# WMI

* Documentatie in subtak van MSDN Library (ook op test)
* Waarom? Snmp heeft weinig OS objecten. Altijd polling. Enkel naam waarde koppels
* Bij wmi kan agent ook melden aan consumer ipv enkel omgekeerd (polling). en methodes nu beschikbaar voor wijzigingen ipv hopen dat alles goed gedaan wordt.

## Architectuur

* Object georienteerd
* WMI klasse: deelaspect van het systeembeheer
* CIM repository: de databank. Bevat specificities van de klassen. De objecten zelf worden hier niet bewaard.
* Master agent => wmi service

1: intrageren met consumers uniform.  
2: verantwoordelijk alle interacties met providers.   
3: db enkel toegangelijk via dit.

* Beheersapplicaties => consumers. Doen beroep op wmi service via bv. Perl
* Via verschillende provider die verantwoordelijk zijn voor aantal WMI klassen.

1. Consumer wilt waarde raadplegen dus vraagt aan WMI service
2. Die vraagt aan db welke provider. Dan vraagt WMI service aan die provider info.

## Namespaces

* Root/cimv2 belangrijkst
* Namespaces goed voor beveiliging

## WMI CIM Studio

* Klasse zoeken via verrekijkertje. Niet gewoon intypen
* CIM\_ alle OS WIN32\_ dingen zijn hier aangepast
* Rechts initieel klasse info
* \_\_ voor system attributen
* Instances knop voor de objecten te zien
* Dubbelklik op een instance op alle attributen van dat object te zien
* Absolute padnaam in \_\_PATH
* Relatieve padnaam \_\_RELPATH  
  opbouw voor klasse: klassenaam(\_\_CLASS)  
  opbouw voor instantie: klassenaam.attribuut=x,attribuut2=y  
  opbouw singleton: klassenaam= @
* \_\_derivation geeft hele hierarchie terug
* \_\_dynasty geeft top terug
* \_\_superclass directe ouder
* Betekenis achterhalen van bv. 5 bij threadState => terug naar klasse en prop qualifiers checken => check values

## Qualifiers

* Rechterklik op klasse paneel
* Extra eigenschap toevoegen
* Waarde afhankelijk taalinstelling
* Klasse-/attribuut-/method-/methodeparameter qualifiers

Object(Klasse)Qualifier:

* Description
* Abstract(geen instanties), dynamic, simpleton welk type klasse
* Provider welke provider moet aangesproken worden voor klasse te manipuleren.

Property(Attribuut)Qualifier

* Description
* CIMTYPE Boolean, int ,..
* Write true dan wijzigbaar zonder methodes. Niet betrouwbare info dus
* Keys maakt deel uit van sleutel klasse.
* ValueMap table met toegelaten warden. Kan zijn dus dat indexering van values hierdoor anders verloopt dan 0..9 bv.
* Values informatievere interpretative van toegelaten warden. Indien ValueMap aanwezig dan is de valuemap de key en values de value, zoals in perl hash. Indien niet is het array

Methode qualifier

* Description
* CIMType / Values / Valuemap voor returnwaarde. Geen CIM vermeld => dan is het int (mogelijke range)
* Privileges methode enkel indien nodige rechten. Nodig voor bv te killen

Methode parameter qualifier

* Description / CIMtype / values / valuemap
* In / out in of uitvoer parameter.
* Optional
* ID geeft sequentie aan vanaf 0

# Methodes

Killen: instanties vragen \_\_process => methods => terminate executen

Create: op klasse en niet object. Kijk eerst naar nodige invoerparameters.

# Programmeren

Objectpad instantie opbouwen

* Loopen over property qualifiers en bijhouden wat keys zijn.

Values opslaan indien ValueMap aanwezig: Hash

Values opslaan indien geen ValueMap aanwezig: Array

Excel gebruiken: Extra namespace connecten

# Registry

* Verzameling 4 à 5 files met parameters
* Analoog aan .conf in linux
* Beschikbaar in StdRegProv
* Klasse zonder objecten. Enkel methodes voor API’s op te vragen (anders te traag)

# Belangrijke klassen

* win32\_localtime
* win32\_operatingSystem
* ip4routeTable
* StdRegProv
* Win32\_thread

numbering threads mag niet overlappen dus handle=>threadid, processhandle=>process id

toestand checken of priveleges veranderen of stoppen mogelijk als je ids weet

* win32\_process
* win32\_share

hier create opdoen indien je zoals ugent H: schijf deel van schijf te beschikking wilt

* \_networkadapter

Bv. kijken welke instantie de ethernet interface is

1. Kolommen checken: Zoek NetConnectionID=Ethernet
2. Dubbelclick hierop voor low level parameters.
3. High level parameters zoeken in \_networkadapterConfiguration. Dit heeft evenveel instanties.
4. Via associator klasse kijken welke de juiste is (check associatortablad)
5. Druk op properties en bekijk het IP adres

# Associator

Voor elke WMI klassenverbinding een associatorklasse. Maakt een doorsnedetabel. Elke verbinding tussen 2 instanties gerepresenteerd door 1 instantie in associatorklasse

Attribuut namen checken dooro links/rechts hoveren rond het knopje om de associatorklasse te bekijken.

Associatorklassen hebben samengestelde sleutel (2 attributen). Elk verwijst naar naar absoluut objectpad naar het object waarnaar gerefereert wordt.

Voorbeeld associator klasse: \_depedentService. Heeft 2 keys en attribuut over de connectie

Enigste ternair (3 keys): \_protocolBinding

# WQL

WMI klasse/object opvragen via wbemtest via predikaten op attributen (geen qualifiers)

Instanties van bepaalde klasse  
*select \* from klassenaam* altijd \* gebruiken

Mogelijkheden WHERE clausule:

* = != <> < <= > >= (not) LIKE IS (not NULL)
* alle backslashen bachslashen \\
* “ “ gebruiken bij strings
* \_\_THIS (verwijst naar 1 klasse)
* ISA ‘klassenaam’
* AND / OR / NOT

*WHERE \_\_CLASS = ‘klassenaam’* geen klassen afgeleid van de from klasse

*WHERE \_\_THIS ISA ‘klassenaam’* analoog?

*Select \* from win32\_networkadapter where netconnectionid = ‘Ethernet’*

*WHERE netw… like ‘%’* analoog aan \* in SQL

## Hoe joinen?

Instanties en dus geen klassen gebruiken

* REFERENCES OF {...} alle **instanties** van associatorklassen verbonden met doelobject (direct of indirect)
* ASSOCIATORS OF {...} alle **instanties** van reguliere objecten gelinkt aan doelobject (eindpunten associaties)
* “ “ gebruiken en altijd \\ best
* In de WHERE clausule van dit soort query mag geen AND staan, maar alles na elkaar

WHERE:

* AssocClass = klassenaam deze associatorklasse met doelobj verbonden
* ResultClass = klassenaam obj van deze klasse
* ResultRole = sleutelattribuutnaam (v associatorklasse) enkel objecten bekomen waarbij vermeld sleutelattribuut verwezen wordt naar een objectpad van eindpunt
* Role = sleutelattribuutnaam (v associatorklasse) enkel objecten via asssociaties bekomen waar sleutelattribuut verwezen wordt objectpad van doelobject
* Bovenstaande vooral voor recursie
* Geen aanhalingstekens
* Resultrole=Partcomponent dan is het een kind
* Resultrole=Groupcomponent dan is het een ouder
* Role=groupcomponent dan krijgde de kinderen ervan

*Associators OF {win32\_directory.Name=”...”} where resultclass = klassenaam*

Toch klassen gebruiken ipv instanties:

* SchemaOnly doelobj is een klasse
* ClassDefsOnly doelobject is instantie
* Where schemaonly

# Notification queries

1. Consumer interesse in een activiteit
2. Creeren objectinstantie in 1 van de subklassen van \_\_event via notification query
3. WMI service stuurt dat naar provider en blokeerd nu en wacht
4. Corresponderende voorwaarden vervuld => gedetecteerd door provider die dit opmerkte door te kijken bij elk van zijn bewerkingen. Anders geen processortijd gespendeerd aan monitoring.
5. Provider meldt dit aan WMI service. Die maakt event object die wordt opgeslaan in de repository
6. consumer wordt nu geactiveerd . hij zal nu object onderzoeken dat in repository zit

Registratie van een event

1. Wbemtest in administratormodus opstarten en connecteren met de namespace
2. Asynchronous aanvinken
3. Notification query klikken
4. WQL query ingeven op een \_\_EVENT subklasse

Klassen bekijken: Wmitools: \_systemclass > indicatedrelation > event > extrinsicevent > ...

DeviceChangeEvent elke parameter change bekijken van devices

VolumeChangeEvent (specifieker) kijken naar USB stick bv die wordt toegevoegd of verwijderd.

*Select \* from win32\_volumechangeevent*

Dan dubbelklikken voor informatie op object

Eventtype=2 wat betekent dat? => check qualifiers for properties bij volumechangeevent

Belangrijke events voor de test:

(Usb stick) volumes

RegistryEvent Verandering register

Win32\_systemtrace > \_processtrace   
telkens process aangemaakt of gestopt wordt(via subklasses of direct op ouderklasse). Indien enkel in bepaalde geinteresseerd dan ProcessName,ProcessID of parentProcessID gebruiken

Win32\_systemtrace > \_threadtrace telkens thread aangemaakt of gestopt wordt

*Select \* from WIN32\_processtrace where processname = ‘calc.exe’*

# Aggregeren

*Select \* from Win32\_ProcessTrace  
Where (ProcessName=’calc.exe’ or ProcessName=’notepad.exe’)*

Aggregeren: indien meerdere notepads.   
Info van alles in 1 keer. Creation/deletion  
Within 5 5 seconden wachten.   
*group within 5 by ProcessName*

Apart type:   
process gecreëerd of verwijderd: elk 1 apart object   
*Group within 5 by ProcessName,* ***\_\_CLASS***

Trigger na bepaald aantal (binnen de within timer): handig indien je spam wilt vermijden van iets  
 \_\_AggregateEvent: heeft attributen  
- Representative: verwijst naar TODO  
- En NumberOfEvents  
*Having NumberOfEvents>=5*

Indien die having getriggerd wordt dan toont hij ook alle vorige instanties van voor dat 5 seconden interval! Daarna blijft query verder checken. Updates pas in volgend object.

Welk process was gestart? => processName   
ook nakijken welke event via TODO

## Snapshots

Je kan dat niet op elk WMI object toepassen. Het moet aan dat basisarchitectuur systeem voldoen.   
Oplossing:

* als geinteressseerd consumer programma gewoon zoals normaal handelen zonder rekening te houden dat er geen provider is die er op kan antwoorden. Wel zeggen om de hoeveel tijd een snapshot
* WMI service zal zelf pollen naar veranderingen (snapshot mechanisme).
* Om de zoveel tijd dus snapshots nemen en snapshots vergelijken met elkaar.
* Indien verandering eventobject creeren en consumer op de hoogte brengen.

Zelfde query van hiervoor hermaken, ervan uit gaande da we snapshot moeten gebruiken:

* Klassen (\_namespaceOperationEvent \_classOperationEvent \_instanceOperationEvent) : zeker altijd subklasse gebruiken. *Select \* from InstanceDeletionEvent* ***OR*** *InstanceCreationEvent* kan echter niet. Dus toch ouderklasse gebruiken maar dan filteren.
* Via targetInstance enkel naar processen kijken en niet files da gemaakt worden ofzo.
* Altijd zo fijn mogelijk dus ook notepad vermelden. Kijken in win32\_process hoe da attr noemt: Name.
* Within hier heeft andere betekenis (snapshot timer)
* Enkel snaps indien het niet anders kan. Hij kan het op de test wel vragen

*Select \* from \_\_InstanceOperationEvent within 2  
Where (\_\_CLASS=’InstanceCreationEvent’ or \_\_CLASS=’InstanceDeletetionEvent’)  
and TargetInstance ISA ‘Win32\_Process’  
and (TargetInstance.Name=’calc.exe’ or TargetInstance.Name=’notepad.exe’)*

* As ge calculator opstart en binnen 2 seconden sluit zal je dus niks zien want snapshot detecteert dit niet.

## Periodieke events

\_\_TimeEvent genereerd periodiek events

\_\_eventGenerator configuratie voor de TimeEvent (om de 2 uur bv. of specifiek tijdstip). Niet in de klasse zelf maar eerst instanties maken (meest linkse icoon, rechtsboven)  
*- IntervalBetweenEvents*=5000 (ms)  
*- timerId*=w5  
- Dan op save duwen: vanaf nu om de 5 seconden een TimerEvent object.

~~Select \* from \_\_AbsoluteTimerInstruction mag niet~~  
*select \* from \_\_TimerEvent*

Specifieke timer  
*select \* from \_\_TimerEvent where TimerId=’w5’*

Hij zegt niet op test daje dat moet gebruiken maar ge moet er aan denken als iets periodiek gebeurd.   
kunt dit gebruiken indien snapshots niet kan.. maar moet je zeker zo hard mogelijk vermijden(kan test vraag zijn tho I guess).

# Standaard consumer programmas

* LogFile en NTEventLog(boeit niet)
* SMTPEventConsumer Stuur mail
* CommandLineEventConsumer commando

1. Query (dat op event reageert) eerst uittesten in wbemtest
2. \_\_EventFilter instance maken
3. Query attribuut: copy-paste volledige query in
4. queryLanguage = WQL
5. Name = F1
6. Save
7. Als die query getriggerd wordtt wil ik mail!
8. SMTPEventConsumer instantie maken
9. Name = m1
10. ToLine = [joris.moreau@ugent.be](mailto:joris.moreau@ugent.be)
11. **Message = %Representative.\_\_CLASS%**
12. **subject = %NumberOfInstances% %Representative.Name%**
13. smtpserver = smtp.ugent.be
14. FromLine = [joris.moreau@ugent.be](mailto:joris.moreau@ugent.be)
15. Save
16. Die 2 aan elkaar koppelen dus instantie maken Associatie klasse (elke keer je een wijziging maakt aan consumer of filter moet je een nieuwe koppeling maken)
17. \_\_PATH kopieren van de **consumer en filter**. Vanvoor telkens vervangen met  *\\.\*
18. \_\_filterToConsumerBinding instantie maken. Filter en consumer invullen met die abs. paden
19. Save

2de voorbeeld: Nu wil ik dat programma wordt afgebroken. Kijken naar ProcessStartName en ProcessName=’calc.exe’ in de query. processID en processName gaje daarvan nodig hebben.

1. Terug EventFilter maken en configureren
2. Terug SMTPEventConsumer maken en configureren (Message = %ProcessName% enkel dat is anders en geen subject in dit voorbeeld)
3. [cmd] Where taskkill dat Path kopieren
4. [cmd] Taskkill /f /pid wil je uitvoeren
5. Instantie maken van CommandLineEventConsumer
6. Name = c1
7. **CommandLineTemplate = taskkillPath /f /pid %ProcessID%** (als je process 0 killed is heel uw pc fucked. Dus opletten hiermee)
8. \_\_PATH kopieren van commandlineconsumer en terug *\\.\* in begin
9. filterToConsumerBinding instantie maken en consumer=commandlineconsumer en filter = eventfilter
10. en ook terug binding instantie voor de mail maken
11. \_\_indicationRelated (hier naar instanties kijken as ge al uw filters wilt zien)

ActiveScriptEventConsumer!! Reactie in 1 attribuut plaatsen en dat is perl script.(labo)

Active directory

Waarom? Beveiliging

Meerdere domaincontrollers: belasting verspreid en indien 1 wegvalt heb je nog andere.

Active Directory in: Ntds.dit =databank (OO)

Group policies. Niets met groupen te maken. Mechanismen dat moet gebeuren bij inloggen. Bv. Group policy da als gebruiker inlogged of pc start da hij privilege krijgt. Of bv die applicatie moet kunnen starten (anders wordt hij geinstalleerd).. of WMI script er nog bij dat dat enkel gebeurd indien geheugen groot genoeg is.

AD is goed uitbreidbaar. Extra klasse / attributen (her)definieren.

Les 4

## Adsiedit.msc (adsie edit)

Connection settings: select a well: default naming  
Computer: select type or domain : “satan.hogent.be”  
Advanced: username / passord: eigen gegevens ingeven

Dan op een objecet ergens rechterklik: properties voor te bekijken (lang wachten)

Relatieve distinquished naam: moet uniek zijn. Als je die allemaal aan elkaar kleeft krijg je Distinguished name.

Canonieke naam: niet belangrijk

ObjectGUID: telkens je nieuw object maakt

ObjectSid: elke computer domein user hebben er 1. Al de rest niet.   
nadeel: bij verplaatsing gebruikers: domein deel van SID moet veranderen

>Filter: uitvinken bovenste (zodat we alles zien)  
sIDHistory: accumulator oude SID’s.   
as ge gebruiker per ongeluk verwijderd: SID weg en kan je niet terugkrijgen(want ze moeten uniek zijn ook in de tijd). Dus als administrator users disablen ipv deleten

UserPrincipalName: username@domeinnaam

sAMAccountName: log je echt mee in. Beperking: 20 letters (oplossing 2 mappen met symbolische link: 1 voor username en 1 voor sAMAccountName)

## Dsquery

Enkel Microsoft

[cmd] dsquery op zoek gaan objeceten met bepaalde conditie

[cmd] dsquery \* DISTINGUISHEDNAME   
 DC=iii,DC=hogent,DC=be voor zoeken in alle domeinen

Verplichte Argumenten:   
 -limit 0 anders beperkt tot 100  
 -s satan.hogent.be welke server  
 -u “username”  
 -p “password

Optionele Argumenten  
 -attr attr1 attr2 enkel bepaalde velden (geen komma’s, gewoon spaties)  
 -filter (givenname=\*a) op basis predikaat tussen haken

Meerdere predikaten: (^&(...)(...)) of (^|(...)(...)) ^ om te escapen

# Ldifde

Algemener bruikbaar als dsquery, niet enkel windows

[cmd] ldifde

Verplichte opties  
 -d DC=iii,DC=hogent,DC=be waar kijken  
 -s satan.hogent.be server  
 -a “username” “password” met spatie tussen  
 -f con: analoog linux “>1”.

Optioneel  
 -l attr1,attr2 komma’s nu  
 -r (givenname=\*a)

# Schemagegevens

Terug connectie maken in ADSI edit. Maar TODO invullen

CN=Aggregate belangrijk voor programmeren

Comment wordt beschreven in CN=User-Comment en niet CN=Comment. LDAPDisplayname is daar Comment Bij comment was dat invoer

# Uuidgen

Getal van 10^40  
Die string moet je gebruiken als ID voor attribuut

# Oidgen

Als softwareontwikkelaar. Nummertje creeren met dat commando in de microsoft tak da je ni die shizzle in nederland moet kopen.

Week5

Dsquery \* -limit 0 –s satan.hogent.be –u “username” –p “test” cn=xxxx,cn=yyyy,dc=… -attr systemflags ldapdisplayname –filter (^&(objectclass=classschema)(systemflags^>=1)) | sort | nl

DefaultSecurityDescriptor default instellingen machtigingen!!

systemOnly betekent afblijven

isDefunct klasse verwijderen gaat niet => defunct aanzetten   
geen objecten kunnen nog gemaakt worden

ObjectClass klasses waar object attributen kan van overerven [tabel]

ObjectCategory Meest typische klasse waarvan object instantie  
niet altijd klasse zelf waar object type van is. Enkel bij user tho: Bij User krijg je OrganizationalPerson,Person,Top

objectClassCategory 1 reguliere klasse  
 3 hulpklasses (kunnen niet van afgeleid worden of objecten gemaakt worden)  
 4  
 0/2 (^| (objectclasscategory=0) (objectclasscategory=2)) geen instanties dienen als template waar anderen van kunnen afleiden

defaultObjectCategory voor bepaalde klasse, als nieuw object, objectCategory instellen met deze value

possSuperiors in welke soort container

wordt er in possSuperiors verwezen naar User?Dan kan je zeggen User object is container object ook al…

Abstract schema: spaart veel werk uit!!

possibleSuperiors / mandatoryProperties / OptionalProperties Acculuminatie van alle info van de overervingsklassen

User zoeken: combinatie 2 predikaten via AND

* objectclass=user alle objecten die van een klasse zijn van opgegeven klasse of afgeleid. Dus ook computers hier.
* Objectcategory=person. Maar dan krijg je ook alle andere persons.

Global catalog

* 1 tabel over sowieso **alle** klassen/objecten heen waarbij ismemberofpartialattributeset=TRUE
* zelf **kiezen** welke attributen(kolommen)

via dns serverrecord vragen bij inloggen waar global catalog staat.

Global catalog maken:

Van geen domaincontroller een global catalog maken: dan ist kapot.

Adsiedit: configuration > CN=Sites > CN=Default-First-Site-Name > CN=Server > CN=LUCIFER > CN=NTDS Settings > properties vragen > options: daarvan laagste bit (domaincontroller is globalcatalog. As ge da op 0 zet stop ie ermee en smijt hij table weg)

Adsiedit: configuration > CN=Sites > CN=Default-First-Site-Name : CN=NTDS Site Settings > properties > options: 5de bit zegt dat group caching enabled staat

Examen: Laat programma lopen op global catalog: poortnummer veranderen en aan programma niks veranderen.

Examen: Wat voor keuzes moet je maken bij installeren server: maak er global catalog van ofniet. Vragen commentateren. Alles hiervoor is antwoord.   
Samenvatting online ergens moet full of shit zijn want hij ziet veel fout antwoord.

Maakt er geen domaincontroller van maar add gewoon features:  
 Server manager > manage > add roles & features > server role: Active Directory Domain Services.

Voor domaincontroller te maken (don’t)  
dcpromo (domaincontroller promotion)

Als dns niet dynamisch updates toestaat zal dcpromo niet lukken

::::::::::::Examenvraag oplossing:::::::::::::

Dcpromo 2 opties:   
/answer bestandsnaam installatie dc beetje automatiseren. Anders veel om de zoveel tijd op ok duwen tijdens installatie.

/adv (advanced) nog nuttiger, als je nieuwe maakt. Database bestaat nog niet. Onmiddelijk na hij dc geworden is begint hij te repliceren (vraagt heel wa gb’s) dus kan network platleggen. En zorgt voor langdure syncronisatie. Daarom van domaincontroller soort backup maken, dat op harde schijf plaatsen van toestel da je wilt promoveren. Dan kan /adv al die backup gegevens inladen. Ook al zijn die gegevens verouderd. Dan nog syncronisatie process voor wa te hernieuwen maar is niet zo veel.

Er zijn voor/nadelen aan meerdere domaincontrollers te maken. Kunt ook terug aan/af zetten (reversible process). Niet tte veel (belasting) maar genoeg (reservefactor, zodat uw systeem niet zonder domaincontroller valt)

Korte namen gebruiken (beperkt tot 15 karakters)

Hij vraagt ook waar hij die file moet plaatsen. Performantiegezien best op gescheiden disken.

Dan fout meestal op dns.

Logfiles checken bij mislopen. Maar beter op voorhand alle mogelijke criteria uitzoeken die kunnen misgaan vo geen tijd te wasten: [cmd] dcdaig/c heel belangrijk

Grep –I failed dcdiag.txt | nl veel te veel txt dus zoeken op failed

Fouten die mislopen moeten allemaal opgelost worden of later zelf al is dc gemaakt kunnen problemen optreden bij upgrades te doen.

Verwijderen van dc:

dcpromo

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

Bs3 les 6

MSDSbehavior version (domein- of forestniveau)

* Hoger = beter
* Bepalen AD functionaliteit

Examen: samenvatting geven van recente versies ten op zichte van oude versie. (15 tal features, waar die horen kwa functioneel niveau boeit niet, wel kunnen opsommen en kunnen uitleggen) (p 46-48.5)  
Wat je wel moet weten is gevolg van functioneel niveau en wat gebeurt ajet verhoogt

* Hardware die aangekocht was kan useless worden door een upgrade (CD rom’s bv). Meestal is upgraden dus altijd interessant zolang hardware er ondersteuning voor biedt.

Domein niveau

1

* Vertrouwensrelaties: master slave concept. Master veranderd dingen en de rest luistert ernaar.
* Zelfstanding SPN objecten maken: wordt in bulk altijd 500 objecten aangevraagd als er nog maar 100 overschieten
* Configuratie groepen (schikken)
* sIDHistory: zodat je machtigingen niet verliest bij veranderingen

2

* bij elke upgrade best mogelijk schemaaanpassingen nodig. Active directory in bulk importeren Dir \*.ldf /0-s
* Nieuwe gebruikers komen in Users container als je niet zelf redirect. Maar geen goeie folder want bv. Beter om studenten container te maken. Alle nieuwe gebruikers studenten en Class is nu organizational unit ipv container. Verschil: **group policies** kunnen worden toegepast op alle objecten die hierarchisch in container zit, maar niet op container die geen organizational unit is. Met redirusr/redircmp default locatie dus omleiden.
* Domeincontroller kan van naam veranderd worden zonder tijd te verspillen met heropstarten
* Vroeger inloggen niet mogelijk zonder global catalog. Nu wel (caching)
* Filtering group policies: group policies niet van toepassing op groepen, wel op takken. Maar noobs hebben dat niet door dus microsoft heeft gezorgd da je kan filteren. Bv.“user X in bepaalde tak kan dat niet doen **behalve** **als** hij lid is van de **groep** Y”. Nadeel: moeilijk te debuggen
* Filteren op WMI scripts. Debugging nog moeiiljker. Opstarten van een group policy hangt af van een WMI script dat uiteindelijk ja of nee zegt. (bv. Mag enkel group policy starten dat hij enkel excel kan openen of icoon zien als hij genoeg geheugen heeft en sterke CPU)

3

* Langere (galoisveld) sleutels (encryptie)
* Fine grained password policies: hoe groot moet paswoord zijn, mag je paswoord hergebruiken, wanneer vervangen. Oorspronkelijk op domain niveau instelbaar, niet op user/group niveau. Nu wel, want admin heeft strictere regels nodig. En anders gaan mensen kneuten da restricties voor hun te hoog zijn.
* DFS replication: mensen willen dat hun desktop wordt opnieuw weergegeven bij heropstarten,...

Forest functionele niveau’s

2

* Bij object creatie zeggen. Objectclass attribuut aanvullen met lijst van hulpklasses
* Dynamische objecten. Zeggen dat object mag verwijderd worden op bepaald tijdstip. Handig voor DHCP/DNS op te kuisen.
* Global catalog word ni telkens van scratch opgebouwd en ge replicieerd aje u veraznderd van gedacht van welke tabellen enzo je wilt
* Read only controllers
* Gans object moet gerepliceerd worden naar andere controllers bij 1 attribuut wijziging. Nu enkel atomaire aanpassingen repliceren.

3

* Enkel interessant bij read only domein controllers
* Sommige attributen mogen niet gekopieerd worden naar read only domein controllers
* En sommige moeten gecached worden
* Site covering probleem: als je domeincontrollers en verschillende sites hebt. Moet bij inlog process altijd domeincontroller aanwezig zijn. DC weet zelf voor welke site hij verantwoordelijk is anders verwijst hij door. Maar wanneer in een domein controller read only stond dan bug. Dan zei degene da moest doorgeven dat er geen was en dan nam die domeincontroller de inlogverantwoordelijk over

4

* Thombstone objects: Kunt dingen zogezegd uit vuilbak halen als je per ongeluk objecten verwijderd hebt

# Vertrouwensrelaties

Als je 2 domeinen hebt die beheert moeten worden ma als gebruiker wil je geen last da ze verdeeld zijn.

Tussen 2 domeine vertrouwensrelatie: Als iemand inlogged op de ene dan mag die user account gaan opvragen in ander domein en opnemen in uw toegangsticket. En sID’s van tweede domein zorgen ervoro da ge in eerste domein machtigingen ook zult krijgen.

Les gemist 5/11

PowerShell

* Kunde zelfde mee doen dan perl kwa COM betreft
* Type libraries inladen gaat niet
* Handig: completion gebruiken
* Vooral belangrijk hoe help werkt
* Variabele in script pane komt automatisch in run pane. Blijven erin zolang powershell runned
* Get-help in aparte powershell met | more
* Voor veel commando’s alliasen
* $var=commando output onthouden dan $var typen voor output
* $var. (punt) typen en dan hebje extra opties. [met (command). Notatie komter niet alles in]

# COM object initialiseren via progid

* Rechtsboven commands
* name: new-object.
* Daaronder comobject: Excel.Applicatiion
* Dan kunje da naar linkerdeel doen
* In var steken $excel = [generated stuff]
* .count enzo op doen of .workbooks
* $wb = $excel.Worbooks $wb.count
* $fso.Drives.count
* $folder=$fso.Get-Folder(“.”)
* Write-Host interessantst (naast elkaar)
* get-command -Noun "date\*"
* $dag=get-date $dag.DayOfWeek

# Uitvoer verwerken

* Help sort
* Help sort –Parameter des\*
* $all | sort –Descending –property version sorteren op version
* Help select –parameter \*
* $all | sort | select -first 10
* $all | sort | select –index 1,5,7
* -property voor te selecteren welke output je wilt
* | select –property version
* $a1=$all | select – first 1
* Get-command | select –first 10 | select \* alles van die 10 tonen. Niet enkel wa hij kiest

## Foreach

* $proces=Get-process
* $proces | select Name,threads
* $proces | foreach{$\_.Threads} alle details v alle threads
* proces | foreach{$\_.Name , $\_.Threads.count} per process hoeveel threads
* proces | foreach{$\_.Name + “ “ + $\_.Threads.count}
* geen completion bij foreach ajet op variabele zoals hierboven doet wel als (get-proces)| foreach

## select+expression

Get-service | select –f 50 | select Name,@{Name=”Aantal”;Expression={$\_.DependentServices.count}}

In powerpoint staat dependent fout geschreven

## Where

Alle objecten waarvoor het juist is

* zie table

# WMI

Belangrijk. (zeker vanaf $location=… slide)

Les gemist

File sharing

# Eerste manier: file explorer

map kiezen > properties > Sharing > advanced sharing knop

1. share this folder aanvinken > naam kiezen waaronder map beschikking naar buitenwereld toe > “permissision” voor 2 soorten afscherming + Caching keuzes knop
2. Permissions: Meestal volledig openstellen  
   Change en full control: write mogelijkheden. Maar ook geen beperkingen op mappen eronder.  
   Meestal zetjet op full control
3. Caching: 2 voordelen: \*Wanneer IO gedaan is wordt ook lokaal gesaved. (betere performantie)  
    \*als network verbonden wordt kan er nog aan gewerkt worden  
   standaard: enkel lokaal gespecifieerde bestanden. Of “niks” of “alles” kiezen
4. Limit number users: voor fabriekenten content te stellen me hun X aantal licensies

# Tweede manier: Console

Fsmgmt.msc

* In sessions aan server zijde zieje wie eraan gekoppeld is / welke bestanden open staan /
* Right click shared -> new share of shares bekijken: zijnr al een aantal standaard. Letter disk + $ (=onzichbaar voor buitenwereld). Maar als admin zieje alle disken van andere toestellen door die shares
* [cmd] cmap van andere computer bekijken [\\computernaam\c$](file:///\\computernaam\c$)
* [\\computernaam\c$\emacs\.emacs](file:///\\computernaam\c$\emacs\.emacs) bepaalde file
* Ipv computernaam kon ook ip adres
* IPC$ voor het namedpipe mechanisme op andere machines
* Voor new share: helsaan op next duwen. Dus niet interessant maar enkel vo te checken wie ervan gebruik maakt enzo die console

# Alternatieve manier

Net share shares bekijken

Rmtshare [\\belial](file:///\\belial) shares op belial

# Nog een andere manier

Fsrm.fsc

File screening management: “iemand die inlogged met naam X kan enkel dat en dat doen”

Quota management is belangrijker: moogt van uw baas maar bepaald aantal disk innemen. Mensen blijven ma shit op hun disk plaatsen. Dus hier kunje ne rem op hun misbruik zetten. Kijken of drempel overschreden wordt. Ofwel niet meer mogelijk dan ofwel foutbericht. 2 onafhaneklijke quote mechanismen.

Disk>properties>quota (is het eerste mechanisme)

In die console het tweede

# Server manager

File and storage servies aanvinken: resource manager / namespaces moet aanstaan

Enable access based enumaration: belangrijk: aje ne share op een hoger niveau zet zieje ook alle andere mappen ook al dajer ni inkan. Maar met deze optie aan te zetten zie je die submappen niet meer. Dus dan moetje niet meer voor iedereen aparte share maken en dus iedereen in 1 submap van 1 overkoepelende share.

# In command prompt

Net share [\\belial\emacs=c:\emacs](file:///\\belial\emacs=c:\emacs) de emacs share op belial instellen op de emacs map op de c schijf

Dir [\\belial\emacs](file:///\\belial\emacs) die kan daar nu aan

[ugent cloud programma voert dit uit]  
met drive letter daje moeten specifieren wel  
 Net use g: [\\belial\emacs](file:///\\belial\emacs)

Net use i /del het loslaten

Net use \* [\\belial\emacs](file:///\\belial\emacs) de laatst mogelijke gebruiken (maar niet goed want ge onthoud best welke drive letter ge gebruikt hebt)

Pushd Net use [\\belial\emacs](file:///\\belial\emacs) (ga naar andere map en kies vrije letter) (niet zeker ofk het juist commando heb met het stuk na pushd, niet gezien voor hij commando losliet ☹ )

Popd terugkeren en extra drive letter wordt ook losgelaten

# Regedit

Shares in map: LanmanServer > Shares

Een share is een extra sleutel daar

Aje als admin ne fileserver moet overzetten. Dan gewoon daar die registry tak overzetten. (right click op shares > export .. dan met dat reg bestand overzetten). In security tak eronder zit wie wat kan doen met die share.

# machtigingen

Rundll32 veel sneller dan gewone interface

Bestand in windows is niet meer dan object: met attributen (inhoud, machtigingen,..)

System (security) access control lijst: voor alles te beginnen loggen of bepaalde dingen van bepaalde personen (opletten voor performatieverlies)

Discretionary access control list = control list (makkelijker uitspreken) = welke acties personen mogen doen