerd worden. Zowel de namen als de leden van universele groepen worden in de global catalog opgenomen, en dus wordt deze zeer groot. Bij voorkeur bevatten universele groepen enkel globale groepen.

11.3 Welke conversieregels gelden er tussen de diverse soorten groepen. Behandel hierbij alle mogelijke combinaties.

Lokale groepen mogen niet naar universele groepen geconverteerd worden als die lokale groepen andere lokale groepen bevatten. Dit omdat een universele groep geen lokale groep kan bevatten.
Als een globale groep een andere globale groep bevat kan dat lid niet geconverteerd worden naar een universele groep. Dit omdat globale groepen geen universele groepen kunnen bevatten.
Er mogen verschuivingen optreden als er geen regels gebroken worden.
Universele groepen kunnen terug naar zowel globale groepen als lokale groepen teruggebracht worden op voorwaarde dat een universele groep leden heeft die tot 1 domein behoren.
Een globale groep wordt per domein gedefinieerd in tegenstelling tot een universele groep dat in de global catalog opgeslagen wordt en dus over de verschillende domeinen van het forest gekend is. Dus als een universele groep leden bevat over meerdere domeinen, is deze conversie niet mogelijk.

Hoofdstuk 12

Configuratie van gebruikersgroepen

12.1 Waar en hoe wordt het (volledige) lidmaatschap van een 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 er deel van uitmaken, achterhalen?

In het properties venster van een gebruikersaccount kan men in het Member Of tabblad lidmaatschap tot groepen configureren. Het memberOf attribuut dat hiervoor gebruikt wordt, is gelinkt aan het member attribuut van de groep en is hier de back-link. Het kan dus niet rechtstreeks gewijzigd worden, dit kan enkel via het member attribuut van de groep.
In het properties venster van een groep kan men in het tabblad Members de groep bevolken. In het Member Of tabblad kan men de groep zelf deel laten uitmaken van een andere groep. De lijst van members wordt dus steeds opgeslagen in een link-kenmerk met in de groep de forward-link members. En in het object dat deel uitmaakt van de groep de back-link memberOf. Doordat memberOf een back-link kenmerk is kan het niet rechtstreeks gewijzigd worden.
Groepsleden kunnen ook uit trusted domeinen geselecteerd worden. AD maakt hiervoor een phantom object aan, dat het object uit het vertrouwde domein vertegenwoordigt. Deze mapobjecten komen terecht in de container ForeignSecurityPrincipals, en kunnen lid worden van lokale groepen in het domein.
Uiteraard zijn de groepen ook te beheren via de Command Prompt door middel van de opdrachten: net group, net localgroup, dsadd group, dsrm group, dsget group en dsmod group.
De verzameling objecten die tot een groep behoren kan men verkrijgen met:

- Door met het commando dsget group het attribuut members op te vragen van een groep.

- In het Members tabblad van de properties van de groep.
- Met behulp van een LDAP query.

12.2 Door wie wordt het lidmaatschap van de diverse groepen bij voorkeur ingesteld?

Dit kan best door de beheerder gebeuren. Lidmaadschap bij een groep kan bepaalde machtigingen met zich meebrengen en het is de taak van de beheerder om ervoor te zorgen dat gebruikers niet meer rechten hebben dan dat ze nodig hebben.
In grote organisaties kan een deel van de beheerstaken gedelegeerd worden naar andere personen. Zij zullen dan bv rechten hebben om een bepaalde subtak of OU te beheren.
Bij subscriptiegroepen kunnen gebruikers zich zelf in en uitschrijven.

12.3 Op welke diverse manieren kan men het beheer van 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.

Men kan in AD de beheerstaken van een OU delegeren aan een groep gebruikers. Hiervoor moet men de ACLs van de OU instellen. Dit kan op drie manieren:

- Via de Delegation of Control Wizard
- Via de properties van de OU
- Via de Command Prompt

12.3.1 Delegation of Control Wizard

Om de wizard op te starten klik je in dsa.msc met de rechtmuisknop op een OU en selecteer je Delegate Control. Je selecteert de groepen of gebruikers waaraan je beheersmachtigingen wil delegeren. Deze hoeven geen deel uit te maken van de groep zelf. Het volgende dialoogvenster toont een lijst met de meest voorkomende beheertaken die voor delegeren in aanmerking komen. Met create a custom task to delegate kan je zelf een gedetailleerde keuze maken tussen alle beschikbare delegeeropties. Het laatste dialoog venster toont ter bevestiging een overzicht van de geselecteerde instellingen.

12.3.2 OU properties

Rechterklik op de OU, dan properties en naar het security tabblad gaan. Daar kan je zowel taken delegeren als de instellingen voor reeds gedelegeerde taken wijzigen. De lijst van molucaire machtigingen waaruit je kan kiezen is afhankelijk van de objectklasse.

12.3.3 Command Prompt

Met de acldiag en dsacls opdrachten. Terug intrekken kan met dsrevoke.

12.4 Aan welke groepen/entiteiten worden rechten in de praktijk toegekend? Bespreek de bijzonderheden van dergelijke groepen/entiteiten, en vermeld er de meest interessante voorbeelden van (telkens met hun bedoeling en hun randeffecten).

Rechten kunnen afzonderlijk aan een individuele gebruiker toegekend worden, maar voor het organiseren van de beveiliging is het beter de gebruiker in een groep te plaatsen, en te definieren welke rechten aan de groep toegekend worden. Verschillende praktische groepen zijn oa:

Backup Operators hebben de bevoegdheid om bestanden en mappen te back-uppen en terug te plaatsen, zelfs als ze geen toestemming hebben om deze bestanden te lezen of te wijzigen.

Account Operator maken en beheren gebruikersaccounts en groepen, en kunnen computers aan het domein toevoegen.

Server Operators kunnen onder andere het systeem vanop afstand uitzetten, de systeemtijd veranderen, de harde schijf formatteren en mappen delen.

Print Operators kunnen printers delen, wissen en beheren.

Administrators hebben bijna elk recht. Toch krijgen beheerders met de ruime bevoegdheden van deze groep geen toegang tot alle bestanden en mappen.

User kunnen programmas gebruiken, maar ze niet installeren.

AD kent ook impliciete groepen, deze hebben geen specifiek lidmaatschap en kunnen op verschillende tijdstippen verschillende gebruikers vertegenwoordigen. Enkele voorbeelden:

Interactive iedereen die de computer lokaal gebruikt.

Network alle gebruikers die via het netwerk zijn verbonden met een computer.

Everyone combinatie van de Interactive en Network groepen.

Authenticated Users alle gebruikers die geauthentificeerd zijn.

System het besturingssysteem, heeft bijna alle bevoegdheden. Processen van het OS hebben deze rechten nodig om te kunnen draaien.

Hoofdstuk 13

Gebruikersprofielen

13.1 Wat is de bedoeling van gebruikersprofielen? Bespreek zowel uit het standpunt van gebruikers, als uit het standpunt van beheerders, en bespreek hierbij de voor- en nadelen.

Op NT4+ computers worden de desktop instellingen voor de werkomgevingen van gebruikers op de lokale computer automatisch gedefinieerd en bijgehouden met behulp van gebruikersprofielen. Dit is in feite een momentopname van de desktop omgeving van een gebruiker. Het definieert een aangepaste desktop omgeving met individuele weergave instellingen, netwerkverbindingen, printerverbindingen en andere spcifieke instellingen. Gebruikersprofielen bieden diverse voordelen:

- Elke gebruiker beschikt over persoonlijke desktop instellingen bij het aanmelden.
- Bij aanmelden worden automatisch de desktop instellingen hersteld die actief waren bij afmelding.
- Ze kunnen ook centraal op een server worden opgeslagen. We spreken dan van roaming gebruikersprofielen.

Gebruikersprofielen zijn afkomstig uit het NT4 tijdperk en niet strikt noodzakelijk in NT5+ omgevingen. Group Policies kunnen namelijk de instellingen van het gebruikersprofiel te niet doen. Maar het blijft wel de eenvoudigste manier om gebruikersinterfaces te configureren.
Met gebruikersprofielen is het voor beheerders mogelijk om voor elke gebruiker een individuele desktop te configureren. Ook kan er één algemeen gebruikersprofiel aangemaakt worden, dat verplicht door alle gebruikers moet gebruikt worden. Gebruikers kunnen terwijl ze aangemeld zijn hier wel wijzigingen aan doen, maar deze zullen niet opgeslagen worden en bij de volgende aanmelding zal terug het standaard profiel verschijnen.

13.2 Geef de verschillende types gebruikersprofielen. Hoe worden deze ingesteld, en waar worden deze bij voorkeur opgeslagen?

Er zijn 3 belangrijke soorten gebruikersprofielen:

Lokale gebruikersprofielen Deze worden automatisch aangemaakt als een gebruiker zich voor de eerte keer aanmeld op een computer. Het wordt op de lokale harde schijf opgeslagen. Alle wijzigingen in dit profiel zijn specifiek voor de gebruiker.

Roaming gebruikersprofielen Dit zijn gebruikersprofielen die op een netwerk share worden opgeslagen. Een gebruiker kan op gelijk welke computer in het netwerk inloggen en zijn eigen gebruikersprofiel zal gedownload worden van de share en getoond worden. Het instellen van een roaming profiel kan door het profilePath attribuut van een gebruikersobject in te vullen. Hier wordt een netwerk pad opgegeven in de vorm: \\servernaam\sharenaam\mapnaam. De mapnaam bevat waarschijnlijk een component van de vorm %username%. Bij het afmelden wordt een kopie van het al dan niet gewijzigde gebruikersprofiel opgeslagen, zowel lokaal als in de netwerkmap. Bij terug aanmelden wordt de timestamp van het lokale en roaming profiel vergeleken, waarmee kan bepaalt worden of het profiel moet gekopieerd worden naar de lokale computer. Roaming profielen bieden samengevat drie grote voordelen: mobiliteit, fouttolerantie en centrale beheerbaarheid. De nadelen zijn een verhoogd netwerkverkeer, langere aanlog- en uitlogtijden en een verhoogd veiligheidsrisico. NT5 en NT6+ roaming profielen zijn helaas onderling niet uitwisselbaar. Men noemt ze respectievelijk v1 en v2 profielen.

Mandatory gebruikersprofielen Deze worden gedefinieerd door een systeembeheerder en zijn verplicht te gebruiken voor alle gebruikers. Wijzigingen die de gebruikers aanbrengen worden niet opgeslagen. In tegenstelling tot roaming profielen, kunnen mandatory profielen gedeeld worden door diverse gebruikers. Ze worden bij voorkeur opgeslagen in de SYSVOL share van domeincontrollers. Mandatory profielen bieden systeembeheerders de meeste controle, maar eisen anderzijds ook het meeste setup werk.

13.3 Geef de verschillende componenten van gebruikersprofielen.

Een gebruikersprofielmap bevat twee belangrijke componenten:

- Het Hive bestand NTuser.dat vormt het register gedeelte van het gebruikersprofiel. Dit omvat ondermeer alle door de gebruiker gedefinieerde instellingen voor de Windows omgeving en toepassingsprogramma's. NTuser.dat.log is een log bestand van handelingen

dat er is om NTuser.dat te beschermen als er veranderingen worden weggeschreven naar schijf.

- Bestanden en snelkoppelingen naar verschillende desktop items, zoals naar toepassingsspecifieke gegevens, locatie op het internet, en de laatst gebruikte documenten. Bestanden en snelkoppelingen worden gestructureerd in diverse mappen. Om de grootte van het gebruikersprofiel te beperken, worden er bij voorkeur enkel snelkoppelingen in het profiel opgenomen, en wordt een deel van het profiel, appdate en local settings, enkel lokaal bewaard. Op NT6+ worden de snelkoppelingen uit het persoonlijk v2 profiel dynamisch aangevuld met de items in de overeenkomstige submappen van het lokale public profiel.

13.4 Over welke alternatieve hulpmiddelen beschikt een beheerder om gebruikersprofielen te configureren?

Een systeembeheerder kan, door de Default user, Default user.V2, Default, All users en Public profielen te manipuleren, standaardinstellingen definiëren die opgenoemen worden in alle individuele gebruikerprofielen. Deze profielen in de NETLOGON share vormen een uitstekende combinatie met roaming profielen.
Een andere optie is dat de beheerder voorgedefinieerde gebruikersprofielen maakt. Hiervoor log je in met een willekeurig gebruikersaccount en maak je als gebruiker het gewenste gebruikersprofiel. Daarna kopieer je als administrator het gebruikersprofiel naar de gewenste netwerk share. Aangezien de NTuser.dat component intern ACLs bevat op registersleutels, kan een op bestandbasis gekopieerd gebruikersprofiel enkel gebruikt worden door de gebruiker die het profiel heeft gecreëerd. Om dit te verhelpen zijn er twee opties:

- Wijzig met de register editor de ACLs op de registersleutels in NTusers.dat.
- Gebruik een specifiek met Windows Server meegeleverd hulpprogramma. Hiermee kan opgeven wie het profiel mag gebruiken in het Permitted to use veld.