Windows Werkcollege 2

# Algemene Windows ***Instellingen***

## PC Naam

Op het eerste zicht zou je denken dat je PC naam niet al te veel uitmaakt, maar dat is niet waar. Buiten het makkelijk kunnen identificeren van welke PC’s er in je netwerk zitten is dit de manier waarop je domain controller jouw PC kan identificeren (zie 1.3). Om ervoor te zorgen dat er geen overlappingen zijn (alsook problemen op je domein) moet je er voor zorgen dat deze namen uniek zijn.

Bij elke Windows installatie wordt er gevraagd te kiezen voor een PC naam. Je kan deze op verschillende manieren veranderen.

A screenshot of a computer

Description automatically generatedRechtermuisklikken op je startknop opent een overzicht van verschillende tools en opties die je vaak nodig hebt in Windows. We zullen in dit werkcollege enkele van deze tools dichterbij bekijken.

Om de PC naam aan te passen kan je onder het kopje System Settings uit het menu kiezen, waarna je System en daarna About kiest. Daar bevindt zich de ‘Rename this PC’ optie.

A close up of a logo

Description automatically generatedOm iets sneller te zijn kan je ook zoeken naar “about” in de zoekbalk. Een andere optie is om de snelkoppeling ⊞ Win+Pause te gebruiken.

|  |
| --- |
| **Opdracht:**  Verander de naam van je VM naar <voornaam>-<verkorte familie naam>-VM |

## Werkgroep

Werkgroepen zijn verzamelingen van pc’s binnen een bepaald netwerk.

PC’s binnen éénzelfde netwerk kunnen verschillende bronnen delen met elkaar zoals printers, scanners, folders en bestanden. Werkgroepen zorgen ervoor dat dit duidelijker getoond wordt aan de gebruiker, maar bevatten voor de rest geen extra meerwaarde. Er is geen enkele vorm van controle en iedereen kan in een werkgroep komen.

## Domein

Een domein is ook een verzameling van computers, maar deze worden beheerd door een Domain Controller. Dit wil zeggen dat wanneer je je PC deel laat uitmaken van een domein, je de controle overdraagt aan de Domain Controller. Dit kan gaan van internetregels, het instellen van een wallpaper, tot het installeren van software en het wijzigen van PC instellingen en accounts.

Aangezien we een naam nodig hebben voor ons domein zullen we een DNS server moeten toekennen die de naam koppelt aan het IP-adres.

|  |
| --- |
| **Opdracht:**  Surf voor het veranderen van je DNS naar <http://desktoposisawesome.be> je zal merken dat deze site niet bestaat. Wanneer je na het veranderen van je DNS hier opnieuw naar surft zal dit weldegelijk een resultaat geven. |

Afbeelding met tekst, schermopname, Lettertype, nummer

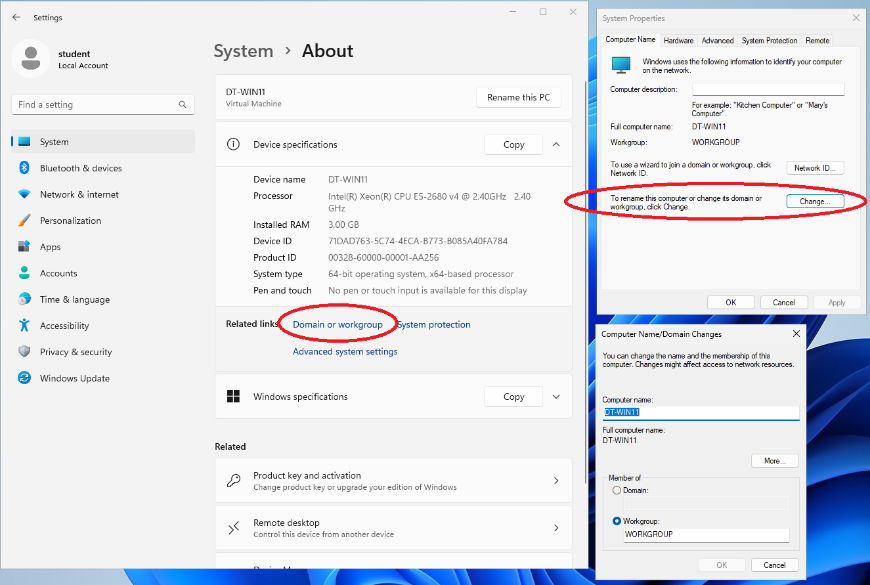
Automatisch gegenereerde beschrijving

Om dit te doen rechtermuisklik je op de startknop en selecteer je ‘Network Connections’. Kies daarna voor ‘Ethernet’. Daar kan je de DNS server assignment aanpassen. Kies om het manueel in te stellen en doe dit voor IPv4.

Preffered DNS Server: 192.168.1.231

Alternate DNS Server: 10.2.10.28

We hebben gezien waar we onze computernaam kunnen veranderen (zie 1.1) onder de “Device specifications” staan er related links. Hier kan je de optie terugvinden om je domein of werkgroep te veranderen (“Domain or workgroup”)



|  |
| --- |
| **Opdracht:**  Voeg je VM toe aan het domein: desktopos.local |

Om in te loggen heb je een Active Directory account nodig die draait op onze Domain Controller. Gebruik volgende gegevens om je toe te voegen aan het domein:

Gebruikersnaam: domainjoiner

Wachtwoord: Student1

Nadat je PC is toegevoegd aan het domein kan je je inloggen op je vm met volgende credentials : Gebruikersnaam: **desktopos.local\domainstudent** Wachtwoord: **Student1**. Merk op dat er dus een nieuwe gebruiker is aangemaakt en dat je dit account moet gebruiken om op het domein te werken.

In tegenstelling tot een werkgroep is een domein dus wel beveiligd en kunnen er folders, bestanden en andere resources gedeeld worden op een beveiligde manier.

# Beheer van Windows

In hetzelfde venster waar je je DNS hebt veranderd, kan je het IP-adres, het subnet mask en de default gateway aanpassen.

|  |
| --- |
| **Opdracht:**   * Zoek in je CLI naar je subnet mask, default gateway en IP (zie werkcollege 1). * Zorg ervoor dat deze statisch in Windows worden geplaatst en niet dynamisch.   Tip: Je zal moeten inloggen met een admin account. In dit geval is dat student dat een lokaal account is. De username die je moet ingeven is dus **.\student** met wachtwoord **Student1** |

|  |
| --- |
| **Opdracht:**   * Controleer met het commando ping in de cli wat het IP-adres is waar [desktoposisawesome.be](http://desktoposisawesome.be) op wordt gehost. |

## Task Manager

Zoals we al gezien hebben in werkcollege 1 kan je de ‘Task Manager’ openen via de shortcut Ctrl-Shift-Esc. Personen die geïnteresseerd zijn in het weten waarom hun PC zo traag loopt, of gewoon interesse hebben om meer in detail te kijken, kunnen dit hier doen.

Microsoft heeft redelijk wat nagedacht over gebruiksvriendelijkheid en heeft ervoor gezorgd dat leken hier wat basistaken mee kunnen verrichten.

De Task Manager bestaat uit een aantal menuitems:

#### Processes

Deze bevat een lijst van alle draaiende processen op je computer. Alhoewel dit op de Virtuele machine anders is, is deze normaal verdeeld in drie verschillende delen. Apps, Background processes en Windows Processes.

Afbeelding met tekst, nummer, software, Lettertype

Automatisch gegenereerde beschrijvingJe kan in een oogopslag kijken naar de load die ze plaatsen op je CPU, je geheugen, je schijf alsook het netwerk. Als je niet weet wat een proces juist doet (of als je deze niet vertrouwt, mogelijk virus), kan je er op rechtermuisklikken en ‘Search online‘ selecteren, om online te zoeken naar wat het juist doet.

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

Als gewone gebruiker heb je hier niet veel aan, maar je kan ook een dump file maken van een bepaald proces.

#### Performance

In de Performance tab kan je verschillende diagrammen terugvinden die een representatie zijn van het systeem gebundeld met nuttige informatie.

* **CPU**: toont het huidige processorgebruik. Indien dit tegen de 100% zit dan ben je momenteel programma’s aan het draaien die processor-intensief zijn. (bv. Je bent ingewikkelde berekeningen aan het uitvoeren). Wanneer je het idee hebt dat je computer niet meer goed reageert op je input, kan je hier eens gaan kijken of de processor misschien een tijdsintensieve taak uitvoert. Soms kunnen programma’s die crashen de processor zo goed als 100% bezig houden zonder effectief iets uit te voeren. Je kan het processorverbruik van die programma’s dan weer bekijken in het tabblad “Processes”. Een proces dat niet meer reageert en veel geheugen of CPU-tijd in beslag neemt kan je best afsluiten.

|  |
| --- |
| **Opdracht: Vul in** |
| Kloksnelheid: |
| Aantal processen: |
| Aantal Threads: |

* **Memory**: toont de hoeveelheid RAM-geheugen dat momenteel gebruikt wordt. Als het geheugen dat vrij is (onder Available) 0MB benadert, dan zal de computer ook merkbaar trager gaan werken. Er is dan immers niet voldoende RAM-geheugen beschikbaar om alle programma’s die openstaan te kunnen draaien. Windows (en ook andere besturingssystemen) zal dan delen van het RAM-geheugen gaan wegschrijven naar de harde schijf om toch bepaalde programma’s in het RAM-geheugen te kunnen laden. Het geheugen op de harde schijf noemt men dan virtueel geheugen of “virtual memory”, omdat het niet echt RAM-geheugen is maar enkel dient als tijdelijke opslagplaats voor gegevens die momenteel niet in het RAM-geheugen passen.

Onder Committed kan je zien hoeveel virtueel geheugen er gebruikt wordt. Wanneer je merkt dat een computer zeer vaak geen geheugen over heeft, kan je best extra RAM-geheugen installeren. In Windows wordt het virtuele geheugen (op de harde schijf) opgeslagen in een bestand pagefile.sys, dat je meestal vindt op de C:\ schijf. (verborgen omdat het een systeembestand is)*.*

*Cached Memory* geeft aan hoeveel geheugen de systeem processen aan het gebruiken zijn.

Zoals eerder aangegeven is de kernel de echte kern van het besturingssysteem, waarin alle laag-niveau functionaliteit (zoals aanspreken van de hardware) zit ingebakken. Paged Pool stelt het virtuele geheugen voor dat de Kernel gebruikt, terwijl de Non-paged Pool het effectieve geheugen is dat de Kernel op dit moment gebruikt.

#### Good to know (Niet te kennen leerstof)

**Opdracht:**

* Verklaar waarom de schijfactiviteit stijgt wanneer het geheugen dreigt vol te zitten.
* Gebruik Run (⊞ Win +R ) en geef dxdiag in als commando. Bekijk hierin de grootte van de pagefile.
* **Schijf**: toont de activiteit van je logische schijven. Als je een groot bestand kopieert zal je merken dat de waarden omhoog zullen gaan. Als het kopiëren langer duurt dan verwacht kan je eens kijken naar de snelheid waarmee dit gebeurt. Dit kan een eerste aanwijzing geven of er al dan niet iets mis is.

|  |
| --- |
| **Opdracht:**  Start enkele programma’s op zodat je ziet dat het RAM-geheugen gebruik stilaan omhoog gaat. Zet zo veel mogelijk programma’s open tot je over de grens van het fysieke geheugen gaat (waarde *Total)*. Je zal merken dat de computer nu regelmatig processen op de harde schijf wegschrijft (in zogenaamde pages) . |

* **Ethernet**: hier kan je te weten komen wat je IP-adres van elke adapter alsook wat het binnenkomende en uitgaande netwerkverkeer van deze adapter is. Aangezien je werkt met Remote desktop zal Sent sowieso niet 0 zijn, maar fluctueren. Wat je wel manueel kan testen is de Received. Als je stil staat met je muis zal je zien dat dit 0 wordt, als je beweegt gaat dit omhoog. Dit is logisch aangezien je de beweging van de muis (de cursor positie) moet doorsturen. Je kan nog verder in detail gaan door te rechterklikken en View netwerk details te selecteren.

Afbeelding met tekst, nummer, lijn, Perceel

Automatisch gegenereerde beschrijving

* De **Resource Monitor**, die je kan open via de 3 puntjes in de rechter bovenhoek te selecteren, laat toe om eventueel nog verder in detail te treden. Zo kan je per proces details weergeven bv. wat het inkomende en uitgaande netwerkverkeer is. Het voordeel is dat deze monitor bijhoudt hoeveel resources het proces in beslag neemt vanaf het moment dat je de gegevens bekijkt. Daarbij kan je per proces makkelijk kijken met welk extern IP-adres het proces verbonden is.

Afbeelding met tekst, software, Multimediasoftware, Computerpictogram

Automatisch gegenereerde beschrijving

#### Good to know (Niet te kennen leerstof)

#### App History

Hier kan je van elke Windows Store App de gebruikte resources opvragen. Zo kan je te weten komen welke app een enorm aandeel heeft aan het trager maken van jouw PC.

#### Startup apps

Microsoft heeft duidelijk geluisterd naar de community en heeft, t.o.v. vorige versies, het uitzetten van starttaken veel makkelijker gemaakt. Dit zijn taken die automatisch starten bij het opstarten van het besturingssysteem. Hier wordt ook een indicatie gegeven hoeveel vertraging ontstaat bij het opstarten van de computer door die bepaalde taken.

#### Users

Hier kan je voor elke gebruiker zoeken hoeveel processorkracht, geheugen, schijf en netwerk resources hij of zij gebruikt. Je kan voorhebben dat een student i.p.v. zich af te melden Windows locked en dat hij, wanneer een andere student zich inlogt, op de achtergrond allerlei processen nog draaiende heeft zodat de PC veel trager is dan verwacht. Als je genoeg rechten hebt kan je de andere gebruiker uitloggen door te rechtermuisklikken en ‘Sign Off’ te kiezen.

|  |
| --- |
| **Opdracht:**  Connecteer RDP via je 2 accounts (zowel domainuser, alsook Student) en bekijk de Users tab. |

#### Details

Deze tab geeft per proces informatie weer. Je kan hier verschillende zaken wijzigen zoals de prioriteit van het proces. Je zal in het Hoorcollege geleerd hebben hoe CPU verdeling werkt en op wat het besturingssysteem zich kan baseren om te bepalen hoeveel processortijd hij gunt aan één bepaald proces.

Windows is Priority based, wat wil zeggen dat hij een proces met een hogere prioriteit meer frequent en langer aan de beurt zal laten dan een proces met mindere prioriteit.

Afbeelding met tekst, schermopname, nummer, Parallel

Automatisch gegenereerde beschrijving

#### Good to know (Niet te kennen leerstof)

Merk op dat elk proces net zoals in Linux zijn eigen ID heeft, het Process ID (PID).

In cmd kan je de processen bekijken d.m.v.. het **tasklist** commando. Je kan deze dan afsluiten door het **taskkill** commando.

|  |
| --- |
| **Opdracht:**  Gebruik in de cli de commando’s **tasklist** en **taskkill** om een bepaald proces te beëindigen. (zorg ervoor dat dit een proces is dat niet belangrijk is voor het besturingssysteem) |

#### Services

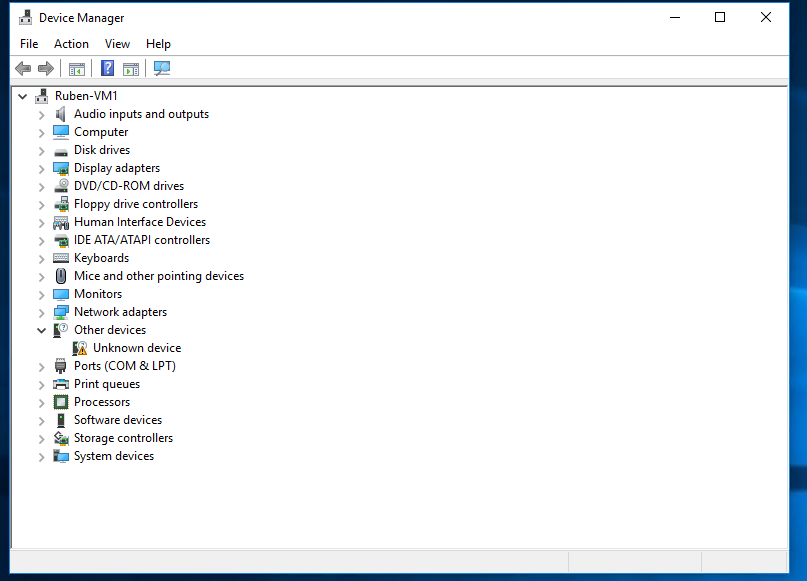
Hier kan je de verschillende Services. Opstarten, afsluiten of herstarter. Als je meer wilt dan dat moet je verder gaan naar Services buiten de Task Manager. Dit kun je makkelijk door te rechterklikken en Open Services te selecteren.

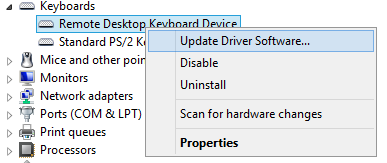
## Device Manager

Je kan de Device manager openen door te rechtermuisklikken op de startknop en Device Manager te kiezen.

#### Good to know (Niet te kennen leerstof)

Je kan dit commando ook opendoen door via run (rechtermuisknop op het start menu of via ⊞ Win  + R) te gaan en devmgmt.msc in te geven. Alhoewel we hier niet verder op in gaan kan dit oproepen via run voor de meeste tools.

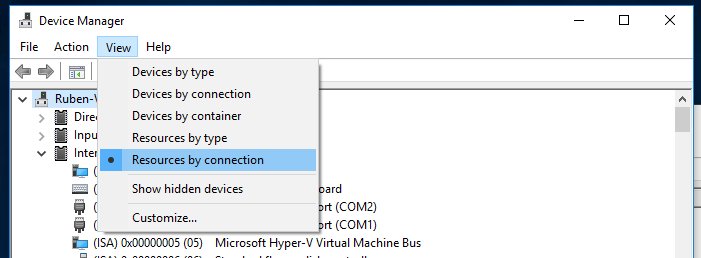
Je kan hier alle hardware bekijken, zoals aangesloten harde schijven, dvd, keyboard, muis, netwerkadapter, geluidskaart, ... Ook minder bekende apparaten (of delen van je computer) zoals de chipsets die op het moederbord voorkomen kan je hier bekijken. Wanneer er problemen zijn met één van de aangesloten apparaten is dit typisch de eerste plaats waar je gaat kijken om de problemen op te lossen. Dat kan dikwijls (indien het om een software fout gaat) door het herinstalleren van een driver. Je klikt daarvoor rechts op het apparaat en kiest “Update Driver Software” (Stuurprogramma’s bijwerken). Ook dit kan uiteraard enkel als je administrator van de computer bent.



Je kan als er sprake is van een unknown device gaan naar de Properties en kijken naar de Details om daar het hardware id op te vragen. Dit is de makkelijkste manier om te weten wat voor hardware het is en naar welke drivers je moet zoeken. Veel apparaten bevatten extra informatie over hun werking, eigenschappen, mogelijkheden, ... Deze extra informatie kunnen we aflezen in het tabblad *Details.*

|  |
| --- |
| **Opdracht:**  Gebruik Device Manager als admin en controleer of de Display Adapter geüpdatet is naar de laatste versie. |

Je kan je View aanpassen zodat je i.p.v. ‘by type’, ‘by connection’ je apparaten toont.



#### Good to know (Niet te kennen leerstof)

**Opdracht:**

* Wat is de provider van het toetsenbord en van de muis? Probeer in het Details tabblad van enkele apparaten meer te weten te komen over de eigenschappen.
* Gebruik Run (⊞ Win +R ) en geef msinfo32 als commando. Bekijk hierin de IRQ kanalen

#### Good to know (Niet te kennen leerstof)

## Microsoft Management Console (MMC)

Microsoft gebruikt voor de configuratie van heel veel instellingen de zogenaamde Microsoft Management Console. Deze Management Console is een soort raamwerk waarin je plug-ins kan laden om bepaalde zaken van je computer te configureren.

Je kan de Microsoft Management Console openen door Start te selecteren en dan **mmc.exe** te typen in het zoekveld. Ook om andere applicaties op te starten kan je gebruik maken van dit handige zoekveld. Je hoeft dan niet heel het menu af te lopen om de nodige applicatie op te zoeken. De voorwaarde is wel dat je de naam van de applicatie juist ingeeft. Op onderstaande afbeelding wordt een geopend MMC getoond:

Graphical user interface, application

Description automatically generated

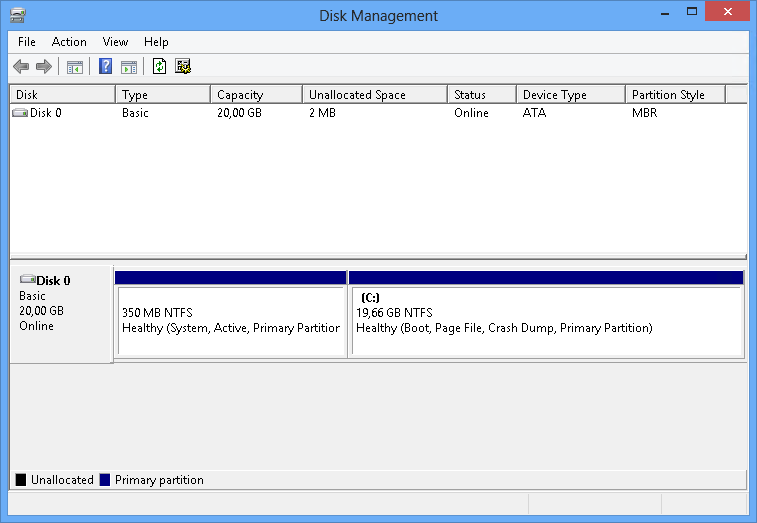
De MMC kan verschillende plug-ins inladen, die op hun beurt toegang geven tot configuraties. Uiteraard heb je voor veel zaken administrator rechten nodig, maar toch kan je ook een heleboel informatie lezen enkel door de plug-in te laden en door de info te bladeren.

|  |
| --- |
| **Opdracht**:  Laad enkele plug-ins in door File -> Add/remove Snap-in te kiezen en daarna enkele plug-ins toe te voegen. Kies bijvoorbeeld de *Device Manager* en *Services* Snap-ins. Kies telkens *Local* wanneer gevraagd wordt van welke computer je deze snap-in wil openen. Je kan i.p.v. je eigen toestellen een ander toestel op je netwerk kiezen en gebruik maken van Remote Management. |

## Disk Management

In een Windows 11 systeem (en ook andere Windows varianten) wordt de harde schijf aan de hand van volumes ter beschikking gesteld aan gebruikers.

In de Disk Management Tool kan je de opdeling van je harde schijf in partities bekijken en wijzigen. Aangezien deze tool enkel voor administrators beschikbaar is, kunnen we deze niet bekijken op de computers van het schoolnetwerk, maar kijk gerust op je virtuele machine. Hieronder wordt een voorbeeld getoond van de Disk Management Tool die de verschillende harde schijven van het systeem weergeeft:



A screenshot of a computer

Description automatically generatedVoor de gewone gebruikers van het systeem is het bestandssysteem wel zichtbaar via Windows Explorer (Verkenner). Hierin kan je niet de fysieke opdeling van een harde schijf in partities bekijken, maar krijg je wel een zicht op de inhoud van de verschillende volumes. Een volume (bv. C:\ of D:\) is een letter die gekoppeld wordt aan een bepaalde partitie, een optische drive, een externe harde schijf of extern opslagmedium in het algemeen. De C:\ schijf is meestal de zogenaamde systeemschijf, waarop belangrijke systeembestanden worden geïnstalleerd die nodig zijn voor het correct werken van het besturingssysteem.

Elk volume heeft een aantal tabbladen die informatie en mogelijkheden van de schijf weergeven. Afhankelijk van wat voor apparaat achter de volumeletter zit (bv. Harde schijf heeft meer mogelijkheden dan optische drive). We bekijken deze tabbladen voor de C:\ schijf. Je kan dit opvragen door te rechterklikken op de schijf in kwestie en het Properties venster te selecteren.

Het tabblad **General**

- Bevat informatie over de gebruikte, alsook de nog beschikbare vrije ruimte op de schijf.

- Bevat de mogelijkheid om bestanden op de harde schijf te comprimeren om plaats te besparen.

- Bevat de mogelijkheid om een index op te bouwen op deze harde schijf, zodat bestanden sneller gevonden kunnen worden bij zoekopdrachten.

Het tabblad **Tools**

A screenshot of a computer error

Description automatically generated- Bevat de mogelijkheid om de harde schijf na te kijken op fouten (bv. Defecte sectoren op de harde schijf)

- Bevat de mogelijkheid om de harde schijf te **defragmenteren**. Wanneer een harde schijf lange tijd gebruikt wordt en veel bestanden verwijderd en aangemaakt werden, zullen de bestanden verspreid zitten over de hele harde schijf. Het kan ook zijn dat bepaalde delen op de harde schijf nog vrij zijn, maar dat de ruimte te klein is om een nieuw bestand te bewaren. Deze inefficiëntie kan opgelost worden door een schijfdefragmentatie. Windows zal bij defragmentatie de bestanden die verspreid zitten over de harde schijf (een individueel bestand kan zelfs opgesplitst in blokken verspreid zitten over de harde schijf) terug samen plaatsen zodat toekomstige toegang tot de bestanden sneller kan verlopen. Het grootste tijdsverlies bij het openen van bestanden treedt vooral op wanneer het bestand verspreid zit over de harde schijf. Schijfdefragmentatie zou een computer dus sneller kunnen laten werken.

**Opdracht:**

Zoek op of het slim is om een SSD te defragmenteren!

#### Good to know (Niet te kennen leerstof)

Het tabblad **security** bevat de toegangsrechten van verschillende gebruikers op dit volume. We bekijken deze gebruikersrechten in het stuk dat handelt over User Management.

Het tabblad **Quota** bevat instellingen die verband houden met de schijfquota’s van elke individuele gebruiker. Een Quota is de maximale grootte van alle bestanden op een bepaalde schijf voor een bepaalde gebruiker. Je kan hier bijvoorbeeld instellen dat Rita 200 MB aan bestanden mag opslaan, terwijl gebruiker John slechts 100 MB mag verbruiken. Op deze manier kan in gedeelde omgevingen (bv. schoolomgeving) waar meerdere gebruikers op eenzelfde systeem werken het harde schijf gebruik toch gelimiteerd worden.

Het **Sharing** tabblad geeft de mogelijkheid om de harde schijf te delen met andere gebruikers/groepen op het netwerk. Ook deze instellingen kunnen enkel aangepast worden door een administrator.

## Windows mappen- en bestandsbeveiliging

Windows ondersteunt al sinds de introductie van Windows NT twee formatteringstypes:

- **NTFS** (New Technology File System)

- **FAT** (File Allocation Table)

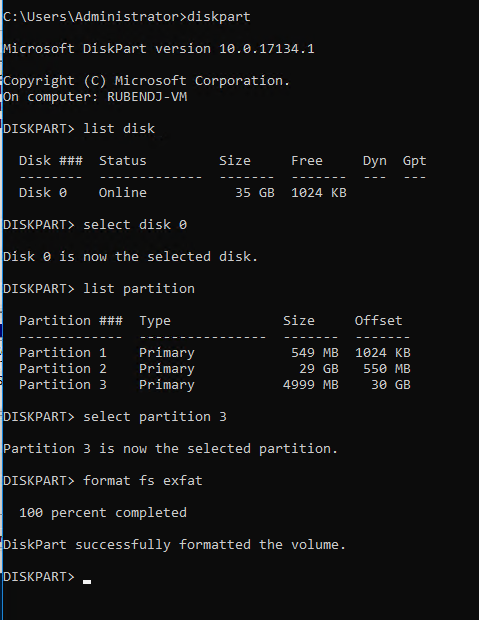
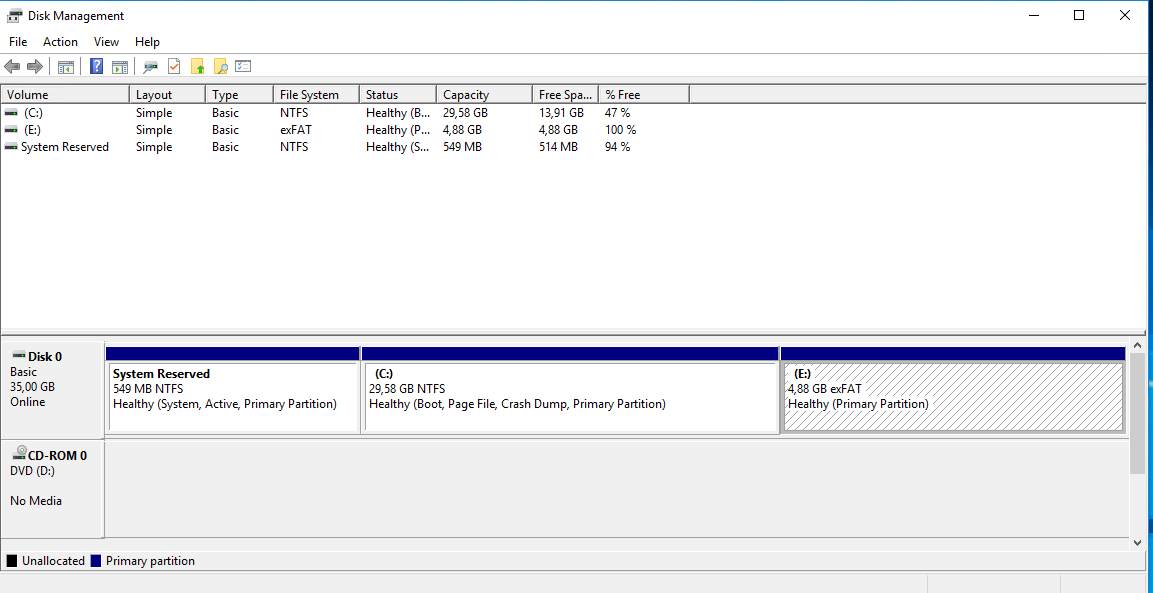
Het grote nadeel van FAT is dat er geen beveiliging op mogelijk is. Alle gebruikers kunnen alle bestanden openen. Ook is de bestandsgrootte op een FAT-volume beperkt tot 4 GB. Het enige voordeel van een FAT-schijf is dat andere besturingssystemen zoals Linux en Mac OS X er zonder problemen mee kunnen werken.

Om tegemoet te komen aan de bestandsgroottebeperking is **ExFAT** in 2006 op het toneel verschenen. Alhoewel ExFAT meer ondersteund is dan NTFS, hebben sommige oudere systemen en distro’s toch problemen met ExFAT.

Je zal straks ook merken dat Windows 11 niet de optie biedt je schijf te formateren met het ExFAT formaat. Om dit op te lossen kan je gebruik maken van externe tools, of de cli.

#### Good to know (Niet te kennen leerstof)

Alhoewel er een **format** commando bestaat is het sneller om via **diskpart** te werken.



NTFS biedt veel uitgebreidere mogelijkheden dan FAT: beveiliging op bestandsniveau, comprimeren van bestanden, encryptie, ... Het is dan ook logische dat op alle huidige Windows-computers gebruik wordt gemaakt van het NTFS-bestandssysteem. Zeker in een netwerkomgeving waar meerdere gebruikers kunnen aanloggen op dezelfde computer is beveiliging van bestanden enorm belangrijk. Elk bestand (en elke map) op een NTFS-volume heeft een owner. Dit is typisch de gebruiker die het bestand heeft aangemaakt. Zoals in Linux kan de owner van een bestand gewijzigd worden, al kan enkel de administrator dit doen. Verder bevat elk bestand en elke map een lijst van gebruikers en groepen met rechten.

|  |
| --- |
| **Opdracht**: Zoek volgende zaken op:   * Wat betekent het als je je harde schijf formatteert? * Wat is het verschil tussen low-level formatting en high-level formatting? * Wat is een Zero bit fill? * Wat is het verschil tussen Quick Format en Full Format? * Maak een nieuwe partitie aan door de C:/ schijf van je VM te verkleinen met 5GB. * Geef deze partitie de Letter E:/ en formateer ze met het FAT formaat. Open de CLI en navigeer naar je nieuw schijf. * Formateer de partitie opnieuw, maar deze keer naar exFAT |

## Toevoegen & Verwijderen van programma’s en features

De bovenste optie bij het rechtermuisknop start menu zorgt ervoor dat je apps kunt verwijderen.

A blue and white background with black text

Description automatically generated

|  |
| --- |
| **Opdracht:**  Installeer één van de handige tooltjes op het einde van werkcollege 1 (test uit) en de-installeer deze hierna. |

Als je in het Settings scherm kiest voor Apps zal je merken dat er nog verschillende extra opties zijn.

A white rectangular object with a black border

Description automatically generated A black text on a white background

Description automatically generated

Je kan bijvoorbeeld kiezen voor Advanced app settings om bepaalde Windows Updates te de-installeren. (Het gebeurd wel vaker dat een update van Windows bij bepaalde gebruikers zorgt voor problemen zodat ze dit best terugdraaien tot er een bugfix komt)

Onder System -> Optional Features kan je features van Windows aan en uit zetten. Bepaalde features staan niet standaard in de lijst, maar onder de Related settings kan je kiezen voor “More Windows features”.

A white rectangular object with a white background

Description automatically generated

Een feature die je waarschijnlijk in je 2de jaar zal nodig hebben is IIS (Internet Information Services)

**Opdracht**: Zet Internet Information Services aan

## UAC (User Account Control)

Het concept van “least user” of “standard user accounts” is in de laatste Windows-versies altijd maar belangrijker geworden. Bij dit concept gaan we ervan uit dat we als gewone gebruiker kunnen werken op ons systeem en dus niet de hele tijd als administrator ingelogd hoeven te zijn.

|  |
| --- |
| **Opdracht**:  Verwoord: Wat is het grote nadeel om als lid van de administrators groep al je programma’s uit te voeren? |

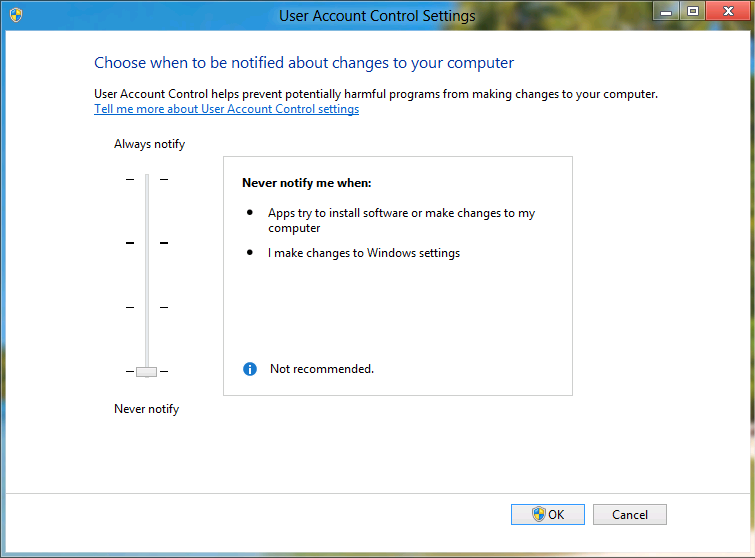
Vanaf Windows Vista wordt het zogenaamde **UAC (User Account Control)** systeem gebruikt. UAC werd speciaal ontworpen om de “least user” mogelijkheden ten volle te benutten en om minder kansen te geven aan spyware en andere verdachte software.

Onder UAC zullen alle gebruikers, ook diegenen die administratieve rechten krijgen, als gewone gebruikers met het systeem interageren. Zolang de gebruiker gewoon blijft werken, zal alles uitgevoerd worden als niet-geprivilegieerde gebruiker en bestaat er dus geen gevaar voor het systeem. Van zodra de gebruiker echter een taak probeert uit te voeren waar administrator rechten voor nodig zijn, zal Windows de gebruiker achter zogenaamde “Administrator Credentials” vragen. Dit gebeurt op volgende wijze, afhankelijk van de gebruiker die momenteel ingelogd is:

- Is de ingelogde gebruiker **zelf geen lid van de administrators groep**, dan wordt zowel een gebruikersnaam als een wachtwoord gevraagd. Deze account moet dan wel lid zijn van de administrators groep om verder te kunnen gaan.

- Is de ingelogde gebruiker zelf **lid van de administrators groep**, dan zal er enkel een toelating gevraagd worden om door te mogen gaan.

Alhoewel dit geen goed idee is geven we mee dat je dit makkelijk kan uitschakelen door de “Change User Account Control settings” op never notify te zetten.

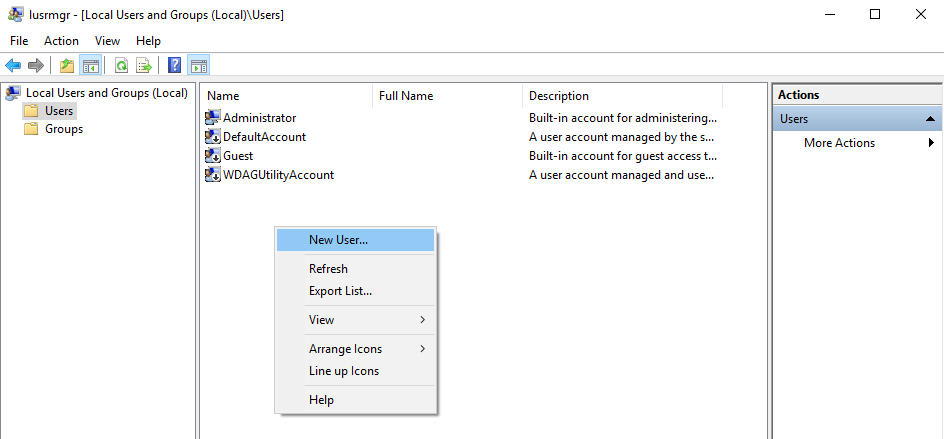


#### User Toevoegen

Een gebruiker toevoegen kan op verschillende manieren. Ja mag gerust deze opdracht op een alternatieve manier uitvoeren (bv. door de Computer Management Tool te gebruiken).

A close-up of a white box

Description automatically generated De manier dat we nu gaan gebruiken is via de lusrmgr tool. Om deze te openen kan je in de Windows Searchbar zoeken naar lusrmgr.msc



Je krijgt in de tool dat je hebt geopend een overzicht van alle gebruikers. De pijltjes naar beneden willen zeggen dat het account disabled is. Hier kan je een nieuwe gebruiker aanmaken.

|  |
| --- |
| **Opdracht:**   * Maak drie nieuwe gebruikers aan, ‘Jimmy’ ,‘Joske’ en ‘Jefke’. * Disable Jimmy’s account. |

Onder groups kan je verschillende groepen vinden die door Windows gebruikt worden. Groepen kunnen gebruikt worden om bepaalde policies (regels) te verplichten, alsook toe te laten dat de gebruikers extra opties en rechten hebben op de PC.

|  |
| --- |
| **Opdracht:**   * We vertrouwen ‘Joske’ met ons leven. Maak hem deel van de Administrators groep! * ‘Jefke’ daarentegen vertrouwen we nog minder dan een gewone gebruiker. Maak een nieuwe groep Noobs aan en voeg Jefke hier aan toe. Zorg ervoor dat de location niet ingesteld staat op het domein maar op de locale PC. |

## User Profiles

Elke gebruiker in Windows krijgt zowel een Registry Hive (zie 2.9) alsook een aantal profiel folders die bewaard worden op het bestandssysteem. In Windows 10 kan je voor elk profiel deze folder terugvinden onder C:/Users.

Bekende folders zijn:

* Documents
* Downloads
* Desktop

Een minder bekende folder is de AppData folder. Deze map is verborgen en je zal dus hidden items moeten aanvinken om deze te kunnen zien. Applicaties gebruiken deze folder voor het bewaren van data en settings die uniek zijn per gebruiker.

Binnen deze folder zijn er drie subfolders.

* Local
* LocalLow
* Roaming

De opsplitsing heeft te maken met rechten en synchronisatie op je domein.

Local wordt gebruikt voor settings die enkel en alleen op die bepaalde PC moeten bewaard worden. Deze instellingen worden niet bijgehouden en doorgegeven wanneer de gebruiker zich met zijn domain account ergens anders inlogt.

LocalLow is een folder die minder rechten nodig heeft om naar te schrijven. Dit zorgt ervoor dat je applicaties kan uitvoeren met minder rechten zonder de functionaliteit van instellingen te verliezen. (Bekijk bv. de protected mode van internet explorer)

Roaming wordt gesynchroniseerd op het domein bij je Domain Controller. Dit zorgt ervoor dat je bepaalde files en instellingen behoudt wanneer je op een andere PC (die in het domein zit) je inlogt.

Om hiernaar te navigeren kan je ook %APPDATA% typen in de explorer navigatiebalk. Dit kan omdat APPDATA een systeemvariabele is (verder meer hierover).

|  |
| --- |
| **Opdracht:**  Bekijk de profiel folders vluchtig. Je zou bv. kunnen instellen dat je de downloadfolder van alle gebruikers elke 24 uur leeg maakt. Om dit te doen zal je tasks moeten aanmaken (zie 2.11). |

## Het Register

In de vijfde editie van de *Microsoft Computer Dictionary* wordt het register als volgt gedefinieerd (hier vertaald vanuit het Engels):

Een centrale, hiërarchische database die wordt gebruikt in Microsoft Windows 98, Windows CE, Windows NT en Windows 2000 (en opvolgers) voor het opslaan van gegevens die nodig zijn om het systeem te configureren voor één of meer gebruikers, toepassingen en apparaten.

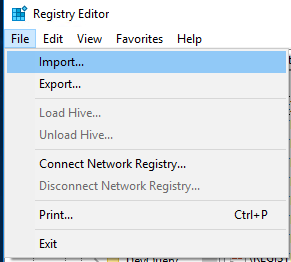
Het register bevat informatie die Windows tijdens het gebruik voortdurend nodig heeft, zoals profielen voor iedere gebruiker, de op de computer geïnstalleerde toepassingen en het type documenten die elke toepassing kan maken, instellingen van eigenschappenvensters voor mappen en toepassingspictogrammen, de hardware die op het systeem is geïnstalleerd en de poorten die in gebruik zijn.

Het register vervangt de meeste op tekst gebaseerde configuratiebestanden die worden gebruikt in MS-DOS en Windows 3.x, zoals Autoexec.bat en Config.sys. Hoewel het register in verschillende Windows-besturingssystemen wordt gebruikt, zijn er bepaalde verschillen tussen de versies.

Een registeronderdeel is dus een groep sleutels, subsleutels en waarden in het register die een verzameling ondersteuningsbestanden bevat waarin zich back-ups van gegevens bevinden. Daarbuiten wordt het register door verschillende programma’s gebruikt om gegevens en instellingen bij te houden. De bestanden voor alle onderdelen behalve HKEY\_CURRENT\_USER bevinden zich in Windows 10 in de map c:/Windows/System32/config. Ook hier kan je gebruik maken van een systeemvariabele nl. %SystemRoot%\System32\Config (zie 2.19).

Om het register te bekijken, kan je gebruik maken van het programma **regedit**. Wanneer je dit programma opent krijg je een zicht op de gigantische database van het register, waarin vele waarden opgeslagen zitten. In het register zitten dus een heleboel variabelen, die ook steeds van een bepaald datatype zijn. Zoals in Programming Essentials waar float, double, char, ... datatypen zijn, zijn ook hier bepaalde datatypen beschikbaar bv. DWORD (Double-Word),

|  |
| --- |
| **Opdracht:**  Zoek op wat Registry hives zijn en ga vervolgens in het register naar HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist, je kan opmerken dat de locaties van de verschillende hives daar opgeslagen worden. |

Het register wordt vaak gebruikt wanneer er bepaalde virussen volledig moeten verwijderd worden die tot diep in het register hun sporen nalieten. Ook bij hardware-problemen (bv. cd-rom die niet meer herkend wordt) kan een eenvoudige register-wijziging wonderen doen. Let echter steeds op bij het wijzigen van register-waarden, aangezien een verkeerde waarde het systeem serieus in de war kan sturen!

Vooraleer je zo maar zaken wijzigt in je register is het goed om een backup te voorzien die je kan gebruiken indien er iets misgaat.

Om dit te doen kan je de register bestanden kopiëren. Om het nog makkelijker te maken kan je een export maken van je hele register of een deel ervan. Dit kan je op een later moment terug importeren.

Om dit deel te besluiten, geven we nog een leuke registry tweak mee om je systeem aan te passen (kan je niet uitvoeren op school, omdat je geen administrator account hebt...) Uitproberen op eigen risico!

Windows 11 toont na het opstarten standaard een **login-scherm waarop alle gebruikersaccounts** staan vermeld. In een kantooromgeving kan dat een nadeel zijn omdat de inlognamen van alle gebruikers dan al bekend zijn bij iemand die eventueel in de pc wil inbreken. Gelukkig is het via een simpele ingreep in het Windows-register mogelijk om deze vermeldingen uit te zetten. (Je kan dit ook bereiken via group policies)

Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: dontdisplaylastusername

Data Type: DWORD

Value Data: 0 = no effect, 1 = do not show last logged on user

|  |
| --- |
| **Opdracht:**   * Maak een backup van je register. * Pas bovenstaande Key aan zodat je de gebruikersnaam van de laatst ingelogde gebruiker niet meer ziet. * Importeer je backup en controleer of de wijziging terug weg is. |

## Systeemvariabelen

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijvingZoals je al kon opmerken uit de vorige opgaven worden er bepaalde paden en gegevens bijgehouden in variabelen. Deze variabelen kunnen door alle programma’s opgevraagd en gebruikt worden. Je kan deze variabelen visueel in Windows opvragen en bewerken. Dit doe je door in Windows Explorer te rechtermuisklikken op ‘This PC’ en te kiezen voor properties.

Navigeer daarna naar Advanced system settings -> Environment Variables.

Afbeelding met tekst, schermopname, Website, software

Automatisch gegenereerde beschrijvingJe kan opmerken dat je systeemvariabelen kan aanmaken voor een gebruiker of voor het hele systeem. Indien het voor een gebruiker is wordt er ook gesproken over Gebruikers variabelen. (In het Engels: System & User Environment variables)

Eén van de meest gebruikte systeemvariabelen is **path**.

Wanneer je een programma opstart vanuit de dos prompt (typ bijvoorbeeld eens notepad in de commandline) gaat dos prompt deze executable (in dit geval notepad.exe) zoeken in directories die zijn opgenomen in de zogenaamde **path**-variabele. Om de huidige waarde van de path- variabele te tonen kan je gewoon het commando **path** uitvoeren.

|  |
| --- |
| **Opdracht:**  Open de CLI en voer het commando path uit. |

Dit zou bijvoorbeeld de volgende waarde kunnen geven:

PATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem

Dit wil zeggen dat bij het opstarten van een programma (door gewoon de programmanaam in te typen) Windows gaat zoeken in c:\Windows\system32, in c:\Windows en in c:\Windows\System32\Wbem

Je kan deze variabele als volgt aanpassen:

**path=”test”**

Hierbij is het nadeel dat je de vorige waarde van de path variabele kwijt bent. (bij het opnieuw opstarten van een dos prompt wordt de oude waarde wel hersteld, om dit op te lossen kan je gebruik maken van het **setx** commando. Opgepast, dit commando kan enkel werken met 1024 characters en het gebeurt dat de path systeemvariabele veel langer is).

Je kan iets toevoegen aan de path variabele door de oude inhoud mee te gebruiken in de toewijzing aan een nieuwe waarde:

**Path = %path%;c:\test**

Bovenstaand commando voegt c:\test toe achteraan de huidige waarde, waarbij we een puntkomma gebruiken om de verschillende directories van elkaar te onderscheiden. In het algemeen kan je variabelen uit de command prompt afdrukken door middel van het commando echo, gevolgd door de naam van de variabele met vooraan en achteraan een procent teken (%). Zo krijg je de inhoud te zien van de variabele computername door volgend commando:

**echo %computername%**

|  |
| --- |
| **Opdracht**:  vul de lijst aan met de waarden die jij kan terugvinden in je systeem voor de variabelen op de volgende pagina. Gebruik dus het echo commando om de inhoud te bekijken. Zoek de verklaring voor elk van deze variabelen. |

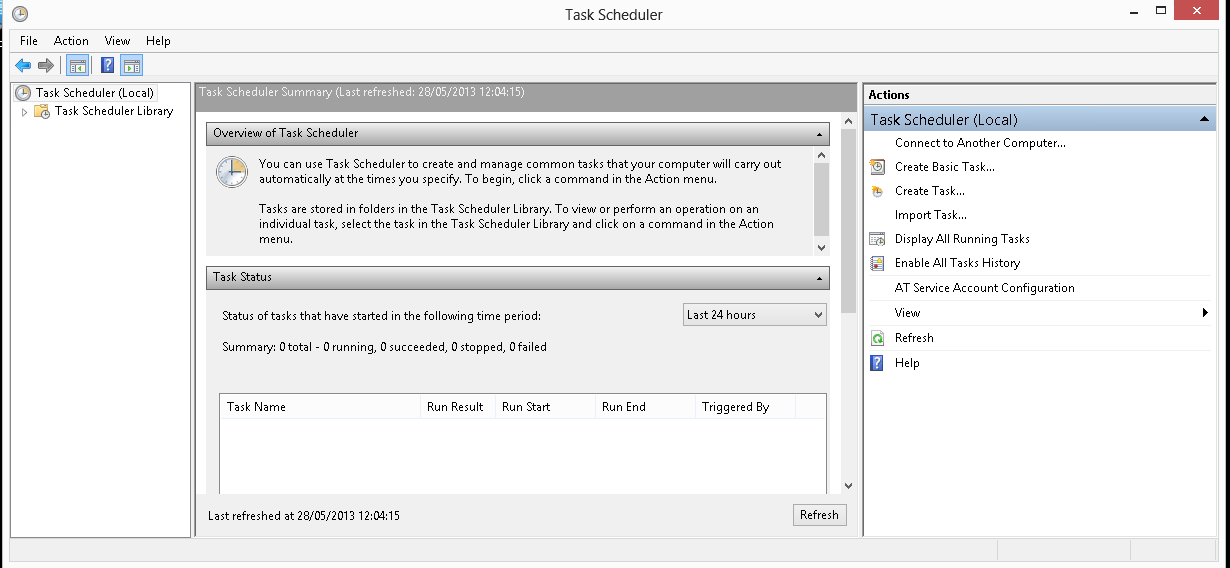
|  |  |  |
| --- | --- | --- |
| Variabelenaam | Waarde op jouw computer | Uitleg |
|  |  |  |
| Appdata |  |  |
| Computername |  |  |
| Localappdata |  |  |
| Path |  |  |
| Pathext |  |  |
| Programfiles |  |  |
| Username |  |  |

#### Good to know (Niet te kennen leerstof)

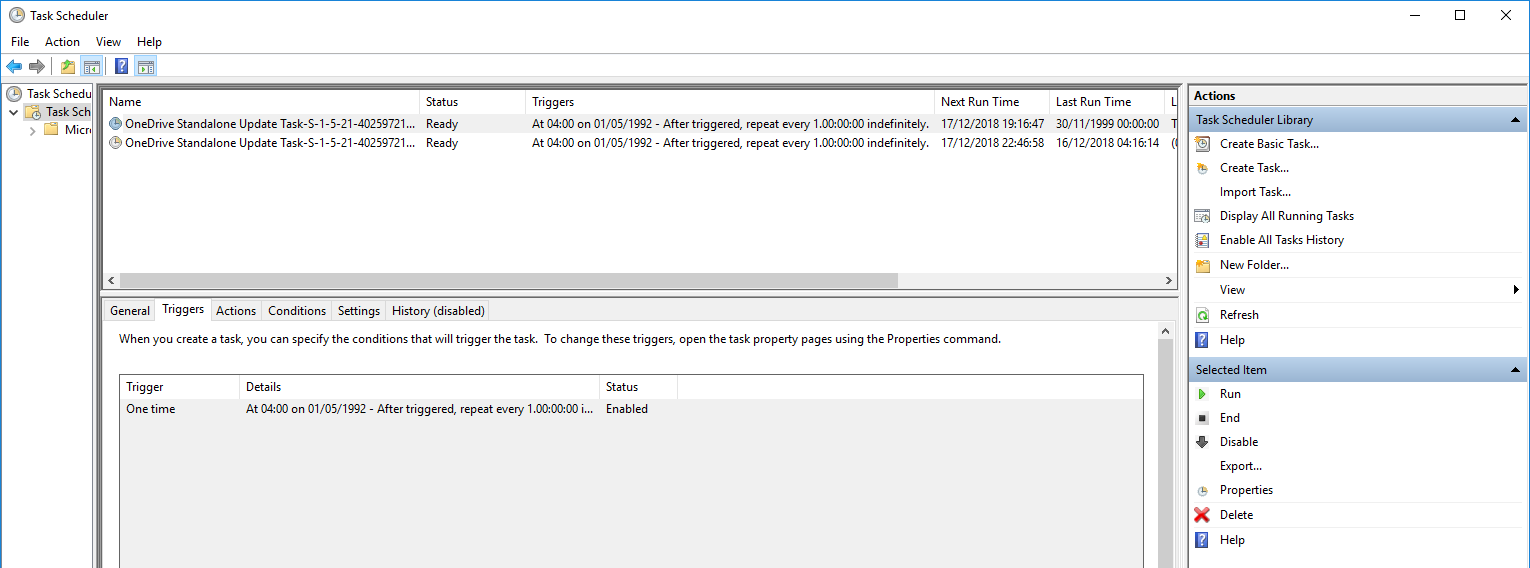
|  |  |  |
| --- | --- | --- |
| Variabelenaam | Waarde op jouw computer | Uitleg |
|  |  |  |
| Errorlevel |  |  |
| Homedrive |  |  |
| Homepath |  |  |
| Os |  |  |
| Processor\_architecture |  |  |
| Processor\_identifier |  |  |
| Temp |  |  |

## Automatiseren van taken in Windows

Zoals voorgaande versies van Windows heeft Microsoft voorzien in de taakplanner of Task Scheduler. Eenmaal je het programma opent zal je een scherm zien met heel wat mogelijkheden:



Het hoofdvenster van de Taakplanner bestaat uit drie panelen: links de bibliotheek met alle ingeplande taken, in het midden de taken zelf (open de library en navigeer naar de verschillende folders) en rechts het actievenster waarmee je de taken beheert. Blader maar eens door de lijst met taken in het middenpaneel.



Je zal zien dat er waarschijnlijk al taken gepland staan.

Je kan zien dat de MicrosoftEdgeUpdateTaskMachineUA Task elke dag opnieuw aangeroepen wordt.

|  |
| --- |
| **Opdracht**:  Pas Deze task aan zodat deze enkel wordt uitgevoerd wanneer de computer Idle is voor 10 minuten. |

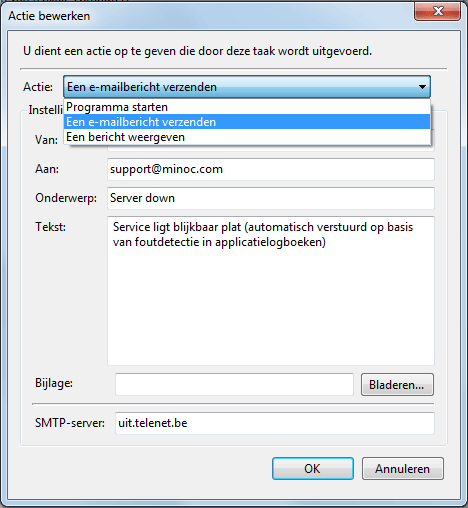
Volg onderstaande stappen om je pc uit te schakelen om 16u45.

* Klik in het rechterpaneel op ‘Create Basic Task’. Dit geeft een Wizard met vier stappen.
* Stap 1: Verzin een passende naam en beschrijving.
* Stap 2: Kies bij de frequentie, dagelijks.
* Stap 3: bij de volgende stap kan je de actie kiezen. Kies voor programma starten waarna we gaan verwijzen naar Shutdown.exe die standaard te vinden is in de c:\Windows\System32 folder. Vul bij Parameters Toevoegen de parameter –S in. (-H sluimerstand, -R herstart, -L afmelden)
* Probeer ook eens: -S -T 60 -C “OVER PRECIES ÉÉN MINUUT SLUIT DE PC AF. SLA NU AL JE GEGEVENS OP!”
* Stap 5: Klik tot slot op voltooien.

Je taak is nu aangemaakt.

Het kan wel zijn dat je bepaalde eigenschappen achteraf nog wilt aanpassen. Als je een Basic Task hebt gekozen zal je zien dat jouw taak niet zal uitgevoerd worden als iemand anders ingelogd is. Om dit aan te passen kan je de taak selecteren in de lijst en het eigenschappenvenster openen.

Ga naar het tabblad ‘Algemeen’ en selecteer hier dat je de taak wilt uitvoeren ongeacht of de gebruiker wel of niet is aangemeld. Je kan ook kiezen om extra taken, na de uitvoering van de taak, uit te voeren.

Als je in het rechterdeel kiest om de geschiedenis van alle taken in te schakelen zal je als je dubbelklikt op een taak en het tabblad geschiedenis opent, een gedetailleerde log te zien krijgen. Probeer enkele taken uit.

|  |
| --- |
| **Extra**: Kan je een event make die automatisch de download folder van alle gebruikers elke dag verwijdert? (Gebruik hiervoor een zelfgeschreven .bat bestand) |

## Power Options

Onder Power options (rechtermuisklik op startknop), kan je instellen wanneer je scherm en je PC in slaapstand moet gaan. Maar de meer handige zaken zitten onder ‘Additional power settings.’ Iets handig is het activeren of deactiveren van Hibernate. Hibernate is niet beschikbaar op de VM’s maar waarschijnlijk wel op jullie persoonlijke laptop. (Zoek, indien je het niet weet, wat Hibernate is en wat de voor en nadelen zijn.)

**Opdracht**: Bekijk de Power Options en zorg ervoor dat de harde schijf nooit deactiveert.

## Event Viewer

Events/gebeurtenissen binnen Windows worden (zo goed als) altijd gelogd. De Event Viewer is een tool die je toelaat om deze logs op een ordelijke manier te bekijken en te filteren. Deze tool laat je toe om te kijken of er al dan niet software en/of hardware-problemen zijn.

Er zijn vijf grote types events die bijgehouden worden in de Event Viewer.

* Application: bevat informatie die te maken heeft met software die geïnstalleerd is.
* Security: bevat informatie die te maken heeft met de beveiliging van je computer.
* Setup: bevat informatie die te maken heeft met de domain controller (enkel wanneer je deel uitmaakt van een domein)
* System: bevat informatie die te maken heeft met de Windows systeem files
* Forwarded Events: bevat informatie die door een andere computer op je netwerk is doorgestuurd naar jouw PC.

Elk event heeft een bepaald Level die aangeeft hoe ernstig een bepaalde fout is. De levels zijn als volgt:

* Information: vertelt je informatief dat er iets is veranderd, gestart of beëindigd.
* Warning: vertelt je dat er iets mis kan gaan of dat er iets begint mis te gaan.
* Error: vertelt je dat er iets is misgegaan maar dat het niet te ernstig is.
* Critical: vertelt je dat er iets grondig mis is en dat iets niet meer werkt zoals het zou moeten. Wat het event veroorzaakt heeft is waarschijnlijk gecrasht.

Als je opzoekingswerk doet omtrent een bepaalde foutmelding kan je niet enkel googelen naar het bepaalde Event ID. Dit komt omdat alle applicaties hun eigen Event ID’s mogen bepalen. Zorg er dus voor dat je steeds de source (en of de applicatienaam) vermeldt.

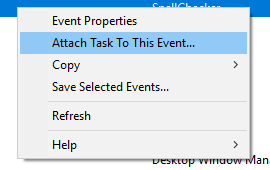
Merk op dat je de Event Properties kunt opvragen per event om meer informatie te verkrijgen.

In het rechter paneel kan je filters instellen waardoor je een beter overzicht krijgt van de bepaalde events die je zoekt. (bv. enkel Errors of enkel events die te maken hebben met een bepaalde applicatie etc…)

|  |
| --- |
| **Opdracht:**   * Zoek het event die afgevuurd wordt wanneer de PC (server) een nieuwe client RDP connectie accepteert (met een bepaald IP-adres en poort). * Maak een nieuwe Custom filter zodat je deze makkelijk kan bekijken. * Sluit de connectie en open een nieuwe Connectie naar je VM. Bekijk of het event is geregistreerd. |

In 2.10 hebben we gezien hoe we bepaalde taken konden automatiseren. In plaats van taken af te vuren op bepaalde tijdsperioden kan je deze ook koppelen aan events.

Je kan dit makkelijk vanuit de Event Viewer doen door te rechtermuisklikken op een event en te kiezen voor ‘Attach Task To This Event’.



#### Good to know (Niet te kennen leerstof)

## GodMode bestaat al sinds Windows 7 en laat je toe om een snelkoppeling te maken naar een overzicht van alle handige tools die je kan gebruiken om je systeem te beheren.

Om dit te doen moet je een folder maken (bv. op je desktop) en deze de volgende naam geven:

GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

# Extra oefeningen

# Hieronder kan je extra commando’s terugvinden die niet te kennen zijn, maar wel gebruikt kunnen worden om het juist aanroepen van commando’s met argumenten en het bekijken van de help file te trainen.

*WMIC*

Je computernaam veranderen kan buiten visueel ook via het WMIC commando:

WMIC computersystem where caption=’huidige\_pc\_naam’ rename ‘nieuwe\_pc\_naam’

In plaats van de huidige pc naam handmatig in te vullen kan je gebruik maken van de systeemvariable computername (zie 2.9).

WMIC computersystem where caption=’%computername%’ rename ‘nieuwe\_pc\_naam’

*schtasks*

Taken die je visueel in de Task Scheduler kan aanmaken kan je ook aanmaken door het commando **schtasks** te gebruiken. Bekijk de help van **schtasks** en probeer een taak aan te maken.

*arp & netstat*

Vorig werkcollege keer hebben we besproken wat een MAC-adres/Fysiek adres is. Met het **arp** commando kan je een lijst krijgen van alle Fysieke adressen op het netwerk.

|  |
| --- |
| **Opdracht:**   * Bekijk de documentatie van het **arp** commando * Geef het fysieke adres van de de desktoposisawesome server en controleer of dit klopt: 00-1d-d8-b7-92-cb |

Met het commando **netstat** kan je kijken naar de status van je poorten.

|  |
| --- |
| **Opdracht:**   * Bekijk met **netstat** de huidige status van je poorten. Kijk in de help om er voor te zorgen dat hij de huidige status elke 3 seconden vernieuwt. * Open daarna een browser en kijk of de status van de poorten veranderen. * Bekijk de status van alle open poorten. |