

# Besturingssystemen III

Bert De Saffel

Master in de Industriële Wetenschappen: Informatica Academiejaar 2018–2019

# Inhoudsopgave

<b>I</b>	<b>Theorie</b>	<b>2</b>
<b>1</b>	<b>WMI concepten</b>	<b>3</b>
1.1	Herhaling SNMP en inleiding WMI . . . . .	3
1.2	CIM Repository . . . . .	4
1.3	Qualifiers . . . . .	4
1.4	Associatorklassen . . . . .	6
1.5	WMI Query Language . . . . .	6
1.6	Notification queries . . . . .	7
<b>II</b>	<b>Examenvragen</b>	<b>8</b>
<b>2</b>	<b>Modelvragen theorie: reeks A</b>	<b>9</b>
2.1	Structuur van Active Directory gegevens . . . . .	9
2.2	attributeSchema objecten (§2.2.4 en §2.2.5) . . . . .	9
2.3	classSchema objecten (§2.2.4 en §2.2.6) . . . . .	10
2.4	Active Directory domeinstructuren (§2.4.4, laatste paragraaf §2.4.5 en §2.4.6) . . . .	10
2.5	Active Directory server rollen (§2.4.7, §2.3 en fractie §2.4.2) . . . . .	10
<b>3</b>	<b>Modelvragen theorie: reeks B</b>	<b>11</b>
3.1	Active Directory functionele niveaus (§2.4.3) . . . . .	11
3.2	Active Directory replicatie (§2.5) . . . . .	11
3.3	Gedeelde mappen en NTFS . . . . .	11
3.4	Machtigingen op bestandstoegang (§3.3) . . . . .	12
3.5	Gebruikersgroepen (§4.2.2 en §4.2.3) . . . . .	12

Deel I

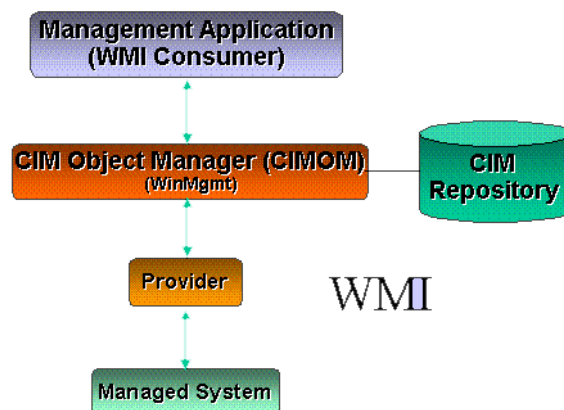
Theorie

# Hoofdstuk 1

## WMI concepten

### 1.1 Herhaling SNMP en inleiding WMI

SNMP had de mogelijkheid om informatie bij te houden van devices die typisch op een netwerk aangesloten zijn zoals printers, routers, workstations en servers. Er was echter nood aan een systeem dat ook informatie van het hele operating systeem kon bevragen. Dit systeem noemt *Wbem*, een uniform systeem voor het bevragen van besturingssystemen zoals windows, HP en solaris. Een Windows specifieke versie hiervan is het *Windows Management Instrumentation* (WMI). Uit figuur 1.1 kunnen vijf componenten afgeleid worden:



Figuur 1.1: Basisarchitectuur WMI

- *WMI Consumer* : Dit zijn gebruikersapplicaties die gebruik maken van de CIMOM (= de WMI Service) om diverse informatie op te vragen. Deze kunnen in diverse programmeertalen geprogrammeerd worden (in dit vak wordt Perl gebruikt).
- *CIM Object Manager* : Wordt ook de WMI Service genoemd en heeft drie functionaliteiten:
  1. Interactie met de WMI Consumer op een **uniforme** manier.

2. De WMI Service is verantwoordelijk voor alle communicatie met de providers. De WMI Consumer hoeft niets te weten over de verzameling Providers. De WMI Service gebruikt de CIM Repository om de juiste Provider te raadplegen.
  3. De CIM Repository is enkel toegankelijk voor de WMI Service
- *CIM Repository*. Dit is een databank zowel waarbij software als hardware componenten als objecten voorgesteld worden. Deze object georiënteerde methode zorgt ervoor dat deze componenten via methoden kunnen aangesproken worden. Voor elke klasse wordt ook bijgehouden door welke provider deze klasse gerealiseerd wordt.
  - *Provider* : Een provider is verantwoordelijk voor een aantal WMI-klassen
  - *Managed System* : Dit zijn hardware componenten die aangesloten zijn aan een werkstation.

## 1.2 CIM Repository

De CIM Repository kan men inspecteren met een WMI-browser. Voorbeelden hiervan zijn *WMI CIM Studio* en *Powershell WMI Browser*. In deze samenvatting wordt gebruik gemaakt van WMI CIM Studio. De inlogprocedure vraagt een namespace die standaard ingevuld staat op **root: CIMV2**. Deze namespace omvat ook de meeste WMI Objecten. Wat deze namespace niet heeft zijn klassen om office documenten zoals excel of word te manipuleren. Indien ingelogd, verschijnt er een scherm met twee panelen. Het linkerpaneel bevat alle klassen gesorteerd op hiërarchische volgorde op basis van overerving. De icoontjes naast elke klasse wordt gegenereerd op basis attributen van die klasse. Het rechterpaneel heeft standaard de *Properties* tab open. Dit tabblad bevat alle attributen van de geselecteerde klasse. Attributen voorafgegaan door 2 underscores zijn systeemattributen en bestaan voor elke klasse. Voorbeelden van zulke systeemattributen:

- **\_\_DERIVATION** : Dit bevat een tabel met de hiërarchie van de overerving waarbij het eerste element de onmiddellijke superklasse is en het laatste element de root van de hiërarchie.
- **\_\_DYNASTY** : Dit bevat de root van de hiërarchie van overerving. Deze informatie is dus dezelfde als het laatste element in het **\_\_DERIVATION** attribuut.
- **\_\_PROPERTY\_COUNT** : Dit veld bevat een nummer met het aantal niet-systeemaanroepen
- **\_\_PATH** : Dit veld bevat het absolute pad van de klasse.

Van elke klasse kan zijn instanties opgevraagd worden door op het icoontje rechts van het save-icoontje te klikken. Er wordt een twee dimensionale tabel weergegeven met per instantie een rij en per attribuut een kolom. Voor elke instantie moet het systeemattribuut **\_\_RELPATH** aangevuld worden met de sleutel van het object. Dit is een string dat bestaat uit meerdere key-value paren dat toegevoegd wordt aan de default waarde van **\_\_RELPATH**. Bij Singletons echter zijn unieke identificaties niet nodig en wordt **\_\_RELPATH** aangevuld met een symbool. Een voorbeeld van een abstracte klasse en een singleton is respectievelijk **CIM\_MonitorResolution** en **Win\_LocalTime**.

## 1.3 Qualifiers

Een qualifier is een key-value koppel waarbij extra eigenschappen kunnen toegevoegd worden. Er bestaan vier soorten qualifiers:

1. klasse-qualifiers. Geeft extra informatie over de klasse.
2. attribuut-qualifiers. Geeft extra informatie over de attributen van een klasse
3. methode-qualifiers. Geeft extra informatie over de methoden van een klasse
4. methodeparameter-qualifiers. Geeft extra informatie over de parameters van de methoden van een klasse.

### Klasse-qualifiers

Deze worden in WMI CIM Studio *Object qualifiers* genoemd:

- De *Description* qualifier geeft tekst terug met informatie over de klasse.
- De *Abstract*, *Dynamic* en *Singleton* qualifiers geven aan, indien hun waarde op *true* staat, dat een klasse abstract, dynamisch of een singleton is.
- De *Provider* qualifier helpt de WMI service te bepalen welke provider moet aangesproken worden om een bepaalde klasse aan te spreken

### Attribuut-qualifiers

De attribuut-qualifiers worden in WMI CIM Studio *Property qualifiers* genoemd:

- De *Description* qualifier geef analoog zoals de klasse-qualifiers tekst terug met informatie over het attribuut.
- De *CIMType* qualifier geeft het type van het attribuut weer, zoals string, boolean, datetime, signed of unsigned int (8, 16, 32 of 64 bits) of referenties naar absolute objectpaden.
- De *Write* qualifier geeft aan, indien deze op *true* staat, dat de het attribuut rechtstreeks wijzigbaar is, zonder hiervoor methodes te moeten aanspreken.
- De *Keys* qualifier geeft aan dat het attribuut deel uitmaakt van de sleutel van het object en bijgevolg ook vermeld moet worden in het objectpad van een instantie.
- ValueMap geeft in een ééndimensionale tabel het domein weer van het attribuut: een expliciete opsomming van de toegelaten waarden. Values geeft een meer informatieve interpretatie van de toegelaten waarden. Indien ook de ValueMap qualifier aanwezig is, kunnen ValueMap en Values best beschouwd worden als respectievelijk de keys en de values van een Perl hash. Indien een ValueMap ontbreekt, dan impliceert Values een ValueMap met oplopende gehele getallen, startend vanaf 0. Values kan dan geïnterpreteerd worden als een Perl array.

### Methode-qualifiers

- De **Description** qualifier geeft uitleg over de methode.
- De **CIMType** qualifier specificeert het return type.
- De **ValueMap** en **Values** worden vaak gebruikt bij een integer returnwaarde om deze waarde te vertalen naar iets zinvols.

- De **Privileges** qualifier specificeert een lijst van privileges die nodig zijn om de methode op te roepen. Indien deze qualifier niet aanwezig is kan eender wie de methode uit voeren.

De bijzonderste methode is de *Create* methode. Dit is een statische methode die onafhankelijk is van een specifieke instantie.

Een voorbeeld van een klasse met enkel statische methoden is **StdRegProv**. Deze klasse bevat methoden die het register kan aanpassen.

### Methodeparameter-qualifiers

- De **Description**, **CIMType**, **Values** en **ValueMap** qualifiers hebben een analoge functie als de corresponderende attribuut- en methodequalifiers, nu toegepast op een individuele parameter van een methode.
- **In/Out** geeft aan dat deze parameter een invoer- (resp. uitvoer-) parameter is. Een parameter kan ook invoer/uitvoer parameter zijn.
- De **Optional** qualifier, indien ingevuld op true, geeft aan dat deze parameter optioneel is. Voor elke optionele qualifier is er wel een default waarde.
- **ID** geeft de volgorde aan (startend met de waarde 0) waarin de parameters als argumenten bij de methodeaanroep moeten opgegeven worden.

## 1.4 Associatorklassen

Stel dat je informatie wenst over de ethernet adapter. De klasse **Win32\_NetworkAdapter** klasse kan alleszins de ethernet adapter filteren, maar er ontbreekt informatie zoals het IP adres. Die informatie bevindt zich in een andere klasse, **Win32\_NetworkAdapterConfiguration**. In beide klasse zijn er echter geen verwijzingen naar de andere klasse. Voor zowel 1:1, 1:n en m:n relaties gebruikt WMI associatorklassen. Dit zijn klassen met meestal 2 attributen die een klasse met een andere klasse associeert. Eén van de instanties van de associatorklasse **Win32\_NetworkAdapterSetting** zal in het eerste attribuut *element* een verwijzing hebben naar de ethernet adapter in **Win32\_NetworkAdapter** en zal in het tweede attribuut *setting* een verwijzing hebben naar de ethernet adapter in **Win32\_NetworkAdapterConfiguration** zodat deze informatie gecombineerd kan worden.

## 1.5 WMI Query Language

WMI Consumers kunnen gebruik maken van **WQL**, een querytaal gebaseerd op SQL waarbij enkel de **SELECT**, **FROM** en **WHERE** clause beschikbaar zijn. Clausules zoals **GROUP BY**, **HAVING** en **JOIN** zijn *niet* mogelijk in WQL. Het opvragen van alle ethernetadapters wordt bereikt met volgend stukje WQL code:

```
select *
from win32_networkadapter
where netconnectionid = 'Ethernet'
```

Attributen die gebruikt worden zijn niet hoofdlettergevoelig. Query's kunnen uitgetest worden in het programma **wbemtest.exe**. Bij het opstarten moet er eerst geconnecteerd worden naar een namespace dat standaard ingevuld is op *root\cimv2*. Indien op de knop *Query* geklikt wordt zal er

een venster verschijnen waarin WQL queries kunnen uitgevoerd worden. Het is ook mogelijk om de instanties op te vragen die gelinkt zijn aan het doelobject via associatorklassen.

```
associators of { win32_directory.name="C:/..." }  
where resultclass=win32_directory  
resultrole=partcomponent
```

Verskillende predicaten in de *where* clause worden niet verbonden met het AND keyword zoals men verwacht, deze wordt namelijk impliciet ingevuld.

## 1.6 Notification queries

Een WMI Consumer kan zich aanmelden aan de WMI Service indien deze een interesse heeft voor een bepaalde gebeurtenis. De provider weet welke consumers geïnteresseerd en zal dan ook de consumers inlichten wanneer de voorwaarden voldaan zijn. Een consumer hoeft hier zelf geen procestijd aan te spenderen. Bij het uittesten van notification queries staat de optie *asynchronous* best aan, anders is de uitvoeringstijd langer. Een voorbeeld van een notification query:

```
select *  
from win32_processtrace  
where processname = "calc.exe"
```

Deze query zal de consumer inlichten wanneer een windows rekenmachine opgestart of afgesloten wordt.



# Deel II

## Examenvragen

## Hoofdstuk 2

# Modelvragen theorie: reeks A

Het examen wordt **volledig schriftelijk** beantwoord. Indien de student dit wenst, wordt het antwoord onmiddellijk na indienen geëvalueerd, en eventueel gevolgd door enkele vragen ter verduidelijking of aanvulling.

### 2.1 Structuur van Active Directory gegevens

1. Bespreek de *diverse namen* die alle Active Directory objecten *identificeren*. (§2.2.1)
2. Wat zijn *SPN objecten* ? Bespreek de *aanvullende naamgeving* voor deze objecten. (§2.2.2)
3. Enkele veel gebruikte klassen (hiermee worden *attributeschema* en *classschema* objecten niet bedoeld) vertonen nog meer identificerende attributen voor hun instanties. Bespreek deze klassen en attributen.
4. In welke *partities* is de Active Directory informatie verdeeld ? Geef de betekenis van elke partitie, hun onderlinge relatie (zowel fysiek als met betrekking tot hun naamgeving), en de replicatiekarakteristieken ervan. (laatste helft §2.2.3)

### 2.2 attributeSchema objecten (§2.2.4 en §2.2.5)

1. Bespreek het *doel* en de *werking* van attributeSchema objecten. Hoe kunnen deze objecten het best *geraadpleegd* en *gewijzigd* worden ?
2. Bespreek de *diverse naamgevingen*, specifiek voor attributeSchema objecten.
3. Bespreek de belangrijkste *kenmerken* van attributeSchema objecten, en op welke waarden die ingesteld kunnen worden.
4. Welke andere types objecten bevat het *Active Directory schema*, en wat is hun bedoeling ? (o.a. §2.2.7)
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. (laatste paragraaf §2.2.6)

## 2.3 classSchema objecten (§2.2.4 en §2.2.6)

1. Bespreek het *doel* en de *werking* van classSchema objecten.
2. Hoe benadert Active Directory het mechanisme van *overerving* ?
3. Bespreek de diverse *naamgevingen*, specifiek voor classSchema objecten.
4. Bespreek de belangrijkste *kenmerken* van classSchema objecten, en op welke waarden die ingesteld kunnen worden.
5. Welke andere types objecten bevat het *Active Directory schema*, en wat is hun bedoeling ? (o.a. §2.2.7)
6. Hoe en met welke middelen kan het Active Directory schema uitgebreid worden ? Waarom moet je en hoe kan je hierbij *voorzichtig* te werk gaan ? (o.a. §2.2.8, lid 1de fractie §2.2.3)

## 2.4 Active Directory domeinstructuren (§2.4.4, laatste paragraaf §2.4.5 en §2.4.6)

1. Wat is de bedoeling van *vertrouwensrelaties* ?
2. Bespreek de verschillende *soorten* vertrouwensrelaties.
3. Op welke diverse manieren kunnen vertrouwensrelaties *gecreëerd* en *gecontroleerd* worden ? Bespreek ook de *optionele configuratiemogelijkheden*.
4. Welke verschillen zijn er in praktijk tussen *NT 4.0* en *Windows Server* domeinstructuren ? Bespreek onder andere telkens de noodzaak om meerdere domeinen in te voeren. Bespreek de alternatieve mogelijkheden bij de *conversie van een NT 4.0 domeinstructuur* naar een Windows Server omgeving.

## 2.5 Active Directory server rollen (§2.4.7, §2.3 en fractie §2.4.2)

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

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

## Hoofdstuk 3

# Modelvragen theorie: reeks B

### 3.1 Active Directory functionele niveaus (§2.4.3)

1. Geef de diverse *functionele niveaus* waarop Active Directory kan ingesteld worden, en welke beperkingen er het gevolg van zijn.
2. Bespreek van elk niveau alle eraan gekoppelde voordelen. Geef hierbij telkens een korte bespreking (*verspreid over de cursus !*) van ingevoerde begrippen.
3. Hoe kan men detecteren op welk niveau een Active Directory omgeving zich bevindt ?
4. Op welke diverse manieren kan men het functionele niveau verhogen of verlagen ?

### 3.2 Active Directory replicatie (§2.5)

1. Wat is de bedoeling van *replicatie* ?
2. Hoe wordt dit in Windows Server (ondermeer ten opzichte van NT 4.0) gerealiseerd: bespreek de verschillende *technische kenmerken* en *concepten* van Windows Server replicatie, en hoe men specifieke problemen vermijdt of oplost.
3. Welke toestellen repliceren onderling in een *forest* ? Welke specifieke gegevens worden hierbij uitgewisseld ?
4. Welke impact hebben *sites* met betrekking tot de replicatie van Active Directory gegevens ? Welke andere Active Directory aspecten worden door sites beïnvloed ? (§2.6.1)
5. Hoe wordt bepaald *tot welke site* computers, servers in het bijzonder, behoren ? (*laatste paragraaf §2.6.2 en fractie §2.6.3*)

### 3.3 Gedeelde mappen en NTFS

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

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

### 3.4 Machtigingen op bestandstoegang (§3.3)

1. Welke rol spelen machtigingen bij de beveiliging van bronnen ? Geef een gedetailleerd overzicht van het *algemeen* (op alle windows objecten toegepast) mechanisme van *machtigingen*.
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.
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 ?
4. Op welke *andere objecten* zijn machtigingen van toepassing ?
5. Wie is *in principe* verantwoordelijk voor het configureren van machtigingen ? Door welke instelling is dit zo vastgelegd ? Hoe kan ervoor gezorgd worden dat enkel *administrators* verantwoordelijk gesteld worden voor het configureren van machtigingen ?

### 3.5 Gebruikersgroepen (§4.2.2 en §4.2.3)

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

5. Op welke diverse manieren kan men het beheer van Active Directory objecten, specifieke attributen van groepsobjecten in het bijzonder, *delegeren aan niet-Administrators* ? Bespreek een aantal technieken om dit delegeren *zo eenvoudig mogelijk* uit te voeren. (partim §4.1.2, en §4.4.2)