

# Theorie vragen BSIII - windows 2014

Andreas De Lille

Augustus 2014

# Inhoudsopgave

<b>I</b>	<b>Modeling - Reeks 1</b>	<b>1</b>
<b>1</b>	<b>Structuur van Active Directory gegevens</b>	<b>2</b>
1.1	Bespreek de diverse namen die alle Active Directory objecten identificeren. (2.2.1)	2
1.2	Wat zijn SPN objecten ? Bespreek de aanvullende naamgeving voor deze objecten. (2.2.2)	3
1.3	Enkele veel gebruikte klassen vertonen nog "meer identificerende attributen voor hun instanties. Bespreek deze klassen en attributen.	5
1.4	In welke partities is de Active Directory informatie verdeeld ? Geef de betekenis van elke partitie, hun onderlinge relatie, en de replicatiekarakteristieken ervan. (laatste helft 2.2.3)	6
1.4.1	Wat?	6
1.4.2	Partities	6
1.4.3	Onderlinge relatie	7

Deel I

Mondeling - Reeks 1

# Hoofdstuk 1

## Structuur van Active Directory gegevens

### 1.1 Bespreek de diverse namen die alle Active Directory objecten identificeren. (2.2.1)

#### Naamgeving van object

De namen zijn logisch en hiërarchisch opgebouwd.

Volgende vier namen zijn steeds beschikbaar.

#### 1. RDN - Relative distinguished name

- Voorbeeld: cn = beelzebub
- Is uniek binnen zijn container.
- Denk aan absoluut path (DN) vs. relatief filepath (RDN).
- Wordt opgeslagen in het cn attribuut van het object.

#### 2. DN - Distinguished name

- Voorbeeld: cn = beelzebub, ou= iii, ou=hogent, ou=be (cn = common name, ou = organisational unit)
- Attributed naming, verschillende attribuut=waarde koppels
- Afgeleid van alle container object waarvan het object hiërarchisch deel uitmaakt.
- Uniek over het hele domein.
- Denk aan absoluut path (DN) vs. relatief filepath (RDN).
- Wordt opgeslagen in het distinguishedName attribuut van het object.

### 3. CN - canonieke naam

- !! Niet hetzelfde als de cn van hierboven. Hier cn = canonieke naam ; hierboven cn = common name als waarde van een DN)
- Voorbeeld: hogent.be/iii/beelzebub
- Samengesteld uit de DN, geeft de DN op een eenvoudigere manier weer.
- De meeste hulpmiddelen in active directory tonen de canonieke naam.
- Wordt opgeslagen in het canonicalName attribuut van het object. (en dus niet in het cn attribuut)

### 4. GUID - global unique identifier

- Globaal uniek (zelfs in tijd) getal van 128 bits.
- Kan en wordt nooit gewijzigd.
- Wordt opgeslagen in het objectGUID attribuut van het object.
- Wordt gegenereerd en toegewezen bij het aanmaken van het object.

## 1.2 Wat zijn SPN objecten ? Bespreek de aanvullende naamgeving voor deze objecten. (2.2.2)

### 1. SPN - Security Principal Objects

- Doel: SPN of Security Principal Objects zijn Active Directory objecten die gebruikt worden om toegang te verlenen tot domeinbronnen.
- Zijn van toepassing op computers, gebruikersrekeningen en domeinen.

### 2. SID - Security ID

- Zijn net als guids uniek in tijd; wanneer een object verwijderd en vervolgens terug aangemaakt wordt, zal het een andere SPN krijgen. Hierdoor kan een object nooit machtigingen van een oude account behouden.
- Opgeslagen in het objectSid kenmerk
- Men maakt gebruik van SIDs naast GUIDs om compatibiliteitsredenen.
- hiërarchische string getallen gescheiden door koppeltekens bijvoorbeeld S-1-5-x-y-z-500. Hierbij is S-1-5 een standaard prefix bestaande uit een revision level en een authority identifier. X,y en z zijn 32bit getallen die specifiek zijn voor het domain, (Domain Subauthority Identifier), 500 is een relatieve ID (RID) dat naar het feitelijke object verwijst.

- SID blijft behouden als het object verplaatst wordt binnen hetzelfde domein. Als er verplaatst wordt naar een nieuw domein zal de SID wijzigen.
- Wordt gegenereerd en toegewezen bij de aanmaak van het object.
- sIDHistory, houdt alle SIDs bij die het SPN in het verleden had om te vermijden dat een gebruiker na verplaatsing van objecten zijn toegang zou verliezen.

### 3. UPN - User Principal Name

- Doel aanmeldingsnamen van gebruikers vereenvoudigen.
- opgeslagen in het userPrincipalName kenmerk.
- Als de UPN enkel gebruikt wordt voor aanmelding, moet hij uniek zijn binnen het volledige forest.
- Bestaat standaard uit [RDN gebruiker]@[UPN suffix] (zonder [ en ])
- UPN suffix kan vervangen worden door
  - DNS domeinnaam van het domein waar de account zich bevindt of het root domein
  - Mag zelfs een willekeurige naam zijn ook, als hij geregistreerd is met behulp van de Active Directory domeins and Trust snap-in.
- Wordt maar sporadisch gebruikt door compatibiliteitsredenen. Vaak maakt men gebruik van: [NetBIOSnaam van het domein]-[SAM accountnaam]. (zonder [ en ]).

### 4. NetBIOS

- Bestaat standaard uit de meest linkse component in de DNS naam van het domein
- Is niet langer dan 15 letters
- deze naam moet uniek zijn in zijn forest

### 5. SAM accountnaam - Security Accounts Manager

- Moet uniek zijn in het domein
- Wordt opgeslagen in sAMAccountName
- Bestaat uit hoogstens 20 karakters, standaard de eerste 20 bytes van de RDN afgesloten door een \$ <sup>1</sup>.
- Deze naam kan op elk gewenst moment veranderd worden.

---

<sup>1</sup>in de cursus staat er bytes p21, voorlaatste paragraaf, ik zou eerder denken dat het letters zijn

## 6. DNS hostname

- opgeslagen in dnsHostName kenmerk
- standaard eerste 15 bytes van de RDN gevuld door de suffix voor de primaire DNS
- Standaard is de suffix de volledige DNS naam van het domein waar de computer toe behoort.
- Er kan afgeweken worden; meer dan 15 chars en andere DNS naam.

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

Komt later aan bod. zaken zoals:

1. LDAPDisplayName
2. Object identifier
3. objectClass (de hiërarchische klassen)
4. objectCategory (de categorie van de klasse van het object)
5. ...

## **1.4 In welke partities is de Active Directory informatie verdeeld ? Geef de betekenis van elke partitie, hun onderlinge relatie, en de replicatiekarakteristieken ervan. (laatste helft 2.2.3)**

### **1.4.1 Wat?**

We noemen de verzameling van alle active directory informatie (objecten en containerobjecten samen met hun meta data (ook objecten)) het gegevensarchief of de directory. Elke domein-controller bevat een kopie van de directory van zijn domein. De informatie is fysiek verdeeld in minimaal 3 categoriën of partities. Cliënt computer houden (uiteraard) geen informatie bij.

### **1.4.2 Partities**

Elke partitie in de directory vormt een aparte eenheid voor replicatie. (zie later)

#### **1. Domeinpartities met domeingegevens**

- bevatten informatie over objecten in het domein: gedeelde bronnen (servers, bestanden en printers) en accounts.
- Bij installatie worden er een aantal standaard objecten aangemaakt, een daarvan is de administrator account
- elk domein zit in een aparte partitie, er zijn dus evenveel partities met domeingegevens als dat er domeinen in het forest zijn.
- deze gegevens hebben bijgevolg enkel betrekking op dit domein en worden niet gedistribueerd naar ander domeinen.
- een subset van deze gegevens wordt opgeslagen in de global catalog

#### **2. Applicatie partities**

- bv dns gegevens
- kunnen geen SPN objecten bevatten
- kunnen niet verplaatst worden buiten de applicatie partitie
- beschikbaar vanaf windows server 2003
- zelf partities maken met adsiedit.msc



### 3. configuratie gegevens

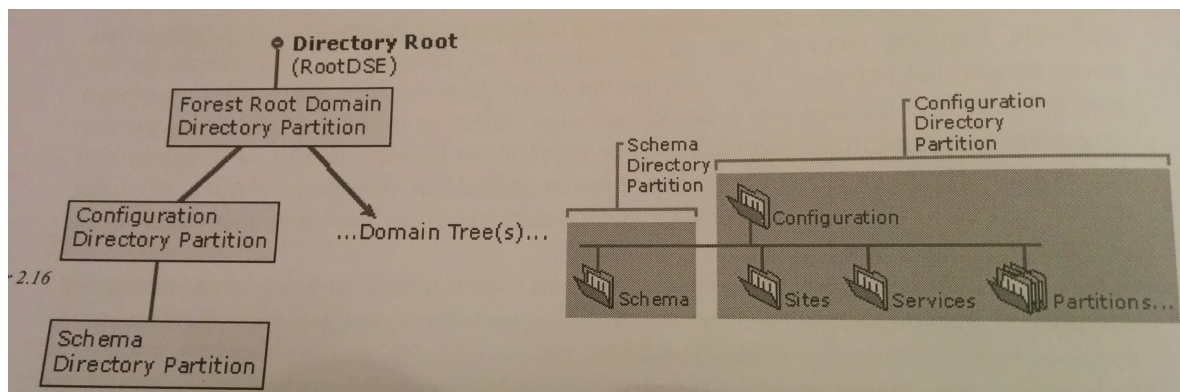
- beschrijven de fysieke topologie van de directory (bv lijst van alle domeinstructuren, locaties van domeincontrollers en global catalog controllers, sites, ..)
- Instellingen voor het hele forest worden vertaald naar kenmerken van objecten in de configuratie gegevens. (bv. uPNSuffixes kenmerk houdt de mogelijke UPN suffixen bij)

### 4. schema

- bevat een formele definitie van alle objecten en kenmerkgegevens die kunnen opgeslagen worden in de directory.
- is uniek voor alle domeinen in het forest.

#### 1.4.3 Onderlinge relatie

- Logische structuur: een boom structuur zie



**Figuur 1.1:** onderlinge relatie van de partities, uit de cursus "Besturingssystemen III - Windows Server (J. Moreau)"

- Het root forrest domein staat