

4 Windows 10 administrator

Inhoudsopgave

4.1	Systeembeheer en onderhoud	3
4.1.1	Instellingen.....	3
4.1.2	Configuratiescherm (Control Panel)	8
4.1.3	WIN-X poweruser menu	10
4.1.4	Windows Services	13
4.1.5	Remote Desktop Protocol (RDP)	16
4.1.6	Admin tools	17
4.1.7	Regedit.exe	20
4.1.8	Start up modes	24
4.2	Beveiligen en delen	26
4.2.1	Gebruikers.....	26
4.2.2	Groepen	28
4.2.3	Acces control list	29
4.2.4	Permissies of machtiging	32
4.2.5	Encryptie	34
4.2.6	Samenvatting:	38
4.2.7	Delen in thuisnetwerk	39
4.2.8	Oefeningen	39
4.3	Schijfbeheer (disk management).....	42
4.3.1	Standaard schijf	42
4.3.2	Partities:	43
4.3.3	Verschillende soorten partities:	44
4.3.4	Twee soorten schijven.....	46
4.3.5	Data stockeren op schijf	46
4.3.6	Onderhoud en herstel.....	47
4.3.7	Extra opslagmedia	48
4.3.8	BitLocker	48
4.3.9	One Drive	49
4.3.10	Oefeningen:	49

Doelstellingen:



- De student kan met een GUI (Graphical User Interface) werken.
- De student kan het systeem beveiligen.
- De student kan een Windows- en Linux-besturingssysteem onderhouden.
- De student kan een Windows- en Linux-systeem installeren en configureren, ook in een virtuele omgeving.
- De student kan met een Windows- en Linux-systeem werken voor dagdagelijkse taken.
- de student kan in PowerShell cmdlets gebruiken om als administrator taken uit te voeren i.p.v. met de GUI.
- de student kan PowerShell cmdlets gebruiken om als administrator bepaalde taken uit te voeren.
- de student kan gebruikers aanmaken en rechten toekennen met behulp van cmdlets.
- De student kan allerlei bronnen raadplegen en beoordelen op bruikbaarheid.



Voordat je aan dit hoofdstuk begint maak je eerst een snapshot van je vm Windows.

Als je het nog niet gedaan hebt: maak ook een (full) kloon van je vm voor later gebruik.

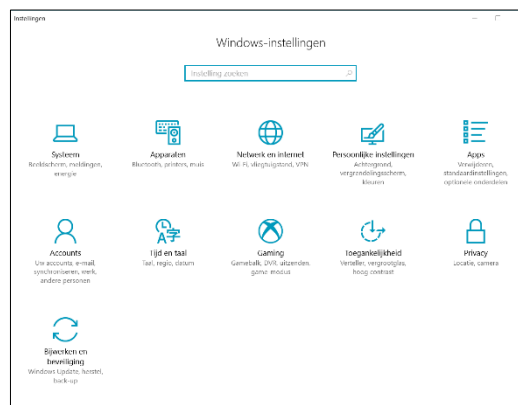
Als er dan iets misloopt bij dit hoofdstuk, heb je nog 2 oplossingen om geen nieuwe installatie te moeten doen.

4.1 Systeembeheer en onderhoud

4.1.1 Instellingen

Systeembeheer en onderhoud gebeurt op verschillende plaatsen in Windows 10. Tijdens hoofdstuk 2 hebben we al verschillende keren instellingen bekeken in zowel instellingen als in het configuratiescherm.

Om het systeem geheel naar de voorkeuren van de gebruiker aan te passen gebeurde dit in de vorige Windows OS oorspronkelijk vanuit het configuratiescherm. Geleidelijk aan verplaatste Microsoft dit naar instellingen en bracht hier gelijktijdig de nodige verbeteringen in aan. Indien een bepaalde aanpassing op het systeem nog niet mogelijk is rechtstreeks in instellingen, is er een link voorzien die naar het juiste tabblad in het configuratiescherm verwijst.



Opdracht: Onderzoek de instellingen en configuratiescherm

Geef 3 verschillende manieren om de instellingen van Windows te bereiken?

Startknop → instellingen

Actiecentrum → alle instellingen

Windowstoets + i

Windowstoets + type instellingen

WIN X poweruser menu

Command prompt of powershell: 'start ms-settings:'

Run (WIN+R)-> ms-settings:

Explorer -> beeld -> settings

Hoe open je het instellingsmenu vanuit Powershell?

'start ms-settings:'

Pin instellingen vast op de taakbalk of in het startmenu.

Onderzoek de verschillende Windows instellingen uit het instellingen venster. Maak voor elk item een persoonlijke beschrijving. Beantwoord voor elk van de instellingen volgende vragen:

Wat kan je allemaal met deze instelling?

Wat is voor een gewone gebruiker interessant?

Voor welke instellingen heb je administrator rechten nodig om aanpassingen door te voeren?

Zorg dat je al de verschillende items en onderliggende instellingen begrijpt en weet terug te vinden.

→ Antwoord via <https://pureinfotech.com/windows-10-system-settings/>

→ https://www.schoonepc.nl/windows10/windows_10_instellingen.html



Opdracht: Enkele Instellingen

- ☐ Bekijk onderstaande instellingen. Vind ze terug op je Windows PC en stel ze in naar jouw voorkeur.
- ☐ 'Downloads van andere pc's toestaan'. Als Windows een update wil 'binnen halen' kan Windows, indien het netwerk traag is, data afhalen vanaf andere pc's. Als de instelling aanstaat kan jouw interface data afhalen van andere pc's en omgekeerd.
- ☐ Waar kan je hotspot 2.0 aan-uitschakelen? Wat is hotspot 2.0?
- ☐ Instellingen > netwerk > wi-fi

Het doel van Hotspot 2.0 netwerken is om mobiele "roaming" te bieden voor Wi-Fi netwerken. Als u zich over de hele wereld verplaatst, verbindt uw toestel u automatisch met beschikbare openbare hotspots. Dit heeft een aantal voordelen:

Openbare hotspots worden eenvoudiger en veiliger: Wanneer u een luchthaven bezoekt, weet uw toestel automatisch welke het echte openbare Wi-Fi-netwerk van de luchthaven is en maakt automatisch verbinding. Je hoeft niet te raden of "FREE_AIRPORT_WIFI" het echte netwerk is, maak handmatig verbinding en klik door een aanmeldscherm.

Netwerkaanbieders kunnen samenwerken: Hotspot 2.0 netwerken zijn ontworpen om beter te werken wanneer serviceproviders samenwerken met andere providers.

Encryptie is verplicht: Veel van de huidige openbare Wi-Fi-hotspots zijn open Wi-Fi-netwerken, wat betekent dat mensen kunnen snuffelen op uw surfen.

Hotspot 2.0-netwerken vereisen WPA2-encryptie op bedrijfsniveau.

Opmerking: Sommige bedrijven noemen deze functie "Passpoint" of "Next Generation Hotspots" in plaats daarvan. Op technisch niveau is het gebaseerd op de 802.11u Wi-Fi standaard.

- ☐ Waar vind je de instellingen om je locatie met Windows te delen? Wat is de default waarde? Sommige apps kunnen toegang vragen/krijgen tot je locatie.
[Settings > Privacy > location](#). Default is locatiedeling ingeschakeld.
- ☐ Waar vind je hoe Windows jouw Windowsgebruik trackt? Wat is de default waarde? Kan je deze optie volledig uitschakelen?
- ☐ Waar kan je jouw diagnostic gegevens bekijken?
- ☐ Wat zijn diagnostische gegevens? Meer info op privacy.microsoft.com
- ☐ Hoe staan de algemeen Privacy setting default?
- ☐ Waar vind je de instellingen voor de nachtlamp? Stel een schema in naar jouw voorkeuren.
- ☐ Buiten de scope van deze cursus maar kijk ook eens naar de settings in gaming. Wat kan je met de game-mode doen?

Opmerking kruisverwijzing:

Bij het snuisteren in de instellingen, zal je merken dat je soms van de ene instellingengroep in een andere groep terecht komt. Zo merk je dat alles samenhangt en dat wijzigingen in de instellingen ook invloed hebben op andere instellingen. Dit maakt dat je soms voor verrassingen komt te staan. Belangrijk is het om altijd goed te weten wat je doet zodat je bij rare bijwerkingen steeds het nodige ongedaan kan maken.



Instellingen via Powershell

Je kan instellingen beheren met de GUI, maar je kan dit ook met PowerShell. Een administrator zal zich de cmdlets eigen maken, omdat dit sneller en directer werkt, je moet niet meer op zoek naar het juiste venster. Zo kan je vanuit PowerShell de standaard apps van Windows 10, die je niet wenst te gebruiken, verwijderen. Bijvoorbeeld om de standaardapp van Xbox te verwijderen:

Get-AppxPackage *xboxapp* | Remove-AppxPackage

Weet wel dat bij een upgrade deze waarschijnlijk weer terug gezet wordt door Microsoft.

Als de slaapstand van de computer niet kan worden geactiveerd, kan het zijn dat in de instellingen de hybride slaapstand uit staat: dit stel je in met het commando (als admin in PowerShell): `POWERCFG /HIBERNATE ON`.

Om een snelle scan van je computer te doen met Windows Defender:

`Start-MpScan -ScanType QuickScan -ScanPath "C:"`

In plaats van "C:" kan je eender welke folder zetten, waar je vreest voor problemen.

Als je met PowerShell (systeem-)instellingen gaat wijzigen en zeker die, waarvoor je administrator rechten moet hebben, is het veiliger om deze eerst te simuleren. Hiervoor kan je de parameter – `WhatIf` gebruiken. Je krijgt dan een beschrijving van wat er gebeurt als je dit commando uitvoert. Verder is er ook de parameter `-Confirm`, vergelijkbaar met `-WhatIf`, maar nu wordt je gevraagd of het moet uitgevoerd worden.

Ook kan je bij veel cmdlets de parameter `-Verbose` (geeft gedetailleerd weer wat er gebeurt) en `-Debug` (geeft gedetailleerd weer wat er gebeurt, maar dan voor de programmeur) gebruiken.

4.1.1.1 *Instellingen Tijd en taal*



Handboek op p152

Deze instellingen stel je in bij installatie van Windows 10, maar misschien is het eindresultaat niet wat je ervan verwacht had. Bijvoorbeeld: je hebt je systeem helemaal in het Engels gezet, maar merkt dat je nu een 'qwerty' toetsenbord hebt, maar jij bent gewend om met een 'azerty' toetsenbord te werken.

Via instellingen tijd en taal kan je de weergavetaal instellen. Als jouw voorkeurtaal er niet tussen staat, kan je steeds een taal toevoegen. Deze taal wordt dan gedownload en geïnstalleerd. Via opties kan je aan een taal een toetsenbord toevoegen. De keuze van weergavetaal gaat dan ook het beschikbaar toetsenbord bepalen. Als je meerdere toetsenborden toevoegt aan 1 taal, kan je steeds switchen tussen de verschillende toetsenborden, afhankelijk van de taak die je wil uitvoeren.

In tijd en taal kan je ook meerdere instellingen wijzigen, bijvoorbeeld welke het valuta teken moet zijn, hoe je decimalen wil aanduiden (punt of komma) of hoe de datum moet weergegeven worden.

Dit doe je bij Datum en tijd en daar kies je voor 'Extra instellingen voor datum, tijd en regio' (= configuratiescherm).



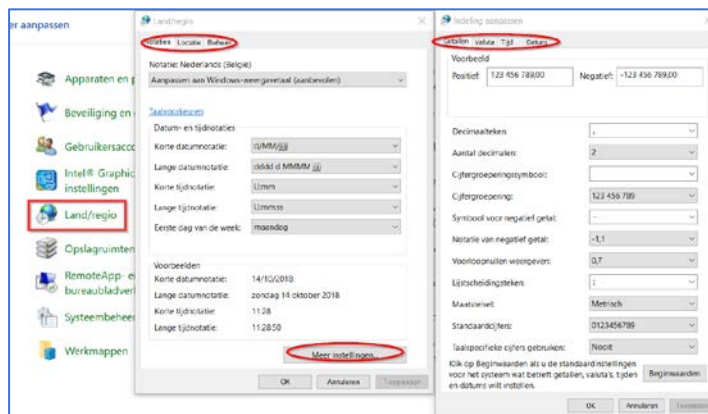
Taal en land instellingen via PowerShell

Huidige weergavetaal instelling opvragen: `Get-WinSystemLocale`.
Weergavetaal veranderen: `Set-WinSystemLocale` met als parameter de juiste waarde (bijvoorbeeld: `nl-BE` of `nl-NL`). Let wel, dit moet je met admin rechten uitvoeren en om het door te voeren moet de computer herstart worden.



Opdracht: Tijd en Taal

- Voeg hier knipsels toe van de vensters waar je taalvoorkeuren, locatie, tijdnnotatie en valuta kan instellen.



- Stel dat je een extern toetsenbord gebruikt op je laptop. Het extern toetsenbord heeft een andere indeling (azerty – qwerty) dan dat van de laptop. Pas Windows aan zodat je makkelijk kan omschakelen tussen de twee toetsenborden.
- Zie geavanceerde toetsenbord instellingen voor het toevoegen van de toetsenbord indeling in het systeem vak.
- Voeg een toetsenbord instelling toe.
- Via de knop in de systeembalk kan je makkelijk omschakelen tussen de twee toetsenborden.

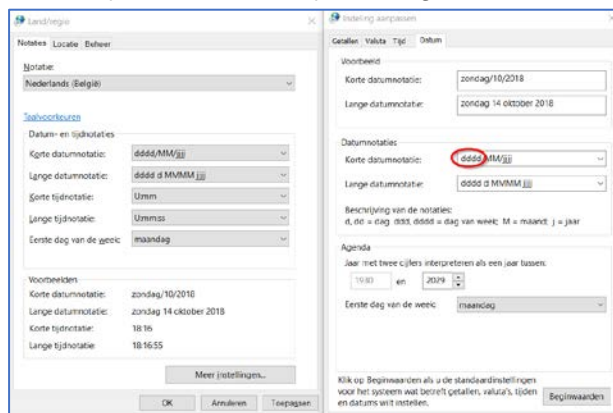
Om te zien welke taalinstelling je voor je toetsenbord hebt, hover je over de taalafkorting in het systeemvak. Om naar de instellingen te gaan om dit aan te passen, klik je op de taalafkorting. Nu opent zich het instellingenvenster voor Tijd en taal > Regio en taal

- Je kan de voorkeur voor het toetsenbord per applicatie instellen.

- Voeg de dag van de week toe aan de klok langs het systeemvak.



Laat ook je naam verschijnen langs de klok.



4.1.1.2 Bijwerken en beveiliging

Items onder bijwerken en beveiliging:

- Windows Update : Bekijk alle instellingen. Je kan hier instellen wanneer je actief bent op de computer en deze dus niet mag uitgeschakeld worden voor updates. Opdracht: stel de werktijd in op uren dat jij actief bent op je computer.
- Onder geavanceerde instellingen kan je ervoor zorgen dat er gedurende 35 dagen geen updates uitgevoerd worden op je computer. Dit is een handige tip voor het examen: zorg ervoor dat je vm niet plots begint te updaten bij aanvang examen of tussendoor. Je verliest dan immers kostbare tijd.
- Windows beveiliging: Als je geen virusscanner installeert, wordt automatisch 'Windows Defender' actief. (zie 4.1.2) Je ziet de lijst waarin je bescherming wordt geboden. Dit is ook de plaats om te zien of Firewall actief is. (zie verder voor Firewall)
- Back-up: Handboek blz 205-206
In Windows kan je op geregelde tijdstippen een back-up laten maken. Hiervoor koppel je best geregeld een externe harde schijf aan je computer.
- Probleem oplossen: Via het item 'probleem oplossen' tracht Windows je te begeleiden met het zoeken naar oorzaken en oplossingen van verschillende (mogelijke) problemen.
- Systeemherstel: Hier kan je het systeem upgraden of helemaal opnieuw installeren. Zorg wel steeds voor een back-up van je persoonlijke data.
- Activering: Hier kan je zien of jouw Windows is geactiveerd. Om alle mogelijkheden te kunnen gebruiken, moet je een actieve Windows hebben.
- Mijn apparaat zoeken: Hiervoor moet je dit aan zetten, je locatie aanzetten en ben je best met een Microsoft account actief.



- Voor ontwikkelaars: als je zelf apps ontwikkeld, moet je hier aanvinken dat die ook moeten toegelaten worden, anders kan je ze hier niet testen.
- Windows Insider-programma: als je hier lid van wordt, dan krijg jij als eerste nieuwe dingen in Windows 10 te zien om uit te testen. Ze verwachten dan wel ook feedback, zodat ze al verbeteringen kunnen aanbrengen voordat deze feature op de markt komt.



Opdracht: Bijwerken en beveiliging (instellingen)

- ☐ Pas de gebruikstijden aan. Waarvoor worden deze tijden gebruikt?
[Deze tijden bepalen of Windows je de vraag stelt om je computer te herstarten om een update uit te voeren.](#)
- ☐ Wat zijn de laatste update's uitgevoerd op jouw pc? [Geschiedenis updates](#)
- ☐ Je kan in Windows 10 updates onderbreken tot 35 dagen. Is het verstandig om dit standaard aan te zetten? Wat tijdens de examenperiodes? [Dit is niet verstandig, je toestel kan veiligheidsrisico's hebben hierdoor. Na die 35 dagen kan je dit niet nog eens aanzetten zonder alle updates van die 35 dagen te installeren.](#)
[Tijdens examens zou dit een optie kunnen zijn, omdat updates soms ook instellingen van externe apps veranderen of een installatie hiervan ongedaan maken.](#)
[Beter is om na een update installatie te controleren of je examenmateriaal nog in orde is.](#)
- ☐ Maak via de back-up instellingen een back-up van (een nieuwe) folder 'MijnBackupbestanden'.
- ☐ Welke opties heb je nog voor een backup van je data? Heeft al jouw data een back-up? [Via back-up alles in de cloud zetten of op een externe harde schijf.](#)
- ☐ Test de probleemoplosser van Windows 10. Is de features iets voor jou?
Over het algemeen is onderstaand een veelvoorkomend scenario. De meeste Windows gebruikers en administrators gebruiken deze feature niet. Maar in sommige gevallen kan het je wel helpen.

Het probleem kan niet met Probleemoplossing worden vastgesteld

U kunt andere mogelijk nuttige opties weergeven.

→ [Feedback geven over deze probleemoplosser](#)

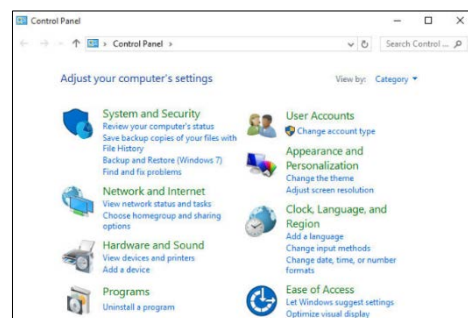
→ [Probleemoplossing sluiten](#)



4.1.2 Configuratiescherm (Control Panel)

Je kan de weergave van het configuratiescherm aanpassen naar persoonlijke voorkeur; ofwel toon je de categorieën ofwel elke instelling met een pictogram.

Soms kom je ook vanuit instellingen, door te kiezen voor extra instellingsopties of geavanceerde instellingen automatisch in het configuratiescherm terecht.



4.1.2.1 Systeembeveiliging

Windows maakt automatisch systeemherstelpunten, maar je kan ook zelf een herstelpunt maken. In Systeem en beveiliging > Systeem > systeembeveiliging.

Je kiest een schijf, die je wil configureren en klikt op configureren. Hier kies je om systeembeveiliging aan te zetten en je geeft aan hoeveel ruimte die herstelpunten mogen innemen op je schijf. Als dit volume bereikt wordt, worden oudere herstelpunten verwijderd.

Als je dit gedaan hebt, zie je dat je een herstelpunt kan maken. Maak een herstelpunt, kies een naam (tijd en datum worden automatisch toegevoegd). Nu wordt een herstelpunt gemaakt. Je krijgt een melding als dit gelukt is.

Als je nu merkt dat het systeem niet goed meer werkt (na nieuwe software installatie, na een update of na aanpassing instellingen ...) kan je je systeem steeds terug zetten naar een vroegere versie.

Hiervoor kies je systeemherstel en dan opent zich een wizard. Normaal gezien heeft dit geen invloed op je persoonlijke data. Nieuw geïnstalleerde programma's of drivers kunnen wel verwijderd zijn na deze actie. Je kan kiezen welk herstelpunt je wil hebben. Let wel op: als je onlangs je wachtwoord veranderde, moet je nog een extra actie ondernemen: een wachtwoord reset schijf maken. Nog even alles bevestigen en het systeem wordt hersteld.

4.1.2.2 Systeemkopie

Een systeemkopie is eigenlijk een volledige back-up. Dit bevat kopieën van alles op je computer. Hiervoor werk je met een externe harde schijf, die je aansluit op je computer. In het configuratiescherm kies je weer voor systeem en beveiliging > bestandsgeschiedenis. Kies nu de externe schijf als opslaglocatie en start de back-up. Als de back-up gemaakt is, kan je het venster sluiten.

4.1.2.3 Firewall

Windows Defender Firewall controleert het in-en uitgaande verkeer tussen je computer en het netwerk (internet is ook een netwerk, weet je nog!)

Systeem en beveiliging > Windows Defender Firewall: hier kan je alle instellingen doen om de acties van de FireWall aan te passen. Je kan de Firewall hier ook uitzetten, wat meestal geen goed idee is.

Als je in de vorige lessen niet kon pingen van je host naar je vm, is verteld geworden dat dit aan de instelling van de Firewall kon liggen. Standaard staat de ping mogelijkheid geblokkeerd. Je kan dit hier aanpassen. Kies voor geavanceerde settings. Kies dan voor 'Inbound Rules' in het linker venster. Kies nu in het rechtervenster voor 'File and Printer Sharing (Echo Request – ICMPv4-In). RMK Enable Rule. Nu zou je wel moeten kunnen pingen van je host naar je vm.

Pingen over een draadloos netwerk wordt in het netwerk van school tegengehouden. Hierdoor is pingen via dat draadloos netwerk tussen studenten niet mogelijk.

4.1.2.4 Windows Defender

Denk er ook aan om je systeem regelmatig te scannen op virussen en spyware. Je kan dit periodiek uitvoeren (instellen), maar als je ergens het gevoel hebt dat er iets mis is, kan je deze scan ook oproepen. Windows Defender is een app, die je dan kan starten hiervoor.



Opdracht: configuratiescherm

- ☐ Laat Windows Defender een snelle scan uitvoeren in je vm. Bespreek het resultaat. Zijn er bedreigingen gevonden? Hoeveel files zijn gescand. Had je een besef dat er zoveel bestanden op de vm staan?
- ☐ Je kan met Windows ook verschillende versies van bestanden bijhouden. Hierdoor heb je ze steeds voor het geval ze verloren of beschadigd raken. Zoek uit hoe en wat je hiervoor nodig hebt.
<Restore your files with File History>: in het configuratiescherm : als je een externe schijf koppelt, kan je kopies van je bestanden hiermee opslaan en terug halen indien nodig.
- ☐ Credentials (referentiebeheer): zoek uit wat dit betekent. Er zijn 2 soorten credentials die door Windows (kunnen) worden bijgehouden. Welke?
Credentials = login = gebruikersnaam + wachtwoord
Dit wordt voor Windows bijgehouden zowel voor apps als wanneer je in Edge inlogt in websites. Deze staan leesbaar in de Credential Manager (Web of Windows)
- ☐ Vergelijk de 'werkwijze' van de credentials met deze van een paswoordmanager. Test een paswoordmanager en kijk wat er gebeurt met het referentiebeheer (credentials). Je hebt altijd een wachtwoord nodig om het wachtwoord in je wachtwoordmanager te kunnen bekijken. Zowel in Windows 10 als bij een browser.

4.1.3 WIN-X poweruser menu

Het 'poweruser menu' kan je vinden door WIN+X of met een rechtermuisklik op de startknop. Volgende items zijn te vinden onder het Windows poweruser menu:

- a) Apps en Onderdelen (Apps and Features): hier kan je onder andere instellen met welke app standaard een bepaald bestandstype wordt geopend.
- b) Mobiliteitscentrum: deze staat wel in het poweruser menu van je laptop, maar niet van je vm.
- c) Energiebeheer (Power Options) : Dit is reeds eerder aan bod gekomen in hoofdstuk2. Hier kan je instellen wanneer het scherm moet uitvallen of wanneer de computer in slaapstand mag gaan.
- d) Logboeken (Event Viewer): hier wordt info over de werking van alles binnen je systeem naartoe gelogd. Je kan hier filters instellen om bepaalde logs eruit te filteren. Sommige logboeken en / of logboek entries (regels) kunnen alleen door de computer zijn Beheerder (Administrator) of een gebruiker met Beheerder (Administrator) rechten worden bekeken.
- e) Systeem (system) : alles wat met je systeem te maken heeft.

- f) Apparaat beheer (Device manager): Hier ga je naartoe als een bepaald apparaat niet goed meer werkt. Je kan hier eventueel nieuwe drivers installeren voor je apparaten.
- g) Netwerkverbindingen (Network Connections) (hoofdstuk 2)
- h) Schijfbeheer (Disk Management (zie dit hoofdstuk 4.3)
- i) Computerbeheer (Computer Management) (gebruikersbeheer zie dit hoofdstuk 4.2.1)
- j) Windows Powershell (hoofdstuk 3)
- k) Windows Powershell als admin (zie verder voor het gebruik)
- l) Taakbeheer (Task Manager) (reeds behandeld in hoofdstuk 2)

Extra info logboeken

Een computer is een complex samenspel van hardware, drivers, het besturingssysteem en allerlei andere software. Wanneer er iets fout loopt is het vaak lastig om uit te vissen wat precies de oorzaak is. Gelukkig houdt Windows zeer uitgebreide logboeken bij van alle gebeurtenissen. Die kunnen een waardevolle hulp zijn bij het troubleshooten.

Wanneer iets niet (langer) loopt zoals het hoort kun je alvast een van de ingebouwde probleemoplossers van Windows aanspreken. Dit brengt jammer genoeg lang niet altijd soelaas en dan komt het er op aan zelf het probleem te diagnosticeren om tot de juiste remedie te komen. Logboeken kunnen hierbij waardevolle informatie aanleveren.

De interface van deze tool bestaat uit drie verticale panelen, zoals vaker het geval bij mmc-modules. Links tref je de diverse logboeken aan. Ben je bijvoorbeeld op zoek naar de oorzaak van 'vastlopers' dan is de kans groot dat je bij de Windows-logboeken en meer bepaald bij Systeem moet aankloppen. Immers, hierin vind je meldingen terug van Windows zelf evenals van geïnstalleerde drivers.

In het logboek Toepassing tref je gebeurtenissen aan van uiteenlopende applicaties en services, voor zover die niet afzonderlijk zijn opgenomen in de Logboeken Toepassingen en Services. Het logboek Setup verzamelt meldingen die tijdens de installatie van toepassingen werden gegenereerd en bij Beveiliging komen onder meer pogingen tot het aanmelden bij Windows en tot het benaderen van beveiligde bronnen terecht. Het logboek Doorgestuurde gebeurtenissen ten slotte brengt notificaties van andere computers uit het netwerk bij elkaar.

Aangepaste en selectieve weergaven

In ditzelfde paneel tref je ook de rubriek Aangepaste weergaven aan. Beheer gebeurtenissen (= een item onder aangepaste weergaven) toont gebeurtenissen van verschillende niveaus (Fout, Waarschuwing en Kritiek), uit de diverse Windows logboeken. Deze weergave kan dus een interessant vertrekpunt zijn bij troubleshooten, maar nog inzichtelijker vinden we de Samenvatting van beheergebeurtenissen.

Die vind je door linksboven Logboeken (lokaal) te openen, waarna je in het bovenste luik van het middenpaneel een overzicht krijgt van de diverse types gebeurtenissen inclusief het aantal gedurende het afgelopen uur, 24 uur en 7 dagen. Bij het troubleshooten zal je vooral op Kritiek en Fout willen focussen. Het volstaat hier het plusje aan te klikken en te dubbelklikken op een gebeurtenis waarvan je vermoedt dat die aan je probleem gerelateerd is. Je krijgt dan een chronologisch overzicht van exact dat type gebeurtenis.

Het probleem met veel logboeken is dat ze vaak een onoverzichtelijke hoeveelheid items bevatten. Als het probleem frequent optreedt kun je overwegen om een of meer logboeken leeg te maken (Logboek wissen), eventueel nadat je de inhoud eerst naar een bestand hebt gekopieerd (Alle gebeurtenissen opslaan als). Beide opties zijn beschikbaar vanuit het contextmenu van een logboek.

Zoals aangegeven kun je echter ook een aangepaste weergave aanmaken. Klik hiertoe de gelijknamige optie in het contextmenu of het rechterpaneel aan en leg alle gewenste criteria vast, waaronder de periode, niveau, logboek of bron, gebeurtenis-id, gebruiker enz. Bevestig met OK en geef je weergave een naam. Die wordt nu netjes toegevoegd aan de rubriek Aangepaste weergaven.



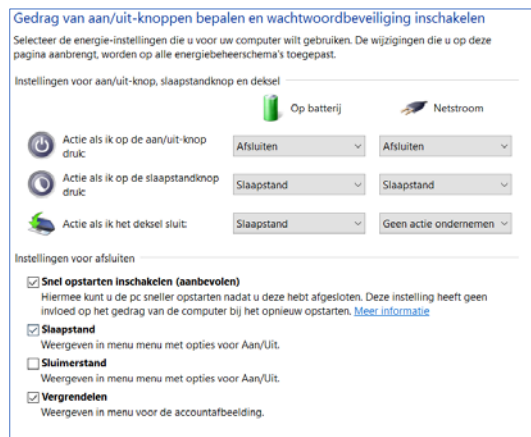
Opdrachten WIN X

- ☐ Ga via WIN X naar de logboeken en bekijk de interface (overloop extra info logboeken).
- ☐ Waar vind je de laatst fouten door Windows gedetecteerd?
 - [Klik op logboeken \(lokaal\)](#), je krijgt een overzicht en samenvatting waar je de laatste fouten kan zien per categorie.
 - [Navigeer naar de categorie Systeem](#).
 - Als u het middelste vak Fout ziet staan, hoeft u er enkel maar op te dubbelklikken om meer details en informatie te verkrijgen.
 - [Logboeken > Windows Logs > Application > Actions :Filter Current Log > Error](#) aanvinken en kijken dat Application staat ingesteld bij Event logs.
- ☐ Je laat je computer onbeheerd achter. Je wil weten wat er gebeurd is gedurende het laatste half uur? Via welke weg kan je hierachter komen?
 - [Gebruik Windows Logboeken!](#)
 - [Om ongeoorloofd gebruikt te achterhalen, volstaat het om de categorie Systeem te selecteren](#)
 - [In het middelste kaderstuk verschijnen dan de datum en uur dat de computer gebruikt werd.](#)
 - [Als blijkt dat de computer gebruikt werd tijdens je afwezigheid is het een peulschil om te achterhalen welke toepassingen werden gestart.](#)
 - [Navigeer naar de categorie Toepassingen. Wat er geschreven, gemaaild of verteld werd vindt u niet terug in de logboeken. Het belangrijkste doel van de Windows-logboeken is uiteraard het opsporen van fouten](#)

- Apparaat beheer: Ga op zoek naar welke processor jouw virtuele machine Windows 10 gebruikt. Zou het een goed idee zijn deze te verwijderen (uninstall device)?
Is dezelfde als die van de host, dus zeker geen goed idee om deze te verwijderen. Zonder processor geen afhandeling van taken.

- Uitbreiding op energiebeheer (hoofdstuk 2); Waar verander je het gedrag van de aan-uit knop?

Configuratiescherm\Alle Configuratiescherm-onderdelen\Energiebeheer\Systeeminstellingen



- Apparaat beheer: Ga op zoek naar welke processor jouw virtuele machine Windows 10 gebruikt. Zou het een goed idee zijn deze te verwijderen (uninstall device)?
- Apparaat beheer: Indien je pc meerdere grafische kaarten heeft. Hoe kan je één van de twee kaarten uitschakelen?



- Mobiliteitscentrum: Zoek uit wat dit is en wat je hier kan instellen. Waarom zou dit niet in je virtuele machine zitten?

4.1.4 Windows Services

Je moet je minstens één keer afgevraagd hebben wat Windows doet draaien en zoveel mogelijkheden biedt voor zoveel verschillende apps? Een cruciaal onderdeel van het antwoord wordt geleverd door de Windows-services (diensten). Door gebruik te maken van de services kan Windows netwerkverbindingen beheren, geluid afspelen via de luidsprekers, wachtwoorden en credentials onthouden, kleuren op het scherm weergeven en ga zo maar door.

Wat zijn Windows-services?

Een service is een applicatie bijna net als elke andere applicatie.

Het verschil tussen diensten en andere programma's is dat ze op de achtergrond draaien en geen gebruikersinterface hebben waar je op kan klikken of tikken. Ze zijn bedoeld om features van het besturingssysteem aan te bieden, zoals web serving, event logging, file serving, printen of error reporting.

Niet alle services zijn ontwikkeld door Microsoft. Sommige applicaties en drivers installeren hun diensten. Security suites zijn een uitstekend voorbeeld, omdat ze verschillende diensten installeren om real-time monitoring van de activiteiten van uw systeem, anti-malware bescherming, firewall bescherming, etc. te bieden. Zij moeten gebruik maken van de voordelen die de diensten bieden. Een van die voordelen is dat ze kunnen worden gestart tijdens het opstarten van het systeem, voor andere programma's en zelfs voordat je jou aanmeldt. Het belangrijkste voordeel is dat ze alles wat op je computer draait kunnen monitoren terwijl ze perfect geïntegreerd zijn in de Windows kern. Op deze manier kunnen ze een hoog beschermingsniveau bieden.

Een ander voorbeeld van een niet-Microsoft dienst kan een SSH-server zijn, vaak gebruikt in kantoren voor veilige verbindingen op afstand of een auto-updating service voor uw webbrowser zoals de Mozilla Maintenance Service van Firefox.

Weten wat of wanneer een dienst iets doet, kan nuttig zijn. Als je bijvoorbeeld weet dat je de functies ervan niet nodig hebt, kun je deze uitschakelen om jouw systeem te versnellen. Als je een router hebt geïnstalleerd om jouw lokale netwerk te beheren, is het waarschijnlijk dat je de service voor het delen van internetverbindingen niet nodig hebt.

Als je een service nodig hebt, maar het is niet zo belangrijk, kan je deze iets later starten, nadat Windows, opstartapps of andere, meer kritieke diensten zijn gestart. Bijvoorbeeld; een van de diensten die we nodig hebben, maar ons leven hangt er niet van af, is de Windows Time service, die de datum en tijd voor Windows en apps synchroniseert. Daarom kan je deze service instellen op een Delayed startup.

Meer info over Windows-service bekijken?

In het venster Services kun je voor elk van de genoemde services vijf dingen zien:

- Naam - De naam van de dienst kan nuttig zijn als je een idee wilt krijgen van wat die dienst doet. Helaas is deze naam echter vaak te cryptisch om je te helpen begrijpen waar het bij de dienst om draait.
- Omschrijving - De beschrijving van de dienst toont korte informatie over het doel of de identiteit van de dienst.
- Status - Geeft aan of de dienst wordt uitgevoerd of dat deze wordt stopgezet.
- Startup Type - Toont hoe de service wordt gestart door Windows. Diensten kunnen automatisch worden gestart, maar met een vertraging, handmatig, of ze kunnen worden uitgeschakeld, wat betekent dat ze nooit worden gestart.
- Aanmelden als - Hiermee kunt u selecteren of de service wordt gestart met het lokale systeemaccount of met een ander gebruikersaccount dat u handmatig opgeeft.
- Opmerking: dubbel klikken op een service geeft ook extra informatie over de service.

- Opmerking: ook in Powershell kan je extra info vinden over services.

Naast Start en Stop zijn er nog enkele andere opties beschikbaar: u kunt de geselecteerde dienst ook pauzeren, hervatten of opnieuw starten. De laatste optie is vanzelfsprekend, net als bij Pauze: het betekent dat de dienst wordt stopgezet, maar alleen voor gebruikersaccounts die geen administratieve of servicevoorrechten hebben, terwijl de dienst voor de laatste nog loopt. Uiteraard start Resume een gepauzeerde dienst voor die accounts.

De actie die je hebt gekozen, wordt alleen toegepast op jouw huidige computersessie. Nadat je Windows opnieuw hebt opgestart, wordt de geselecteerde service hervat in de standaardtoestand.

Start-up type:

Veranderen van het start-up type kan door het venster eigenschappen (rechtermuis klik op de service) (Of via powershell!)

- Automatisch: de service start bij het opstarten.
- Automatisch (Delayed Start): de service start pas nadat het systeem alle andere services die zijn ingesteld om automatisch te starten heeft geladen.
- Handmatig: de service start alleen wanneer deze nodig is.
- Uitgeschakeld: de service start nooit, zelfs niet als de functionaliteit ervan door andere Windows-diensten of apps wordt gevraagd.

Hoewel je dit kan doen, raden wij je aan om het type Startup niet te wijzigen voor services, tenzij je weet wat je aan het doen bent. Het is vooral gevaarlijk om een service uit te schakelen, omdat andere systeemcomponenten er afhankelijk van kunnen zijn. Dit kan leiden tot een slecht werkend besturingssysteem of app, of zelfs tot het uitvallen van het opstarten.

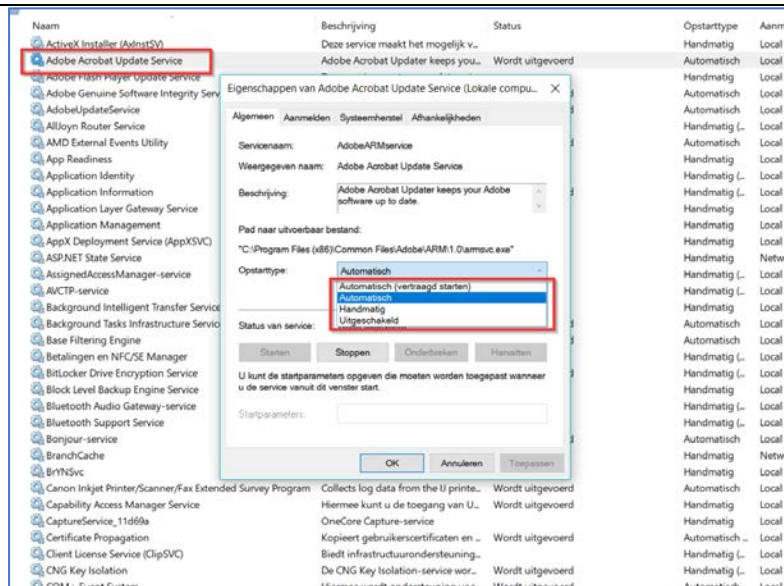


Opdracht: Windows services

- ☐ Zoek drie services die je kan uitschakelen zonder dat je dagelijks Windows gebruik er last van heeft. (Zoek zelf eens online naar het gebruik van services van Windows. Je zal snel zien dat Windows gebruik maakt van veel services en dat het moeilijk is om deze allen te kennen!)

Doe dit zowel via Windows GUI als via Windows Powershell

Zie Artikel: <https://www.digitalcitizen.life/which-windows-services-are-safe-disable-when>



- ☐ Je kan voorkomen dat Windows tijdens de examens updates installeert door een bepaalde service uit te schakelen. Welke?
Dit is de update service van Microsoft. Het is echter sterk af te raden deze service te stoppen!!!
- ☐ Installeer FileZilla Client en kijk welke service(s) hier bijkom(t)(en). Hiervoor had je eerst kunnen kijken of je al een service van FileZilla hebt. Nu zou die er in elk geval moeten bijgekomen zijn.

4.1.5 Remote Desktop Protocol (RDP)

Extern bureaublad of remote desktop is een extra feature die in Windows 10 zit. (niet in de Home editie). Hierdoor is het mogelijk om van elders toch op jouw computer taken uit te voeren. De veiligste manier is dat je het zo instelt dat je je altijd moet inloggen, als je van op afstand op je computer wil werken. Hiervoor moet je wel je systeem juist instellen, zodat remote of van op afstand inloggen wordt toegestaan.

Let wel: hiervoor moet je computer wel aanstaan, mag niet in slaapstand zijn.

<https://support.microsoft.com/en-us/help/4028379/windows-10-how-to-use-remote-desktop>



Opdracht: Remote desktop

Opdracht: Stel je vm zo in, dat je van je host kan inloggen op je vm computer. Log nu in vanop je host (met de computernaam en als dat niet lukt, kan je altijd met het IP-adres van je vm proberen.)

Enable remote desktop met PowerShell commando:

```
(Get-WmiObject Win32_TerminalServiceSetting -Namespace
root\cimv2\TerminalServices).SetAllowTsConnections(1,1) | Out-Null
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace root\cimv2\TerminalServices -
Filter "TerminalName='RDP-tcp']").SetUserAuthenticationRequired(0) | Out-Null
```

This is for running locally, but you can also add a -computername to the gwmi to set it on a remote machine. Obviously, then you would need to have RPC enabled.

Dit uitproberen tussen je vm en je hostmachine: <https://www.coolblue.be/nl/advies/remote-desktop.html>

4.1.6 Admin tools

Om Windows optimaal te beheren en te onderhouden moet je je vaak een weg banen door een doolhof van uiteenlopende configuratievensters. Microsoft heeft echter al lang een meer uniforme en gecentraliseerde beheertool die het elke computerbeheerder wat makkelijker moet maken.

Zie ook docs.microsoft: [administrative-tools-in-windows-10](https://docs.microsoft.com/nl-nl/windows/administration/windows-administration/windows-administration-10)

Admin tools kan je openen vanuit:

- Start menu > Windows systeembeheer
- Configuratie panel (icon) > systeembeheer (admin tools)
- Settings > about >
- Via pad in Windows verkenner
(%ProgramData%\Microsoft\Windows\StartMenu\Programs\administratieve Tools of C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools)
- Via een snelkoppeling op het bureaublad.

Admin Tool	Beschrijving	*
Component Services	Configureer en beheer Component Object Model (COM) componenten. Component Services is ontworpen voor gebruik door ontwikkelaars en beheerders.	NIET
Computer Management	Beheer lokale of externe computers met behulp van een enkele, samengevoegde desktoptools. Met behulp van Computer Management kan je veel taken uitvoeren, zoals het monitoren van systeemgebeurtenissen, het configureren van harde schijven en het beheren van systeemprestaties.	2+4
Defragment and Optimize Drives	Gebruik 'Defragment and Optimize drives' om de computer efficiënter te laten werken. Windows defragmenteert en optimaliseert schijven automatisch als onderdeel van het reguliere onderhoud.	4.5
Disk Cleanup	Verminder het aantal onnodige bestanden op de schijven de computer. Het verwijdert tijdelijke bestanden, maakt de prullenbak leeg en verwijdert veel andere items die u misschien niet meer nodig hebt. Windows voert automatisch Disk Cleanup uit als onderdeel van het reguliere onderhoud.	4.5
Event Viewer	Informatie bekijken over belangrijke gebeurtenissen, zoals het starten of stoppen van een programma of een beveiligingsfout, die worden geregistreerd in gebeurtenissenlogboeken.	
Hyper-V Manager	Toegang en management tot het Windows virtualisatieplatform Hyper-V.	NIET
iSCSI Initiator	Configureer geavanceerde verbindingen tussen opslagapparaten op een netwerk.	NIET

Local Security Policy	De beveiligingsinstellingen bekijken en bewerken.	4.x
ODBC Data Sources	Gebruik Open Database Connectivity (ODBC) om gegevens van het ene type database (een gegevensbron) naar het andere te verplaatsen.	NIET
Performance Monitor	Bekijk geavanceerde systeeminformatie over de centrale verwerkingseenheid (CPU), geheugen, harde schijf en netwerkprestaties	4.3
Print Management	Beheer printers en afdrukservers op een netwerk en voer andere administratieve taken uit.	4.3
Resource Monitor	Bekijk hoe de systeembronnen worden gebruikt door processen en services. Resource Monitor kan je helpen bij het analyseren van niet-responsieve processen, het identificeren van de apps die bestanden gebruiken en het beheren van processen en diensten.	4.3
Services	Beheer de verschillende services die op de achtergrond op uw computer draaien.	4.1.4
System Configuration	Identificeer problemen die de correcte werking van Windows in de weg staan.	4.3
System Information	Bekijk details over de computer, besturingssysteem, hardware en software, inclusief stuurprogramma's - ook bekend als msinfo32.exe	2
Task Scheduler	Plan programma's of andere taken die automatisch worden uitgevoerd.	4.x
Windows Firewall with Advanced Security	Configureer geavanceerde firewall instellingen op zowel deze computer als externe computers in het netwerk	4.4
Windows Memory Diagnostic	Controleer het geheugen van uw computer om te zien of het goed werkt.	4.3

**Behandeld in de cursus/vak OS-Windows*

Uitgelicht: prestatiemeter

Open de prestatiemeter: (Sneltoets = win+R en hierin 'perfmon' en in dat venster zie je links de prestatiemeter. Klik deze aan.) Er verschijnt een leeg grafiekvenster: het is namelijk de bedoeling dat je hier zelf aangeeft welke systeemonderdelen de tool precies moet meten en in een grafiek weergeven. Dat doe je door het groene plusje aan te klikken. Er duikt een nieuw dialoogvenster op waarin je in een uitklapmenu uit talloze computeritems kunt kiezen. Klik het pijltje naast zo'n item aan om nog meer in detail te kunnen werken. Voorbeeld: bij Fysieke schijf tref je maar liefst 21 onderdelen aan. Wanneer je één of meerdere van deze onderdelen selecteert, verschijnen in het onderste venster alle betrokken instanties. Je beslist zelf voor welke van deze schijven je de geselecteerde items wilt laten onderzoeken. Breng je selectie naar het rechterpaneel over met de knop Toevoegen. Zodra je met OK bevestigt, keer je terug naar de grafiek.

Opmerking eigen stijl: De Windows Prestatiemeter bepaalt in eerste instantie zelf het uitzicht en de duur van de grafiek van de gekozen items. Dat kun je echter aanpassen. Dubbelklik op zo'n item om de weergave te wijzigen.

Gegevensverzamelaarsets

Het is een hele mond vol, maar in het linkerpaneel van de Prestatiemeter tref je nog een interessante optie aan: Gegevensverzamelaarsets. Hiermee kun je prestaties op de achtergrond meten over een langere periode.

Werkwijze: Open de rubriek Gegevensverzamelaarsets en klik met de rechtermuisknop op Gedefinieerd door de gebruiker. Kies Nieuw / Gegevensverzamelaarset. Geef de set een geschikte naam en stip Handmatig maken (geavanceerd) aan. Druk op Volgende en kies (voor onze doeleinden) Prestatiemeteritem. Wil je echter bepaalde registerwaarden opvolgen, dan kies je hier Systeemconfiguratiegegevens. Druk nogmaals op Volgende en duid alle gewenste items aan via Toevoegen. Bepaal het gewenste interval voor elk van de geselecteerde items (bijvoorbeeld elke 15 seconden). Bevestig twee keer met Volgende. Kies Deze gegevensverzamelaarset nu starten, of kies Opslaan en sluiten als je de set pas later wilt uitvoeren. Rond af met Voltooien.

Je kunt de controle op elk moment starten en stoppen door je set te selecteren bij Gegevensverzamelaarsets/Gedefinieerd door de gebruiker / en de start- of stopknop in te drukken. Naderhand kun je het bijhorende rapport bekijken in het linkerpaneel, door bij Rapporten/Gedefinieerd door de gebruiker op de naam van je set te dubbelklikken. Het is eveneens mogelijk de controle op gezette tijden te activeren. Klik de naam van je set aan bij Gegevensverzamelaarsets met de rechtermuisknop en kies Eigenschappen. Op het tabblad Schema voeg je de gewenste tijden toe via de knop Toevoegen. Op het tabblad Stop-voorwaarde is het mogelijk aan te geven onder welke omstandigheden je zo'n controle automatisch wilt laten beëindigen.

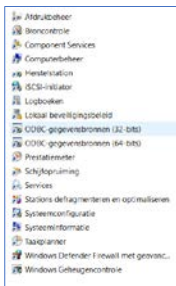
Systeemdiagnose

Vanuit de Prestatiemeter is het ook mogelijk een snelle systeemdiagnose te laten uitvoeren. Die controleert je systeem op een hele reeks onderdelen: van slecht of niet functionerende hardwarecomponenten tot bijvoorbeeld een 'dirty bit'-controle op schijven (dit laatste kan voorkomen wanneer hangende schrijfp opdrachten niet tot een goed einde zijn gebracht). Je start zo'n diagnose als volgt: open Gegevensverzamelaarsets /Systeem, selecteer System Diagnostics (Systeemdiagnose) en start de controle. Na precies één minuut vind je het resultaat van deze test terug bij Rapporten/Systeem/System Diagnostics. Klik de diagnose aan: bovenaan het rapport krijg je een overzicht van de vastgestelde fouten en waarschuwingen.

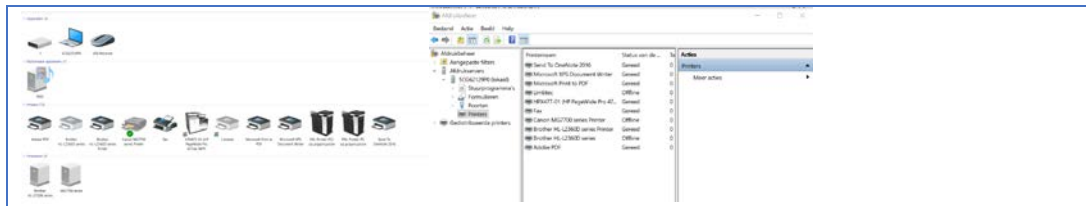


Opdracht: Admintools

- ☐ Voeg via een printscreen een beeld toe van de admintools van Windows 10.



- ☐ Bekijk de admin tool afdrukbeheer. Wat is het verschil met configuratiescherm>printers?



- ☐ Vergelijk de tool broncontrole met tabblad processen in taakbeheer (ctr-shift-esc)

⇒ Achtergrond info:

Je bent op je pc aan het werken en je stelt vast dat je systeem merkbaar trager reageert, wellicht omdat het druk bezig is met het uitvoeren van een ander proces of andere taak. Maar welk proces of welke taak?

⇒ In eerste instantie kun je daarvoor het Windows Taakbeheer aanroepen (Ctrl+Shift+Esc). Hier klik je dan op Meer details. Op het tabblad Processen zie je vervolgens van iedere toepassing en ieder proces hoeveel procent het van het processor-, geheugen-, schijf- en netwerkgebruik in beslag neemt. Klik de gewenste kolomtitel aan voor een aangepaste sortering. Het tabblad Prestaties geeft je voor zowel de processor, geheugen, schijven als netwerkadapters een gebruiksoverzicht van de afgelopen minuut.

⇒ Klik hier de link Broncontrole openen aan om voor elk onderdeel in detail te zien welke processen voor elk gebruik precies verantwoordelijk zijn. Deze snelle analyse kan je al op het spoor zetten van processen en toepassingen die op het moment zelf wel erg veel systeembronnen gebruiken.

- ☐ Maak via de prestatie meter een eigen (naar keuze) schema op. (zie stappenplan in dit werkboek)
- ☐ Maak een diagnose rapport en analyseer het.

4.1.7 Regedit.exe

Het register is een database in het besturingssysteem Windows, waarin instellingen worden opgeslagen van zowel het besturingssysteem zelf, applicaties, gebruikers en apparaten. Het register wordt ingelezen bij het opstarten van Windows en het gebruikersaccount en wordt bij vrijwel alle daaropvolgende handelingen geraadpleegd.

De bestandsassociaties, die bepalen welk programma wordt uitgevoerd om een bestand te openen, zijn bijvoorbeeld terug te vinden in het register.

4.1.7.1 Register indeling

Het register is een volgens een overzichtelijke boomstructuur opgebouwde database en bevat een enorme hoeveelheid aan registersleutels en registerwaarden. De boomstructuur is vergelijkbaar met de opbouw van het bestandssysteem op de interne schijf zoals deze in de Windows Verkenner wordt getoond. De registersleutels zijn vergelijkbaar met de mapjes, de registerwaarden met de bestanden.

Het register is opgedeeld in zes secties, "Hives" genaamd en heeft per sectie een boomstructuur. Elke sectie begint met HKEY, hetgeen staat voor "HandleKEY". Een toevoeging wordt een KEY (Sleutel) genoemd.

- HKEY_CLASSES_ROOT
Koppelt bestandstypen aan de juiste programma's. HKCR is overigens een combinatie van de subsleutels HKLM\SOFTWARE\Classes en HKCU\SOFTWARE\Classes.
- HKEY_CURRENT_USER
Bevat de configuratiegegevens van het ingelogde gebruikersaccount, hierin staan dus de instellingen op gebruikersniveau. Is er een tweede administratoraccount aangemaakt, dan kan deze sleutel met relatief weinig risico's worden getweakt.
- HKEY_LOCAL_MACHINE
Bevat algemene gegevens voor de configuratie van de computer, onafhankelijk van het ingelogde gebruikersaccount.
- HKEY_USERS
De hoofdsleutel van alle gebruikersprofielen. Eigenlijk is HKCU (de sleutel voor het ingelogde gebruikersaccount) een subsleutel van HKU.
- HKEY_CURRENT_CONFIG
De informatie in deze sleutel wordt gebruikt voor het op dat moment gekozen hardwareprofiel (doorgaans is er slechts één beschikbaar) en komt overeen met de subsleutel HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current.
- HKEY_DYN_DATA *deze zit in onze vm er niet bij.*

Voorbeelden:

De volgende keys zijn enkele instellingen van het besturingssysteem en kunnen worden aangepast:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Op deze plaats kunnen verwijzingen naar bestanden worden gemaakt. Deze bestanden worden dan uitgevoerd nadat een gebruiker inlogt.
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
Idem, alleen wordt in dit geval het commando eenmalig uitgevoerd na het inloggen. Na het inloggen verdwijnt het commando uit de lijst.

Het gaat hier om enkele voorbeelden; het register bestaat doorgaans uit honderdduizenden sleutels en het zou te ver gaan ze hier allemaal te benoemen. Daarnaast maken op het besturingssysteem geïnstalleerde programma's zelf

sleutels aan. Aanpassingen aan het register dienen altijd met zorg te worden uitgevoerd. Aanpassingen kunnen, indien de gebruiker onbekend is met het register, desastreuze gevolgen hebben voor de werking van programma's en het besturingssysteem.

De opslaglocatie van de registerwaarden

De registerwaarden worden weggeschreven naar bestanden die bij het opstarten van de computer worden ingelezen. De registerwaarden die systeemspecifieke gegevens bevatten (HKLM), worden weggeschreven naar bestanden in de map C:\WINDOWS\system32\config. Het gaat daarbij om bestanden met namen zoals DEFAULT, SAM, SECURITY, SOFTWARE en SYSTEM. De accountspecifieke instellingen (HKCU) worden weggeschreven naar het bestand NTUSER.DAT in de persoonlijke map (C:\Gebruikers\inlognaam). Om deze bestanden te kunnen zien, moet in de Windows Verkenner (via Opties, tabblad Weergave) de optie Beveiligde besturingssysteembestanden verbergen (aanbevolen) worden uitgevinkt.

4.1.7.2 Regedit

De registers kunnen bekeken (en gewijzigd) worden via regedit.

→ Run (WIN+R) → Regedit

Je kan nu alle wijzigingen aanbrengen die je in het register wil aanbrengen, wat waarschijnlijk niet moet gebeuren, tenzij je vertrouwd bent met het toevoegen, wijzigen of verwijderen van registersleutels en waarden.

Wijzigingen in het register

Worden er onherstelbare wijzigingen doorgevoerd, dan kunnen er grote problemen ontstaan (waaronder het niet meer opstarten van Windows). Het kan namelijk erg lastig zijn een eenmaal verwijderde (of gewijzigde) registerwaarde te herstellen naar de oorspronkelijke waarde wanneer daar vooraf geen back-up van is gemaakt.

Maak eerst een back-up van het register

Voor de zekerheid kan beter eerst een back-up worden gemaakt van de registersleutels waarin wijzigingen zullen worden aangebracht. Treden er onverhoopt problemen op, dan kan de back-up weer worden teruggezet waardoor de wijzigingen in het register teniet worden gedaan.

Het maken van de back-up gaat als volgt: selecteer een registersleutel in de registereditor en stel de onderliggende registerwaarden (via Bestand, Exporteren) veilig in een bestand met de extensie REG. Dergelijke bestanden zijn uit te lezen met een simpele teksteditor zoals Kladblok. Het importeren van REG-bestanden in het register gaat op vergelijkbare wijze met de optie Importeren of vanuit de Windows Verkenner door op het betreffende bestand te dubbelklikken.

Wijzigen en/of toevoegen van registerwaarden

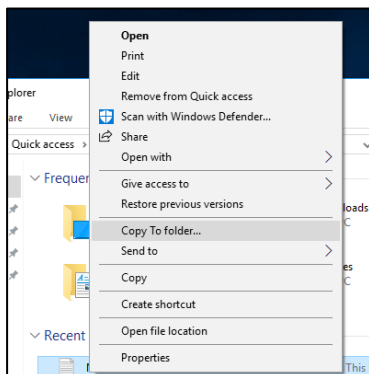
Nadat via de registersleutels (in het linker venster van de registereditor) naar een specifieke registerwaarde (in het rechter venster) is genavigeerd, kan de registerwaarde worden gewijzigd door erop te dubbelklikken. Naar gelang het type (Tekenreeks, DWORD, Binair, etc.) wordt het bijbehorende venster geopend en kan de betreffende registerwaarde worden gewijzigd.

Het aanmaken van een nog niet bestaande registerwaarde is ook eenvoudig. Klik daarvoor met rechts in het rechter venster en kies voor Nieuw (of via de menubalk Bewerken, Nieuw), gevolgd door de gewenste waarde. Er kan direct een naam aan de nieuwe waarde worden gegeven (de naam kan ook in een later stadium nog worden gewijzigd via Bewerken, Naam wijzigen). Door op de nieuwe registerwaarde te dubbelklikken, kan deze van gegevens worden voorzien.



Opdracht: Registers

- ☐ Open het register:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
In dit register zie je de software die bij opstart van Windows wordt opgestart.
- ☐ Open het register:
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
In dit register zitten de services van Windows. De DWORD-waarde Start geeft het opstarttype aan (2: Automatisch, 3: Handmatig, 4: Uitgeschakeld)
- ☐ Toevoegen van het item 'naar map kopiëren aan het contexmenu' (rechtermuisknop)
 - o Open het register:
HKEY_CLASSES_ROOT\ALLFileSystemObjects\shell\ContextMenuHandler
 - o Klik met rechts op *ContextMenuHandlers* en kies voor: *Nieuw > Sleutel*
 - o Geef deze sleutel de naam: *Naar map kopiëren*.
 - o Selecteer de zonet aangemaakte sleutel en dubbelklik in het rechter gedeelte op *Standaard*
 - o Bij het dialoogvenster dat volgt (Tekenreeks bewerken), vult u onderstaande tekenreeks in onder waardegegevens:
{C2FBB630-2971-11d1-A18C-00C04FD75D13}
 - o Bevestig met OK.
 - o Sluit het register af via Bestand > Afsluiten.
 - o Herstart de computer.



- Mobiliteitsvenster toevoegen (in VMware) :

Open de opdrachtprompt als admin en voer volgende commando's uit aan de prompt:

```
reg add HKEY_CURRENT_USER\Software\Microsoft\MobilePC\AdaptableSettings /v  
SkipBatteryCheck /t REG_DWORD /d 1 /f
```

```
reg add KEY_CURRENT_USER\Software\Microsoft\MobilePC\MobilityCenter /v  
RunOnDesktop /t REG_DWORD /d 1 /f
```

Windows toets + R : mblctr en dan ok.

Via de registers is nu aangepast dat er mobiliteitsvenster beschikbaar is.

4.1.8 Start up modes

Met de veilige modus start u Windows in een eenvoudige toestand. Hierbij wordt een beperkt aantal bestanden en stuurprogramma's gebruikt. Dit is een handige manier om problemen met uw pc op te lossen. Als het probleem bijvoorbeeld in de veilige modus niet optreedt, weet u dat standaardinstellingen en stuurprogramma's niet de oorzaak van het probleem zijn.

Er zijn twee versies van de veilige modus: Veilige modus en Veilige modus met netwerkmogelijkheden. Ze zijn vergelijkbaar, maar Veilige modus met netwerk bevat de stuurprogramma's en services die u nodig hebt om toegang te krijgen tot internet en andere computers in het netwerk.



Opdracht: Startup modes

- Start Windows op in veilige modus en vergelijk de werking met normale modus.

Doe dit vanuit Windows in normaal gebruik en vanuit het aanmeldscherm.

Vanuit instellingen:

- Druk op de Windows-logotoets + I op het toetsenbord om Instellingen te openen. Als dat niet werkt, selecteert u de **Startknop** linksonder in het scherm en vervolgens **Instellingen**.
- Selecteer **Bijwerken en beveiliging > Herstel**.
- Selecteer onder **Geavanceerd opstarten** de optie **Nu opnieuw opstarten**.
- Nadat uw pc opnieuw is opgestart en het scherm **Kies een optie** wordt weergegeven, selecteert u **Probleemoplossing > Geavanceerde opties > Opstartinstellingen > Opnieuw opstarten**.
- Nadat uw pc opnieuw is opgestart, ziet u een lijst met opties. Selecteer **4** of **F4** om uw pc in de **veilige modus** op te starten. Of selecteer **5** of **F5** voor **Veilige modus met netwerk** als u toegang tot internet wilt.

Vanuit het aanmeldscherm:

- Start uw pc opnieuw op. Wanneer het aanmeldingsscherm wordt weergegeven, houdt u de Shift-toets ingedrukt en selecteert u tegelijk **Aan/uit Opnieuw opstarten**.
- Nadat uw pc opnieuw is opgestart en het scherm **Kies een optie** wordt weergegeven, selecteert u **Probleemoplossing > Geavanceerde opties > Opstartinstellingen > Opnieuw opstarten**.
- Nadat uw pc opnieuw is opgestart, ziet u een lijst met opties. Selecteer **4** of **F4** om uw pc in de veilige modus op te starten. Of selecteer **5** of **F5** voor **Veilige modus met netwerkmogelijkheden** als u toegang tot internet wilt.

Vanuit een zwart scherm:

Als er een zwart of leeg scherm verschijnt waardoor u het aanmeldingsscherf niet kunt bereiken, probeert u het volgende; drukt tegelĳkertĳd op de Windows-logotoets + Ctrl + Shift + B. Als u zich in de tabletmodus bevĳndt, drukt u drie keer binnen 2 seconden tegelĳkertĳd op zowel Volume omhoog als Volume omlaag. Als Windows reageert, klinkt een korte pieptoon en knippert het scherm of wordt dit gedimd terwĳl Windows probeert het scherm te vernieuwen.

Meer info op: <https://support.microsoft.com/nl-be/help/12376/windows-10-start-your-pc-in-safe-mode>

4.2 Beveiligen en delen

Authenticatie vs. autorisatie.

Authenticatie is het vaststellen van de identiteit van de gebruiker (naam, paswoord, ...)

Autorisatie is het vaststellen met gebruik van de identiteit of de gebruiker toegang (rechten) heeft om het gevraagde te mogen gebruiken. (app, lezen/schrijven in bestand, ...)

Als je maar 1 gebruiker (account) hebt op een computer en deze computer is met geen enkel netwerk verbonden, is het niet noodzakelijk de autorisatie telkens te controleren. Waarschijnlijk gaat deze gebruiker administrator zijn en is er geen twijfel of hij bepaalde diensten / bestanden op de computer mag gebruiken.

Windows 10 is een besturingssysteem dat meerdere gebruikers op 1 computer toe laat, dus moeten ook de authenticatie en de autorisatie ingesteld worden.

4.2.1 Gebruikers

In hoofdstuk 2 is er al aangegeven dat je meerdere gebruikers op 1 computer met Windows 10 kan aanmaken. Deze accounts kunnen verschillende rechten krijgen bij aanmaken. De 2 die het meest gebruikt worden zijn de administrator en de standaard gebruiker. In de volgende uitleg wordt deze beperking aangehouden.

Bij het installeren van Windows 10 op de computer wordt er standaard een administrator account aangemaakt. Dit wil zeggen dat het account waarmee je de vm hebt gemaakt, is de administrator in je vm.

We maken nu nog 2 extra lokale, standaard accounts; Mark en Mieke. Voor hun unieke gebruikersnaam gebruik je het wachtwoord pxl. Denk eraan dat je met een administrator account moet zijn ingelogd om een nieuw account te kunnen aanmaken.



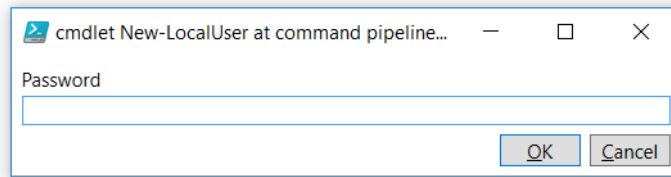
Gebruikers via Gui

Gebruikers aanmaken kan je via instellingen >accounts > Family & other people. Windows wil je forceren om dit met een Microsoft account te doen, wat je niet moet doen. Je doorloopt de Wizard en je Mark is aangemaakt.



Gebruikers via PowerShell

. Je kan ook via PowerShell (run as admin) een gebruiker aanmaken met het cmdlet New-LocalUser *naam*. Er verschijnt dan een pop-up om het wachtwoord in te geven.



```
PS C:\Windows\system32> New-LocalUser Mieke  
cmdlet New-LocalUser at command pipeline position 1  
Supply values for the following parameters:
```

Na uitvoeren van het cmdlet krijg je bevestiging dat Mieke als user is aangemaakt. Deze zit dan echter nog niet in de groep Users, waardoor deze niet zichtbaar wordt in het login scherm. Voer volgend ook uit:

Add-LocalGroupMember -Group Users -Member Mieke

Nu kan je ook met Mieke inloggen.

Voor gebruikersbeheer in PowerShell heb je volgende cmdlets ter beschikking:

- Get-LocalUser
- Set-LocalUser
- Rename-LocalUser
- Remove-LocalUser
- Disable-LocalUser
- Enable-LocalUser

Je kan in PowerShell (en in de GUI) ook bepalen hoe het wachtwoord er moet uitzien: GUI: Local Security Policy (SECPOL.MSC) of PS: NET ACCOUNTS;

Minimum lengte: NET ACCOUNTS / MINPWLEN:8

Let wel, dit geldt dan voor alle gebruikers en dan zou ons wachtwoord pxl niet geldig zijn!

Opmerking wachtwoorden

Wachtwoorden zitten gecodeerd (password hash) opgeslagen in de security accounts manager SAM, die zich bevindt in C:\windows\system32\config\sam .

Windows maakt voor elke gebruiker (en elke groep) een unieke herkenningscode: de SID (security identifier). Deze SID wordt door het systeem aangemaakt. Een SID is uniek in zijn scope (domein of plaatselijk) en kan in die scope nooit opnieuw gebruikt worden.

Elke keer een gebruiker aanmeldt wordt een *access token* gemaakt; hierin zitten de SID van de gebruiker, de SIDs van elke groep waartoe deze behoort en al zijn rechten in het systeem.



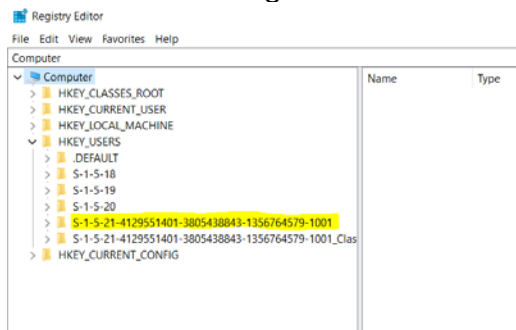
SID via PowerShell

Je kan de SIDs opvragen in PowerShell voor alle accounts op je computer met het cmdlet met parameterwaarde 'win32_useraccount':
'Get-WmiObject win32_useraccount' .



SID in het register

De SID zitten ook opgeslagen in het register. Om dit op te roepen, moet je 'regedit' typen in de zoekbalk van de taakbalk. Hier vind je dan de SID van de huidige ingelogde gebruiker bij HKEY_USERS. Zie voor meer info over registers 4.1.7



Opdracht: SID

- ☐ Voer het commando 'Get-WMIObject win32_useraccount' uit in PowerShell. Je krijgt nu een lijst met de SID's van alle gebruikers. Wat valt je op?
- ☐ Wat is het WDAGUtilityAccount?
- ☐ Welke parameter kan je gebruiken om de SID van 1 gekende gebruiker op te halen?

Er worden bij installatie meerdere accounts aangemaakt, die echter verborgen zijn: Administrator, guest en DefaultAccount en sinds de update van 2017 ook WDAGUtilityAccount (Windows defender application guard).

deze kan je activeren als extra wachter bij het surfen op internet. Je bepaalt wat veilige websites zijn en al de rest wordt gezien als onveilig (browsen met Edge of IE). Deze sites worden dan in Edge een Hyper-V container geopend, zodat alles op je machine veilig is.

-Filter "Name=gebruikersnaam"

4.2.2 Groepen

In computerbeheer zit gebruikersbeheer. Hierin zit de mogelijkheid om ook groepen aan te maken. We gaan 2 groepen maken: studenten en leraars, Mark is een student en Mieke is een leraar.

Dit kan ook weer op 2 manieren:



Groepen via PowerShell

New-LocalGroup studenten

en om Mark aan de groep toe te voegen:

Add-LocalGroupMember -Group "studenten" -Member "Mark"

PowerShell cmdlets i.v.m. groepen:

- Get-LocalGroup

- Get-LocalGroupMember
- Set-LocalGroup
- Rename-LocalGroup
- Remove-LocalGroup
- Remove-LocalGroupMember



Groepen via Gui

Computerbeheer (computer management) > Local users and Groups
 >Groups : in het venster waarin de groepen opgesomd zijn (en dat zijn er default al een heleboel) RMK → new group en dan vul je venster in
 → je voegt Mieke toe aan de groep leraars. (checknames gebruiken in het add venster)

Je kan ook enkel de file Local Users and Groups openen: windowstoets + r en dan LUSRMGR.MSC en dan ok.

Handboek: thema 3 pg 65

Gebruikersaccountbeheer of User Account Control (UAC)

Gebruikersaccountbeheer of User Account Control (UAC) is een techniek in Windows om bepaalde taken te beveiligen. Als je bijvoorbeeld een taak wil uitvoeren, die enkel door een administrator mag uitgevoerd worden, wordt dit gecontroleerd en zo nodig wordt achter een administrator wachtwoord gevraagd. Standaard is die UAC ingeschakeld en het is geen goed idee deze uit te schakelen. Je kan wel het veiligheidsniveau instellen. Hoe hoger het niveau, hoe meer controle, hoe meer pop-up vensters met waarschuwingen. Dit niveau kan je in het venster gebruikersaccount instellingen wijzigen veranderen.

Als je met meerdere gebruikers op 1 computer werkt is het soms wel gewenst dat je bepaalde bestanden of mappen kan delen of juist moet kunnen afschermen. In NTFS zit dit, zoals al eerder aangegeven, ingebouwd.

Met behulp van onze gebruikers Mark en Mieke en hun respectievelijke groepen studenten en leraars gaan we dat nu verder bekijken.

4.2.3 Acces control list

NTFS bestandssyteem (gezien in hoofdstukken 1 en 2): elke map, elk bestand krijgt een eigenaar. De eigenaar bepaalt de toegangsrechten tot de map of het bestand en kan die ten allen tijde wijzigen.

Een gebruiker die een map of bestand creëert wordt automatisch eigenaar van die map of dat bestand.

Dus een gebruiker krijgt het recht om zijn eigen bestanden of mappen te beheren, hij moet hiervoor geen administrator zijn.

Er zijn verschillende basismachtigingen, maar nog meer geavanceerde machtigingen.

In de eigenschappen van een bestand of map bij beveiliging / geavanceerd / tabblad delen staat wie de eigenaar is.

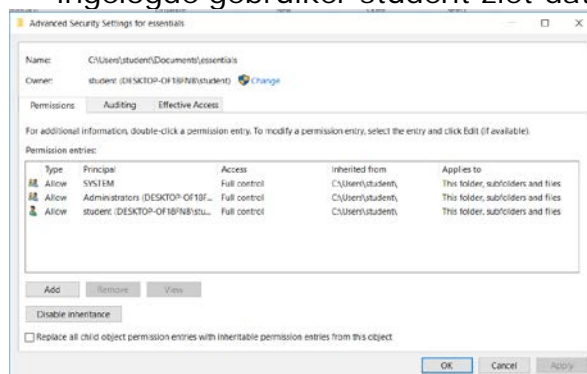
De NTFS permissies worden bijgehouden in de ACL (access control list) van dat bestand of die map. Dit wil dus zeggen dat je zowel op mapniveau als op bestandsniveau permissies kan instellen. Standaard worden permissies overgenomen van bovenliggende mappen, maar dit kan je wijzigen. Ook kan je een onderliggend bestand andere machtigingen geven dan de bovenliggende map, op die manier overschrijf je de rechten van de map.

Per soort toegang kan je instellen dat je dit toe laat (allow) of weigert (deny) aan een bepaalde groep of gebruiker. Je bepaalt hiermee wie toegang heeft tot bestanden en mappen en welk soort toegang (lezen, schrijven, ...).

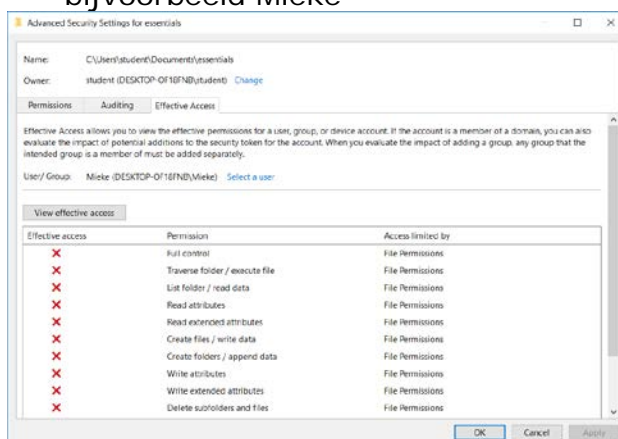


NTFS machtigingen via Gui

- Opvragen en instellen van de NTFS machtigingen doe je via de GUI in de eigenschappen (properties) van een bepaalde map of een bepaald bestand.
- Onder het tabblad **Security** vind je de permissies per gebruiker.
- Voorbeeld: Op een map essentials in de documenten map van de ingelogde gebruiker student ziet dat er zo uit:

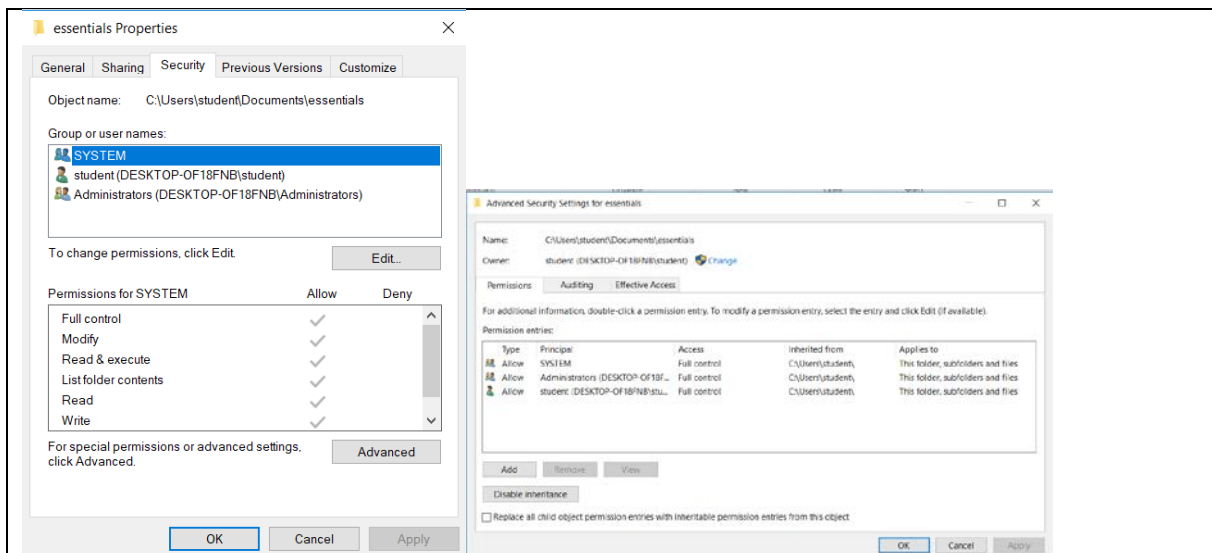


- Je kan ook de toegang voor een bepaalde gebruiker bekijken: bijvoorbeeld Mieke

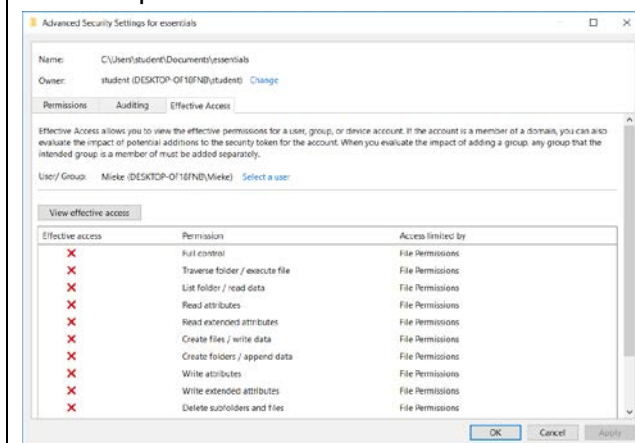


Opdracht: SID

- ☐ Maak in de documentenmap van je huidige gebruiker een map 'essentials' aan.
- ☐ Bekijk wat de ACL is van de huidige gebruiker op deze map en de permissies. (voeg knipsels toe van je scherm.)



- ☐ Bekijk de effectieve toegang van gebruiker Mieke op die map. Maak hier ook een knipsel van.



ACL via PowerShell

In PowerShell kan je de ACL opvragen met Get-Acl en het pad en wijzigen met Set-Acl

Opvragen:

```
PS C:\Users\student> Get-Acl .\Documents\essentials |fl

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Users\student\Documents\essentials
Owner     : DESKTOP-OF18FNB\student
Group     : DESKTOP-OF18FNB\None
Access    : DESKTOP-OF18FNB\leraars Allow ReadAndExecute, Synchronize
           NT AUTHORITY\SYSTEM Allow FullControl
           DESKTOP-OF18FNB\student Allow FullControl
           BUILTIN\Administrators Allow FullControl

Audit     :
Sddl      : O:S-1-5-21-4129551401-3805438843-1356764579-1001G:S-1-5-21-4129551401-3805438843-1356764579-513D:AI(A;OICI;0x1200a9;;;S-1-5-21-4129551401-3805438843-1356764579-1005)(A;OICIID;FA;;;SY)(A;OICIID;FA;;;S-1-5-21-4129551401-3805438843-1356764579-1001)(A;OICIID;FA;;;BA)
```

Wijzigen:

Om te wijzigen ga je eerst het recht in een object steken en dan dit object instellen in acl. Dit zijn dus verschillende stappen die je moet doen, je kan er dus best een script van maken. Zie voorbeeld bij 4.2.4

4.2.4 Permissies of machtiging

Gebruikers

- Lokale gebruikers: alle gebruikers op deze PC
- Externe gebruikers: gebruikers op het netwerk
- Systeemgebruikers: programma's

Groepen

- Ingebouwde groepen: administrators, Iedereen
- Zelf groepen maken om gebruikers in onder te brengen. (komt uitgebreid aan bod in Server OS)
- Zijn belangrijk voor de permissies.

Permissies instellen per item

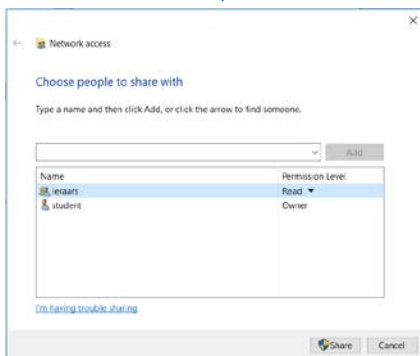
- Je kan op elk item (map of bestand) afzonderlijke permissies instellen voor een gebruiker of voor een groep.
- Standaard worden permissies van bovenliggende items overgenomen. Dit wil zeggen, dat als je leesrechten hebt op een map, je ook leesrechten hebt op de inhoud van die map. Je kan dit uitvinken voor een bepaalde map.
- Je hebt 3 soorten permissies: toestaan of weigeren kan je aanvinken, maar als je niks aanvinkt, wordt die actie niet toegestaan, maar ook niet geweigerd. Deze nuance is zeer belangrijk omdat weigeren sterker is dan toelaten. Dit wordt in opdracht 2 uitgewerkt.



Opdracht: Permissies

- ☐ Je bent nog steeds ingelogd met je eigen account. Voeg de groep leraars toe aan de map essentials en geef hen leesrechten. (voeg knipsels toe met stappen hiervoor).
- ☐ Kijk nu in PowerShell naar de acl van de map essentials. (knipsel toevoegen)
- ☐ Open in de GUI de effectieve toegang voor de map essentials en bekijk de toegang voor Mieke. Is deze gewijzigd ten opzichte van vorige keer (het knipsel in 4.2.3)? Schrijf je conclusie op.
[Mieke mag nu lezen in de map, omdat Mieke deel uitmaakt van de groep leraars. Mieke krijgt dus dezelfde rechten dan de hele groep.](#)
- ☐ Maak in de map essentials een bestand 'vak.txt' aan. Zet hierin de tekst: Leraars mogen dit lezen, maar mogen dit niet wijzigen. Doe dit met een opdracht in PowerShell.
[Set-Content \\$env:UserProfile\Documents\essentials\vak.txt "Leraars mogen dit lezen, maar mogen dit niet wijzigen."](#)

- ☐ Log in met Mieke en ga op zoek naar de documenten map van de student. Vind je deze? Heb je een verklaring hiervoor?
Dit komt omdat machtigingen wel naar onderliggende mappen worden doorgegeven, maar niet naar bovenliggende mappen.
- ☐ Log terug in met je eigen account. Ga in je verkenner naar de map essentials. Deel deze map met de groep leraars, enkel leesrechten op de gedeelde map.
Je kan deelrechten met het tabblad delen (Share) instellen in de verkenner of met het tabblad delen (share) in eigenschappen (properties). Beter is om enkel de map te delen via geavanceerd delen. Zo komt de boomstructuur van de deler niet zichtbaar, maar komt de map onder netwerk in de verkenner. Ook hier kan je kiezen voor verborgen mappen door achter de naam van de map in het deelvenster een \$-teken te zetten. (zie handboek thema 12)



- ☐ Log nu in met Mieke en kijk of je de map nu wel vindt. Open het document vak.txt. Voeg er de regel 'mag ik schrijven' aan toe. Sla dit op. Lukt dit? Wat moet je doen?
Hij opent het dialoogvenster om het bestand ergens op te slaan, je kan dit niet gewoon opslaan.
- ☐ Log zelf terug in en zorg in de acl van vak.txt dat Mieke in dit document mag schrijven. (=schrijfrechten)
Controleer dit weer in de effectieve toegang.
- ☐ Log nu met Mieke in en probeer opnieuw om de tekst 'mag ik schrijven' toe te voegen in het bestand. Kan je dit opslaan?
Ja, nu mag Mieke dit wel opslaan in de map van de andere gebruiker.
- ☐ Log zelf terug in en bekijk het bestand.



ACL instellen via PowerShell

In PowerShell kan je de ACL instellen of wijzigen. Hiervoor moet je de rechten in een object steken en deze toekennen aan een item.

Veronderstel dat je nu de groep leraars volledige toegang wil geven op het bestand vak.txt.txt

Hiervoor heb je meerdere commandoregels nodig, dus maak je best een script. Onderstaand script wordt uitgevoerd vanuit jouw gebruikersmap. Als je dit script wil testen, moet je eerst een document vak.txt.txt aanmaken in de essentials map.

```
#eerst haal je de acl van het bestand/map op waar je de rechten wil wijzigen
$acl = Get-Acl .\Documents\essentials\vak.txt.txt
#leraars alle toegang geven op dit bestand
$toegangsRegel = New-Object System.Security.AccessControl.FileSystemAccessRule("Leraars","FullControl","Allow")
$acl.SetAccessRule($toegangsRegel)
$acl | Set-Acl .\Documents\essentials\vak.txt.txt
```

Toegang kan je achteraf controleren met Get-Acl
 .\Documents\essentials\vak.txt.txt

Besluit

- Effectieve toegang tot een map of bestand is een optelsom van verschillende rechten: delen + ACL
- Effectieve toegang is het resultaat van alle machtigingsvermeldingen (overerving van rechten) → bekijk het in het tabblad van permissies.



Opdracht: Permissies

Even laten zien dat een deny (weigering) geen goed idee is.

- ☐ Log zelf in. Stel in dat de leraars in vak.txt niet mogen schrijven. (met een deny of weigering).
- ☐ Log terug in als Mieke, open het bestand vak.txt en typ: 'ik mag hierin schrijven'. Sla dit op. Lukt dit? Verklaar.

Dit lukt niet, want een deny is veel krachtiger dan een allow. Dus ook al heeft Mieke schrijfrechten, door het feit dat leraars geweigerd wordt om te schrijven, mag Mieke toch niet schrijven.

Besluit

- Weigeren (deny) heeft voorrang op toestaan (allow).
- Weigeringen instellen wordt afgeraden omdat het dan moeilijk wordt om iemand toch dingen afwijkend van de groep waar die in zit toe te staan. Er is dus een groot verschil tussen iets niet toestaan en iets weigeren!!!!
- Bovenstaande uitleg is voor gebruikers op dezelfde computer. Dit wordt in OS Advanced bij Servers nog verder uitgewerkt. (trajectschijf 2)

4.2.5 Encryptie

We hebben besproken hoe je mappen en bestanden kan delen of aan bepaalde gebruikers machtigingen geven om bestanden te lezen, te wijzigen of mappen en bestanden al dan niet te mogen verplaatsen. Deze rechten worden overgeërfd door onderliggende mappen en bestanden en soms heeft iemand ongewenst toch toegang tot persoonlijke mappen. Om er nu voor te zorgen dat persoonlijke mappen ook persoonlijk blijven, kan je de inhoud encrypteren.

In Windows 10 (niet aanwezig in de Home editie) heb je 2 mogelijkheden om je eigen materiaal te beschermen: Bitlocker en EFS. Bitlocker bespreken we onder schijfbeheer, want dit is een manier om je hele schijfinhoud te encrypteren.

EFS

Met EFS (Encrypting file system) kan je mappen of bestanden encrypteren. Hier al onmiddellijk een waarschuwing: exporteer je EFS-certificaat naar een veilige locatie, zodat je je sleutel altijd kan terugvinden, ook als er iets zou misgaan met Windows op je computer. Zonder certificaat kan je immers niet meer bij je versleutelde inhoud.

Het versleutelen van een bestand/map is verbonden aan de gebruiker die de versleuteling doet. Dit wil zeggen dat een andere gebruiker op de computer de inhoud niet kan bereiken.



Versleutelen of encrypteren van een bestand:

1. Open verkenner.
2. RMK op het bestand of map die je wil encrypteren.
3. Eigenschappen (properties)
4. In tabblad Algemeen > geavanceerd.
5. Inhoud versleutelen om gegevens te beveiligen aanvinken.
6. Ok en in het vorige venster Toepassen.
7. In het pop-up venster kan je nu kiezen of je alleen dit bestand of ook de bovenliggende map wil versleutelen. Hier kies je alleen dit bestand en ok.
8. Als je nu in de verkenner gaat kijken dan zie je dat er een slotje op je bestandspictogram staat.

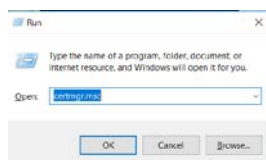
Opmerking opslag Key

Vergeet nu niet je certificaat en sleutel op een externe opslagruimte op te slaan, bijvoorbeeld een USB stick. Je kan dit ook doen, de volgende keer dat je inlogt op Windows, maar doe het! Het is geen goed idee te kiezen om het nooit te back-uppen.

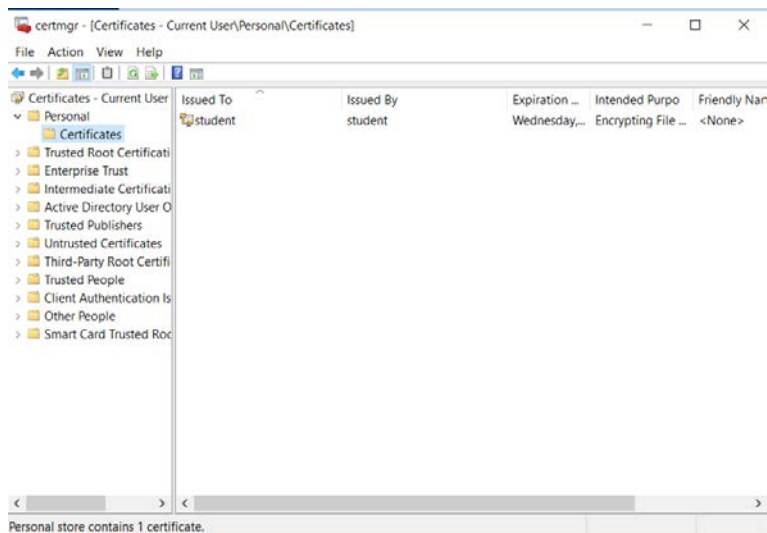
Om het certificaat en de sleutel extern op te slaan kies je dit en doorloop je de Wizard, kies het voorgestelde. File to Export: browse hier naar je aangesloten externe opslagruimte en geef de file een naam.

Indien je de sleutel vergeet op te slaan, omdat je niet snel genoeg op de melding geklikt hebt, kan je dit nog steeds doen. De sleutel zit nl in je certificaat manager opgeslagen.

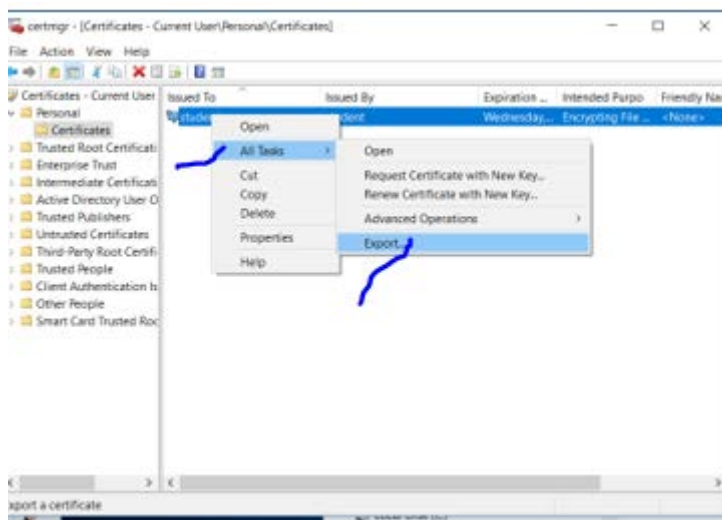
Hier geraak je via het venster windowstoets+R en dan vul je certmgr.msc in.



Onder de map 'Personal' vind je een map 'certificates' en hierin zit je sleutel.



Klik rechtermuisknop op sleutel en kies dan 'All Tasks' en dan 'Export' en dan start ook de Wizard om je sleutel op te slaan.



Ondanks het feit dat je je bestand geëncrypteerd hebt, kan je een andere gebruiker toch toegang geven tot dit bestand. Hiervoor moet je zijn sleutel aan jouw bestand toevoegen.

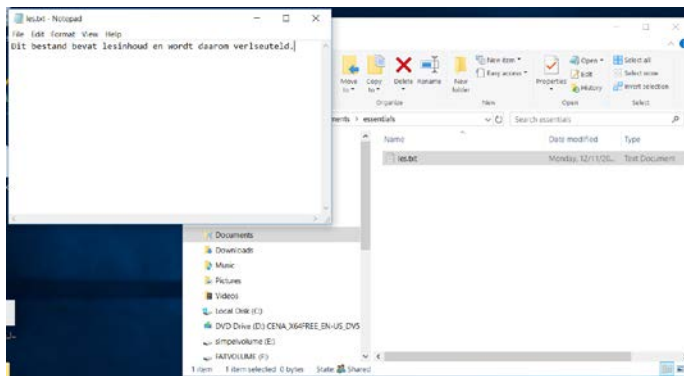
Om een sleutel te hebben, moet een gebruiker wel minstens 1 keer een bestand of map geëncrypteerd hebben.

⇒ Let op: een USB heeft standaard bestandsinstelling FAT32 (zie eerder): encryptie is enkel bij NTFS bestandsinstelling → maar toch blijft die encryptie op het bestand bestaan.



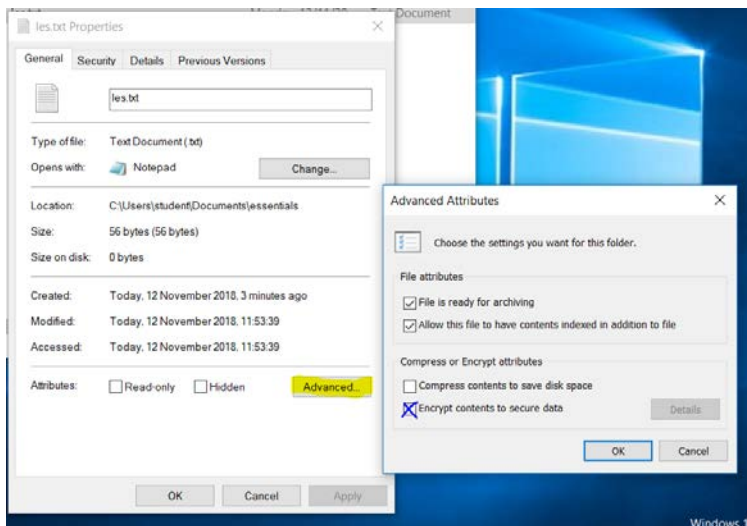
Opdracht: EFS

- Maak een bestand les.txt in de map essentials. Zet hier tekst in: dit bestand bevat lesinhoud en wordt daarom versleuteld.

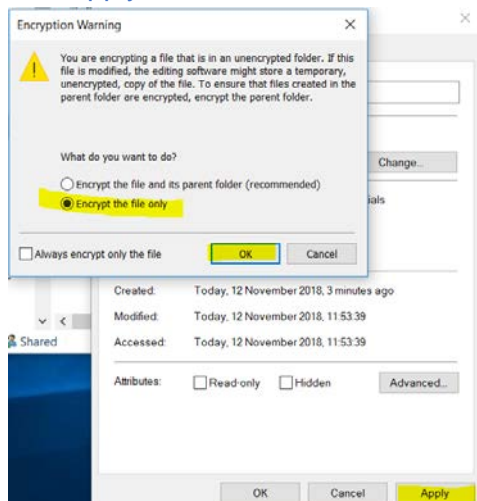


- Versleutel dit bestand zoals hierboven beschreven. Zorg nu dat Mieke dit bestand kan lezen.


Als student:



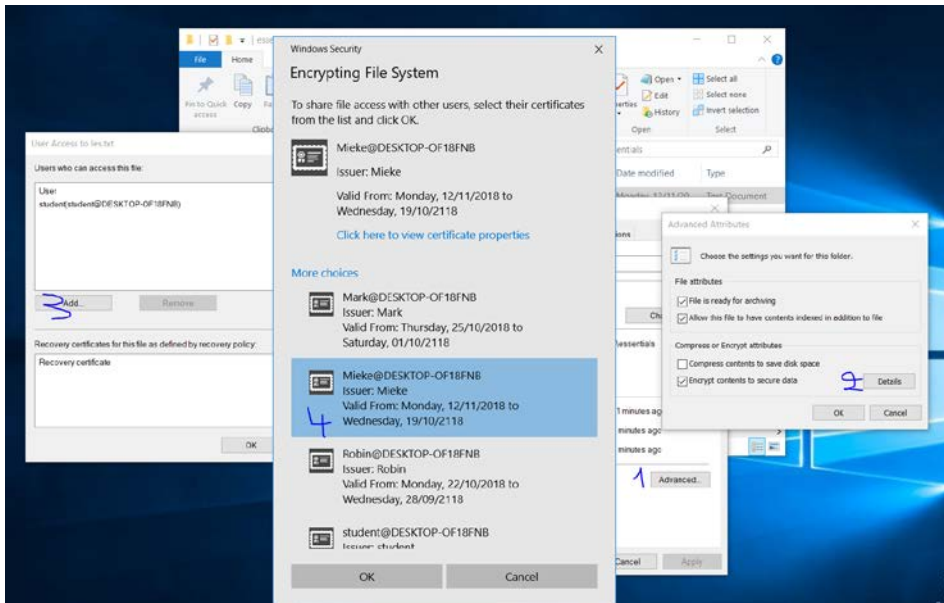
Dan apply en enkel het bestand:



Dan krijg je de optie om je sleutel op te slaan, doe dit ook. Anders moet je dit toch later doen, zodat je dit niet kwijtraakt.

Name	Date modified	Type
 les.txt	Monday, 12/11/20...	Text Document

Daarna bij Mieke inloggen en bij haar een document sleutelvoorbeeld.txt versleutelen, zodat zij ook een certificaat heeft. (screenshots zijn eender)
Terug inloggen als student en dan de sleutel van Mieke aan het document les.txt toevoegen:



1. Kies in properties Advanced, dan op Details bij encrypted. In het volgende venster op Add en dan kies je de juiste persoon uit de lijst om toe te voegen. In ons geval Mieke . en dan ok in alle openstaande vensters .

□ Test de werking

Log terug in als Mieke en als je de permissies juist hebt staan, zie je dat Mieke het document kan openen en lezen/schrijven.



EFS via PowerShell

Hier moet je eerst zelf een certificaat aanmaken met een script zodat je een public key en een private key hebt. Je kan het nu met die public key versleutelen en met de private key decoderen. Dit is geen leerstof binnen dit opleidingsonderdeel, maar voor wie het eens wil proberen:

<https://mcpmag.com/articles/2017/10/05/encrypting-data-with-powershell-cmdlets.aspx>.

4.2.6 Samenvatting:

Encryptie

- bestandsinhoud versleutelen
- niet leesbaar zonder sleutel
- afgedwongen door complexe wiskunde

Permissies:

- toegang toelaten of weigeren
- leesbaar en schrijfbaar op schijf

- Afgedwongen door Windows

Delen:

- Mappen en/of bestanden zichtbaar maken voor andere gebruikers
- Mappenstructuur wordt zichtbaar voor anderen.

Besluit:

- Encryptie en machtiging: het meest restrictieve telt
- volledig beheer + versleuteld + geen toegang = geen toegang
- schrijven toegestaan + versleuteld + toegang = schrijven
- besluit: elk moet toegang bieden opdat ook toegang mogelijk is.

4.2.7 Delen in thuisnetwerk

In hoofdstuk 2 werd netwerken besproken. We hebben nu telkens items gedeeld en hier rechten aan toegekend voor groepen of individuele gebruikers. Maar natuurlijk kan je ook delen over het netwerk.

Thuisnetwerk vind je in handboek in thema 12.



Opdracht: Delen in het thuisnetwerk

- ☐ Maak een tweede vm aan. Pas nu het delen over het netwerk toe volgens de uitleg in het handboek.

Als je over het netwerk deelt is het geen goed idee om te delen gewoon via de knop delen in het tabblad, maar ga je geavanceerd delen. Deze hele uitleg vind je in het handboek terug.

4.2.8 Oefeningen

Oefeningen1

Maak met behulp van PowerShell een nieuwe gebruiker Mo (wachtwoord pxl) aan en maak hem lid van de groep studenten.

New-LocalUser Mo

Add-LocalGroupMember -Group Users -Member Mo

Add-LocalGroupMember -Group studenten -Member Mo

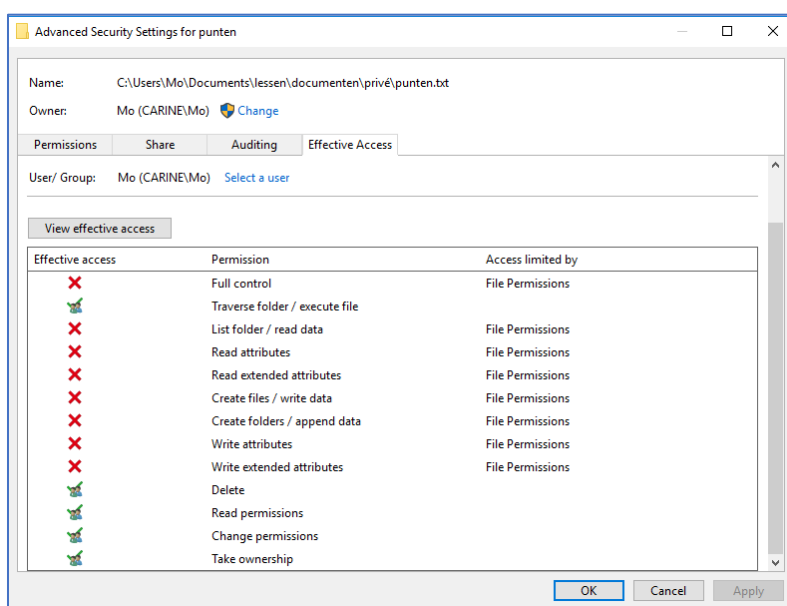
exit

Oefeningen2

(GUI of PowerShell)

- Elke gebruiker is automatisch eigenaar (met full control) over een item dat hij/zij zelf aanmaakt.

- Log in met gebruiker Mo en maak een map 'lessen' in zijn documentenmap.
- Maak, in deze map 'lessen', een map 'documenten'. In die map documenten maak je een map 'privé'. Daarin zet je het document 'punten.txt'.
- Bekijk de effectieve toegang van Mo op het document 'punten.txt'
- Stel nu volgende rechten in:
 - De map lessen deel je met gebruikers en met studenten: lezen is toegestaan.
 - De map lessen voor studenten: schrijven is geweigerd
 - Lezen is geweigerd voor studenten op de map privé.
- Open het document 'punten.txt'. Bekijk de rechten van Mo op de map 'privé' en op het document 'punten.txt'.



- Verklaar wat je ziet.

Omdat Mo in de groep studenten zit, mag hij in zijn eigen map niet meer lezen of schrijven.

Oefening 3

- Maak bij Mark een map 'lessen' aan en zorg dat studenten hierin mogen lezen.
- Zet er een document "lesinhoud.txt" in en zorg dat Mo hier full access op heeft.
- Laat Mo het document verwijderen. (delete, dus naar de prullenbak)
[Dit lukt omdat Mo full access heeft.](#)
- Laat Mo een nieuw document 'nieuwelesinhoud.txt' maken in de map lessen van Mark. Lukt dit? Bekijk de rechten en de effectieve toegang voor Mo.
[Dit lukt niet omdat Mo enkel leesrechten heeft op de bovenliggende map lessen.](#)

- Kijk in welke prullenbak het verwijderde document zit. Plaats het terug. (Restore)
Het zit in de prullenbak van Mo, hij kan dit niet terug zetten omdat hij enkel leesrechten heeft op de map lessen, waar dit dan naar teruggezet wordt.

4.3 Schijfbeheer (disk management)



Handboek. Thema 9 schijfbeheer



Voor schijfbeheer moet je ingelogd zijn met een administrator account. Vooraleer je ook maar iets gaat wijzigen aan je bestaande indeling op de schijven: maak altijd eerst een backup van je data!

Met schijfbeheer kan je:

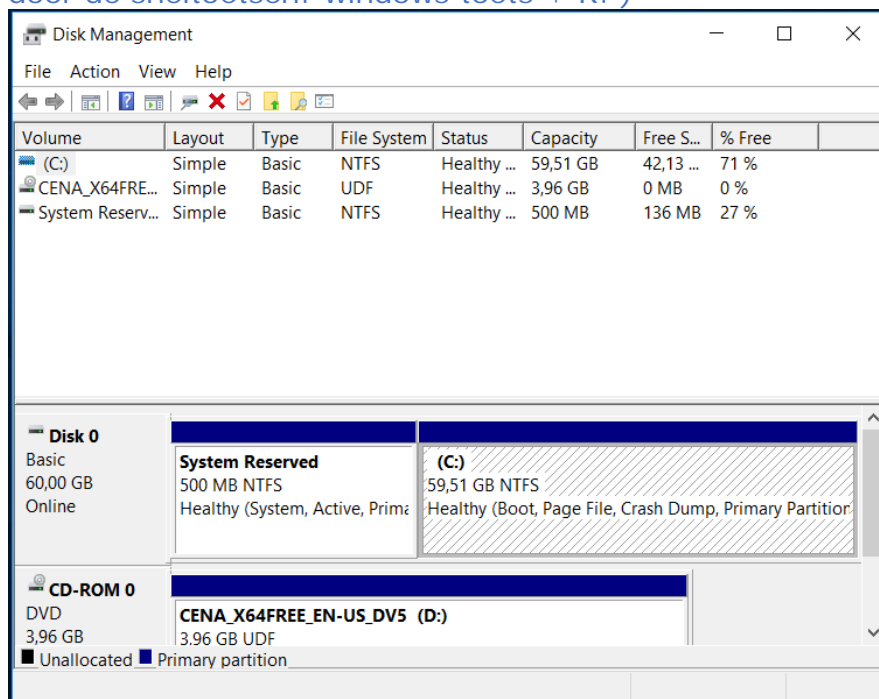
- Partities maken en beheren (vergroten, verkleinen, verwijderen)
- Stationsletters toekennen aan volumes
- bepalen of een schijf een standaard ('basic disk') schijf of een dynamische ('dynamic disk') is, eventueel omzetten van standaard naar dynamisch en in sommige gevallen ook andersom.
- meerdere gekoppelde schijven beheren: extra mogelijkheden indien meerdere dynamische schijven gekoppeld zijn.
- formatteren



Opdracht: Je eigen situatie

- ☐ Bekijk je eigen situatie in schijfbeheer.

rechtermuisklik op startknop ⇒ kies schijfbeheer of 'disk management' (of menuoptie uitvoeren (run) en typ: diskmgmt.msc ⇒ Uitvoeren krijg je ook door de sneltoetsen: windows toets + R.)



4.3.1 Standaard schijf

Er is 1 schijf: deze is standaard en bevat het boot systeem van Windows.

Goed om weten: Windows OS kan enkel booten van een standaard (basic) schijf.

Een schijf is in dit geval een fysieke schijf (je kan het vastnemen). Als je een schijf toevoegt aan het systeem krijgt deze van schijfbeheer automatisch een identificatienummer, zoals disk 0, disk 1, CD-ROM 0 Dit wordt grafisch weergegeven beneden in schijfbeheer venster.

Bovenaan staat een meer gedetailleerde informatie van de stations, als zijnde het bestandssysteem en de nog beschikbare ruimte op de schijf.

De traditionele harde schijf wordt echter steeds meer vervangen door een SSD-disk. Dit is reeds in hoofdstuk 1 besproken.

Een harde schijf is opgedeeld in kleine stukjes die we sectoren noemen. Een sector was vroeger typisch 512 bytes groot. Tegenwoordig zien we ook vaak sectoren van 4 kB groot.

4.3.2 Partities:

Partities of volumes zijn delen van een fysieke schijf die zich op een bepaalde manier gedragen. Dit gedrag wordt bepaald door het besturingssysteem en het bestandssysteem waarmee ze geformatteerd zijn. Meer info voor de opbouw van de harde schijf vind je ook in hoofdstuk 1.

4 mogelijke bestandssystemen:

4.3.2.1 FAT32:

- Bijna elke besturingssysteem kan er naar schrijven en ervan lezen,
- er zit geen ingebouwd veiligheidssysteem in,
- wordt vooral gebruikt voor USB of externe schijven, die tussen verschillende machines, met verschillende OS gebruikt worden.
- Schijven tot maximaal 2TB en bestanden tot 4GB
- Partitie max 32GB (theoretisch tot 2TB)

4.3.2.2 Ext4:

- Wordt gebruikt door Linux.
- Duidelijke verbetering ten opzichte van de vorige versies wat performantie, betrouwbaarheid en capaciteit betreft.
- Er wordt geen gebruik gemaakt van blokken met eenzelfde grootte, maar er wordt een startpunt en eindpunt bijgehouden van waar iets is weggeschreven. Hierdoor beperkt Linux fragmentatie.
- Om Ext4 in Windows 10 te gebruiken heb je extra software nodig.

4.3.2.3 NTFS:

- New Technology File System
- Gebruikt vanaf Windows NT
- Gebruik van bepaalde gegevensstructuren bevorderen de prestatie en de betrouwbaarheid t.o.v. Fat32.
- Er wordt gebruik gemaakt van metadata voor elk bestand, deze wordt niet mee gekopieerd naar een FAT32 partitie
- Beperkte uitwisseling gegevens met Linux en Mac OS X, afhankelijk van de versie (alleen lezen of ook schrijven)

- 32bit bestandssysteem
- Ingebouwde beveiligingsmogelijkheden (wachtwoorden, instellen toegangsrechten)
- Onbeperkte grootte van de schijf, bestandsgrootte wordt beperkt door grootte volume (tot 16 TB in de praktijk, een uitvoerbaar bestand mag niet groter dan 2Gb zijn)
- Partitiegrootte tot 256 TB

4.3.2.4 HFS plus:

- Wordt gebruikt door Apple
- Grootte volumes en bestanden is afhankelijk van het besturingssysteem
- Kan door Windows gebruikt worden, mits het installeren van extra software



de meest logische om te gebruiken voor Windows 10 zijn Fat32 en NTFS:

Opmerking:

- Je kan enkel Fat32 converteren naar NTFS zonder data verlies, indien er voldoende vrije schijfruimte op het station voor handen is. Indien je dit met volume E (ingesteld als fat32) wil doen, geef je in CMD (als admin) het volgend commando : *convert E: /fs:ntfs* en dan wordt gevraagd naar een naam voor volume E.
- Converteren van NTFS naar FAT32 kan enkel door formateren, in dit geval blijft data **niet** behouden.

4.3.3 Verschillende soorten partities:

4.3.3.1 Primaire partitie:

- Krijgt een stationsletter
- Deze kan niet verder opgedeeld worden
- Windows kan enkel van een primaire partitie opstarten: de opstartpartitie waar de Windows systeembestanden staan: **C:** dit wordt ook wel een systeempartitie genoemd. (= actieve partitie)

4.3.3.2 Logische partitie

- Bevindt zich in een uitgebreide partitie
- Is een eenvoudig volume.
- Krijgt een stationsletter.

4.3.3.3 Samengestelde volumes

- Minstens 2 schijven:
- Gespiegeld of 'mirrored' volume : 2 partities op 2 fysieke schijven met gelijke grootte. Beide partities bevatten dezelfde data, zo heb je altijd een back-up.

- 'spanned' volume: logisch volume dat fysiek over 2 of meer schijven verdeeld is. Is het volume op de ene schijf vol, wordt op de volgende schijf verder geschreven/
- 'striped' volume: de gegevens worden verdeeld over 2 fysieke schijven. Er worden telkens blokken data weggeschreven in stripes, beurtelings naar de 2 schijven. Wegschrijven data verloopt snel, maar bij verlies van 1 schijf is alle data onbruikbaar geworden.

4.3.3.4 Partities zonder stationsletter

- Er wordt automatisch een 'System Reserved Partition' (Recovery) of 'Original Equipment Manufacturers' (OEM partitie) aan van 500 MB zonder letter (sinds de update april 2018 wordt er soms wel een stationsletter aan toegevoegd)
- o.a. de bootbestanden in de 'Boot Configuration Data' (BCD) store en de opstartbestanden voor 'Bitlocker Drive Encryption' zitten hier in.
- Een uitgebreide of 'extended' partitie: (zie oefening 1)
 - deze kan wel onderverdeeld worden in maximaal 24 logische partities
 - voordeel omdat stationsletters beperkt zijn door ons alfabet
 - kan enkel op een schijf met MBR indeling
 - Een extended partitie aanmaken kan in een terminal.
 - Windows toets + r → diskpart + ok → terminal opent in DISKPART
 - Nu select disk x (waarbij x het nummer van de schijf is)
 - >create partition extended size=xxxx (=grootte partitie)
 - >create partition logical size=xxxx (=grootte logische partitie, Kleiner dan extended partitie)
 - >assign letter=X (X=stationsletter, kan dus eender welke letter zijn)
 - Nu opent zich een venster om de logische schijf te formateren.

```
DISKPART> create partition extended size=1000
DiskPart succeeded in creating the specified partition.
DISKPART> create partition logical size= 500
DiskPart succeeded in creating the specified partition.
DISKPART> assign letter=F
DiskPart successfully assigned the drive letter or mount point.
DISKPART>
```

Resultaat:

Disk 1 Basic 2,00 GB Online	logische station f (F:) 500 MB NTFS Healthy (Logical Drive)	500 MB Free space	1,02 GB Unallocated
---	--	----------------------	------------------------

- Een mounted partitie
 - een partitie mounten in een lege map (let op: op een NTFS-volume)
 - aantal is onbeperkt: voorwaarde een lege map
 - vrije ruimte nodig op je schijf (eventueel ruimte vrijmaken)
 - is een eenvoudig volume

- kan aangemaakt worden door de wizard te doorlopen, waarmee je de koppeling legt met de lege map

4.3.3.5 *opmerking stationsletters:*

Letters A en B zijn voorbehouden voor diskette stations en D voor CD/DVD drive, elk extern opslagstation krijgt een vrije letter, dus best enkele letters overhouden hiervoor)

4.3.4 Twee soorten schijven

4.3.4.1 *standaard schijf of 'basic disk' in MBR*

- 4 primaire partities of 3 primaire partities en 1 uitgebreide partitie
- bevat enkel eenvoudige of 'simple' volumes

4.3.4.2 *dynamische schijf of 'dynamic disk'*

- Ondersteunt een onbeperkt aantal volumes.
- Converteren van 'basic' naar 'dynamic' mag nooit met de schijf waarop de primaire partitie staat. Probeer dit eens! (er verschijnt nu een waarschuwing dat je dan niet meer kan booten van deze schijf)
- Ondersteunt 'simple' volumes: grootte kan aangepast worden, op voorwaarde dat het volume rechtstreeks op een dynamische schijf gecreëerd werd. (niet indien dit al op een standaard schijf is aangemaakt, en die schijf later geconverteerd werd naar een dynamische schijf)
- Voor de andere volumes moet je meerdere dynamische schijven geïnstalleerd hebben.
- Gespiegelde, spanned, striped en Raid worden op een dynamische schijf gezet. Indien je deze op een standaard schijf probeert te formateren krijg je een waarschuwing, want booten kan alleen van een standaard schijf en als je deze omzet naar een dynamische schijf, kan je systeem niet meer booten.

4.3.5 Data stockeren op schijf

De allereerste sector van een harde schijf is niet onderdeel van een partitie en bevat typisch informatie over de indeling van de schijf: de partitietabel. Er wordt hier ook bijgehouden van welke partitie het systeem moet opstarten. Die eerste sector komt in 2 vormen voor: MBR (Master Boot Record) en GPT (GUID Partition Table):

MBR

- kan maximaal uit 4 primaire partities bestaan. Je kan wel een extended partitie gebruiken om zo ook meerdere logische partities toe te voegen.
- Gevoelig aan fouten: als de eerste sector van de harde schijf fouten bevat, komt de werking van het MBR in gedrang

GPT

- De opvolger van MBR
- Houdt een redundante kopie van zichzelf bij op de laatste sector zodat de eerste sector zichzelf kan herstellen als de eerste sector fouten bevat
- grotere en meerdere partities mogelijk op een standaard schijf
- ondersteunt 128 primaire partities (heeft geen uitgebreide partities)

- Bevat niet alleen een partitietabel maar ook een “protective MBR”. Dankzij dit stukje kan GPT zich voordoen als een MBR met maar 1 primaire partitie. Dat wordt gebruikt zodat GPT ook gebruikt kan worden op systemen die enkel MBR ondersteunen.

converteren van MBR naar GPT op een basic disk is enkel mogelijk voordat de schijf de eerste keer gepartitioneerd wordt.

4.3.6 Onderhoud en herstel



Handboek blz 201

4.3.6.1 Defragmenteren

- Fragmentatie ontstaat vanzelf door opslaan, wijzigen en wissen van bestanden
- Besturingssysteem vult lege ruimtes op, die ontstaan zijn door eerdere schrijfbewegingen (wijzigen, wissen). Als de lege ruimte te klein is, wordt de rest in de volgende lege ruimte gezet.
- Defragmenteren is bestanden terug samenvoegen op schijf.

SSD vs HDD

Een HDD:systeem wordt traag, omdat bestanden moeten samen gezocht worden. Een SSD:systeem blijft snel, ook al staan gegevens op duizenden plaatsen verspreid opgeslagen
conclusie: HDD defragmenteren, SSD niet.

4.3.6.2 Optimaliseren

Het optimaliseren kan je plannen in Windows 10, zodat dit automatisch gebeurt. Om een SSD - schijf te optimaliseren kan je

- Indexering zoekfunctie beperken, verplaatsen of uitschakelen
Een SSD is zo snel met het uitlezen van bestanden dat het onnodig is de bestanden te laten indexeren. Schakel de zoekfunctie uit (via het configuratiescherm, onderdeel Indexeringsopties).
- volume verkleinen
- Virtueel geheugen verkleinen, verplaatsen of uitschakelen
(via configuratiescherm, onderdeel Systeem, taak Geavanceerde systeeminstellingen, tabblad Geavanceerd, Prestaties, knop Instellingen , tabblad Geavanceerd, knop Wijzigen.)
- Schakel de hybride slaapstand/sluimerstand uit
Elke keer dat de computer in de hybride slaapstand gaat, wordt het RAM-geheugen naar het bestand hiberfil.sys op de SSD-schijf weggeschreven. Dit kan worden uitgeschakeld met het commando `POWERCFG /HIBERNATE OFF` in het opdrachtvenster (te openen via het Win-X startmenu, Opdrachtprompt (als administrator opstarten)).
- Verplaats persoonlijke mappen naar een extra interne schijf
Door een extra (harde) schijf aan de configuratie toe te voegen en de mappen met persoonlijke bestanden (bv Documenten, Afbeeldingen) hiernaar te verplaatsen wordt het aantal schrijfacties op de SSD-schijf

aanzienlijk verminderd. Tevens blijft er meer ruimte over voor toepassingen.

4.3.7 Extra opslagmedia



Handboek thema 9 blz 188-200

4.3.8 BitLocker

Vroeger werden vooral desktop computers gebruikt, m.a.w. deze werden ergens geïnstalleerd en bleven daar staan. Risico op verlies van het toestel was beperkt.

Nu worden meer en meer mobiele toestellen of laptops gebruikt en ook de data op de desktop computers is niet meer veilig, omdat deze toestellen ook met internet verbonden zijn.

We hebben al gezien dat je mappen en bestanden kan encrypteren, zodat deze niet zomaar door iedereen gelezen kunnen worden. Maar als je veel data hebt opgeslagen, kan dit wel een tijdrovende bezigheid zijn.

Een andere manier om je data te beveiligen is om alles wat op de schijf staat te encrypteren. In Windows 10 (niet in de Home editie) wordt zo een systeem meegeleverd: BitLocker.

Om BitLocker te kunnen gebruiken op je computer moet je opslagschijf minstens 2 partities hebben en Trusted Platform Module (TPM ook wel ISO/IEC 11889). Je kan bij het opstarten van BitLocker controleren of jouw computer deze kan gebruiken. In de virtuele omgeving is TPM niet aanwezig, maar als administrator moet je wel weten hoe die op een fysieke computer kan ingesteld worden. Je kan in de bios die TPM aanzetten.

BitLocker is niet opensource, dus niemand weet hoe het je data beschermt en of het dit altijd doet.

Inschakelen BitLocker is in het Configuratiescherm: BitLocker beheren > BitLocker inschakelen.

Het programma controleert of je computer over TPM beschikt; indien deze niet aanstaat, moet je je computer opnieuw opstarten. (verwijder wel alle externe opslagmedia). Wanneer je computer opnieuw opgestart is (met de wijziging van TPM) dan krijg je het BitLocker venster en moet je een wachtwoord instellen. Dit wachtwoord ga je voortaan steeds bij het opstarten van je computer moeten invoeren, anders start die niet volledig op. Je krijgt nu een herstelsleutel, die je zeker moet bewaren (afdrukken, opslaan op usb of ...). Deze heb je nodig om in noodsituaties toch je computer te kunnen ontgrendelen.

Nu moet je kiezen hoeveel je wil versleutelen. Versleutel wat er nu reeds op staat, nieuwe bestanden worden later automatisch versleuteld bij opslaan als je BitLocker hebt aanstaan. (nieuw (als het enkel op Windows 10 computer gebruikt wordt) of compatibel (als de schijf ook met vroegere Windows computers gebruikt wordt)).

Het versleutelen wordt pas doorgevoerd als je de computer opnieuw opstart. Dit kan even duren, maar je computer werkt gewoon. (Misschien wel iets trager tijdens dat versleutelen). Er wordt een melding gegeven als het encryptieproces klaar is. Vanaf dan wordt alles automatisch versleuteld bij opslaan. Denk er wel aan dat je vanaf nu dat BitLocker wachtwoord moet ingeven bij opstarten van de computer.

4.3.9 One Drive

Bij Windows 10 krijg je een online opslagcapaciteit van 5GB gratis= OneDrive. Je kan ervoor kiezen om deze uit te breiden. Deze opslagruimte is via internet van verschillende toestellen bereiken en je kan de map op je harde schijf volledig synchroniseren met OneDrive online, of gedeeltelijk. Zoek in het handboek hoe je dit doet en bekijk ook de mogelijkheden om items te delen met andere toestellen, die al dan niet op Windows draaien en met of zonder een Microsoft account. [Zie ook handboek onder schijfbeheer.](#)

4.3.10 Oefeningen:

Voeg in je vm 3 schijven toe met een grootte van 2GB. Een extra schijf toevoegen aan je vm doe je voordat je deze opstart via 'edit virtual machine settings'. Als je de vraag gesteld wordt, kies je om 2 schijven GPT en 1 schijf als MBR in te stellen.

Tip: maak knipsels van je stappen!

Oefening 1:

Maak 40000Mb vrij op je eerste schijf (waar de C schijf op staat). Maak nu een uitgebreid volume (of extended partition) van 10000Mb

Noteer hier de stappen die je moet doorlopen. Maak een knipsel van het eindresultaat: zowel in schijfbeheer als in de verkenner.

Let op: deze oefening werkt enkel als je drive 0 als mbr is ingesteld. Je kan dat niet meer converteren na installatie van Windows 10, vermits er dan al partities zijn aangemaakt. Gebruik voor deze oefening dan de aparte schijf, die je als mbr hebt ingesteld.

- Windows toets + r → diskpart + ok → terminal opent in DISKPART
- Nu select disk 0
- >create partition extended size=10000 (=grootte partitie)

Oefening 2:

Schijf 1 MBR:

Maak een uitgebreid volume (of extended partition) van 1000Mb

Noteer hier de stappen die je moet doorlopen. Maak een knipsel van het eindresultaat in schijfbeheer als in de verkenner.

Windows toets + R → diskpart → terminal:

```
DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> create partition extended size=1000

DiskPart succeeded in creating the specified partition.

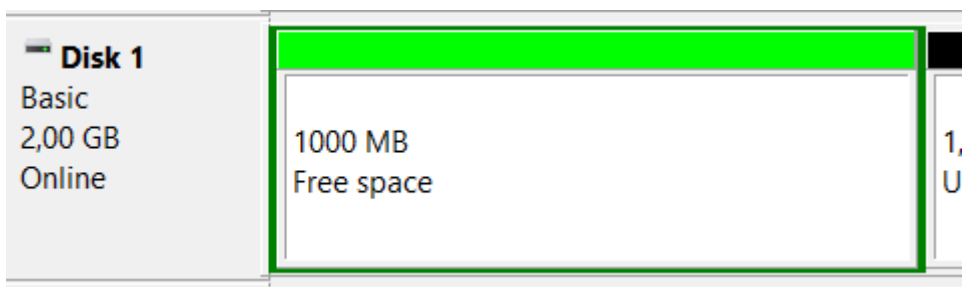
DISKPART> create partition logical size = 500

DiskPart succeeded in creating the specified partition.

DISKPART> assign letter=Z

DiskPart successfully assigned the drive letter or mount point.

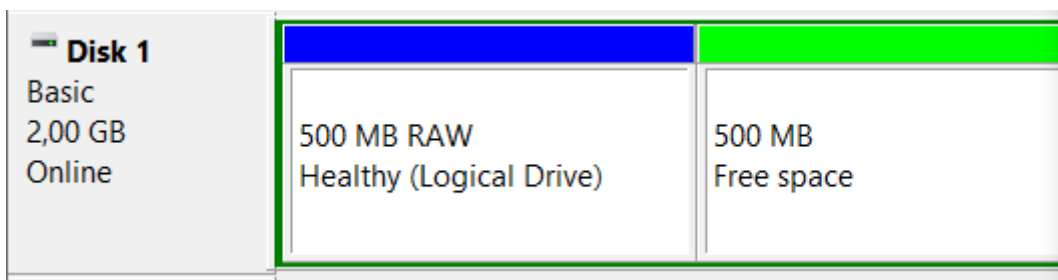
DISKPART>
```

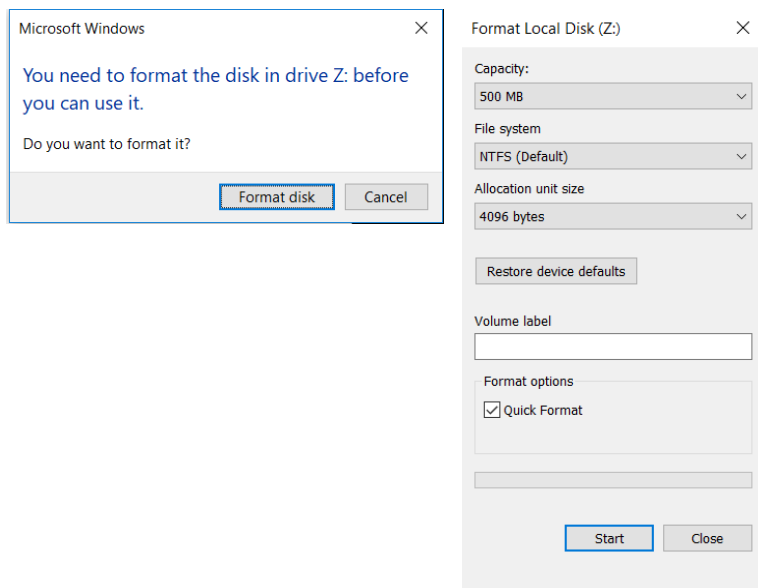


Eerst de uitgebreide partitie aanmaken.

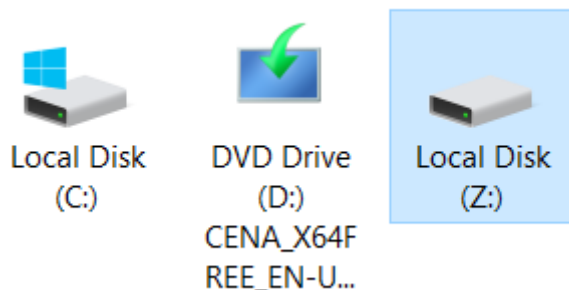
Maak in de uitgebreide partitie op schijf 1 een logisch station met de letter Z en een grootte van 500Mb. Noteer de stappen, maak knipsels : eindresultaat in schijfbeheer en verkenner.

In de uitgebreide partitie een logische partitie aanmaken in de terminal. Deze formateren als erom gevraagd wordt.





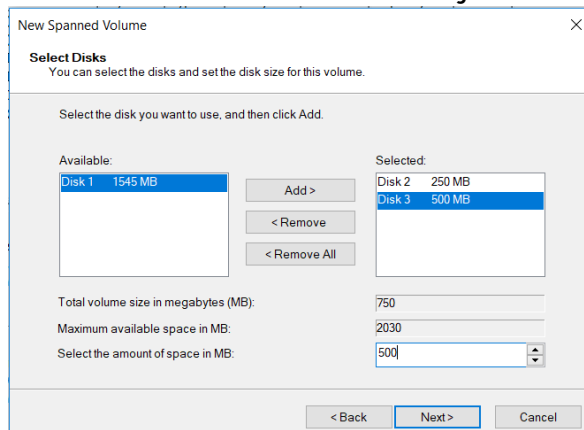
Devices and drives (3)



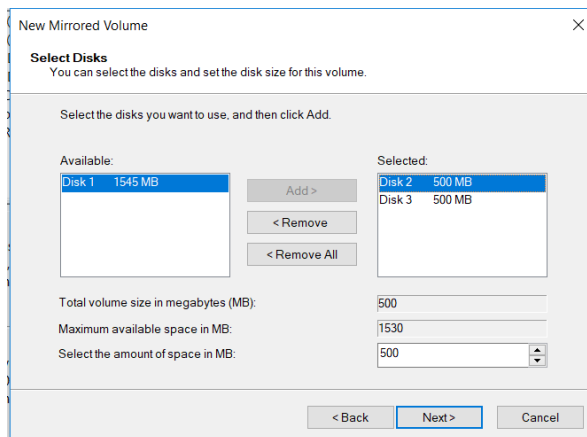
Oefening 3:

Maak van schijf 2 en 3 dynamische schijven.

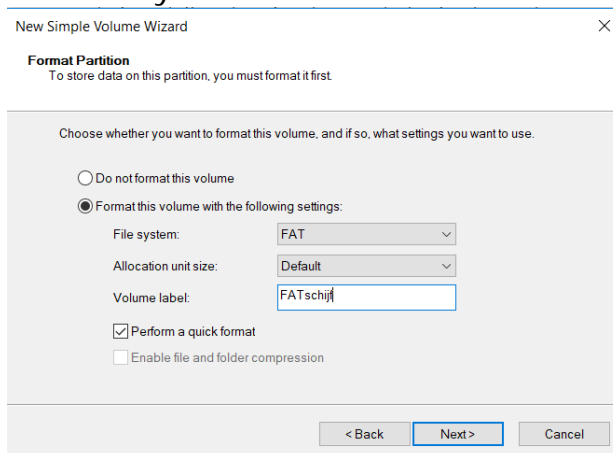
- Maak een spanned volume (E:) van 750 Mb met de naam 'overvloeien' met stationsletter E: 250MB in schijf 2 en 500MB in schijf 3



- Gebruik schijf 2 en 3 om een gespiegelde schijf te maken van 500 MB. Noem dit 'spiegelen' en stationsletter G



-
- Maak op schijf 3 een volume van 1Gb met stationsletter F en bestandssysteem FAT32. Naam= FATSchijf.



-
- Maak nu een knipsel van de situatie in schijfbeheer.

Disk 2 Dynamic 1,98 GB Online	overvloeien (E:) 250 MB NTFS Healthy	spiegelen (G:) 500 MB NTFS Healthy	1,25 GB Unallocated	
Disk 3 Dynamic 1,98 GB Online	overvloeien (E:) 500 MB NTFS Healthy	spiegelen (G:) 500 MB NTFS Healthy	FATSCHIIF (F:) 1000 MB FAT Healthy	32 MB Unallocated

Oefening 4:

Zet een paar .txt bestanden op de F schijf. Converteer nu de FATSchijf naar het bestandssysteem NTFS (met commandline) Noteer wat er gebeurt. Lukt het?


```
C:\Windows\system32>convert F: /fs:ntfs
The type of the file system is FAT.
Enter current volume label for drive F: FATschijf
Volume FATSCHIJF created Sunday, 21/10/2018 22:01
Volume Serial Number is 28DD-E5BF
Windows is verifying files and folders...
File and folder verification is complete.

Windows has scanned the file system and found no problems.
No further action is required.

1.048.297.472 bytes total disk space.
    49.152 bytes in 3 hidden files.
    753.664 bytes in 5 files.
1.047.494.656 bytes available on disk.

    16.384 bytes in each allocation unit.
    63.983 total allocation units on disk.
    63.934 allocation units available on disk.

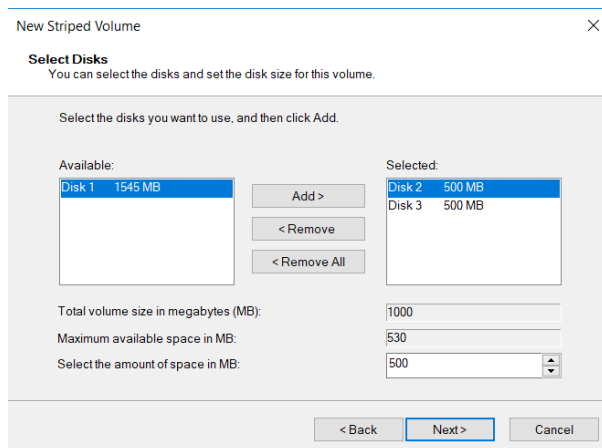
Convert cannot run because the volume is in use by another
process. Convert may run if this volume is dismounted first.
ALL OPENED HANDLES TO THIS VOLUME WOULD THEN BE INVALID.
Would you like to force a dismount on this volume? (Y/N) y
Determining disk space required for file system conversion...
Total disk space:          1024000 KB
Free space on volume:      1022944 KB
Space required for conversion: 6089 KB
Converting file system
Conversion complete

C:\Windows\system32>_
```

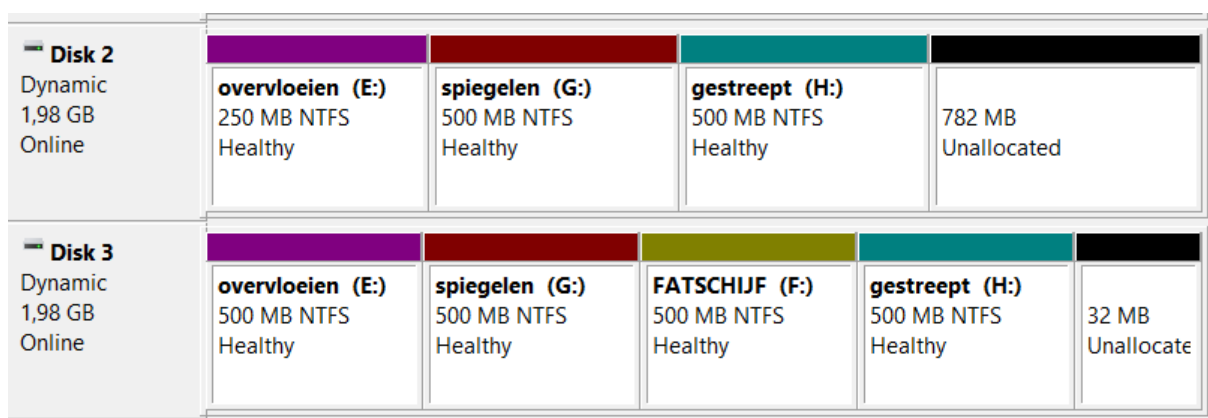
Oefening 5:

Verklein het volume van de F schijf tot 500Mb

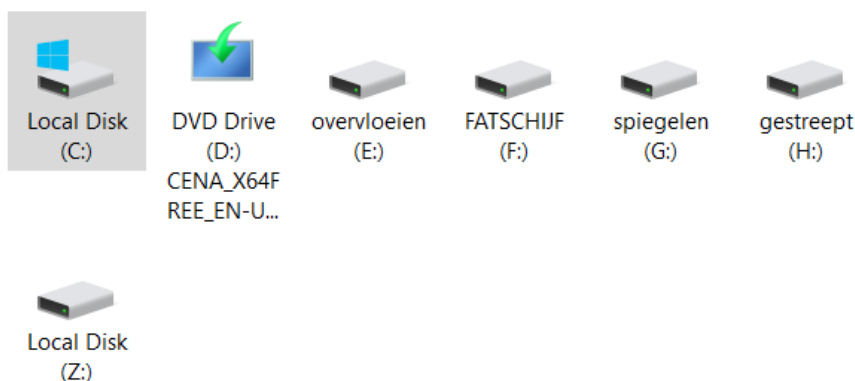
Maak een striped volume op schijf 2 en 3 van 500MB met de naam 'gestreept' en stationsletter H.



Noteer alle stappen en maak weer een knipsel van schijfbeheer en je verkenner.



▼ Devices and drives (7)



Oefening 6:

Breek de spiegel en gebruik de vrijgekomen 500MB van schijf 2 en schijf G om een spanned volume met grootte 1Gb te maken met de naam 'gebrokenSpiegel'.

Wat stel je vast?

Noteer alle stappen en maak weer een knipsel van schijfbeheer en je verkenner.

Spiegel breken, dan volume verwijderen opdat je het kan samenvoegen. Een gebroken spiegel kan je niet in 1 keer volledig verwijderen, je verwijdert slechts 1 deel per keer. Als je een gewone spiegel verwijdert, is wel alles weg.

Op schijf 2 neemt die een ander stuk van 500Mb om samen te voegen met de 500Mb op schijf 3.

New Spanned Volume X

Select Disks
You can select the disks and set the disk size for this volume.

Select the disk you want to use, and then click Add.

Available:		Selected:
Disk 1 1545 MB	Add >	Disk 2 500 MB
	< Remove	Disk 3 500 MB
	< Remove All	

Total volume size in megabytes (MB):

Maximum available space in MB:

Select the amount of space in MB:

Disk 2 Dynamic 1,98 GB Online	overvloeien (E:) 250 MB NTFS Healthy	500 MB Unallocated	gestreept (H:) 500 MB NTFS Healthy	GebrokenSpiegel 500 MB NTFS Healthy	282 MB Unallocated
Disk 3 Dynamic 1,98 GB Online	overvloeien (E:) 500 MB NTFS Healthy	GebrokenSpiegel 500 MB NTFS Healthy	FATSCHIIF (F:) 500 MB NTFS Healthy	gestreept (H:) 500 MB NTFS Healthy	32 MB Unallocate

Devices and drives (7)

