

IT Systems & Devices

Windows Server

Windows Server Configuratie
Versie 1.2.0 | 03-2024

Inhoudsopgave

Introductie Windows Server	3
Het ICT Lyceum.....	4
Aanmaken virtuele machine	5
Configuratie virtuele machine.....	8
ISO	8
Host-Only.....	9
NAT	9
Installatie Windows Server.....	10
Gecontroleerd afsluiten	13
Herstelpunten / Snapshots.....	14
Basis configuratie Windows Server	15
De 'Administrator'	15
Installatie VMWare Tools	17
Configureren van de naam en het netwerk	18
Aanpassen tijdzone	23
Installatie en configuratie Active Directory Domain Services	25
Roles and Features	25
AD DS en DNS	25
Configuratie Active Directory Domain Services	30
De Prefix	31
Global Catalog Server	32
RODC.....	32
NetBIOS-naam	33
Active Directory Users and Computers	38
Installatie en configuratie tweede domain controller	41
Configuratie AD02	41
Pingen.....	43
Default Gateway.....	45
Preferred en Alternate DNS.....	45
Member server toevoegen aan domein.....	47
Inloggen op het domein	50
Fouttolerantie / Redundancy	50
Configuratie AD DS op server AD02	51
Routing en DHCP	54
Installatie Routing and Remote Access + DHCP	54

DHCP - Configuratie DHCP op server AD01	59
APIPA	60
Configuratie DHCP	60
De DHCP-Scope.....	61
Opruimen van snapshots?.....	71
Installatie en configuratie DHCP op AD02.....	73
Configuratie en installatie Windows Client.....	74
Installatie Windows 11.....	77
Wijzigen van computernaam en koppelen aan het domein	84
Configuratie AD DS – Organizational Units (OU's)	87
Aanmaken Security Groups.....	93
Het inrichten van DNS	96
Schijfbeheer en Shares	103
Het aanmaken en koppelen van een nieuwe schijf	103
NTFS.....	110
ReFS	111
Het aanmaken van een Share	114
Aanmaken van gebruikers in het domein	121
Inloggen Windows 11 werkstation op domein	124
Aanmaken én delen van een netwerkprinter	127
Uittdelen van shares en printers via GPO (Group Policy Management)	134
Toepassen van Quota's op gedeelde folders	145
Uittdelen van achtergrond en instellen van beveiliging via GPO	148
Instellen achtergrond via GPO	148
Client beveiliging via GPO.....	151
User Home Folders	155
Quota op de homedrives.....	158
Instellen Shadow Copies – ook wel “Backups”.....	159
Terughalen van Shadow Copies	162
Testen Previous Versions	162
Remote Desktop.....	163

Introductie Windows Server

Tijdens deze readers gaan we werken met Windows Server. Windows Server is feitelijk gezien de ‘grote broer’ van de door jullie bekende Windows 10 of Windows 11 (ook wel Windows Client genoemd). We gaan in op het bouwen van een netwerk, het koppelen van jullie client (module 1) aan de serveromgeving en bijvoorbeeld het delen van bestanden met aangemaakte gebruikers.

In de vorige module hebben jullie uitgebreid kennis gemaakt met Windows Client. Deze kennis gaan jullie nu uitbreiden en koppelen met een nieuwe Windows Server omgeving.

Om goed van slag te kunnen gaan, ben je het volgende nodig:

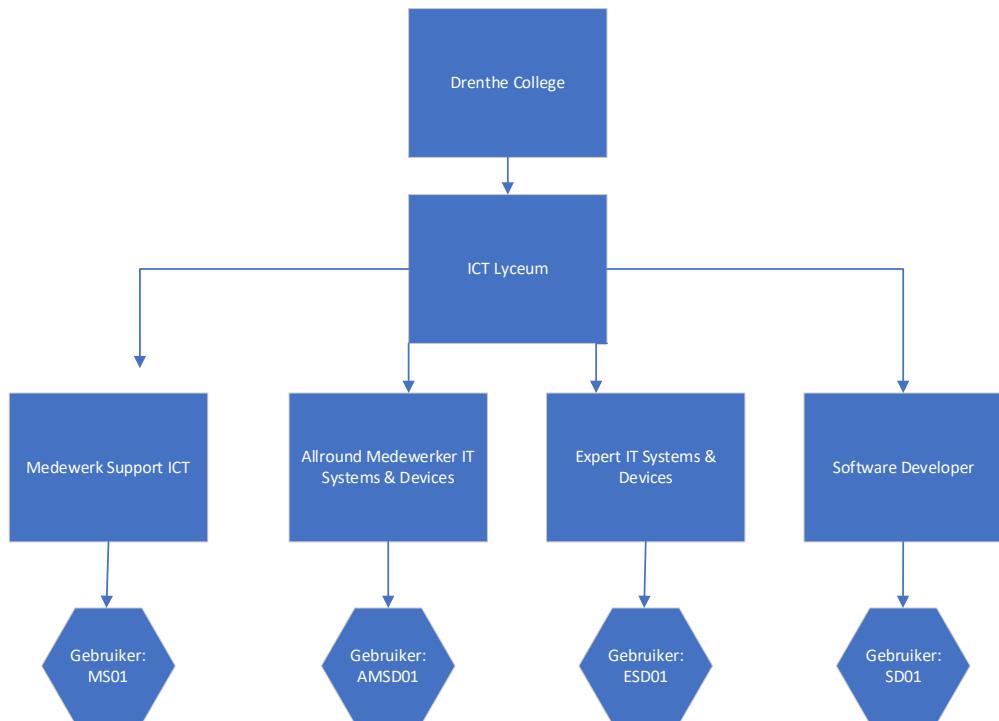
- Basiskennis Microsoft Windows (Kennis Windows Client is een pré)
- De ISO van **de Engelse versie** Microsoft Windows Server (te downloaden via o.a. <https://portal.azure.com>)
- VMWare Workstation Pro

Het ICT Lyceum

Met Windows Server gaan we een netwerkomgeving bouwen voor het 'ICT Lyceum'. Een netwerk binnen het Drenthe College, voor de opleidingen ICT. De opleiding wordt aangeboden door het Drenthe College.

Binnen het ICT Lyceum zitten verschillende opleidingen; Medewerker Support ICT, Allround Medewerker IT Systems & Devices, Expert IT Systems & Devices én Software Developer.

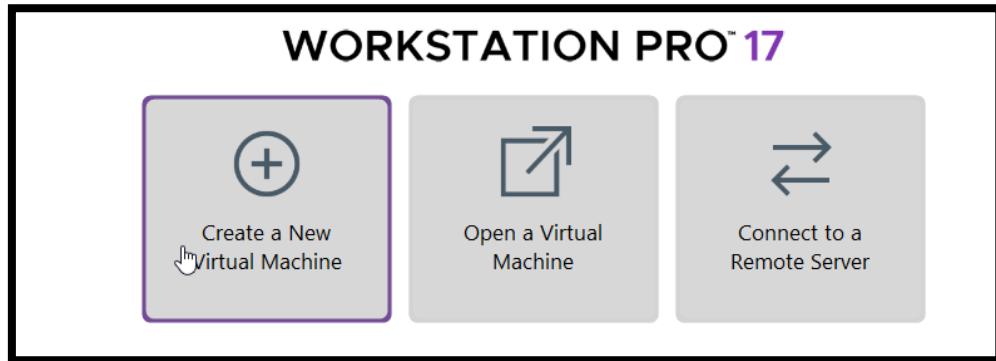
Voor al deze opleidingen gaan we in deze reader uiteindelijk een stuk reserveren in het netwerk en aanmaken als groep in de Active Directory (ook wel een Organizational Unit genoemd, zie H7).



Aanmaken virtuele machine

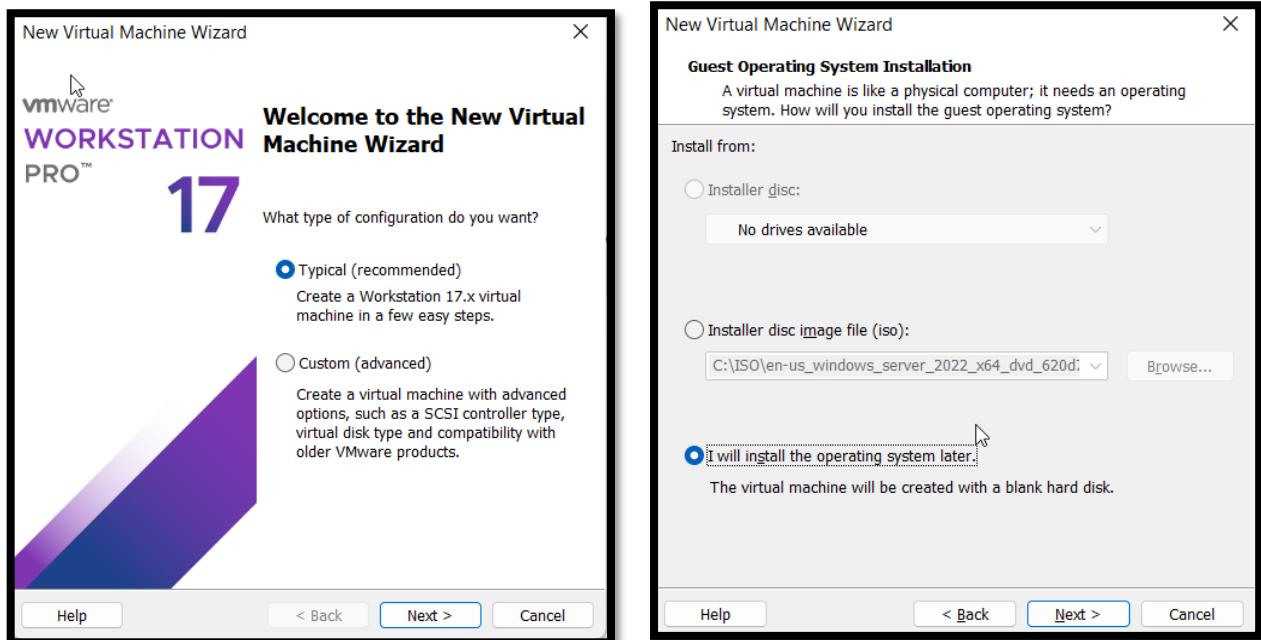
Om te kunnen beginnen met Windows Server, gaan we eerst binnen VMWare Workstation een nieuwe **virtuele machine** aanmaken, verder te noemen; de **VM**. Dit is bijna hetzelfde als met de Windows Client uit module 1, alleen zetten we de specifieke instellingen nét even wat anders dan bij de client.

We beginnen met het aanmaken van een nieuwe machine door simpelweg te kiezen voor **Create a new virtual Machine**:



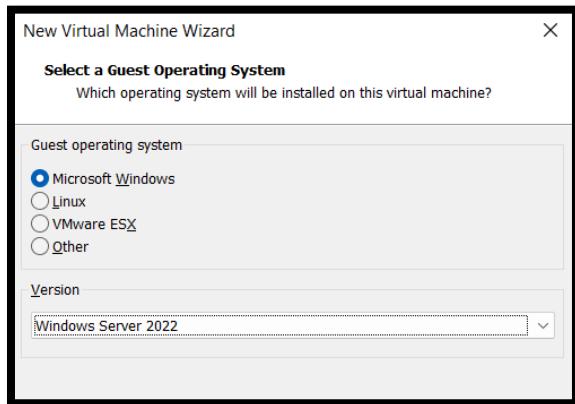
Wanneer je hierop drukt, opent de Wizard om een nieuwe configuratie te starten, je kiest hierbij in principe altijd voor **Typical**. Wanneer je voor Custom kiest, zal VMWare een extra gebruiker aanmaken in je virtuele machine, waarmee je later in de reader problemen kunt krijgen gezien hij hiermee automatisch, zonder wachtwoord, inlogt.

Tevens zorg je ervoor dat de optie **I will install the operating system later**. Is aangevinkt:



In het volgende scherm kies je het gewenste Operating System.

In dit voorbeeld is dat **Windows Server 2022** maar hier kies je de voor jou meest relevante versie.



In principe maakt het hier weinig uit wat je kiest, het is echter zo dat VMware Workstation op basis van deze template de basisinstellingen voor je klaarzet. Mocht je bijvoorbeeld Windows Server 2003 kiezen, heb je minder CPU-kracht en minder memory nodig dan een Windows Server 2022.

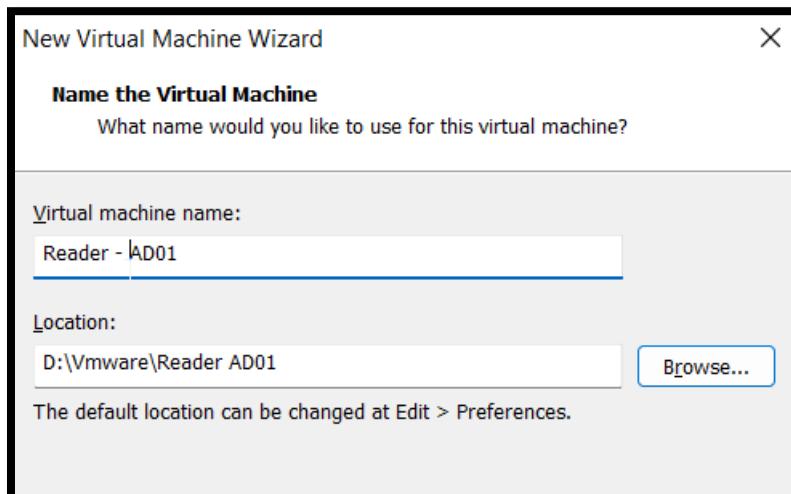
Deze instellingen zijn altijd later te wijzigen (!)

De Virtual Machine name mag je zelf bepalen. Houdt er rekening mee dat we, in deze reader, minimaal 2 servers én een client gaan gebruiken.

Je doet er dus verstandig aan om te kiezen voor een naam waaraan je snel herkent welke machine dit is. Dit kan, als je bijvoorbeeld een Active Directory-server gaat maken (komen we later in de reader op terug), dat je hem **AD01** noemt. De volgende server kan dan bijvoorbeeld eenvoudig **AD02** heteren.

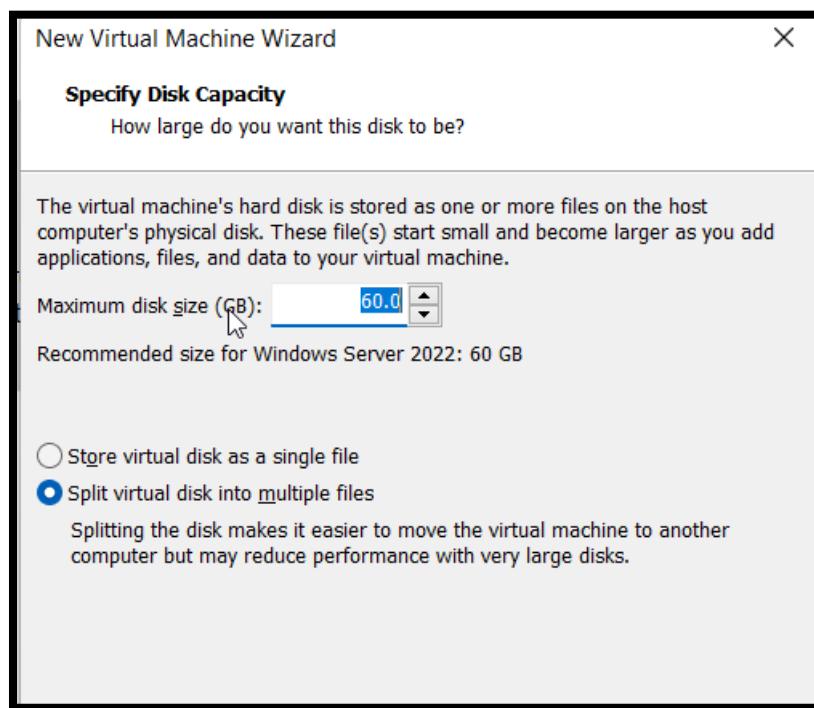
Bij Location is het **ZEER BELANGRIJK** dat je ervoor zorgt dat de machines **NIET** in je OneDrive gezet worden. OneDrive is namelijk gebouwd om te synchroniseren met de Cloud van Microsoft Azure. Hele mooie functie, zet hier ook zeker je bestanden/huiswerk etc. in, maar geen virtuele machines! Omdat deze vaak erg groot zijn, probeert OneDrive dit namelijk in stukje te uploaden naar de Cloud waardoor deze corrupt raken. Wanneer dit eenmaal is gebeurd, zal je opnieuw moeten beginnen met je installatie. Ik zet ze dus altijd in een aparte map op mijn (extra) harddisk van mijn laptop.

Mocht je dit niet hebben, is het aanmaken van een mapje op je C:\-schijf (**Virtuele Machines** bijvoorbeeld) voldoende.

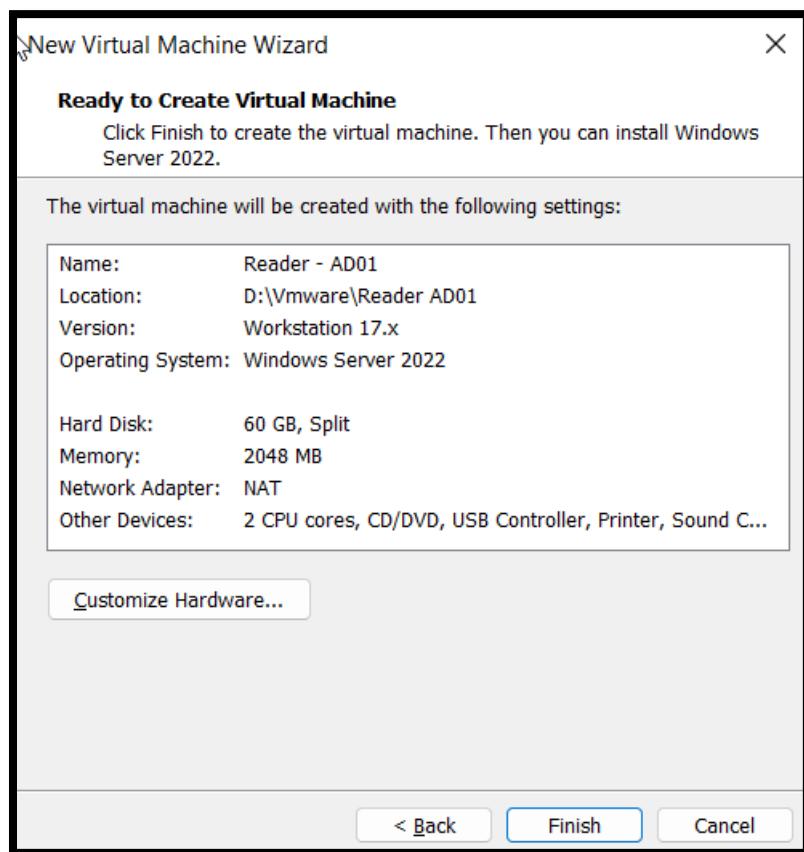


Wanneer je weer op Next druk, kies je de grote van de harddisk. Deze is in eerste instantie ca. 60GB.

Later in de reader gaan we hier een extra schijf bij toevoegen. Voor nu veranderen we niets en kiezen we wederom voor Next.



Gevolgd door **Finish**:

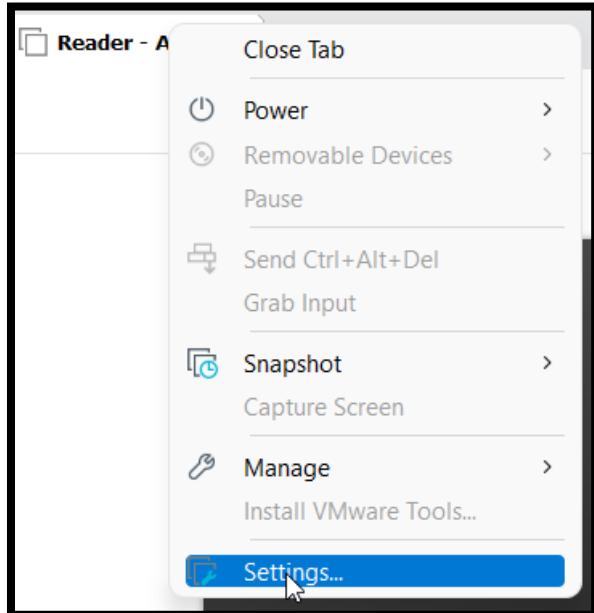


Je hebt nu je eerste virtuele server klaargezet.

Configuratie virtuele machine

Nu je de basis hebt klaar staan, kunnen we daadwerkelijk beginnen met de *configuratie* en *installatie* van je eerste **Windows Server**.

Om te beginnen, klik je in VMWare Workstation, je zojuist aangemaakte VM (Virtuele Machine) aan met de **rechtermuisknop** en kies je voor Settings.

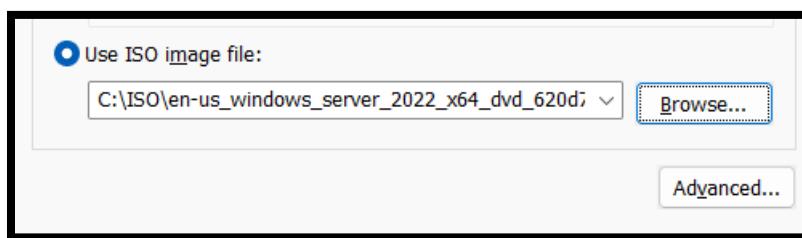


We wijzigen hierbij de volgende instellingen:

Geheugen -> **4GB**

Processors -> **2 processors en 2 cores per processor** (totaal dus 4)

CD/DVD -> **Use ISO image file** -> bestand welke je van Microsoft Azure hebt gedownload. In mijn voorbeeld Windows Server 2022:



ISO

Een ISO is eigenlijk een “virtuele DVD”, ofwel, de installatie van bijvoorbeeld je **Operating System (OS)**. Het is altijd aan te raden om, wanneer je een ISO hebt gedownload, deze centraal op je laptop te plaatsen zodat je hem eenvoudig nogmaals kunt gebruiken én je alle ISO's bij elkaar hebt, bijvoorbeeld in een mapje **C:\ISO**. Via de portal van Microsoft Azure (<https://portal.azure.com>) kun je altijd de benodigde ISO's downloaden. *Houd er hierbij wel rekening mee dat het downloaden soms erg lang (soms zelfs 1 a 2 uur) kan duren.*

Zorg er ALTIJD voor dat je een Engelse variant downloadt van de Windows Server versie! Er is ook een Nederlandse versie, echter is het oplossen van problemen of functies dan vaak erg lastig omdat de vertaling niet altijd even goed is.

Host-Only

De (eerste) Netwerk Adapter zetten we op Host-Only. Dit houdt in dat het verkeer binnen je laptop (je host dus) blijft. Hij kan dus **niet** communiceren met het internet van je eigen installatie van Windows op je laptop.

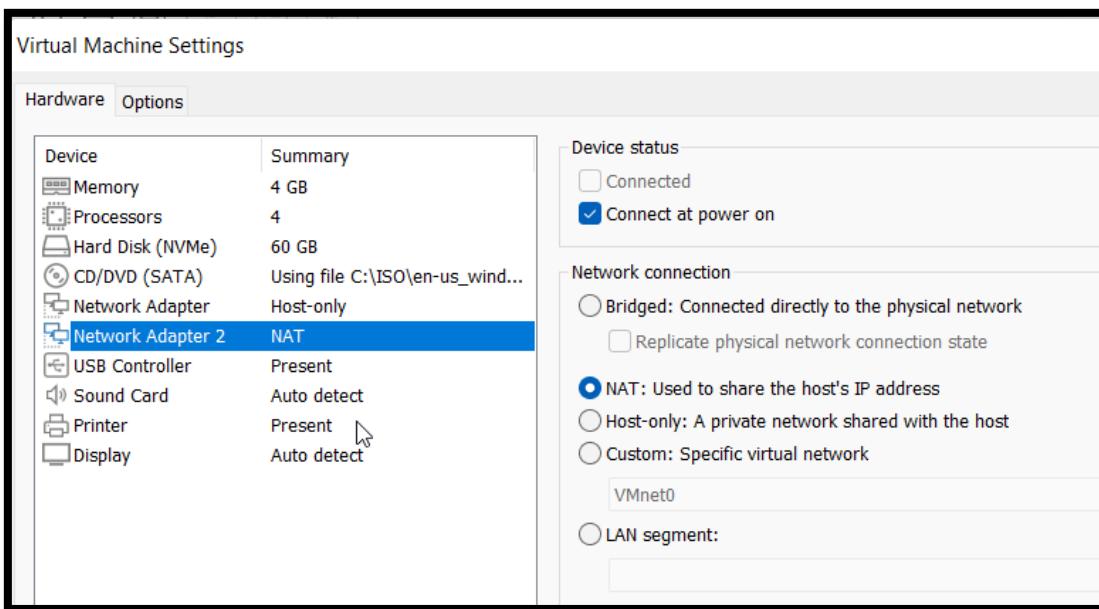
Deze kaart zetten we op Host-Only, omdat deze ervoor gaat zorgen dat hij verbinding kan gaan maken met de te bouwen omgeving; De andere server en natuurlijk uiteindelijk je client.

Wanneer je deze instelling niet aanpast (standaard staat hij op **NAT**) kan het goed zijn dat je straks geen koppeling kunt krijgen tussen je twee servers en/of je client. Hoe we dit concreet doen zie je op de afbeelding hier onder.

NAT

NAT staat voor *Network Address Translation*, heel diep gaan we hier nu niet op in, echter is het wel een ideale instelling om bijvoorbeeld te zorgen voor internet op je VM. Hiermee gaan we ook werken en daarom voegen we, **alleen op deze VM**, een extra netwerk adapter toe.

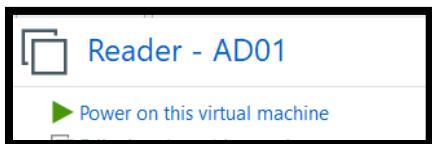
Dit is eenvoudig te doen door onder in de **Settings** te kiezen voor **Add**, gevuld door **Network Adapter** en **Finish**. Uiteindelijk moet je configuratie er (ongeveer) zo uit zien:



Wanneer dit allemaal goed staat, kiezen voor **OK**.

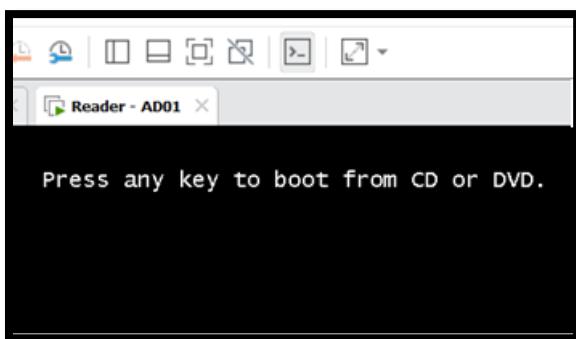
Installatie Windows Server

Je kunt nu je Virtuele machine, AD01, gaan opstarten, door op het groene pijltje (**Power On this virtual machine**) te klikken:

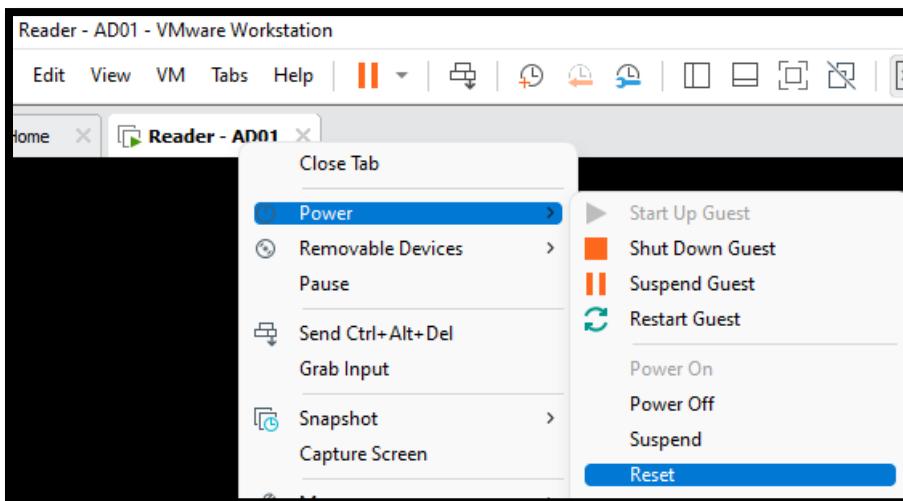


De configuratie van je machine is nu helemaal in orde dus kunnen we eindelijk gaan beginnen met de installatie van het daadwerkelijke **Windows Server Operating System (OS)**.

Wanneer je de machine hebt aangezet, is het belangrijk dat je het scherm in VMWare Workstation activeert (door eenvoudig in het zwarte scherm te klikken). Na het aanzetten heb je ca. 4 seconden om op een **willekeurige knop** te drukken op het moment dat je dit scherm ziet:



Doe je dit te laat, dan start de installatie simpelweg niet en moet je de machine even een reset geven om het opnieuw te proberen:



Wanneer het 'gelukt' is, zal je zien dat de installatie van Microsoft Windows Server gaat starten door middel van het tonen van het Microsoft-logo.

Let op!

Wat belangrijk is om te onthouden binnen het gebruik van een Virtual Machine, is hoe je “er weer uit komt”. Wanneer je namelijk in een zogeheten console-sessie gaat, door het scherm van VMware dus aan te klikken wanneer je de machine inschakelt, zal je merken dat je muis en toetsenbord niet meer helemaal lekker werken buiten de machine om. Wil je dus bijvoorbeeld in je eigen laptop naar Word of PowerPoint of naar je mail, dan kun je daar niet heen omdat je ‘gekoppeld’ zit in de console sessie.

Dit ontkoppel je eenvoudig door de toetsen **CTRL+ALT** een keer tegelijkertijd in te drukken. Je merkt dan dat je gelijk je muis weer kunt gebruiken buiten de VMware sessie om.

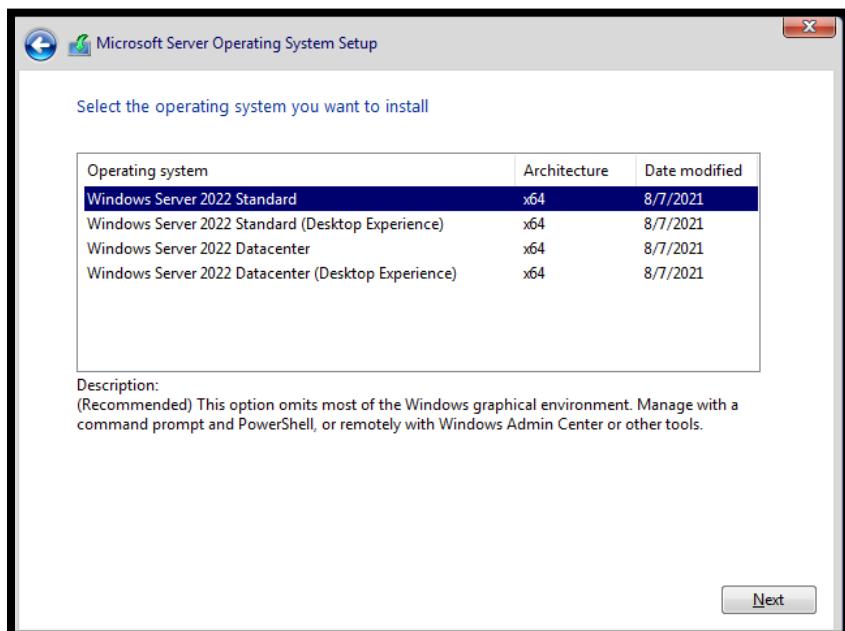
Wanneer de installatie verder loopt komt je na enkele minuten, dit kan overigens wat langer duren bij laptops met tragere (HDD) schijven, in het eerste installatiescherm. Je kiest er hier direct voor om op **Next** te klikken. De taal staat op Engels en de rest kunnen we, desgewenst, later aanpassen. Je kunt daarna gelijk op **Install Now** klikken.

Nu de installatie dan eindelijk daadwerkelijk gestart is, beginnen we eventueel met het invoeren van je **product key**, deze is te vinden in de Portal van Azure. Deze heb je echter voor deze installaties niet nodig. Na de installatie zónder key, is een omgeving altijd 180 dagen vrij beschikbaar.

Binnen deze tijd hebben wij dit project klaar en is het dus feitelijk gezien zonde om hiervoor je product code te gebruiken. Je kunt hem namelijk slechts enkele keren activeren!

We kiezen dus voor '**I don't have a product key**'.

Het scherm wat we hier te zien krijgen, is een zeer belangrijke. Je hebt hier namelijk **twee** belangrijke keuzes:



Namelijk de **Core**-versie en de **Desktop Experience**-versie. Achter de **Core** versie staat niets, dit zijn dus de bovenste en de derde optie zoals je kunt zien in de afbeelding hierboven. De **Windows Server Core** is een zeer krachtige tool, waarbij alles wordt ingesteld via de **Command Line Interface**, ofwel **CLI**. Hiermee gaan we wellicht later nog aan het werk, door middel van PowerShell, echter willen we eerst eens kennis maken van de Grafische versie van Windows Server, ook wel de **GUI** genoemd (**Graphical User Interface**).

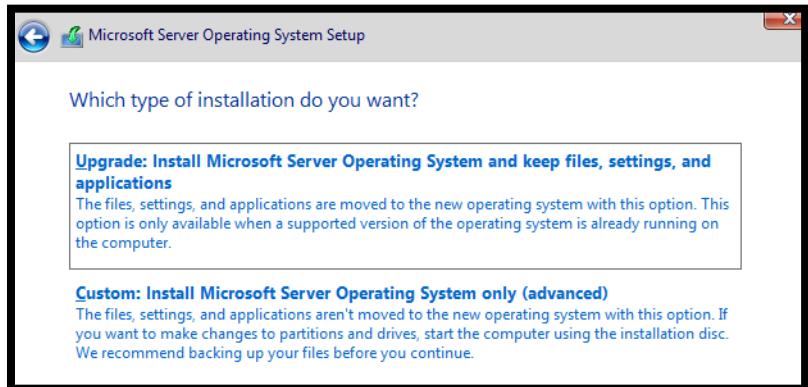
Dus we kiezen hier voor een **Desktop Experience**-versie gevuld door **Next**. Of je hierin Standard of Datacenter kiest, maakt niet veel uit. Dit is slechts een licentie kwestie in de praktijk.

Kies je hier toch per ongeluk voor een NIET Desktop Experience, dan zou je je machine opnieuw moeten gaan aanmaken.

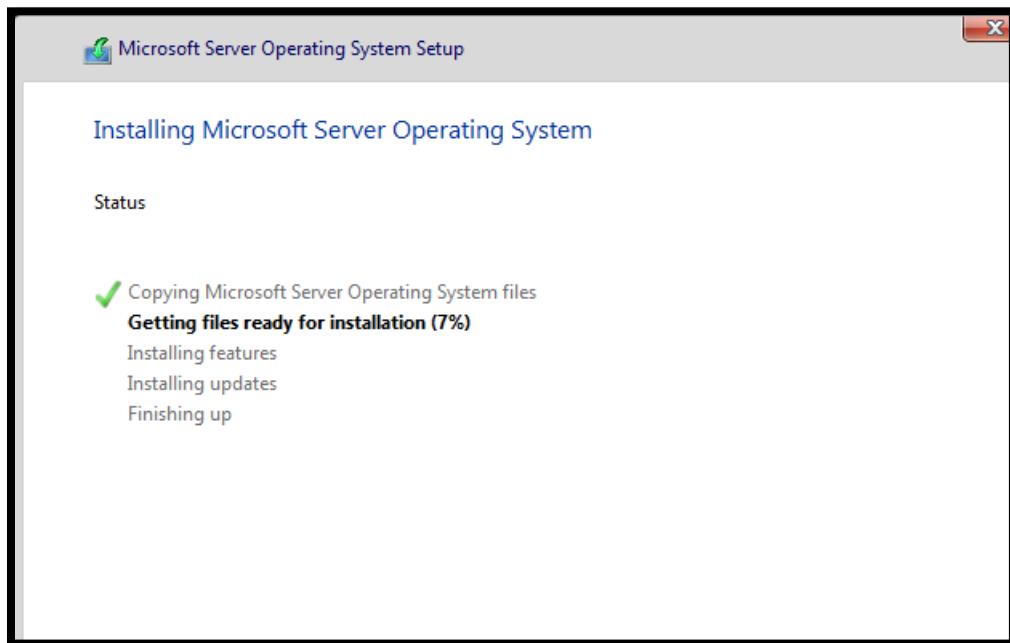
We gaan akkoord met de Voorwaarden (vinkje) en kiezen wederom voor **Next**.

Nu hebben we 2 opties, **Upgrade** of **Custom**. Eigenlijk kun je hier alleen voor **Custom** kiezen, gezien het feit een Upgrade alleen mogelijk zal zijn wanneer je reeds een installatie hebt gedaan en deze wil

'upgraden' naar een nieuwere/hogere versie. Aangezien wij een nieuwe machine aan het maken zijn, is **Custom** dus het meest logisch.



In het volgende scherm kun je aangeven op welke harddisk je de installatie wilt plaatsen. Gezien we in Hoofdstuk 1 hebben gekozen om (eerst) slechts 1 harddisk toe te voegen, is deze keuze dus vrij eenvoudig. Je selecteert deze en kiest voor **Next** en je ziet dan direct dat de installatie gaat beginnen.



Zodra dit klaar is, dit kan afhankelijk van je harddisk (SSD of HDD) zo'n 5 tot 25 minuten duren, is **Windows Server** geïnstalleerd en kunnen we daarmee écht kennis gaan maken. In tussentijd kun je vast het onderstaande doorlezen.

Gecontroleerd afsluiten

Het is belangrijk om een Windows Server, of eigenlijk elke server, gecontroleerd af te sluiten. Wat hiermee bedoeld wordt, is dat is je hem niet gewoon 'uit drukt' door Power Off te kiezen bijvoorbeeld, maar dat je bewust kiest om hem af te sluiten via de **Windows-knop**.

Doe je dit namelijk niet, is de kans groot dat er dataverlies op treedt of dat de server onherstelbaar beschadigd raakt.

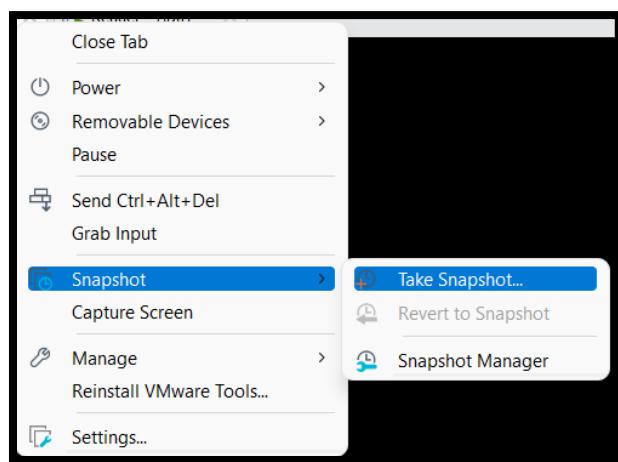
Wanneer je je laptop bijvoorbeeld gewoon uitdrukt, is er vaak weinig aan de hand. Dit komt doordat Windows Client weinig 'achtergrond taken' draait. Een server daarentegen is altijd (24/7) bezig met

taken, services, opdrachten, scans etc. omdat deze daarvoor gemaakt is.
Wees hier dus altijd van bewust tijdens afsluiten óf herstarten.

Herstelpunten / Snapshots

Een belangrijke functie tijdens het configureren of installeren van een VM, is het maken van herstelpunten ofwel Snapshots. In VMware Workstation is hiervoor een eenvoudige tool ontwikkeld waarmee je snel en eenvoudig Snapshots (letterlijk: fotokopieën) kunt maken van de huidige status van je Virtuele Machine.

Je doet dit binnen VMware Workstation eenvoudig door met de rechtermuisknop op je machine te klikken en te kiezen voor Snapshots. Op dezezelfde manier kun je ook snel en eenvoudig teruggaan naar een gemaakte herstelpunt.



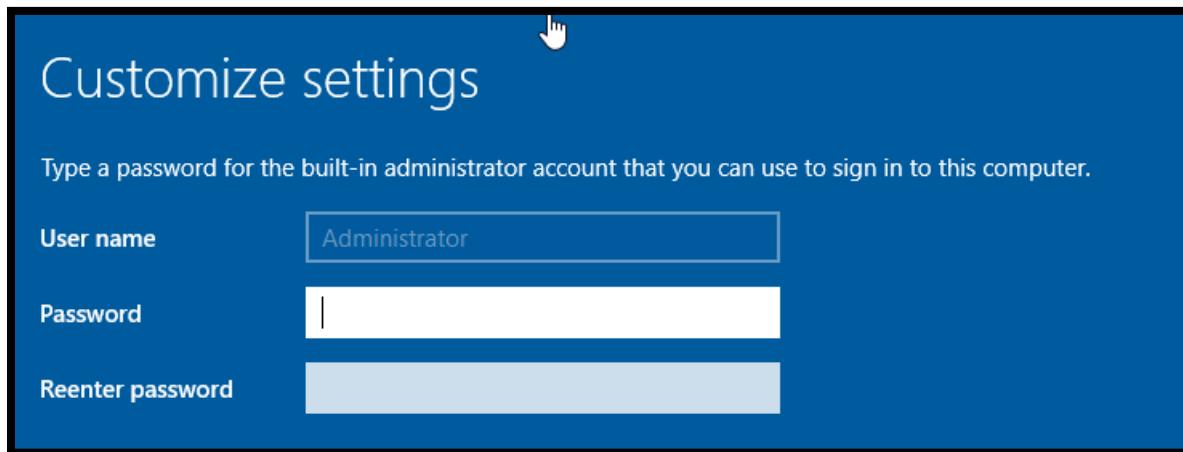
Het is altijd raadzaam om een snapshot te maken, **vlak vóór een belangrijke wijziging of update**. Op die manier kun je namelijk snel en eenvoudig teruggaan naar het punt waar je was, mocht er onverhoop iets fout gaan tijdens de installatie of configuratie, zonder dat het grote consequenties heeft.

Een belangrijke regel is echter wel, dat wanneer je meerdere **domain controllers** hebt draaien, je altijd van hetzelfde moment een snapshot moet maken en/of terugzetten. Domain Controllers maken namelijk gebruik van een database (ook wel de Global Catalog genoemd) en wanneer je hiervan meerder hebt, moet deze altijd intact blijven. Zet dus **nooit** slechts 1 domain controller terug naar een vorig punt, maar altijd beide servers wanneer nodig om eventuele problemen te voorkomen.

Het is niet gezegd dat dit **altijd** problemen oplevert, maar je kunt er maar beter voor zijn dan dat je achteraf denkt 'ohja.... dat had ik moeten doen'.

Basis configuratie Windows Server

Direct na de feitelijke installatie van Windows Server, wordt er gevraagd om een nieuw wachtwoord voor de **Administrator**.



Dit wachtwoord moet je goed kunnen onthouden (*of opslaan in een digitale kluis zoals bijvoorbeeld KeePass*) en moet voldoen aan enkele eisen. Standaard moet deze bestaan uit;

- Minimaal 8 tekens
- Een kleine letter
- Een hoofdletter
- Minimaal 1 speciaal teken (bijvoorbeeld !&*%#).

In deze reader gebruiken we voor elke user het wachtwoord **Welkom01!** Voer deze dus in het bovenstaande scherm **2x** in en kies voor Finish.

De 'Administrator'

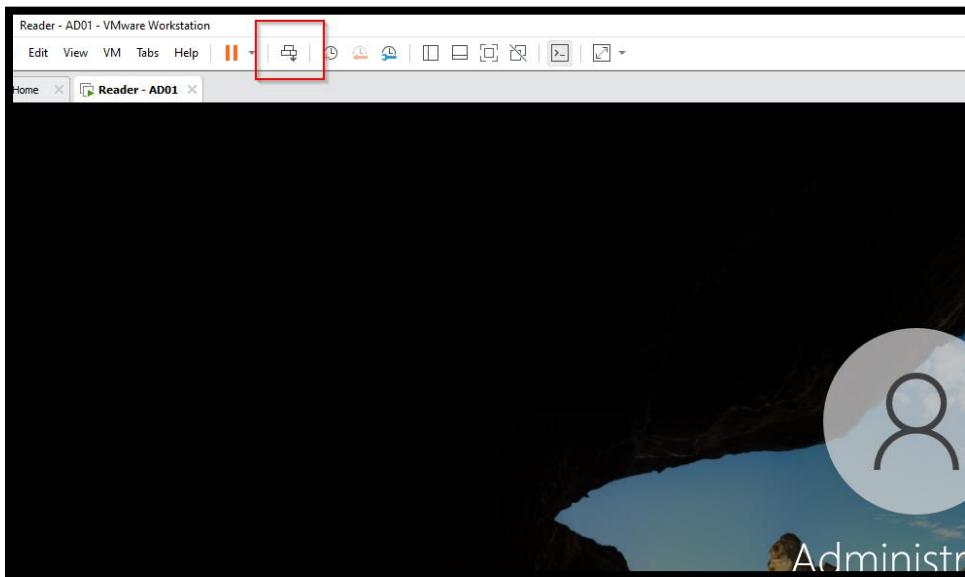
De Administrator is de beheerder van je machine en heeft dan ook **alle** rechten hierop. Dit account kan dan ook niet worden verwijderd. Het is dus altijd raadzaam om voorzichtig om te gaan met dit account en vooral het wachtwoord hiervan, in de praktijk moet je deze dus *zeker niet delen!*

In het werkveld (of in latere projecten; **tip!**) zal je merken dat dit account ook vaak niet gebruikt wordt. Vaak is deze gekopieerd naar zogeheten 'sub-admin' accounts, welke gekoppeld óf hernoemd zijn naar de daadwerkelijke beheerders. Zo kan een account als **J.Pijnaker** net zoveel rechten en machtigingen hebben als de échte administrator, maar is déze eenvoudig weg te gooien of uit te schakelen wanneer deze uit dienst gaat. Hiermee voorkom je dus, dat je het daadwerkelijke administrator account constant moet aanpassen.

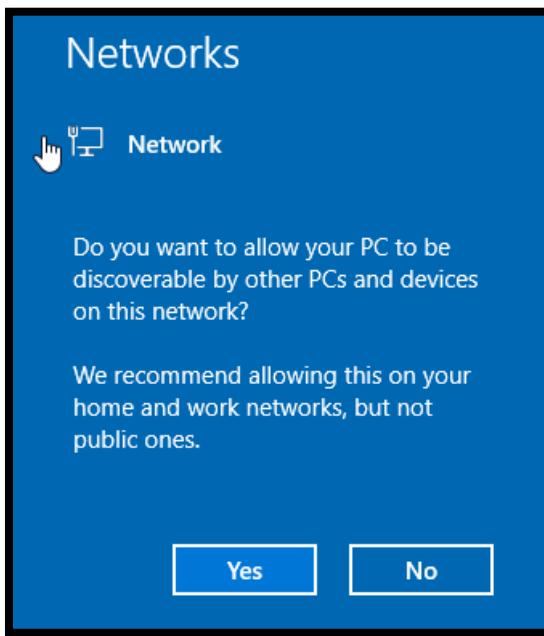
In de praktijk kun je een admin-groep maken met alle beheerders hierin. Aan deze groep koppel je dan bijvoorbeeld specifieke rechten. Dan mogen deze beheerders bijvoorbeeld wel gebruikers aanmaken/wijzigen etc. maar weer geen nieuwe structuur bouwen in het domein door middel van OU's te maken of te wijzigen. Hierover overigens later meer!

Voor de opdrachten die wij gaan doen, is het juist wél belangrijk om dit **administrator** account te gebruiken, omdat we nu even alle rechten nodig hebben om goed te kunnen ervaren wat deze allemaal mag.

Voor het inloggen gebruik het je zojuist ingesteld wachtwoord. Je kunt ‘Controle-Alt-Delete’-knopje gebruiken binnen VMWare Workstation om het station te ontgrendelen:



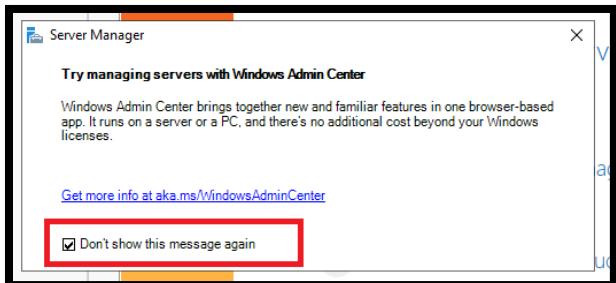
Je logt hier in met het zojuist ingestelde wachtwoord. Na de eerste keer inloggen, vind je aan de rechter kant van je scherm een grote blauwe balk met Yes en No erop. Dit is voor het zogeheten **Network Discovery**. Feitelijk zorgt dit ervoor dat deze server dan gevonden kan worden door andere machines in je netwerk. Zeker iets wat wij uiteindelijk willen, dus hier kiezen we voor **YES** zodat we dit later niet nogmaals hoeven op te zoeken en te activeren.



Tegelijkertijd valt je op dat er een groot scherm is geladen, dit is de **Server Manager**. Deze start eigenlijk altijd automatisch en van hieruit is **alles** te beheren voor je server. Je kunt dit eventueel uitschakelen, maar aangezien je feitelijk gezien altijd deze nodig bent, is het wel zo handig dit aan te laten staan.

De (eventueel) rode schermen mag je negeren voor nu, vaak zijn dit services van je zojuist geïnstalleerde server die nog niet zijn gestart (delayed startup) of nog niet zijn geconfigureerd.

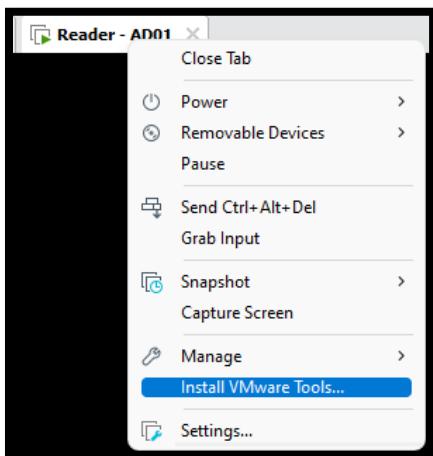
Wanneer je de pop-up die verschijnt bij het starten van de Server Manager niet meer wilt zien, kun je deze eenvoudig uitschakelen via het vinkje '**'Don't show this message again'**'.



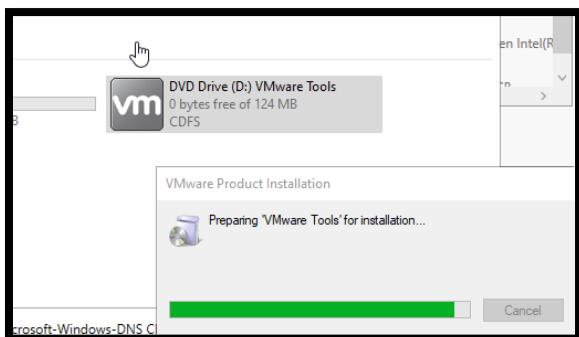
Installatie VMWare Tools

Voordat je goed kunt gaan werken met je VM, is het belangrijk om **VMware Tools** te installeren in Windows. Dit is een kleine tool welke meekomt met VMware Workstation en die zorgt voor een betere belevening binnen je VM. Zo installeert hij (extra) drivers voor je videokaart, je toetsenbord en muis en bijvoorbeeld je netwerkadapters.

De installatie start je eenvoudig door in VMWare met de rechtermuisknop te klikken op je VM en te kiezen voor **Install VMware Tools**. Druk wanneer je in je VM aan het werk bent, dus eerst op **CTRL+ALT** om je sessie te ontkoppelen.



Binnen je Windows omgeving wordt er nu een virtuele "DVD" gekoppeld welke je kunt openen via de Verkenner. Wanneer je de Windows Verkenner opent, op This PC drukt en vervolgens deze "DVD" opent (dubbelklikt) zal de installatie van **VMware Tools** gaan starten.



De installatie voltooij je '**default**', **dat wil zeggen dat**; je bij de installatie kiest voor **Typical** en dus verder geen wijzigingen hoeft te doen, maar gewoon op 'next, next, install' kunt drukken. Het knipperen van je scherm tijdens de installatie (binnen VMware) is heel normaal. Na de installatie is een herstart nodig, deze voer je gelijk uit door op **Yes** te klikken.

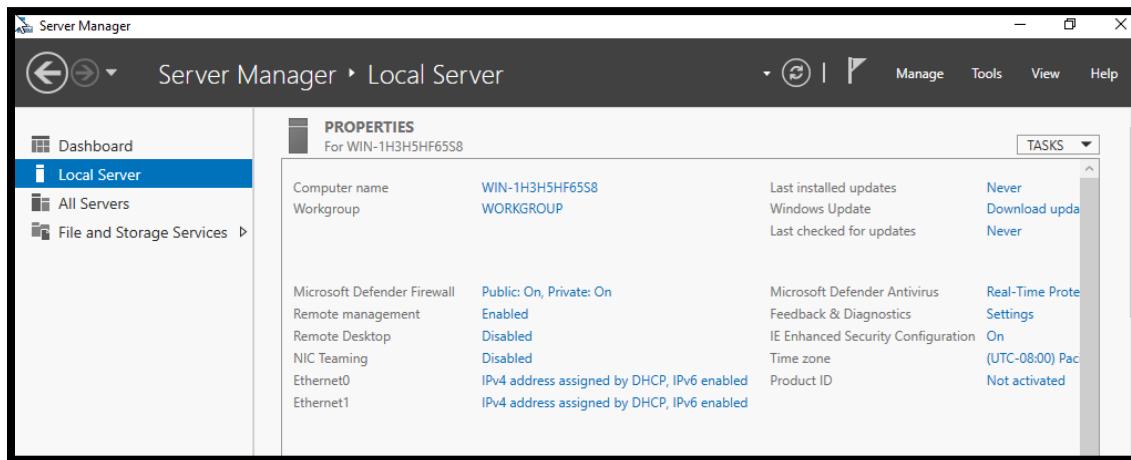
Na de herstart log je weer in als Administrator en wacht je even tot de Server Manager weer voor je staat zodat we verder kunnen met de configuratie.

Configureren van de naam en het netwerk

Na een installatie is het belangrijk om voor jezelf altijd een paar eenvoudige stappen standaard als eerst uit te voeren. Voor de Windows Server zijn dit de Computernaam én de netwerkinstellingen.

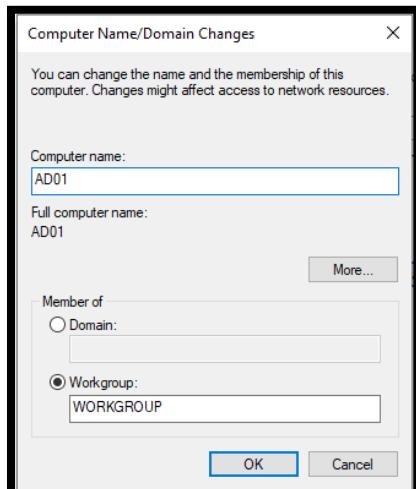
Netwerkinstellingen kun je (uiteindelijk) altijd nog wel wijzigen, maar de computernaam is lastiger en zeker niet wenselijk wanneer je straks je eerste **Domain Controller** hebt geïnstalleerd. Hier komen we later op terug, maar het is alvast nuttig om te weten waarvoor je dit het beste gelijk kunt doen.

We gaan om te beginnen, binnen de **Server Manager**, voor **Local Server** in het menu aan de linker kant. Dit is feitelijk je lokale, huidige, server dus. Je kunt binnen de Server Manager namelijk ook kiezen om vanaf deze plek meerdere Windows Servers te beheren, vandaar deze naam.

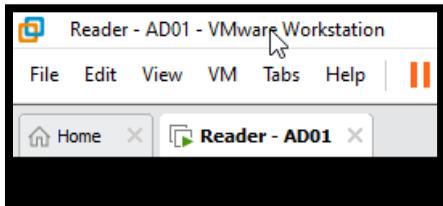


Je ziet dat de **Computer name** nu een vreemde samenhang is van cijfers en letters, niet te begrijpen en dus gaan we die gelijk aanpassen naar iets wat wél logisch is.

Dit is eenvoudig te doen door op de naam te klikken en daarna te kiezen voor **Change**.



We wijzigen de naam **WIN-1H3H5HF6558** in de naam **AD01**. AD staat voor **Active Directory** (zoals vermeld in [H1 – aanmaken virtuele machine](#)) en het is onze eerste server dus vandaar **01**. Eigenlijk dezelfde naam als hoe mijn VM binnen VMWare Workstation heet dus:

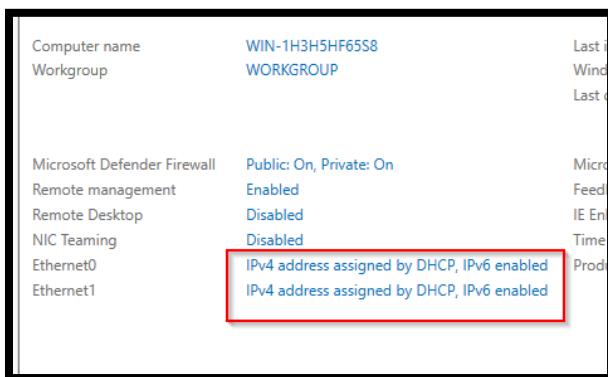


Wanneer ik nu op **OK** klik, geeft Windows de melding dat ik mijn server moet herstarten. We kiezen hier nu nog even voor **OK** gevolgd door **Close** en dan doen we **Restart later** aangezien we ook gelijk even het netwerk goed gaan zetten.

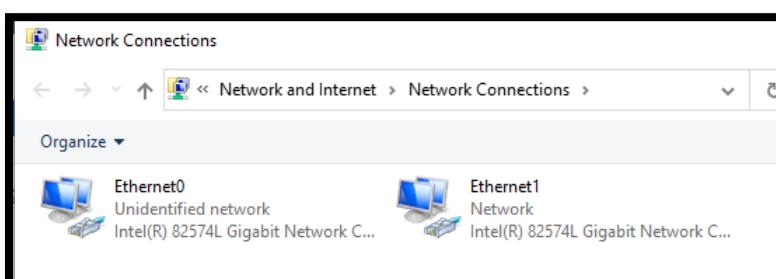


Het netwerk instellen is relatief eenvoudig, dit werkt namelijk op dezelfde manier, door op het adres te klikken welke je wilt wijzigen, het is echter eerst belangrijk om te achterhalen welke netwerkkaart op **Host-Only** en welke op **NAT** staat. Zoals gezegd zorgt de netwerkkaart die op NAT staat namelijk straks voor internet, en de Host-Only voor de verbinding tussen de onderlinge VM's.

Om dit uit te zoeken klikken we eerst op 1 van de 2 blauweIpv4 adressen:

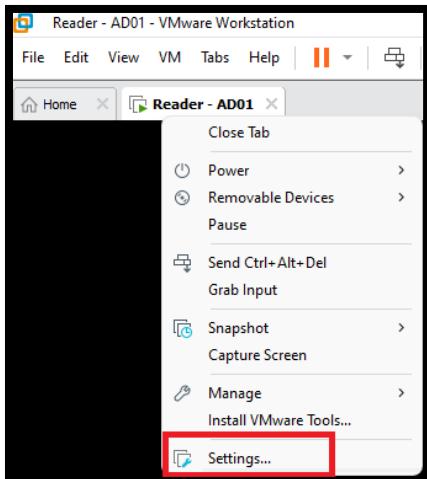


Nu wordt het **Netwerkcentrum** geopend en zien we dat beide kaarten actief zijn, ze staan aan.

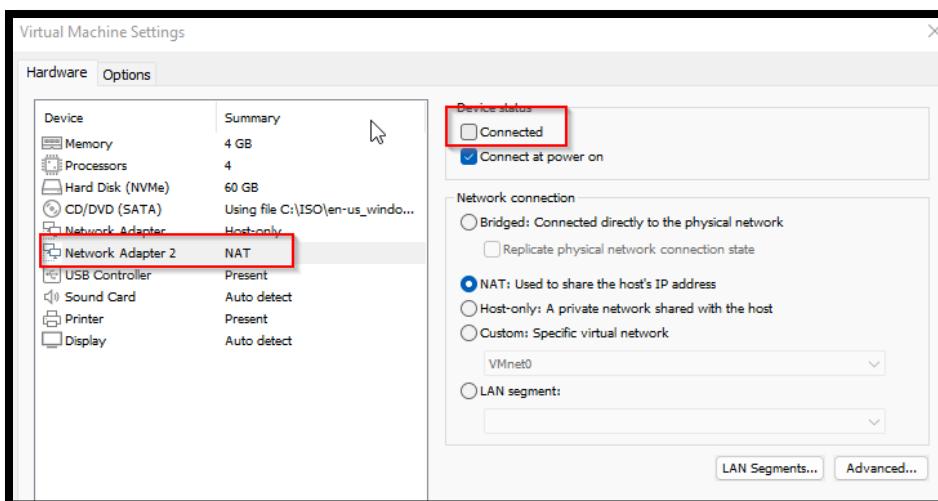


We kunnen hier op dit moment echter nog steeds niet echt iets mee omdat we niet precies weten welke adapter welke functie (NAT of Host-Only) heeft, **dus gaan we via de Settings van VMWare een van de twee adapters uitschakelen.** Op die manier vinden we straks binnen de VM welke we hebben uitgeschakeld en dus welke functie deze heeft.

Je ontkoppelt jezelf even uit de VM (**ctrl+alt**) en we kiezen zoals gezegd voor Settings op je VM:

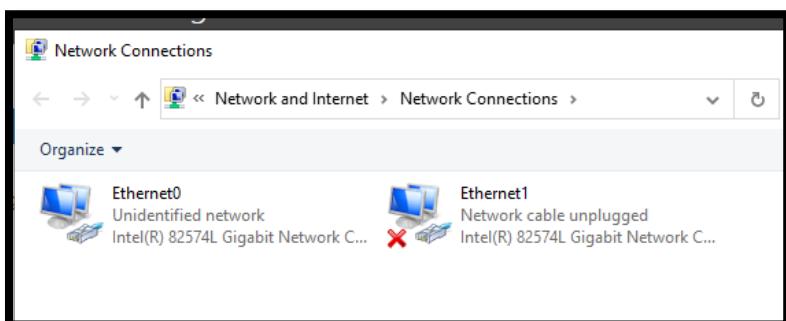


En schakel het vinkje op de Network Adapter 2 (NAT) bij Connected uit:

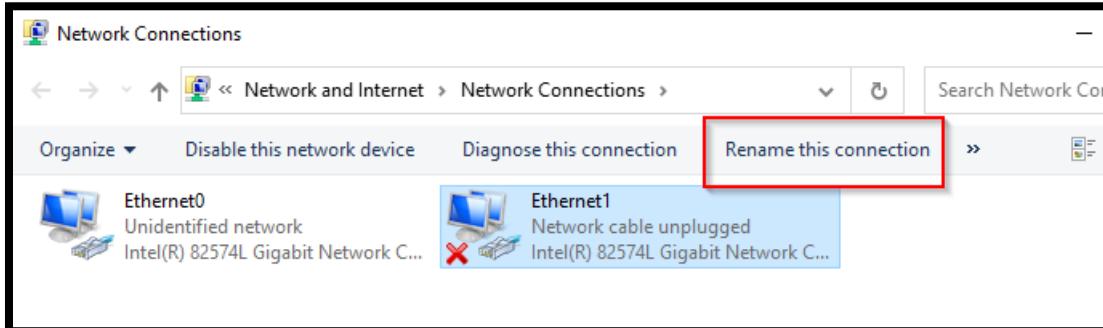


Nu kies je onderin voor **OK** en ga je terug naar je Windows Server.

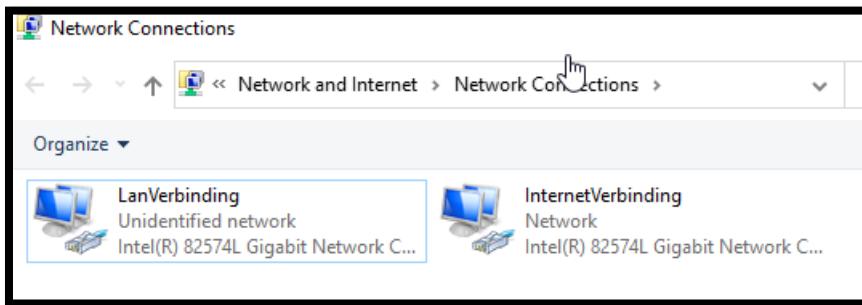
Je ziet nu een rood kruis staan bij 1 van de 2 netwerkverbindingen. Je weet nu dus, dat de verbinding met het kruis, je adapter is die op NAT staat en dus je internetverbinding moet zijn.



Om het overzicht te behouden, gaan we die adapter hernoemen naar **InternetVerbinding** en de andere noemen we **LanVerbinding**. Later in de reader is het namelijk van belang dat je weet welke adapter zorgt voor de LAN-verbinding waarmee de machines onderling communiceren en welke adapter dus zorgt voor de internettoegang. Je selecteert hier een adapter en vervolgens kies je bovenin voor **Rename this connection**:



Nu we ze beide hebben hernoemd, kun je het vinkje op de adapter met NAT weer op **Connected** zetten, het ziet er in Windows Server dan zo uit:



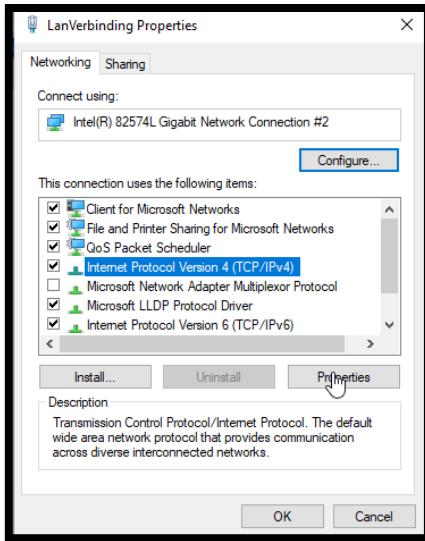
De **InternetVerbinding** laten we even met rust, die gaan we later gebruiken om je andere VM's te voorzien van internet, zónder dat deze 2 netwerkadapters nodig zijn.

De **LanVerbinding** gaan we nu configureren. LAN staat voor **Local Area Network**. Dus eigenlijk een lokaal netwerk. Gezien deze op Host-Only staat, is hier zeker sprake van een LAN en dus goed toepasbaar!

Deze **LanVerbinding** gaan we een vast, statisch, IP-adres toekennen. Op deze manier weet je altijd welk IP-adres deze server heeft, anders dan bij een Dynamisch adres, waarbij deze regelmatig kan wijzigen natuurlijk.

We doen dit door met de rechtermuisknop te klikken op de **LanVerbinding** en te kiezen voor Properties.

In het scherm wat naar boven komt, dubbel klik je op **Internet Protocol Version 4 (TCP/IPv4)** of je selecteert deze en kiest dan nogmaals voor Properties.



In dit scherm kunnen we daadwerkelijk een '**static IP**' in gaan stellen, dus een IP-adres wat bij deze server vast wordt ingesteld en niet meer (automatisch) wijzigt. Wanneer een IP-adres automatisch wijzigt heet dit een '**dynamisch IP**'.

We kiezen hier voor een IP-adres met klasse-C aangezien het een klein netwerk betreft.

IP-adres: **192.168.101.11**

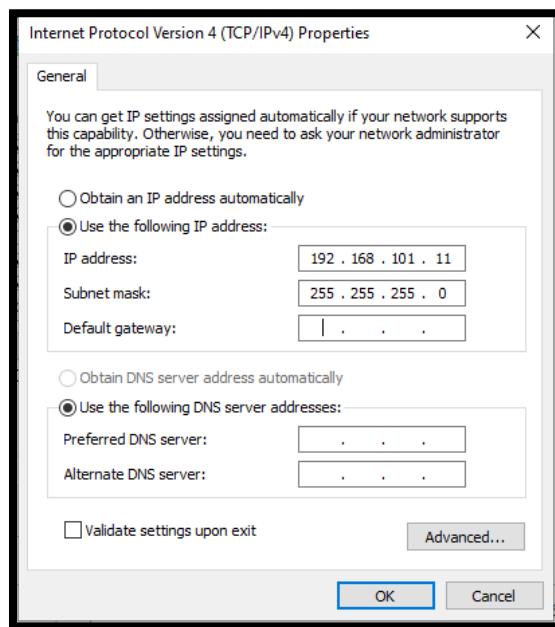
Subnetmask: **255.255.255.0** (of ook wel **/24**)

Default Gateway: **laten we leeg**

Preferred DNS Server: **laten we leeg**

Alternate DNS Server: **laten we leeg**

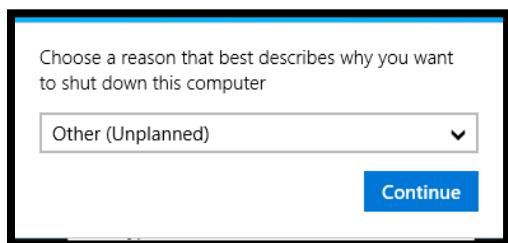
Dit ziet er dan zo uit en dan klik je op **OK**:



Nu dit klaar is, kunnen we de Server gaan herstarten, zodat ook de servernaam aangepast wordt. Dit is het makkelijkste door met de rechter muisknop op het Windows-icoon links onderin te drukken en

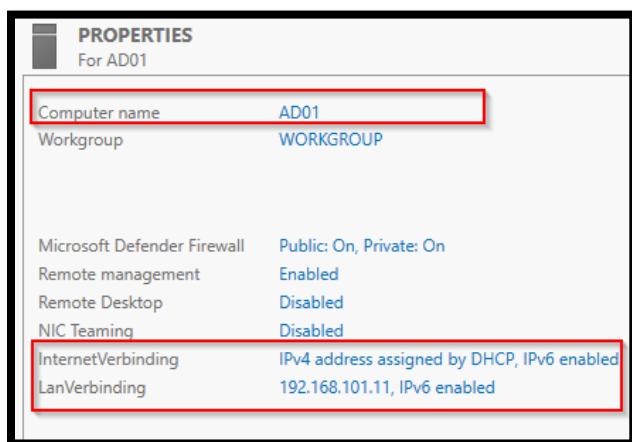
te kiezen voor **Shutdown or Sign out -> restart**

Bij het uitvoeren van de herstart komt er eerst nog een tussenscherm, hierin kun je als beheerder aangeven waarvoor de herstart is.



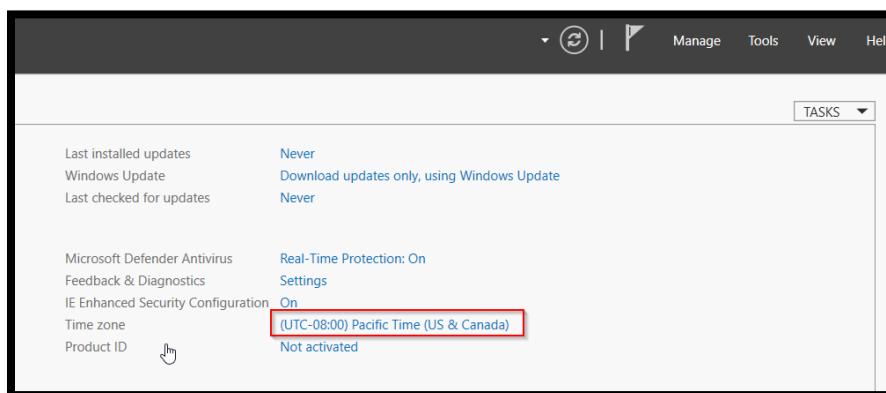
Dit kun jij (of je collega) later terugvinden in je logboek van de server. Voor nu kun je gewoon kiezen voor **Other (Unplanned)**.

Wanneer we opnieuw zijn ingelogd en kijken bij **Local Server** ziet dit er zo uit:

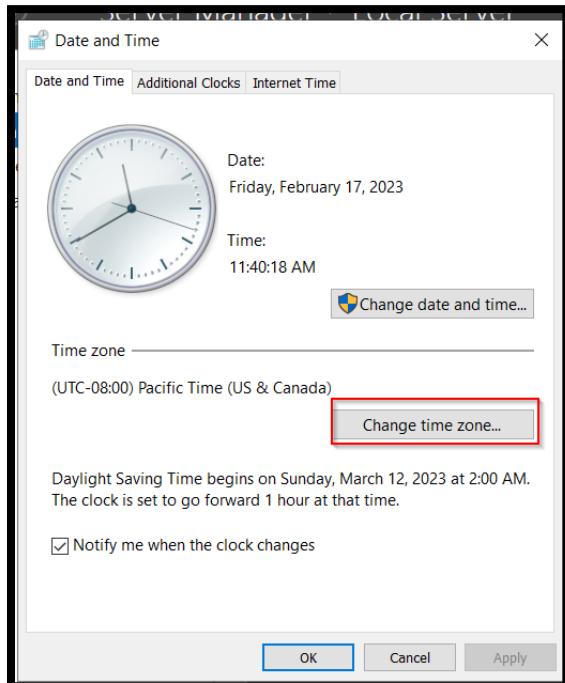


Aanpassen tijdzone

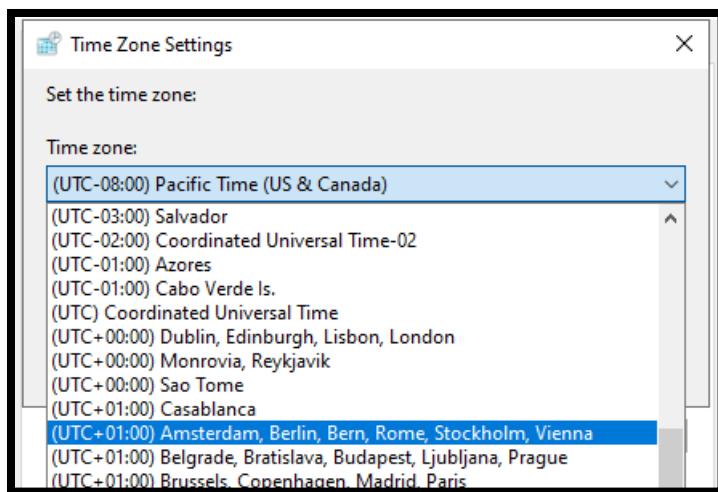
Als 'laatste' gaan we de Time Zone aan passen naar Amsterdam, die staat standaard op Pacific Time (UTC-08:00). Deze pas je aan door te klikken naast **Time Zone**:



En daarna kies voor **Change Time Zone**



Je kiest hier voor **Amsterdam (UTC+1:00)** gevuld door twee keer **OK**.



De **basisconfiguratie** is nu klaar.

Voordat we nu verder gaan, maken we eerst weer een **Snapshot** om de omgeving veilig te stellen. Geef deze ook een handige naam zodat je straks goed weet tot waar dit punt terug gaat. Mocht je twijfelen hoe dit ging, dan kijk je nog even voorin de reader bij de uitleg.

Mocht er namelijk iets fout gaan in de volgende stap, kunnen we dan eenvoudig terug naar dit moment en hoeven we dus niet helemaal opnieuw te beginnen met de installatie.

Installatie en configuratie Active Directory Domain Services

Nu we de basis configuratie van de server klaar hebben, kunnen we gaan beginnen met het aanmaken van een domein.

Een domein is feitelijk gezien **het hart van de organisatie** (in software termen). Je maakt hier de organisatiestructuur aan, gebruikers, groepen, computers etc. Tevens beheer je hiermee wat men wel en vaak vooral wat men niet mag. Dat doe je door middel van Group Policies. Dit beheer je allemaal op een zogeheten **Domain Controller**, de beheerserver van je domein dus eigenlijk.

Group Policies zijn policies die worden verspreid over het domein waarin regels staan die gelden voor je bedrijf. Hierin geef je dus aan wie bij welke mappen mag, welke achtergrond ze krijgen, welke printer er moet worden weergegeven of aan welke eisen een wachtwoord moet voldoen.

Allemaal **beheertaken** die jij als beheerder kunt gaan regelen wanneer je een domein hebt ingericht.

Roles and Features

Om hiermee aan de slag te gaan, moeten we echter eerst software installeren in de Windows Server. Deze staan allemaal al ‘klaar’ binnen Windows Server, echter moet je ze als administrator (beheerder) van je domein, nog even activeren en instellen.

Deze software heet in de server een ‘role’. Door een Role te installeren, activeer je als het ware dit stukje software. Om het ook te kunnen beheren, heb je een ‘Feature’ nodig. Ook deze zitten al in je server ingebakken, maar ook die moeten geactiveerd worden.

Heel simpel gezegd is de Role dus het stukje software en is de Feature het stukje beheer software.

AD DS en DNS

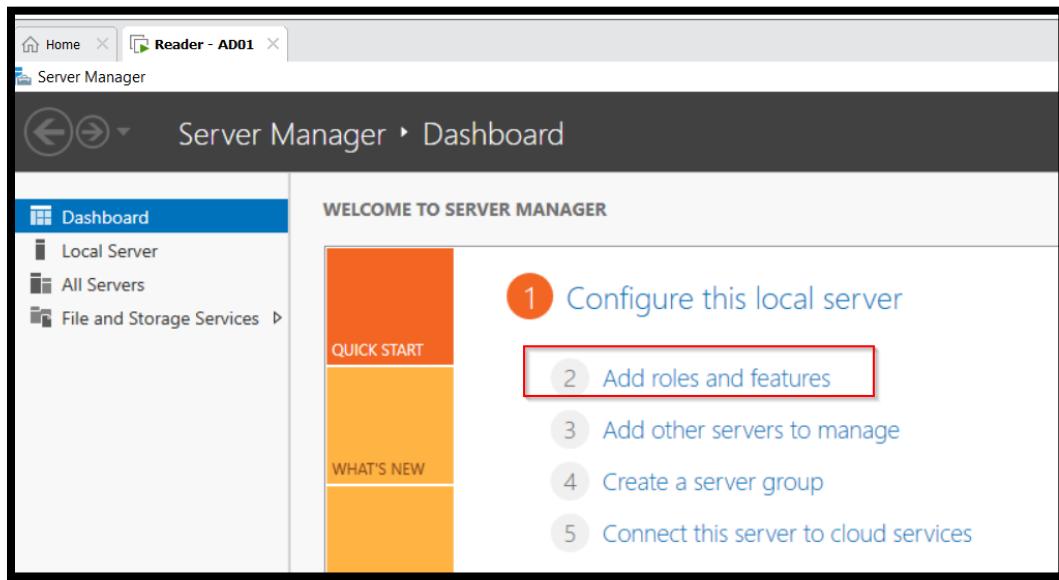
Om dus te beginnen met het aanmaken van je nieuwe domain, is het nodig om twee rollen + bijhorende features te installeren; **AD DS en DNS**.

AD DS is de Active Directory Domain Service, Hiermee beheren we straks ons domein.

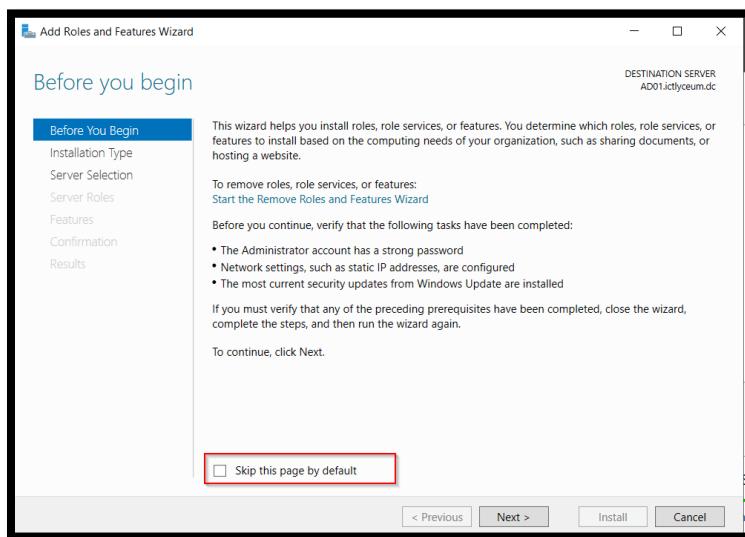
DNS staat voor Domain Name Services. Eenvoudig gezegd zet deze namen om in IP-adressen en IP-adressen in namen; jouw server zet de naam **AD01 in de DNS** dus om naar **192.168.101.11** en wanneer je kijkt naar dit IP **192.168.101.11**, dan geeft de DNS zijn hostname **AD01** terug.

Het omzetten van dit geheel het ook wel **resolven**. Hiermee gaan we later verder.

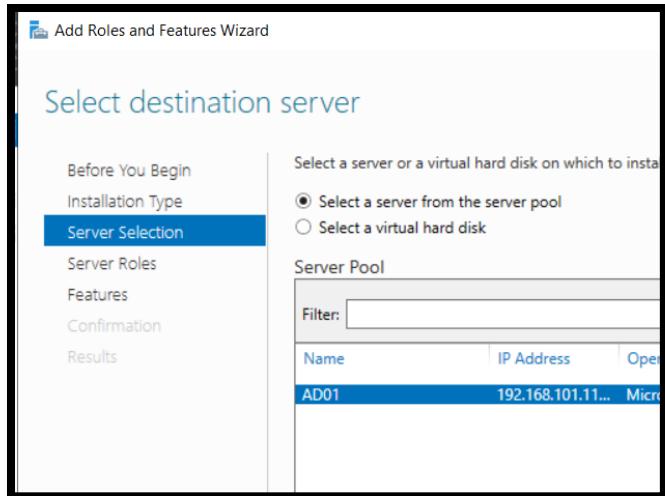
We beginnen via de Server Manager, door aan de linkerkant te klikken op **Dashboard** en vervolgens in het hoofdscherm te kiezen voor **Add Roles and Features**;



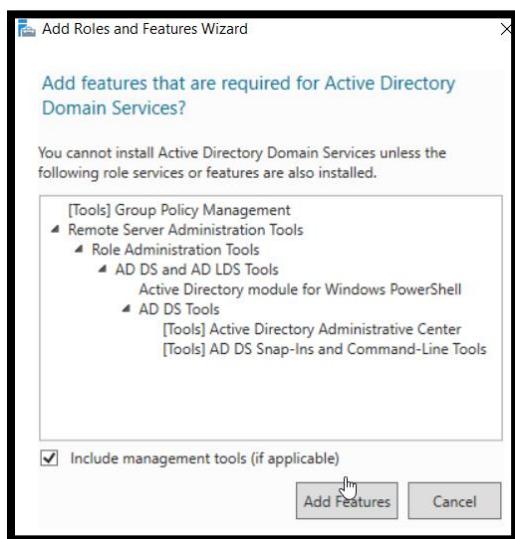
Je komt nu in een wizard waarin je allerlei opties hebt, ook om bijvoorbeeld iets te installeren op een andere server, maar dat gaan we nu niet doen. In het eerste scherm zetten we een vinkje aan bij **Skip this page by default** zodat we hem niet telkens weer te zien krijgen.



Omdat wij de installatie gewoon willen doen op onze huidige server, kiezen we voor onze '**AD01**' gevuld door **Next**

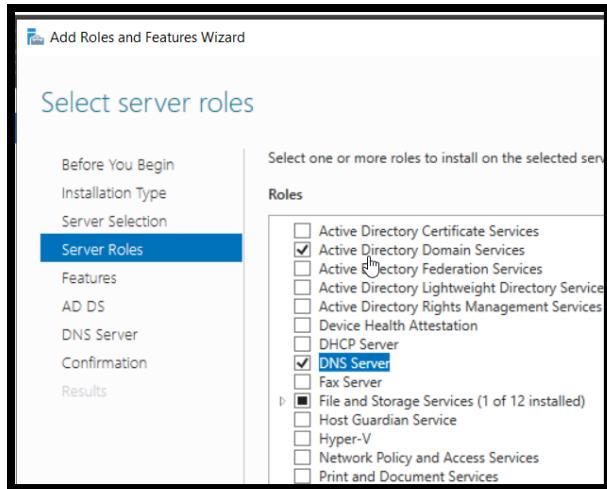


Wanneer je bij het tabblad **Server Roles** de role **Active Directory Domain Services** (dus AD DS) aan klikt, zal je zien dat er automatisch een pop-up tevoorschijn komt met de vraag of je de bijhorende (en benodigde) features wilt installeren. Uiteraard kiezen we hier voor **Add Features** en zorgen we dat (wanneer nodig) het vinkje bij **Include management tools** aan staat.



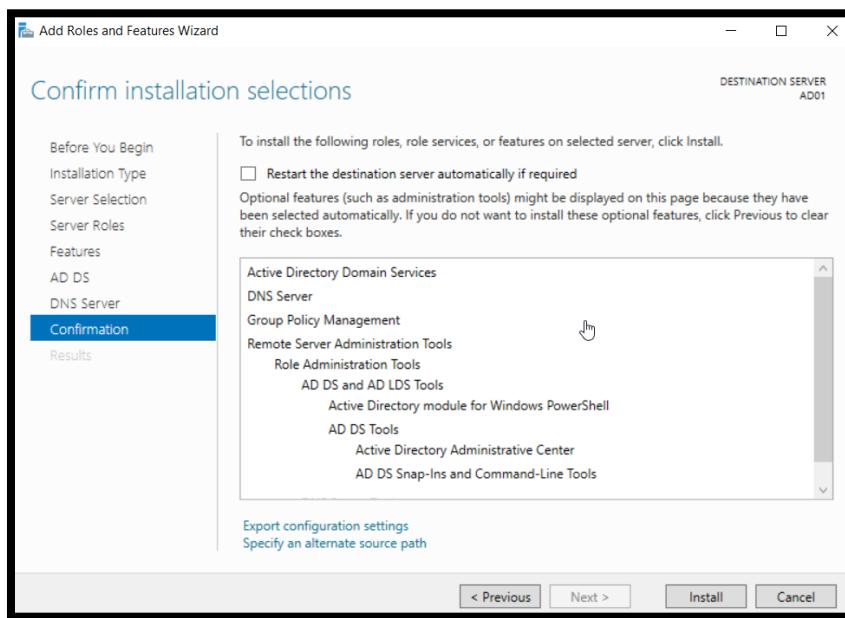
Voor de role DNS geldt hetzelfde uiteraard.

Als je ze beide hebt aangevinkt, moet het er ongeveer als volgt uitzien:

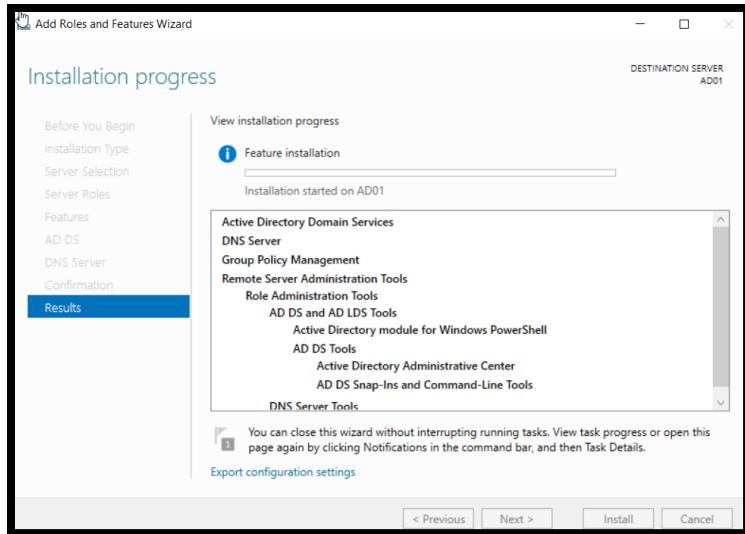


Je kiest nu 2x voor **Next**. Dan kom je in een venster wat je een beetje extra informatie geeft over de AD DS en de DNS. Deze mag je doorlezen en daarna kun je verder gaan door op **Next** te drukken.

Op het laatst komt er nog een bevestigingsscherm, waarmee je nog eenmaal kunt doorlezen of je alles hebt aangevinkt wat je wilt hebben, en dan kies je voor **Install**



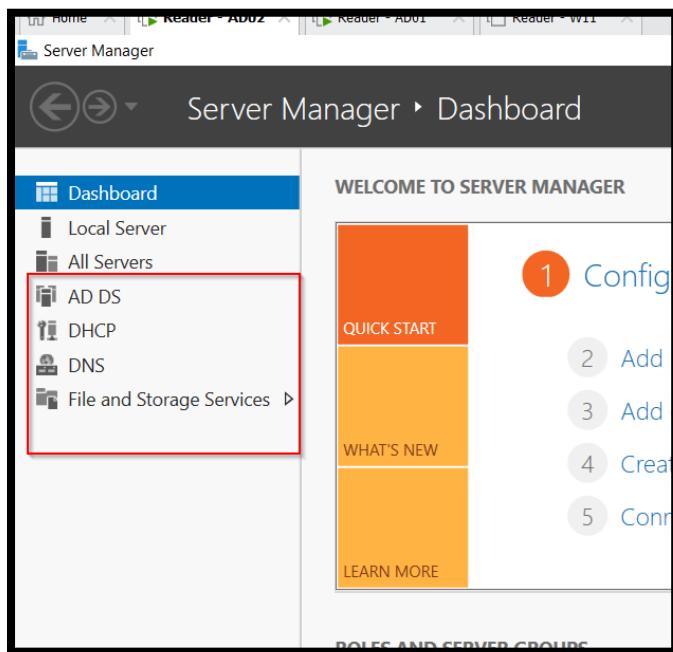
De installatie zal gaan starten, je kunt dit scherm desgewenst sluiten door op Close te drukken



Na de volledige installatie kunnen we met de configuratie gaan beginnen.

Het is erg nuttig om te weten dat je altijd bij de start van de Server Manager, aan de linker kant, kunt zien welke rollen er allemaal zijn geïnstalleerd op server waarop je werkt.

Dit lijstje past zich volledig dynamisch (automatisch) aan wanneer je een role installeert of verwijderd en geeft veel inzicht wanneer je 'even snel' iets opzoekt.

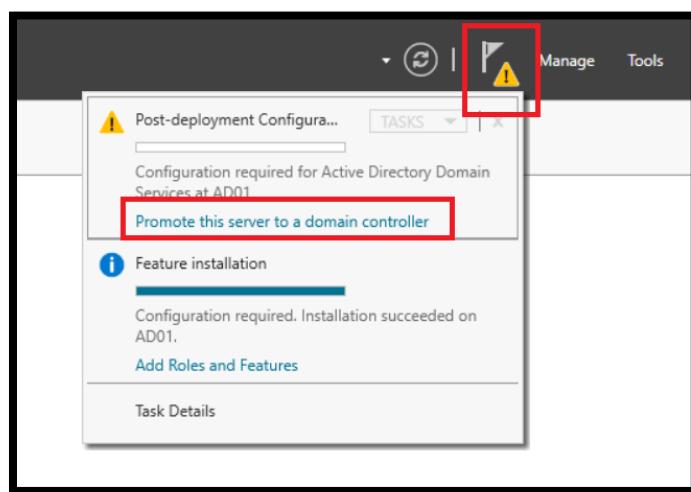
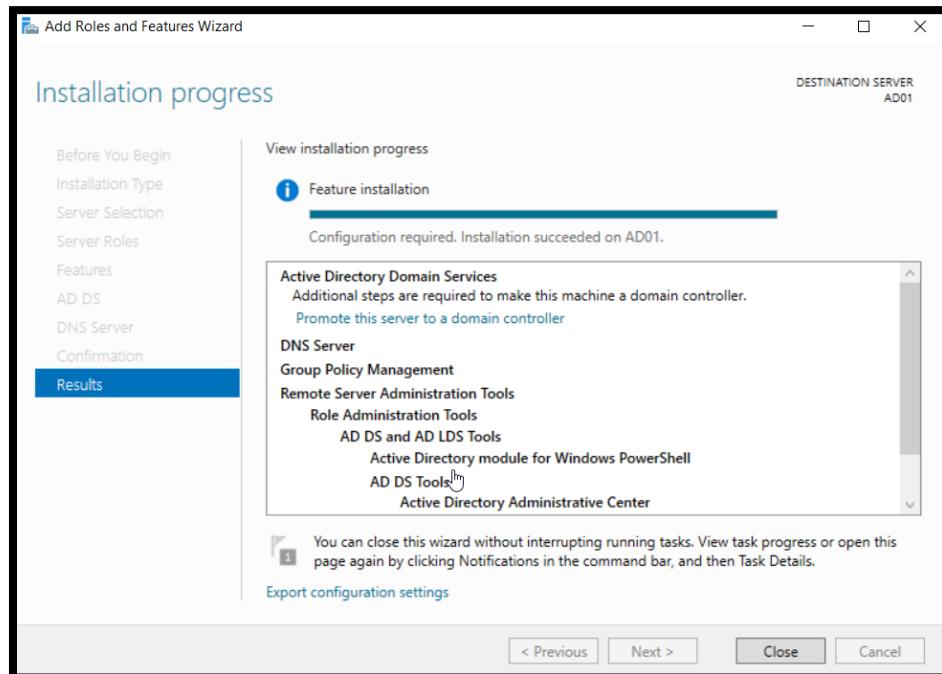


(LET OP: de DHCP-role is op dit moment nog niet zichtbaar, deze volgt later pas)

Configuratie Active Directory Domain Services

Wanneer de installatie van je nieuwe rollen en features klaar is, kunnen we beginnen met het instellen van de gewenste domeinnaam.

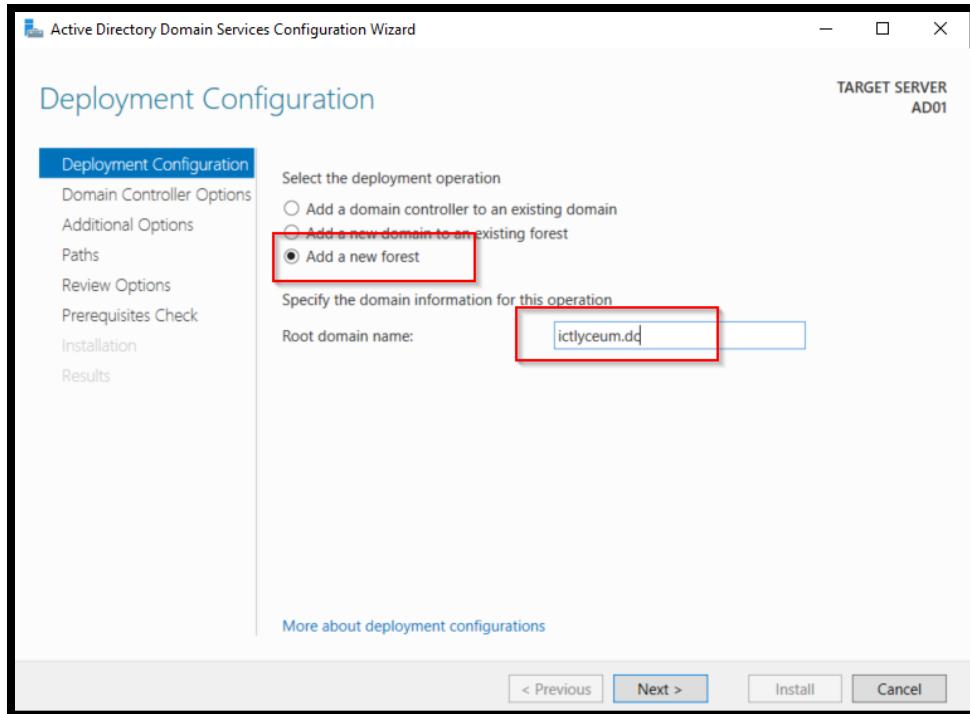
Dit kan eenvoudig gestart worden door in het installatiescherm te kiezen voor '**Promote this server to a domain controller**', of als je dit scherm reeds gesloten, via het uitroepje rechtsboven in de Server Manager op het inmiddels verschenen vlaggetje:



Zodra je deze activeert, krijg je wederom een wizard te zien waarmee we een domein gaan opzetten.

Het domein wat we gaan maken, heet '**ictlyceum.dc**'. Deze naam voer je in en vervolgens druk je op **Next**.

Over je domeinnaam moet je overigens altijd goed nadenken en het bespreken binnen het bedrijf of het team waarmee je werkt. Deze is namelijk niet te wijzigen (op een normale manier...). We gaan ook, omdat dit de eerste Domain Controller is, een nieuw **Forest** aanmaken.



Forest

Een Forest is eigenlijk de overkoepelende veiligheid laag van je domein. Een forest kan meerdere domeinen bevatten. Doordat deze domeinen dan binnen hetzelfde forest vallen, is er automatisch een 'trust' (vertrouwensband) tussen deze domeinen en kunnen ze elkaar dus bereiken wanneer je dit wilt.

De Prefix

Het stukje achter de '.' (punt) heet de **prefix**. Dit mag in principe alles zijn binnen een intern netwerk, daarom gebruiken wij hier **.dc** (Drenthe College..).

In sommige gevallen wijst men naar een prefix met **.local**. Dit is echter in de praktijk een **échte no-go** (!), probeer dit dus ten alle tijden te voorkomen.

Het kan namelijk zijn dat je een beveiligingscertificaat, ofwel een **SSL Certificaat**, moet aanvragen voor het domein wat je opbouwt. Wanneer je dan voor een **.local** hebt gekozen is dit niet mogelijk. Vandaar dat je hier altijd **vooraf** over moet nadenken.

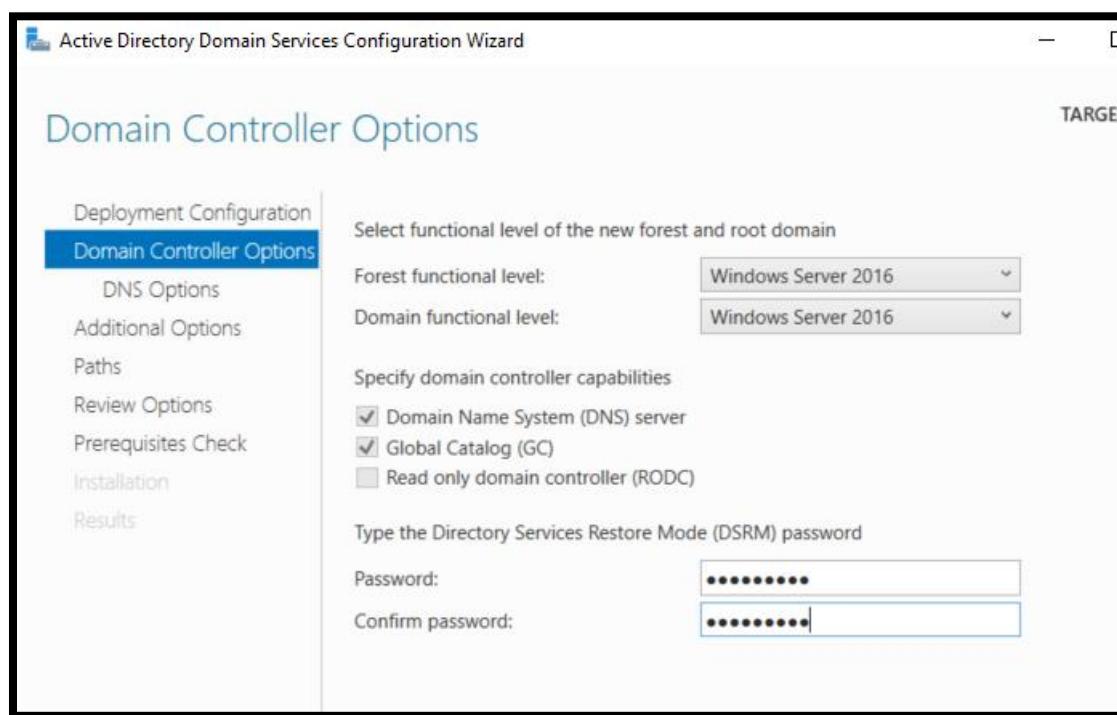
Wanneer je nu op **Next** drukt, checkt Windows Server even (globaal) of dit akkoord is. Zonder de prefix bijvoorbeeld kun je niet door naar de volgende stap.

In dit deel geef je op welke **Forest Functional Level** en welk **Domain Functional Level** je wilt gebruiken. Hoe hoger het level, hoe meer (nieuwe) functionaliteit je tot je beschikking hebt in het domein. Het is echter zo, dat sommige servers bij een te hoge level, niet meer mogen verbinden met de nieuwe domain controllers, dus controleer altijd goed of je nog oude(re) servers in je domein hebt hangen voordat je dit (eventueel) aan gaat passen.

In onze omgeving is dit onze enige server nog, en kiezen we dus voor de laatst mogelijke versie. Op het moment van schrijven dit **Windows Server 2016**.

Ook geven we in deze stap ons DSRM-wachtwoord op. Met dit wachtwoord kun je, wanneer er iets misgaat in je domein, een deel van je directory services herstellen. Noteer deze altijd goed.

Voor nu mogen we deze best gelijk maken met het Administrator wachtwoord, ik maak er hier dus weer **Welkom01!** van.



Zoals je ziet is het vinkje bij Global Catalog en bij DNS nu niet te wijzigen.

Global Catalog Server

De Global Catalog Server is eigenlijk een soort grote database, waarin alle (belangrijke) gegevens van je domein opgeslagen worden. Denk hierbij aan alle netwerkobjecten uit het domein en alle eigenschappen hiervan. Tevens worden ook netwerkobjecten uit eventuele andere domeinen hierin opgeslagen, zodat alles binnen het **forest** goed beschikbaar is voor alle servers die dit nodig zijn.

De eerste domein controller binnen je domein is **altijd** GC, ook wel GCS (Global Catalog Server) hierin heb je ook geen keuze. Bij alle extra domein controller kun je hiervoor tijdens de installatie wel of niet kiezen.

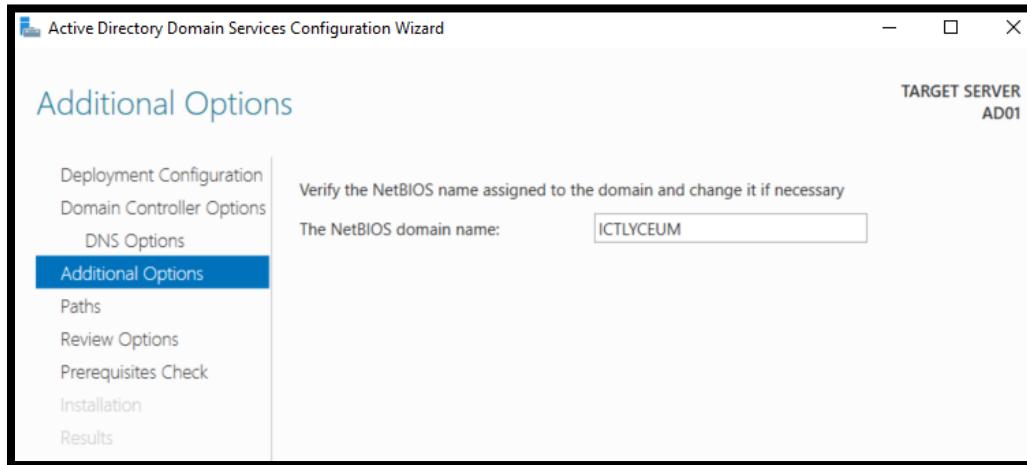
RODC

Zoals je hier ook kunt zien, is er een optie om te kiezen voor Read Only domain controller, de RODC. Deze optie is nu nog uitgeschakeld, maar is bij een eventuele volgende domain controller wél beschikbaar. De RODC is een eenvoudige versie van de domain controller die vaak op wat minder veilige plekken wordt geplaatst, omdat er bijvoorbeeld geen optie is deze achter slot en grendel te plaatsen. Ook plaatst men deze vaak op plekken waar geen deskundige beheerder zit. Het grote voordeel van een RODC is namelijk dat deze enkel een 'read only' versie van het domein bevat. Hiervan uit kunnen er dus geen wijzigingen aangebracht worden op het domein.

In de volgende stap kun je niets aanvinken. Je ziet hier wel een (gele) melding over de DNS, hij geeft aan de zone nog niet te kunnen vinden, en dat klopt gezien we nog niets hebben aangemaakt. We kunnen dus gewoon verder klikken naar de volgende stap.

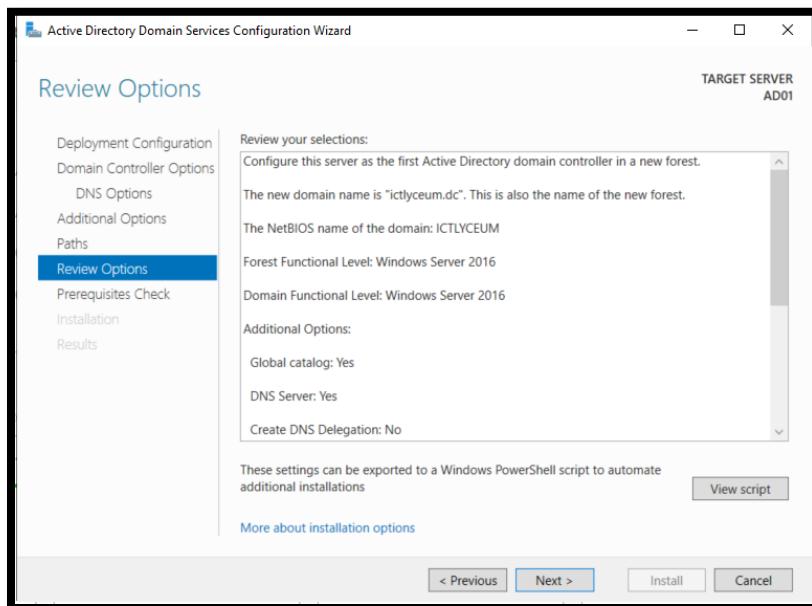
NetBIOS-naam

Bij 'Additional Options' heb je de keuze je NetBIOS-naam (Network Basic Input Output System) aan te passen. Deze naam gebruik je bijvoorbeeld bij pre-2000 servers. In het jaar 2000 is Microsoft overgestapt naar het DNS-systeem en werd NetBIOS eigenlijk 'overbodig'. In Server 2022 wordt deze optie echter nog altijd ondersteund. De NetBIOS naam is altijd je domeinnaam, maar dan **zonder** je prefix. In ons geval dus ICTLYCEUM.



Bij Paths staan alle standaard mappen, hier blijven we af en wijzigen we dus niets aan. We kiezen simpelweg voor **Next**.

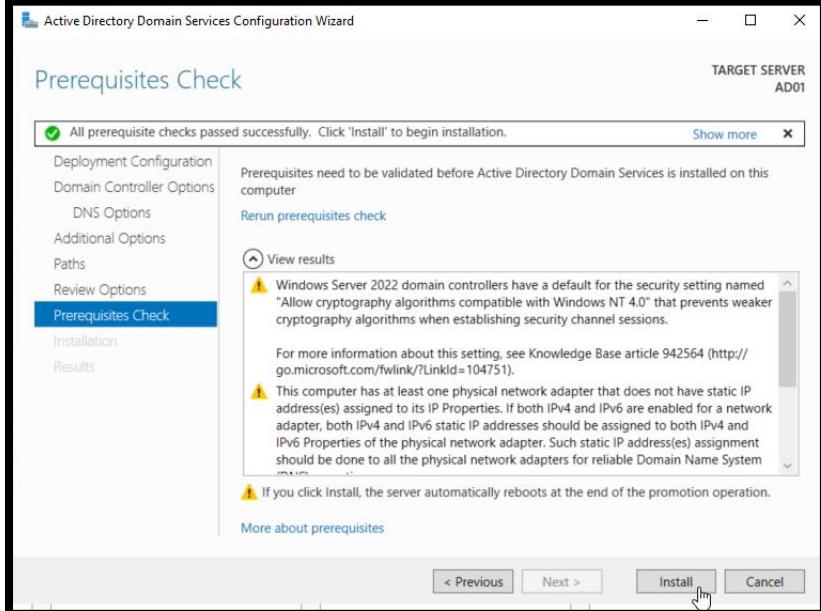
Nu krijgen we, bij Review Options, een overzicht te zien van alle gemaakte keuzes en opties. Mocht hier iets niet kloppen, kun je eenvoudig via het menu aan de linkerkant aanpassingen doen en vervolgens weer teruggaan om nogmaals te controleren of alles klopt. Is dit zo, dan kies je voor **Next** en verzorgt Windows nog een laatste check.



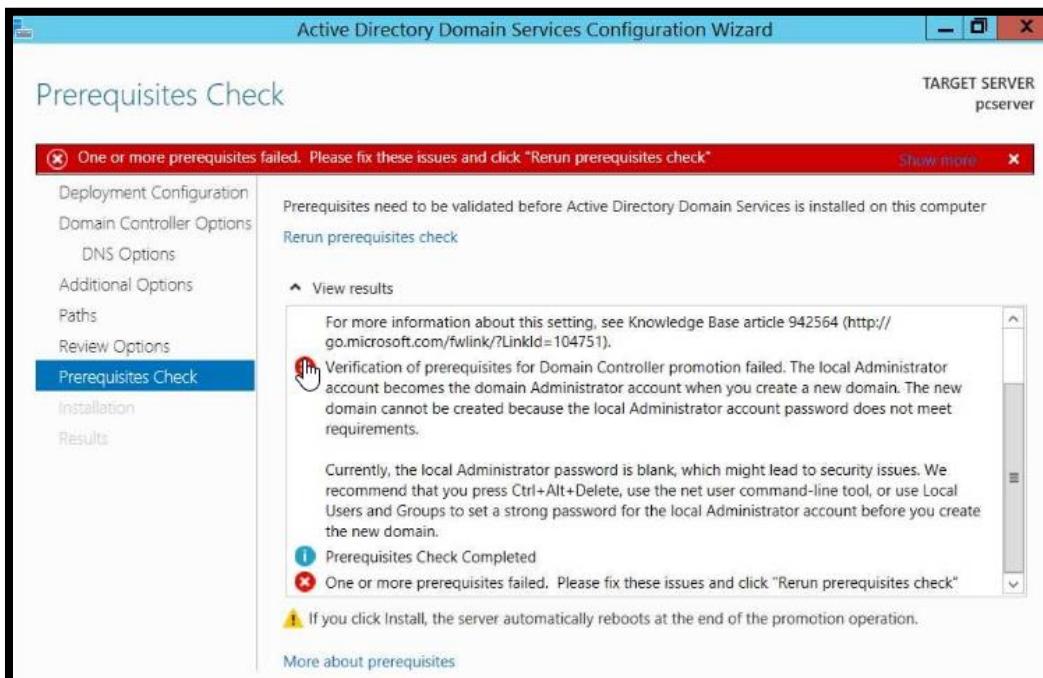
Wanneer tijdens deze controle alles goed is, verschijnt er links boven in een groen bolletje. Je kunt dan tevens op **Install** klikken om de configuratie/installatie van je domein te starten.

Standaard tref je hier 3 (gele) waarschuwingen aan. Deze gaan o.a. over IPv6 (deze is niet geconfigureerd) en over een stukje compatibiliteit met Windows NT 4.0 (dit komt uit 1996 en zorgen dus mogelijk voor een veiligheidsprobleem in een live-omgeving).

Deze kun je voor nu negeren en je kunt hier dus op **Install** klikken.



Mocht je deze melding zien staan:

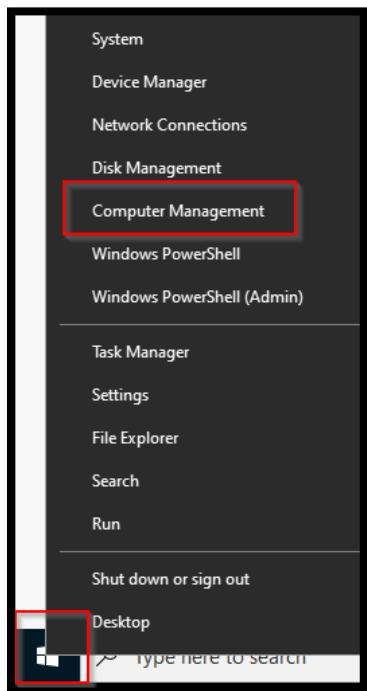


Betekend dit altijd dat het lokale administrator account geen wachtwoord heeft. Dit is noodzakelijk omdat dit account straks tijdens de installatie wordt omgezet naar het domein-administrator account en deze dient **altijd** een wachtwoord te bevatten.

In een uitzonderlijk geval moet je via de **CLI** (Command Line Interface) aan zetten dat het 'local administrator account' een wachtwoord **moet** bevatten. Dan doen we dit even via: Start -> CMD -> ENTER. We komen dan in de DOS-prompt en daar voeren we het volgende uit:
`net user Administrator /passwordreq:yes`

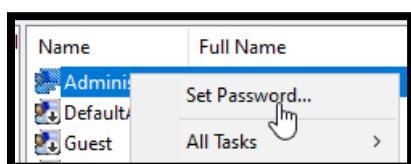
We krijgen dan de melding te zien dat het succesvol is, en daarna kun je weer verder.

Mocht dit optreden, is dat eenvoudig te wijzigen door met je rechter muisknop op de **Windows-knop** te drukken en te kiezen voor **Computer Management**:



Vervolgens kies je voor **Local Users and Groups** en daarna voor **Users**.

Je ziet hier het betreffende Administrator-account staan, hierop klik je met je rechtermuisknop en dan kies je voor **Set Password...**



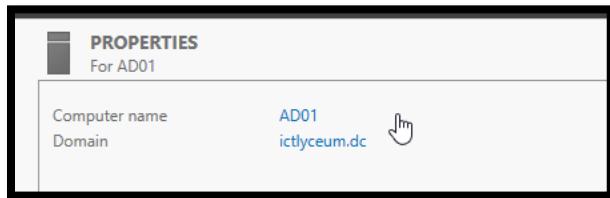
Wanneer je nu teruggaat naar de Wizard waarin we het domein aan het opzetten zijn, en je kiest voor 'Re-Run', moet er daarna een groen balletje komen zodat je verder kunt (**Install**).

Na de herstart zal je zien dat er nu niet meer staat: **Administrator** maar **ICTLYCEUM\Administrator**. Je kunt vanaf nu namelijk niet meer inloggen op het lokale Administrator account omdat deze vanaf nu is omgezet naar een domein-account.

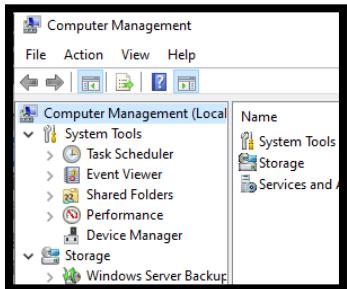


Hier kun je inloggen met je wachtwoord, in deze reader **Welkom01!**

Als we nu ingelogd zijn zie je direct op de Server Manager bij Local Server, dat er niet meer staat **Werkgroep** maar nu staat er **Domain**:



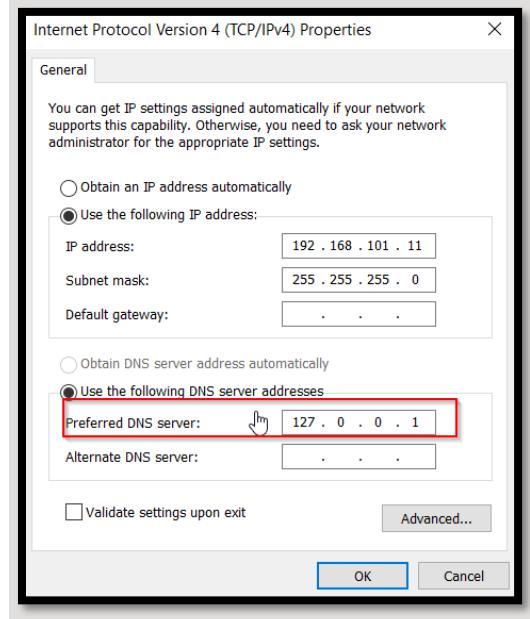
Wanneer we nu nog even gaan kijken bij de **Computer Management** (Rechter muisknop op de Windows-knop), we openen dan weer de **MMC** en daarin zullen we zien dat de **Local Users and Groups** zijn verdwenen omdat ze dus zijn gemigreerd (overgezet) naar het domein toe.



Een andere belangrijke wijziging is het aanvullen van de DNS. Zoals je weet hebben bij het configureren van de LANVerbinding netwerkkaart, **geen** DNS ingevuld. De Role ADDS heeft echter wel een DNS server nodig om correct te kunnen werken. In dit geval, omdat dit onze eerste domain controller is, moet hij naar zichzelf kijken om het domein **ictlyceum.dc** te kunnen 'resolven' (omzetten) naar een IP adres.

Microsoft heeft er voor gekozen om standaard het DNS record van de host (je VM dus) zelf in te voeren bij de installatie van de ADDS + DNS. Élke machine/host die je installeert binnen een netwerk, heeft een eigen privéadres, welke altijd **127.0.0.1** is, dit adres heet ook wel de **Local Loopback**.

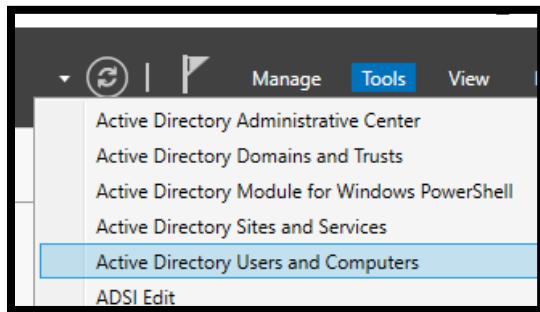
Ga je vervolgens bij de IPv4 instellingen kijken, dan zie je dat deze **127.0.0.1** netjes automatisch tijdens de configuratie van de AD DS is aangevuld:



Technisch gezien kun je dus deze eenvoudig aanpassen naar 192.168.101.11 in dit geval, aangezien dit nu dezelfde netwerkkaart is, maar dat is niet nodig voor nu en daarom laten we dit zo staan.

Active Directory Users and Computers

De gebruikers en groepen staan op een domain controller onder **Users and Groups**, deze kunnen we rechts bovenin de Server Manager vinden onder **Tools -> Active Directory Users and Computers**



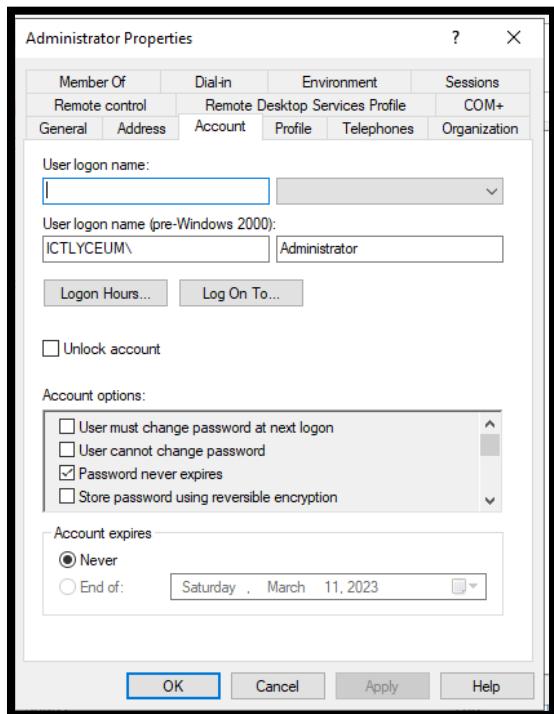
In deze tool gaan we later eventuele gebruikers, groepen en OU's (Organizational Units) aanmaken. Een OU wordt gebruikt om structuur te maken binnen je domein, maar hierover later meer!

De lokale gebruikers en groepen vind je nu onder de **OU Users** van je domein:

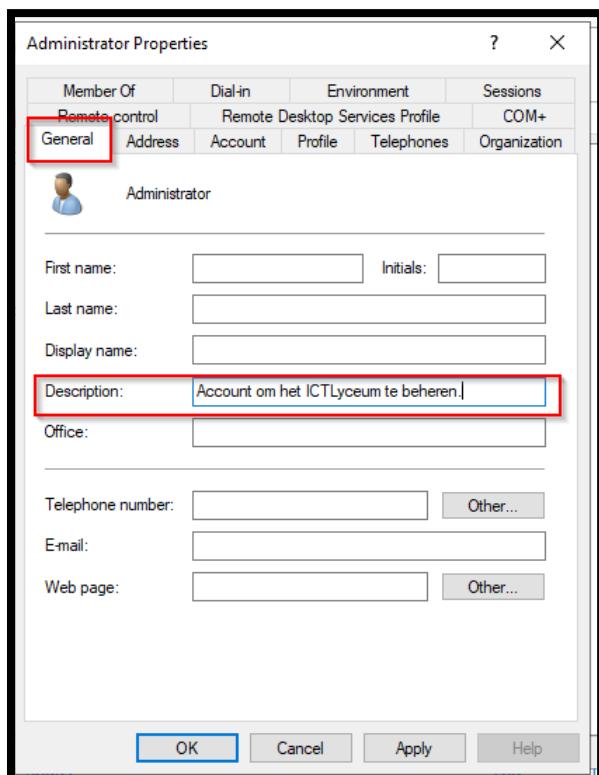
A screenshot of the 'Active Directory Users and Computers' window. The left pane shows a tree view of the directory structure under 'ictlyceum.dc'. A red box highlights the 'Users' folder under the 'Builtin' container. The right pane displays a table of users and groups. A red box highlights the first user entry, 'Administrator', which is a 'User' type account. The table columns are 'Name', 'Type', and 'Description'.

Wanneer je dubbel op een account klikt open je de **Properties (eigenschappen)** van dit betreffende account.

Open deze voor de **Administrator** en controleer via de verschillende tabbladen welke opties en mogelijkheden je hier allemaal hebt.



In het tabblad General, zetten we bij **Description**: 'Account om het ICTLyceum te beheren.' Druk op **Apply** om dit ook daadwerkelijk toe te passen. Klik je dit nu gewoon weg wordt het namelijk **niet** opgeslagen.



Je zult láter zien dat deze omschrijving weggezet wordt in de Global Catalog database en dus straks automatisch naar voren komt op je tweede domeincontroller, zonder dat je het hier nogmaals moet aan gaan passen.

Wanneer je in de OU **Domain Controllers** kijkt, vindt je hierin jouw server, de **AD01**. Deze server is **GCS, Global Catalog Server**.

Name	Type	DC Type	Site
AD01	Computer	GC	Default-First-Si...

De andere OU, **Computers**, is nu nog leeg zoals je kunt zien. Die zal straks gevuld worden wanneer we een **member server** gaan toevoegen. Dit is eigenlijk simpel gezegd een server die je lid maakt van je domein `ictlyceum.dc`.

Omdat we best veel hebben gewijzigd, maken we even weer een **Snapshot** van je VM met een bruikbare naam. Zekerheid voor alles!

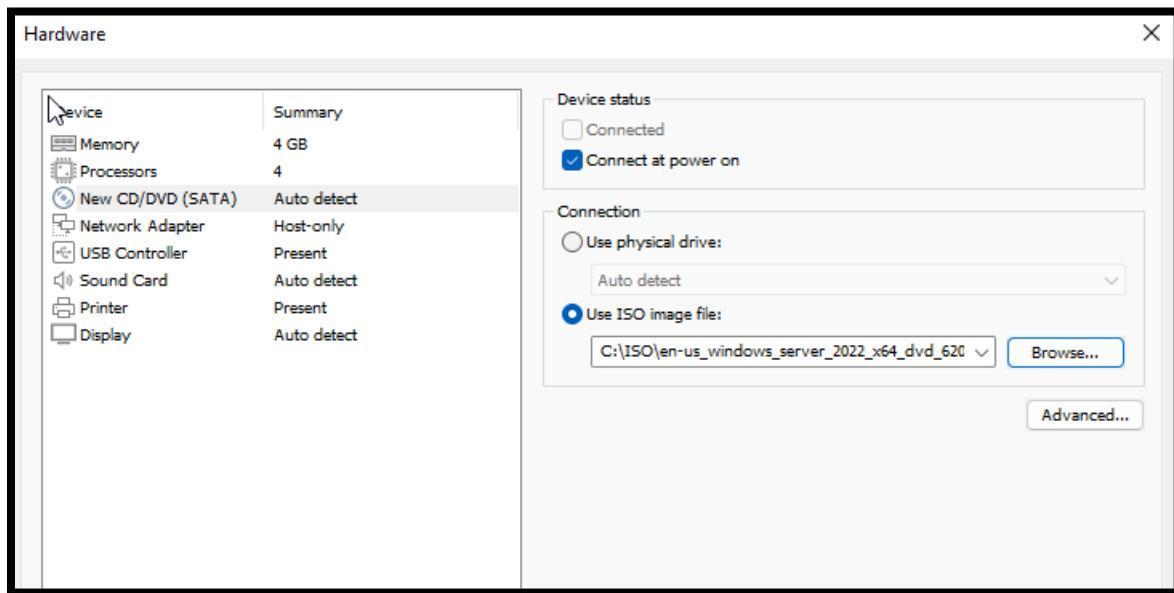
Voor nu zijn we even klaar met deze server. We gaan nu éigenlijk precies hetzelfde doen op een nieuw aan te maken VM, welke we **AD02** gaan noemen.

Installatie en configuratie tweede domain controller

Het aanmaken van de VM is identiek aan de AD01, echter krijgt deze slechts 1 netwerkkaart. Je kunt bij twijfels gewoon even terugkijken bij de configuratie van de AD01. De netwerkkaart van deze server zetten we op **Host-Only** zodat hij verbinding kan maken met de netwerkkaart van **AD01** die ook op host-only staat.

Denk tijdens de configuratie ook weer goed aan de locatie van je machine, zodat hij **NIET** naar je OneDrive verwijst. Die van mij zet ik weer in een aparte map op mijn D-schijf: **D:\Vmware\Reader AD02**

Na het aanmaken van de nieuwe VM, moet de configuratie er zo uit zien:

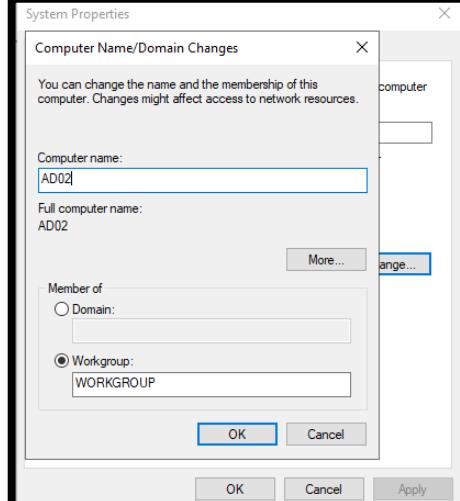


Wanneer je de machine opstart, kun je de installatie van Windows Server gaan starten. Let ook hier weer goed op dat je kiest voor een versie met de toevoeging "**(Desktop Experience)**"!

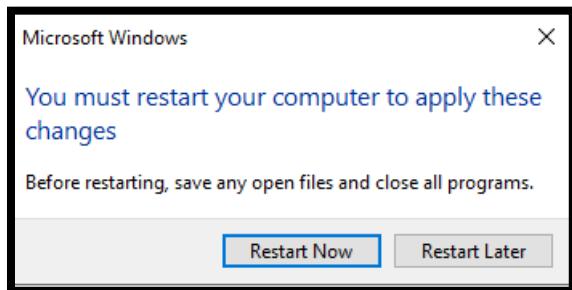
Configuratie AD02

Na de installatie en configuratie van Windows, zetten we ook hierop de role **AD DS** en **DNS**. Uiteraard gaan we eerst beginnen met de basis stappen; de naam en het netwerkgedeelte én de **VMware Tools**.

De naam passen we aan door op de huidige naam te klikken binnen de **Server Manager**. Deze server heet AD02.



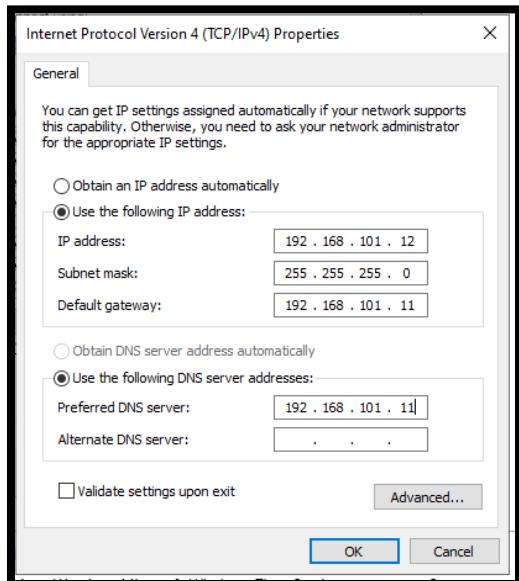
Wanneer je dit hebt gewijzigd, kies je na het opslaan voor **OK** gevolgd door **Restart Later**, omdat we eerst gelijk het netwerk even goed gaan instellen.



Dit doen we door eenvoudig op de netwerkkaart te klikken:

A screenshot of the "Server Manager" interface showing "Local Server" properties. The "PROPERTIES" tab is selected for "WIN-MR9FKONTDC9". In the "Network adapter" section, the "Ethernet0" row is highlighted with a red box around the text "IPv4 address assigned by DHCP, IPv6 enabled". Other network adapter settings shown include Microsoft Defender Firewall (Public: On), Remote management (Enabled), and Remote Desktop (Disabled). The operating system version is listed as Microsoft Windows Server 2022 Standard.

We hernoemen hem naar **LANverbinding** en stellen het volgende in:



Zoals je ziet, hebben we hier het IP-adres **192.168.101.12** ingesteld en de Default Gateway + de Preferred DNS Server zijn ingesteld op **192.168.101.11**.

Na het opslaan (dus drukken op **OK**) zorg je ervoor dat je even de **VMware Tools** (zie hoofdstuk [Installatie VMware Tools](#)) installeert en dat je een herstart uitvoert.

Om de basisconfiguratie van deze server af te krijgen, hoeven we dan alleen nog de tijd even goed te zetten zodat deze gelijk loopt met de *primary domain controller*, AD01 dus.

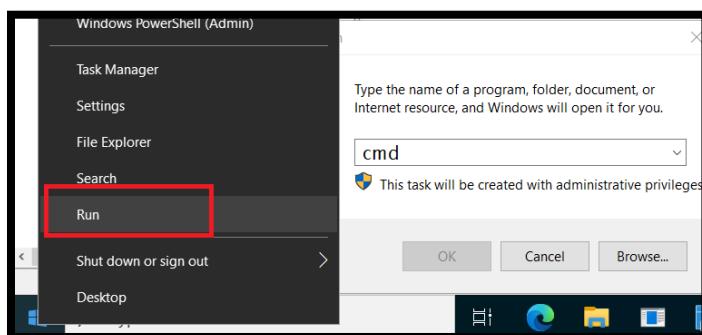
In principe moeten de servers elkaar nu ook kunnen bereiken op netwerk niveau. In VMware hebben we tenslotte aangegeven dat ze beide op **Host-Only** staan ingesteld en omdat ze beide in hetzelfde netwerkbereik zitten (192.168.101.x).

Pingen

Dit kunnen we testen door te pingen naar elkaar. **Pingen** is het sturen van een ‘echo-verzoek’ naar een adres wat je wilt bereiken. Wanneer deze aanwezig/bereikbaar is, geeft deze reactie op de ping door middel van reageren met IP-adres van dit device en de benodigde tijd hiervoor.

Pingen kan zowel op IP-basis als op DNS-naam. Mocht je gaan pingen op naam en je krijgt niets te zien, dan herkent je DNS deze naam mogelijk (nog) niet en is het dus nodig om eerst eens te kijken of je wel kunt pingen op IP-basis.

Om te pingen van server AD01 naar AD02, gaan we altijd beginnen met pingen op IP-basis. We openen hiervoor eerst de Command Prompt. We drukken hiervoor met de rechter muisknop op de Windows-knop en kiezen voor **RUN -> CMD <enter>**.

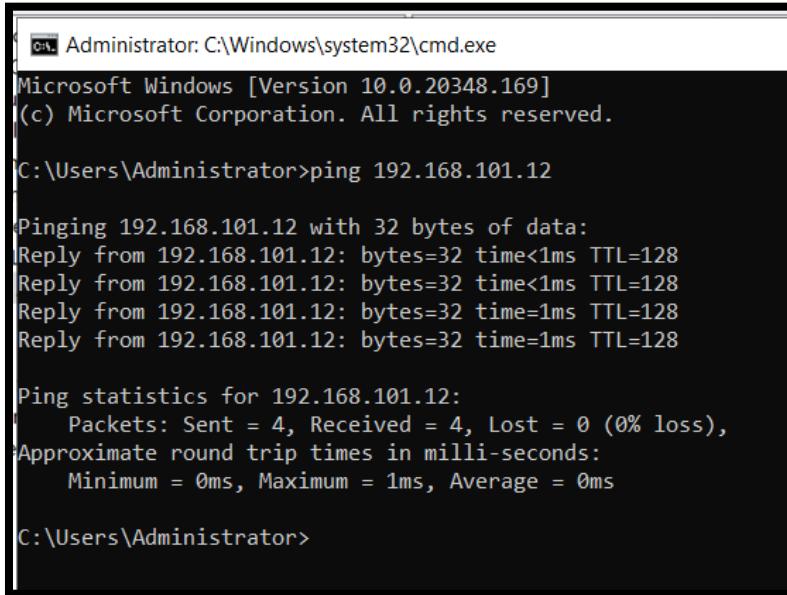


In het DOS-scherm wat we nu te zien krijgen, typen we **PING 192.168.101.12** (het ingestelde IP-adres van server AD02 dus).

A screenshot of a Windows Command Prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The window displays the Microsoft Windows [Version 10.0.20348.169] copyright information and the prompt 'C:\Users\Administrator>'. The user has typed 'ping 192.168.101.12' and is awaiting a response.

Als alles goed is ingesteld, dan zouden we nu een reactie moeten krijgen van deze server en weet je dat je netwerkverbinding in orde is.

Deze reactie ziet er als volgt uit



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.169]
(c) Microsoft Corporation. All rights reserved.

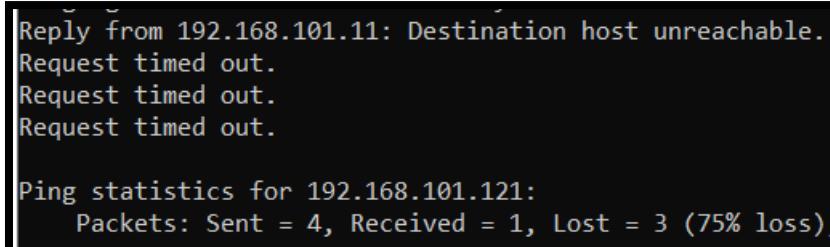
C:\Users\Administrator>ping 192.168.101.12

Pinging 192.168.101.12 with 32 bytes of data:
Reply from 192.168.101.12: bytes=32 time<1ms TTL=128
Reply from 192.168.101.12: bytes=32 time<1ms TTL=128
Reply from 192.168.101.12: bytes=32 time=1ms TTL=128
Reply from 192.168.101.12: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.101.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

In sommige gevallen krijg je echter, ook wanneer alles goed staat, helaas geen reactie:

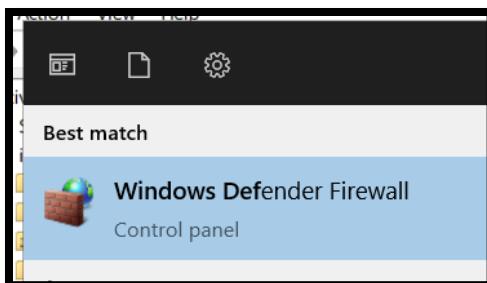


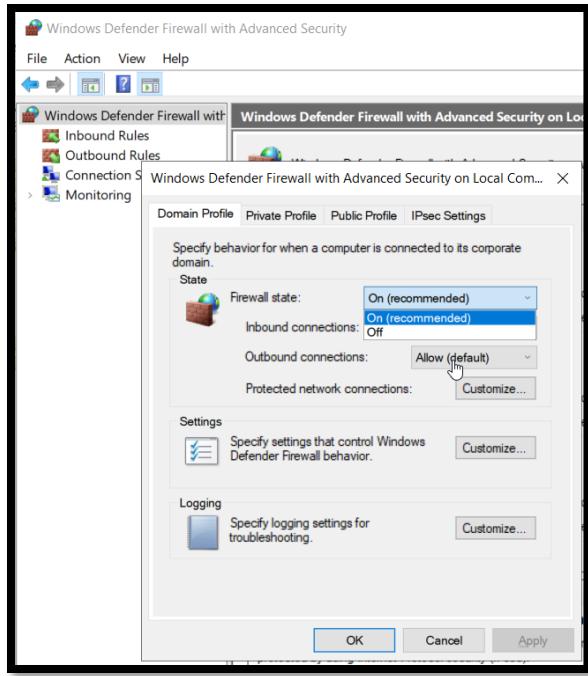
```
Reply from 192.168.101.11: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.101.121:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

Dit wordt dan veroorzaakt door de Windows Server Firewall. Mocht je dit krijgen of mocht je hierover twijfelen, dan kun je er voor kiezen om (als test) even de firewall uit te schakelen. De ping moet dan namelijk wél goed gaan. **Om nu verder te kunnen gaan is er slechts reactie vanaf één server naar de andere nodig, beide niet.**

Deze zet je uit door via het startmenu te zoeken naar Windows Defender en vervolgens te kiezen voor **Properties**





De **Firewall State** in alle tabbladen (Domain-, Private- en Public Profile) zet je hierbij op **Off**.

Mocht het pingen dan nog altijd niet werken moet je gaan troubleshooten, eigenlijk het mooiste werk in de IT. Je begint hierbij door te controleren of je beide machines inderdaad wel op **Host-Only** staan en bijvoorbeeld of je geen typfouten hebt gemaakt in de IP-adressen (een veel gemaakte fout is bijvoorbeeld **192.186.101.11** ipv **192.168.**)

Default Gateway

De default Gateway is eigenlijk simpelweg gezegd ‘de weg naar buiten’. Dus het adres wat je neerzet bij Default Gateway kan een router zijn, die thuis in de meterkast hangt, maar in dit geval wordt dit je eerste server, die we later gaan inrichten zodat hij het ‘LAN-verkeer’ naar buiten kan routeren.

We gaan hier mee bezig nadat we server **AD02** hebben toegevoegd aan het domein.

Preferred en Alternate DNS

De **Preferred DNS Server** is bij een **Member Server or Client** (je client is dus bijvoorbeeld je Windows 10 of 11 machine) altijd je primaire (**eerste**) domain controller. Dit houdt dus concreet in, dat je op elke ‘extra’ server in je netwerk, verwijst naar je eerst geïnstalleerd domeincontroller in je netwerk.

Dit hoort zo, omdat deze server straks helpt om je domeinnaam te gaan vinden. We willen namelijk in dit specifieke geval deze tweede server straks gaan koppelen aan het door jouw gecreëerde domein.

Zonder de juiste DNS server, gaat deze server straks nooit de naam ‘**ICTLYCEUM.DC**’ vinden omdat deze dan (in ieder geval volgens de nieuw geïnstalleerde Windows Server) niet bestaat/niet vindbaar is.

De **Alternate DNS Server**, is eigenlijk zoals de naam al zegt; de alternatieve DNS server. Dus heb je, naast je eerste domain controller, nog een andere DNS server die je wilt gebruiken (bijvoorbeeld een DNS server van Google -> 8.8.8.8 of 1.1.1.1) dan vul je die daarin. *In onze omgeving laten we deze*

Alternate DNS Server leeg. Bij de configuratie van AD DS op server AD02 wordt deze namelijk automatisch ingevuld.

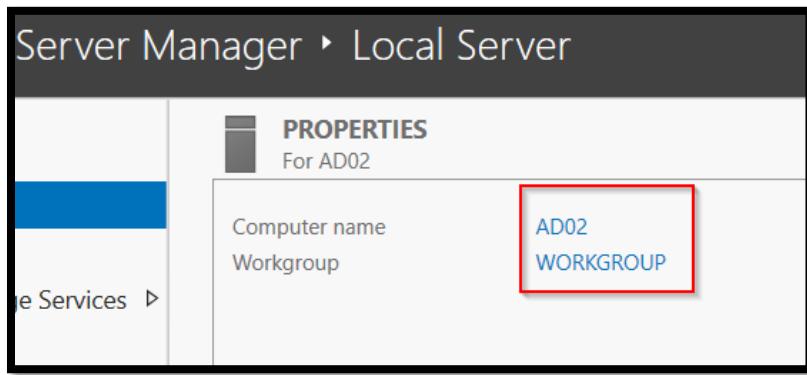
Member server toevoegen aan domein

Nu we de basisinstellingen (naam + IP, de klok én VMware Tools) weer klaar hebben gemaakt, kunnen we deze gaan toevoegen aan het door jou gemaakte domein **ICTLYCEUM.DC**. Het toevoegen van een member server aan het domein, heet eigenlijk het *joinen* van een server aan een domein.

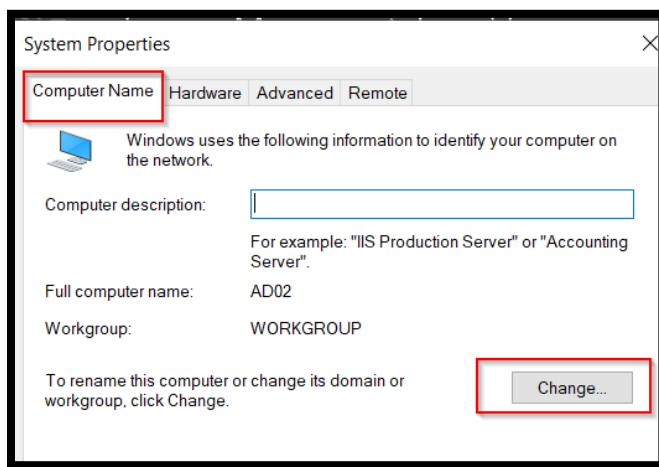
Voordat we hiermee beginnen, maken we even een **Snapshot van deze machine, mocht er namelijk iets fout gaan bij het installeren/configureren, kunnen we eenvoudig terug.**

Het toevoegen van deze member server aan het domein is bijna identiek aan dat van een werkstation/client aan je domein. Probeer dus of je de stappen kunt onthouden zodat dit straks wat eenvoudiger is.

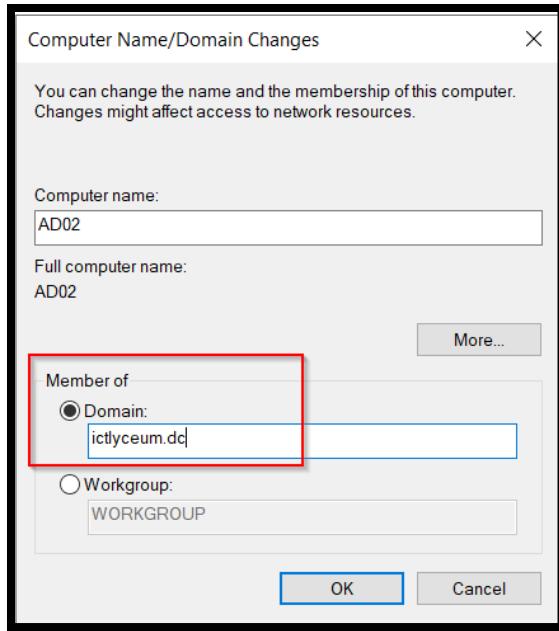
De stappen die we hiervoor moeten doen zijn relatief eenvoudig. We beginnen zoals altijd in de Server Manager, bij Local Server. We klikken hier op de (reeds aangepaste) computernaam **AD02** óf op de **WORKGROUP**.



Wanneer je dit hebt gedaan, komt het scherm na voren waar we ook de computernaam hebben gewijzigd. We kiezen dus wederom voor Change



Echter wijzigen we nu de naam niet, maar gaan we het balletje welke bij **WORKGROUP** staat, verzetten naar het balletje bij **DOMAIN**. Daar voeren we vervolgens onze domeinnaam volledig in.

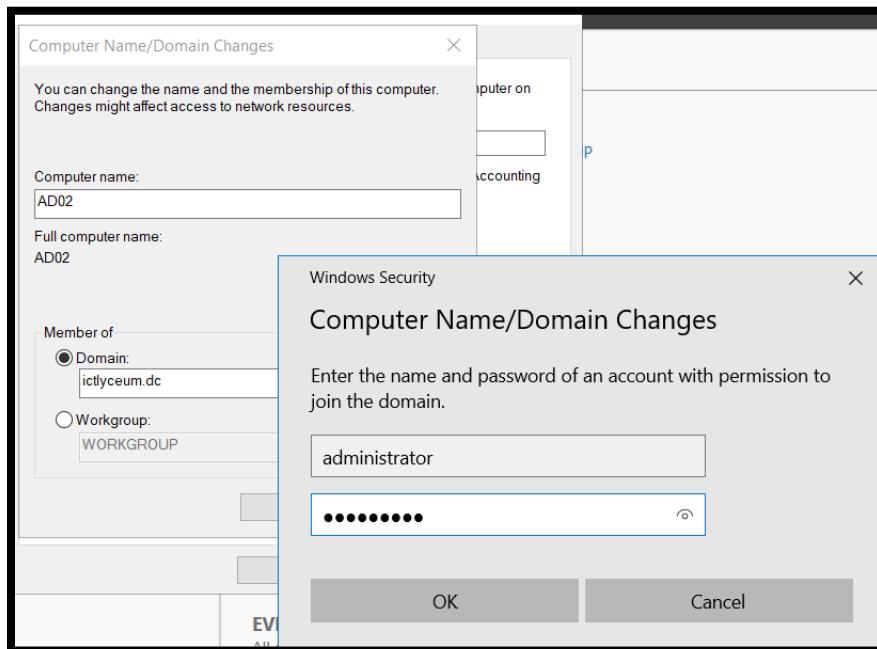


Daarna kies je voor **OK**, zodat we de server daadwerkelijk kunnen koppelen aan het domein. Zodra je op **OK** hebt geklikt, gaat je server namelijk opzoeken, via de opgegeven DNS-servers, naar het opgegeven domain.

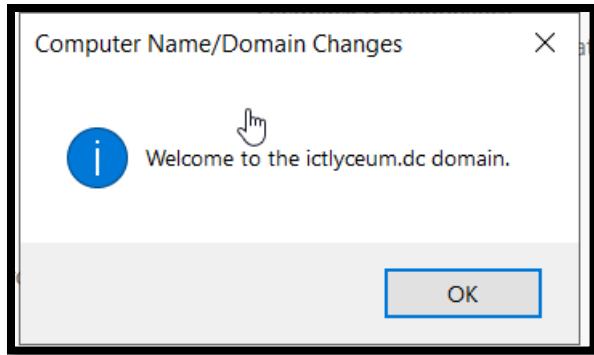
Als hij hem gevonden heeft, merk je dat je hierop dient in te loggen. Het kan natuurlijk niet zo zijn dat iedereen alles maar mag toevoegen en daarom is dit beveiligd door Microsoft.

De gegevens die je hiervoor nodig bent, zijn simpelweg de gegevens waarmee je inlogt op je domain controller, dus gebruiker **Administrator** + bijhorend wachtwoord **Welkom01!**

(Of je hier administrator met óf zonder hoofdletter doet maakt niet uit binnen Windows!)



Wanneer je op **OK** drukt, checkt hij de credentials (ofwel: inloggegevens) en wanneer dit akkoord is heet hij je vriendelijk welkom bij het domein. Dit kan een seconde of 20 duren, dus ga niet overal op klikken omdat je denkt dat hij niets doet.



Hier druk je op **OK** (2x) en dan herstart je je server.

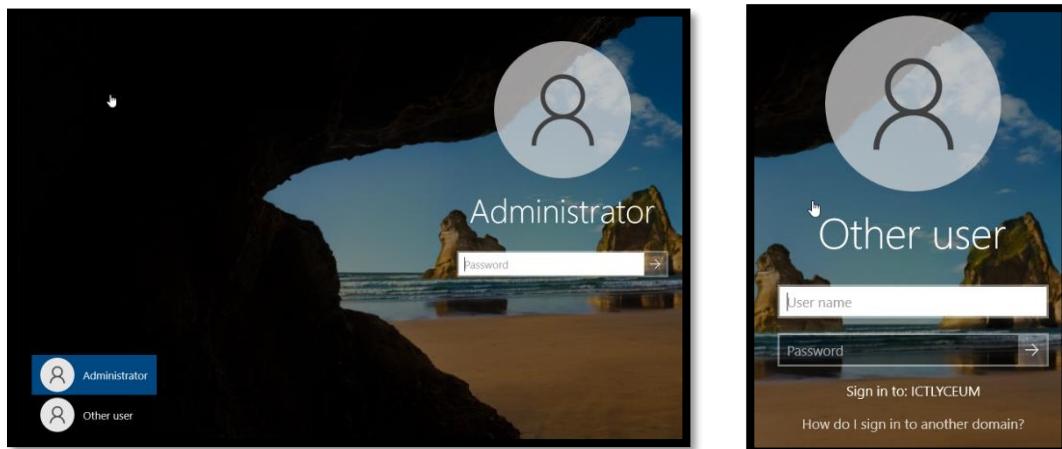
In een enkel geval gaat het aanmelden (*joinen*) van een client of server op het domein niet goed. Soms is het dan nodig om de prefix even weg te halen en het nogmaals te proberen. Je meldt je client/server dan aan op de **NETBIOS-naam**. Als dat wel goed gaat kán het zijn dat de DNS een probleem heeft, maar hoeft dat niet direct een probleem te betekenen. Je kunt dan wel gewoon verder met de volgende stappen.

Nu hoor ik je denken;

Maar....., kon dit dan niet gewoon tegelijkertijd met het wijzigen van de servernaam???

Het antwoord daarop is; **Ja zeker**, dat had gekund! Én de volgende keren ga je dit waarschijnlijk ook zeker zo uitvoeren. Alleen om nu bewust te worden van de benodigde stappen heb ik er voor gekozen dit even op deze manier te laten doen.

Na de herstart hangt je AD02 in het domein van het **ICTLyceum**. Je kunt zien door links onderin, bij het inlogscherm, te kiezen **Other User**.



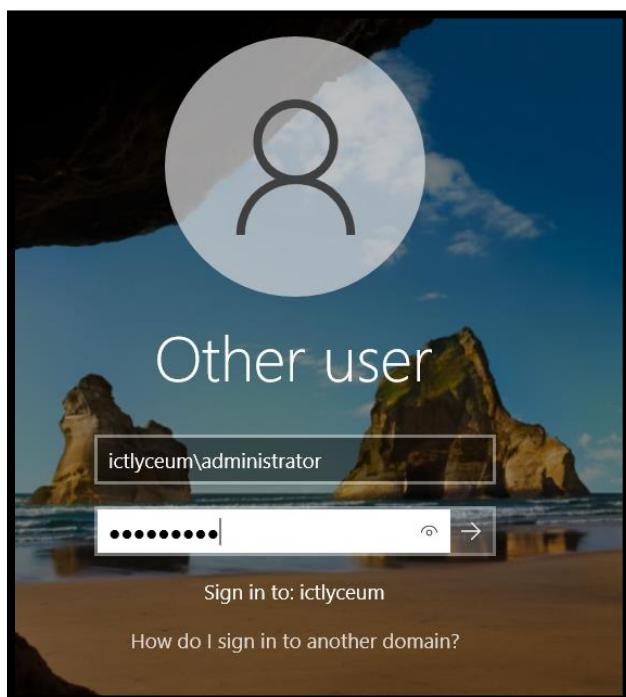
Wanneer je daarop geklikt hebt, zie je gelijk al dat hij in wil loggen op het netwerk van het ICTLyceum (**Sign in to:ICTLYCEUM**, een mooie bevestiging dus dat hij daadwerkelijk op het domein is aangemeld.

Inloggen op het domein

Inloggen op een domein nadat je een server (óf client) hebt toegevoegd, doe je altijd door gebruik te maken van het **NETBIOS-naam + \je gebruikersnaam óf gebruikersnaam@volledigedomeinnaam**.

In sommige gevallen is het niet nodig om de domeinnaam\NETBIOS-naam ervoor te zetten. Maar leer jezelf dit gewoon aan, zodat dit altijd goed gaat. In onze omgeving wordt het dus:

ICTLYCEUM\Administrator óf dus administrator@ictlyceum.dc



Zodra je bent ingelogd, ben je dus nu ingelogd als de beheerder van het domein en heb je dus alle rechten op deze machine én kunnen we van deze machine nu dus ook een domeincontroller maken.

Maar eerst gaan we even kijken of hij deze AD02 ook daadwerkelijk heeft aangemaakt in ons domein. Hij zegt van wel, maar is het ook daadwerkelijk zo? Hiervoor openen we op de **server AD01** even via **Tools, Active Directory Users and Computers** weer en gaan nu naar de **OU Computers**. Deze was eerst leeg, maar nu zien we hier inderdaad de AD02 nu staan. Hij is dus nu officieel lid van dit domein.

A screenshot of the Active Directory Users and Computers (ADUC) management console. The left pane shows a tree view of the directory structure under 'ictlyceum.dc', with 'Computers' being the selected node. The right pane displays a table with one row: 'AD02'. The table has three columns: 'Name', 'Type', and 'Description'. The 'Name' column shows 'AD02', the 'Type' column shows 'Computer', and the 'Description' column is empty. The entire window has a standard Windows-style title bar and menu bar.

Fouttolerantie / Redundancy

Door dit te doen op deze AD02, zorgen we er eigenlijk voor dat we een fouttolerantie creëren in het domein. Dus stel server AD01 valt uit, wordt geüpdate of start simpelweg niet meer op, dan kan

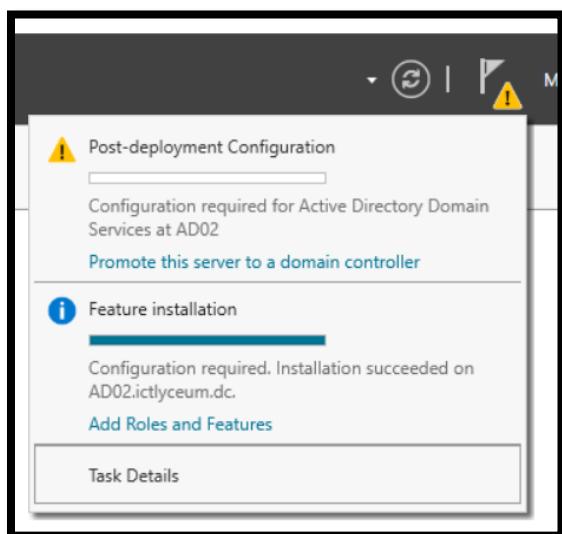
AD02 alle rollen automatisch overnemen waardoor niemand in de organisatie dus zal merken dat er iets aan de hand is. In de ICT noemt men dit ook wel 'redundancy'.

Om te zorgen dat we deze redundancy kunnen bouwen, moeten we op de **AD02** de benodigde rollen gaan installeren. We beginnen hier met de rollen **AD DS** en **DNS**. Zorg ervoor dat deze beide worden geïnstalleerd zodat je straks ná de installatie deze AD02 kunt promoten als domeincontroller.

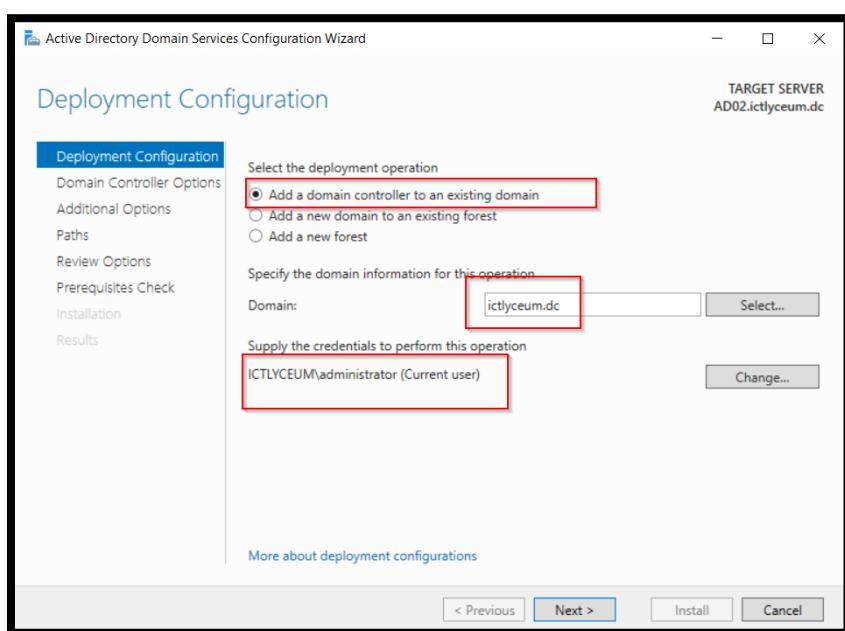
Mocht je twijfelen hoe dat nou precies ging, [lees dan vanaf pagina 25 tot 30](#) nog een keer rustig door.

Configuratie AD DS op server AD02

Wanneer je de installatie hebt voltooid kun je als het goed is via het vlaggetje wederom gaan kiezen voor **Promote this server to a domain controller**

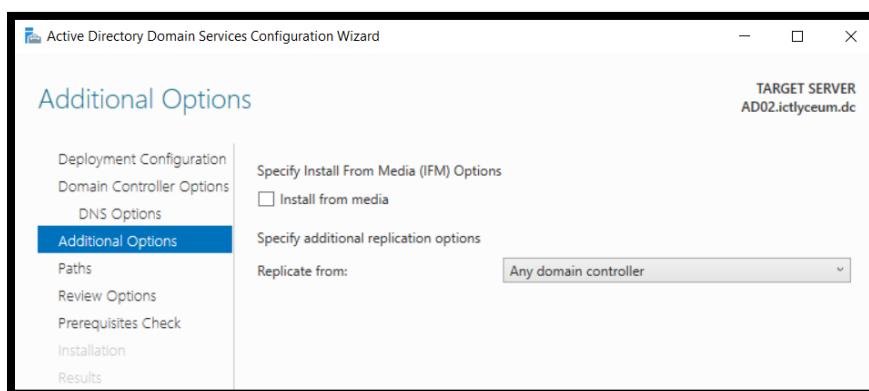


Deze Configuration Wizard ken je inmiddels, echter hebben we op déze machine al wél een domein. We gaan nu dus niet kiezen om een **New Forest** aan te maken. Dit keer kiezen we voor de optie **Add a domain controller to an existing domain**.



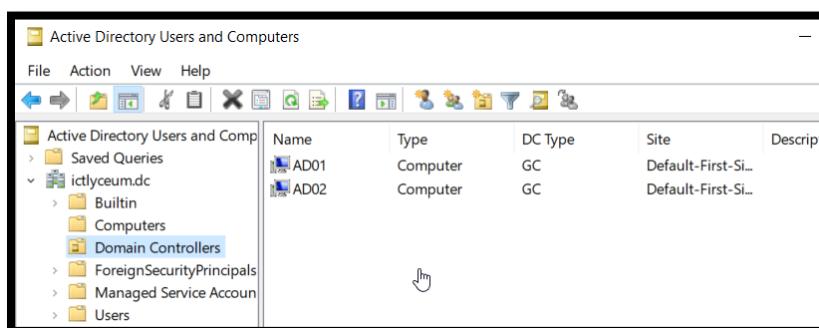
Zoals je ziet zijn er, doordat we in de stappen hiervoor deze server al aan het domein hebben gejoint (toegevoegd), al enkele belangrijke gegevens ingevuld voor ons. Waaronder de domeinnaam en de beheerder van het domein (**ICTLYCEUM\administrator**).

Als dit er bij jou ook zo uit ziet, kunnen we door naar de volgende stap en kies je dus voor Next. Eigenlijk doorloop je nu alle stappen weer, die we bij de eerste domein controller ook hebben gevolgd, totdat we bij **Additional Options** aankomen. Hier hoeft je eigenlijk niets te doen, maar is het wel even van belang dat je weet wat er hier gebeurt. In dit punt kun je namelijk aangeven vanaf welke domain controller je wilt dat er gerepliceerd wordt. Dit kan nuttig zijn wanneer je bijvoorbeeld lokaal een (primaire) domeincontroller hebt staan maar ook een in bijvoorbeeld Duitsland ergens met een wat slechtere verbinding. In dat geval kies je hier uiteraard de dichtstbijzijnde. Voor nu laten we dit gewoon voor wat het is.

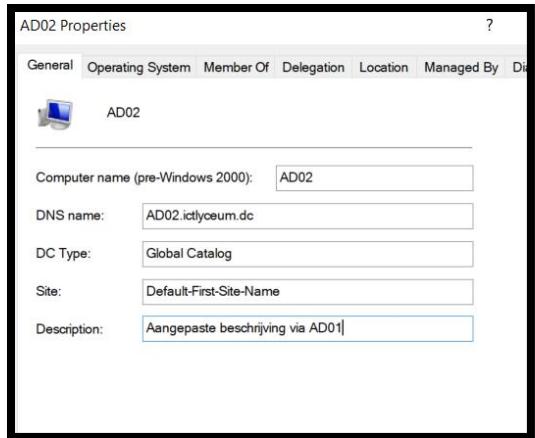


We kiezen weer Next tot we bij Results aankomen en we op Install kunnen drukken. Nadat je wordt uitgelogd gaat de server herstarten en vervolgens heb je je tweede domein controller alweer draaien!

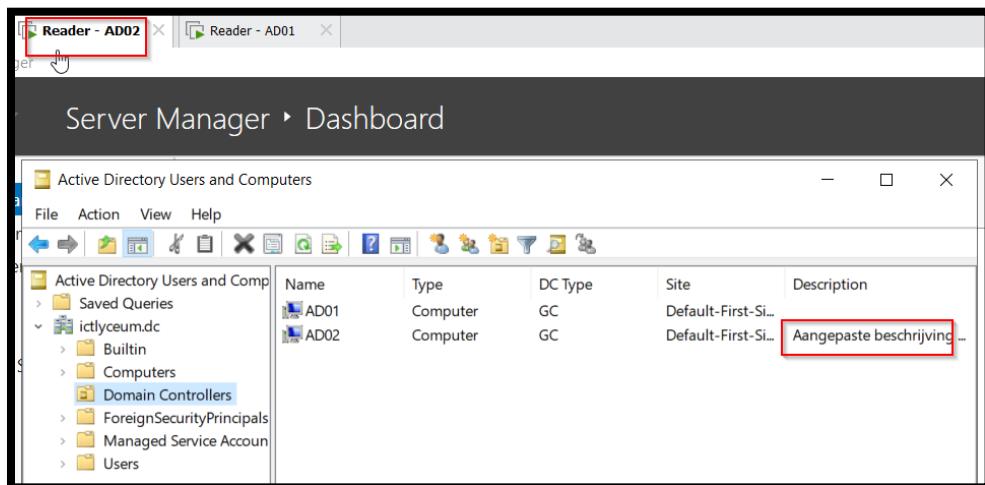
Je checkt dit op de server **AD01** via de **Active Directory Users and Computers** en je zult hier zien dat hij nu **UIT** de OU **Computers** is, maar nu staat bij de OU **Domain Controllers** en je ziet dat hij tevens GC is (tenzij je dit uiteraard hebt uit gevinkt bij de *Domain Controller Options* in de **Configuration Wizard**).



We gaan nu dubbel op de Domain Controller **AD02** dubbelklikken en bij Description zetten we: **Aangepaste beschrijving via AD01**.



Vervolgens openen we op de server **AD02** óók via **Tools, Active Directory Users and Computers** en daar zien we dat bij de Description van de **AD02**, deze wijziging is doorgevoerd (dit kan enkele minuten duren in sommige gevallen!):



Zoals je ziet, repliceren de domain controllers dus samen. Wanneer je nu ook een nieuwe OU, gebruiker of security aanmaakt, is het binnen enkele seconden (tot heel soms minuten) repliceert (of eigenlijk gesynchroniseerd) met de andere domain controller. Het maakt verder niet uit of je de wijzigingen op AD01 of op AD02 doet.

Routing en DHCP

We hebben nu al een mooie basis staan van een zakelijk netwerk. De belangrijkste servers draaien, we hebben een netwerk ingericht en we kunnen bezig met het aanmaken van gebruikers en beveiligingsgroepen. Deze laatste gaan we op een later moment koppelen aan gedeelde mappen, zodat we eenvoudig kunnen beheren wie tot wat voor mappen (shares) toegang heeft binnen het netwerk, maar daarover later dus meer.

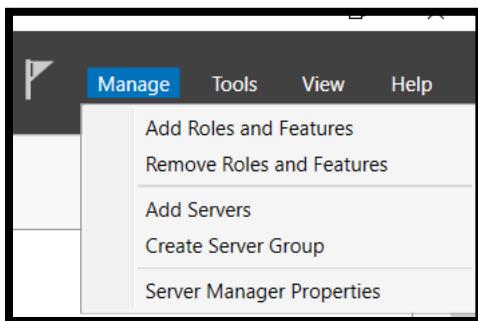
We gaan nu eerst zorgen dat we van server AD01 een router maken. Heel eenvoudig gezegd, gaan we ervoor zorgen dat alle andere VM's binnen dit werk (dus de VM's die op Host-Only zijn 'aangesloten eigenlijk') het internet op kunnen via AD01. Het enige wat we hiervoor nodig zijn is de rol 'Routing and Remote Access', een tweede netwerkkaart op de AD01 welke verbonden is met NAT (hebben we reeds klaargemaakt in H1) én we moeten zorgen dat de weg naar buiten (= Default Gateway zoals jullie inmiddels weten) wijst naar dus de AD01. Klinkt best eenvoudig en eigenlijk is dat ook wel zo.

Jullie kennen allemaal de router in je meterkast thuis. Daarin plug je een kabel (of daarmee maak je verbinding via je WIFI) en dan heb je internet. Dit apparaat gaan we nu eigenlijk instellen binnen de Windows Server.

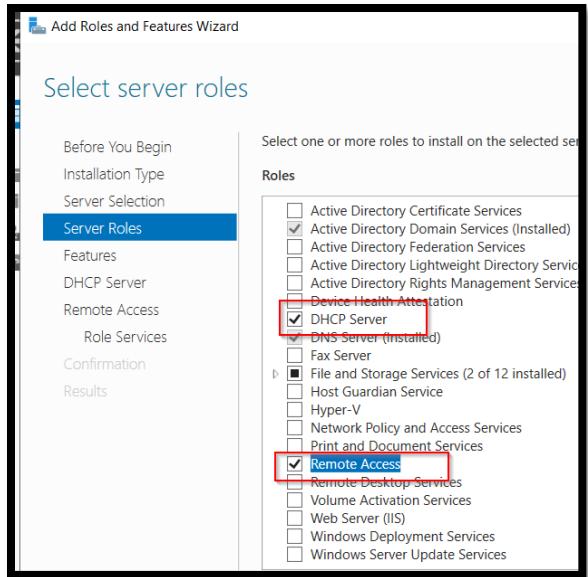
Installatie Routing and Remote Access + DHCP

Om hiermee te beginnen installeren we een nieuwe rol. Aangezien deze configuratie heel kort is, pakken we gelijk de rol DHCP mee aangezien we deze direct daarna klaar gaan maken. Wat DHCP doet behandelen we straks, maar we nemen zoals gezegd dus direct deze role vast mee.

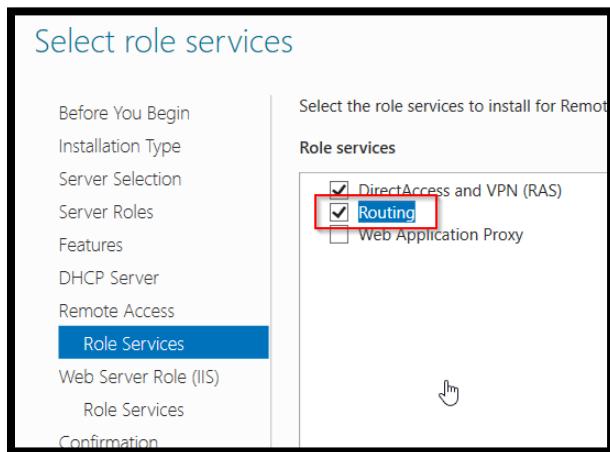
We kiezen dus op de AD01, via de Server Manager, voor **Add Roles and Features**



We gaan direct door naar Server Roles en kiezen hier de role **DHCP Server** (+ uiteraard benodigde Features) en de role **Remote Access**. Die laatste klinkt wellicht wat vreemd, maar dit is een role welke meerdere rollen kan instellen binnen deze rol.



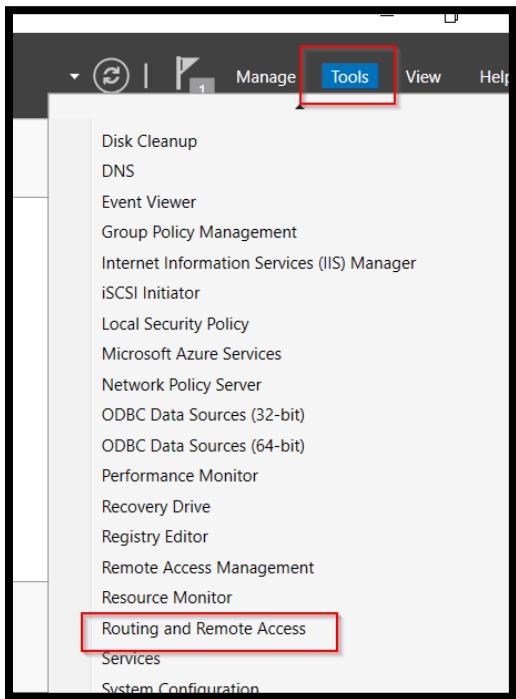
Wanneer je doorgaat via de knop Next, komen we uiteindelijk bij het tabblad **Role Services** uit. Hierin kunnen we kiezen welke Role we dus daadwerkelijk binnen deze Role (Remote Access) willen gebruiken. Hier kiezen we voor **Routing**, aangezien we een router willen maken. Je kiest er, net als altijd, voor om ook de benodigde Features te installeren.



Zoals je zult merken, vinkje hiermee automatisch ook de role DirectAccess and VPN (RAS) aan.

Die laatstbenoemde gebruiken we niet (direct) maar zijn wel nodig om Routing te kunnen opzetten. We gaan de boel installeren en wanneer hij klaar is vinden we deze nieuwe role onder het tabblad **Tools -> Routing and Remote Access**.

Configuratie Routing and Remote Access

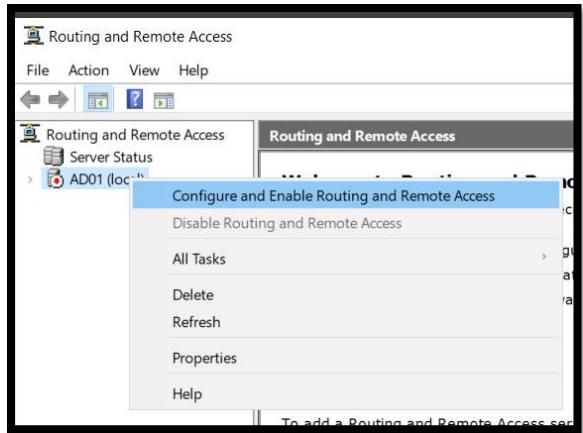


Wanneer we deze openen, komen we in een console scherm van Windows, ook wel de MMC genoemd (Microsoft Management Console). Hierin zien we onze server staan met een rood pijltje naar beneden, deze is op dit moment nog **down..**



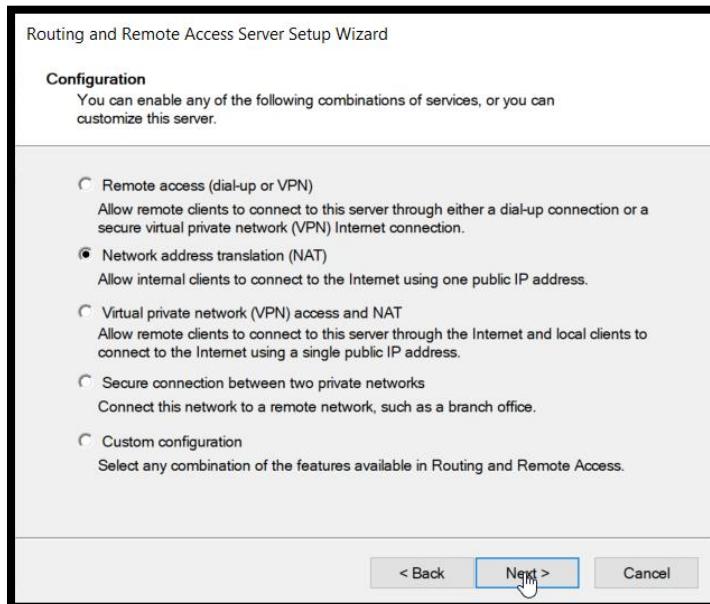
Om deze role (goed) te laten werken, moet dat rode pijltje groen en naar boven wijzen (**Up**). Daar gaan we dus even voor zorgen.

Dit doen we door met de rechtermuisknop te klikken op de servernaam (AD01 (local)) en te kiezen voor **Configure and Enable Routing and Remote Access**.



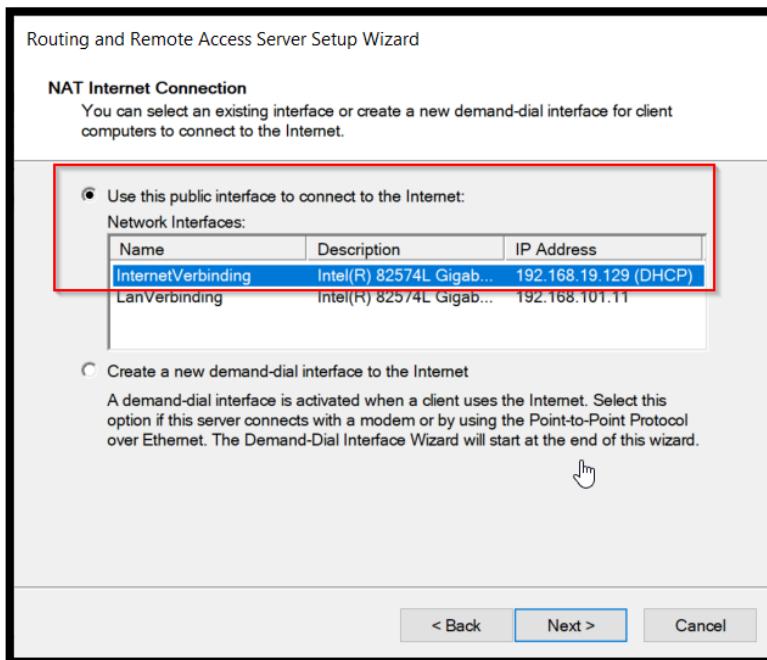
Je krijgt eerst wat informatie te zien over wat je allemaal kunt met deze tool, dit mag je even rustig doornemen. Daarna kies je voor Next.

Vervolgens kiezen we hier voor NAT (**Network Address Translation**), we willen tenslotte het verkeer gaan vertalen van het interne netwerk naar het externe netwerk (intern = LAN, extern = Internet).



In het scherm hierna, is het de bedoeling dat je aangeeft welke netwerkadapter aan het internet gekoppeld is. Nu valt waarschijnlijk het kwartje; **Ah, daarom moest ik die netwerkkaart hernoemen!?** Precies!

Hier kiezen we dus natuurlijk onze **InternetVerbinding** netwerkkaart (die in je Setting van VMware op NAT staat dus)



Nu zit er in Windows Server een kleine bug, waardoor er in sommige gevallen in de afbeelding hierboven geen netwerkkaarten te zien zijn en/of er een melding staat dat je 'slecht 1 netwerkkaart hebt geïnstalleerd', je kunt dan niet verder met deze wizard, je hebt namelijk minimaal 2 netwerkkaarten nodig.

Deze bug is simpel op te lossen, door gewoon even de Wizard te stoppen door op Cancel te drukken en vervolgens de Wizard opnieuw te starten volgens bovenstaande stappen. Je zult zien dat je dan wél 2 netwerkkaarten te zien krijgt (uiteraard alleen wanneer je dit allemaal goed hebt ingesteld aan het begin....).

Nadat je jouw netwerkkaart gekozen hebt welke met internet verbonden is, waarschijnlijk met de naam **InternetVerbinding**, klikken we op Next, gevolgd door Finish.

Je krijgt nu een melding te zien dat er mogelijk problemen zijn omdat de firewall niet automatisch geconfigureerd kan worden, dat is prima en je drukt op OK.



Je hebt de router nu succesvol geconfigureerd.

Je kunt het eenvoudig even controleren door bij IPv4 te kijken bij **General** (Algemeen). Je zult dan zien dat je bij **Incoming bytes** en **Outgoing bytes** verkeer ziet langskomen:

The screenshot shows the 'General' tab in the 'IPv4' section of the Routing and Remote Access console. It lists network interfaces with their types, IP addresses, and byte counts. A red box highlights the 'Incoming bytes' and 'Outgoing bytes' columns for the 'InternetVerbinding' interface.

Interface	Type	IP Address	Incoming bytes	Outgoing bytes
Loopback	Loopback	127.0.0.1	0	0
LanVerbinding	Dedicated	192.168.101.11	5,784,671	4,887,289
InternetVerbinding	Dedicated	192.168.19.129	13,869,805	1,417,568
Internal	Internal	Not available	-	-

Een andere (mooiere) test, is door te kijken of je op de AD02 nu daadwerkelijk internet hebt. Deze had dat natuurlijk niet, maar je had al wél de Default Gateway ingesteld tijdens de netwerkconfiguratie, dus in theorie zou dat moeten werken nu.

We gaan dus op server **AD02** via Microsoft Edge naar <https://www.drenthecollege.nl> als test. Als het goed is zie je dan de website van het Drenthe College, ondanks een eventuele melding rechts onder in de server waarbij staat dat er geen internetverbinding is, dit kan namelijk altijd even duren voordat de server dit 'verwerkt' heeft, **maar zegt dus niet altijd dat dat ook klopt**.

In een enkel geval gebeurt het wel eens dat je nu wel internetverbinding hebt via de AD01, maar dat de DNS niet mee komt en je dus niet naar de bovenstaande website kan komen. Dit kun je even testen door te proberen te pingen naar 8.8.8.8. Mocht je dan antwoord krijgen dan weet je dat de verbinding naar buiten functioneert en je dus 'iets' aan de DNS moet doen.

Je kunt dan eenvoudig even een tweede DNS-server (8.8.8.8) toevoegen aan de netwerkkaart van de AD02 om te kijken of alles dan wél werkt.

Om we weer wat werkend hebben opgeleverd, maken we voor de zekerheid weer even een **Snapshot**

DHCP - Configuratie DHCP op server AD01

Nu de router klaar is, gaan we de DHCP-server configureren. DHCP staat voor **Dynamic Host Configuration Protocol**. Eigenlijk dus 'het verzenden van een configuratie naar dynamische hosts', dynamische host kun je lezen als smartphones, tablets, laptops/computers etc.

Simpeler gezegd gaan we dus een server inrichten welke de netwerkconfiguratie van óns netwerk gaat uitdelen aan dynamische apparaten (hosts dus).

Wanneer er in een netwerk **geen** werkende DHCP-server draait, of wanneer deze bijvoorbeeld is gecrashed/uitgeschakeld is of wat dan ook, krijgen je dynamische apparaten dus geen netwerk informatie en zijn ze nooit in staat het netwerk te benaderen. Op dat moment kunnen ze dus niet printen, het internet niet bereiken en zelfs geen data bereiken welke normaliter op het netwerk bereikbaar zou zijn. Je kunt er dan natuurlijk altijd voor kiezen om elk apparaat een **static (statisch/vast)** IP-adres te gaan geven, maar in een organisatie met bijvoorbeeld 500-werkstation, 200 iPads en nog een stuk of 60 laptops kom je van die theorie vermoedelijk al snel terug.

Daarom is het juist inrichten van een DHCP-server best wel cruciaal in het een netwerkomgeving. Nog mooier zou zijn wanneer je zelfs tweé DHCP-servers gaat inrichten zodat je een soort back-up hebt. Dit gaan wij dus ook bouwen.

APIPA

Een laatste onderdeel wat uitgelegd moet worden voordat we beginnen met de installatie is APIPA.

APIPA (*Automatic Private IP Addressing*) is een protocol wat Microsoft heeft bedacht voor autoconfiguratie van netwerkapparaten (veelal Microsoft software gerelateerd, maar ook printers van bijvoorbeeld Brother maken hier gebruik van).

Dit protocol zorgt ervoor dat, wanneer er geen (bereikbare) DHCP-server beschikbaar is, het apparaat (dus je laptop bijvoorbeeld) toch een DHCP-adres toegewezen kan krijgen; een APIPA-adres. APIPA controleert om de 5 minuten op de aanwezigheid van een DHCP-server. Als eenmaal een DHCP-server is gevonden stopt APIPA en de DHCP-server vervangt het APIPA-adres + de bijhorende overige (eventueel) meegezonden gegevens (zoals router/DNS etc). Indien er veel APIPA-clients in een netwerk zijn veroorzaakt dit veel broadcastverkeer. Het is dus altijd belangrijk om dit soort problemen zo snel mogelijk te detecteren en dus op te lossen.

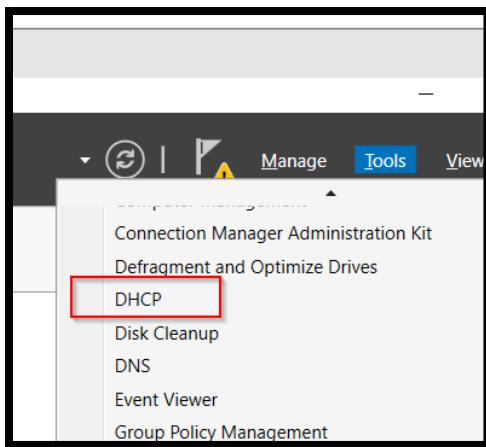
Een APIPA-adres herken je altijd onmiddellijk wanneer je de netwerkinstellingen bekijkt, deze begint namelijk altijd met **169.254(.*)**.

```
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::548d:41aa:894a:2709%5(Preferred)
Autoconfiguration IPv4 Address. . . . . : 169.254.222.194(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

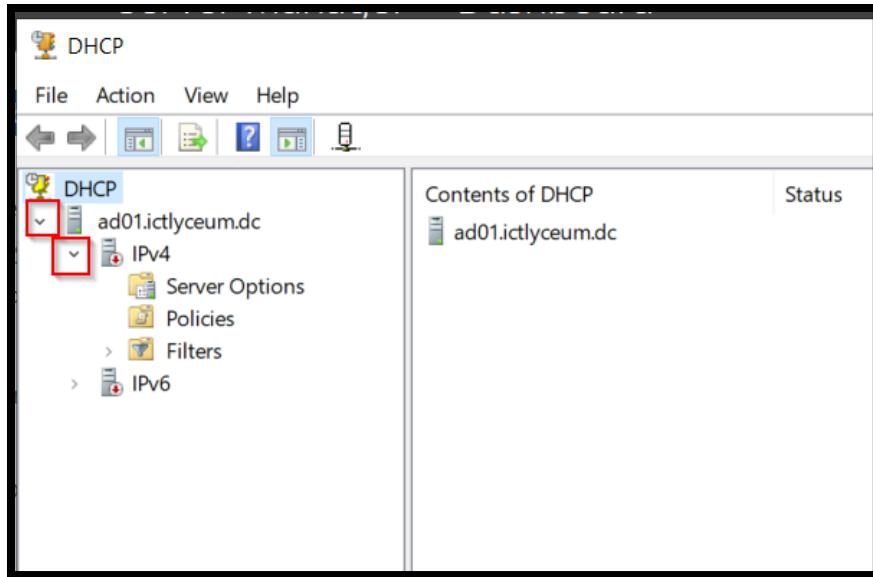
APIPA heeft officieel als reeks: **169.254.0.1 t/m 169.254.255.254**, of ook wel: **169.254.0.1 /16**

Configuratie DHCP

We starten de configuratie van de DHCP door op de AD01, via de Server Manager, naar Tools te gaan en dit keer te kiezen voor **DHCP**



We komen dan wederom in een MMC-scherm terecht waarin we door middel van de 'pijltjes naar beneden' alles voor IPv4 gaan uitklappen zodat we het kunnen instellen.



Zoals je gelijk ziet, zien we hier (net als bij Routing and Remote Access) ook een rode pijl naar beneden, wat dus betekend dat hij **down** is. Uiteraard moet deze ook naar boven (**Up**) wijzen straks in het groen, maar daarvoor moeten we eerst het een en ander gaan configureren.

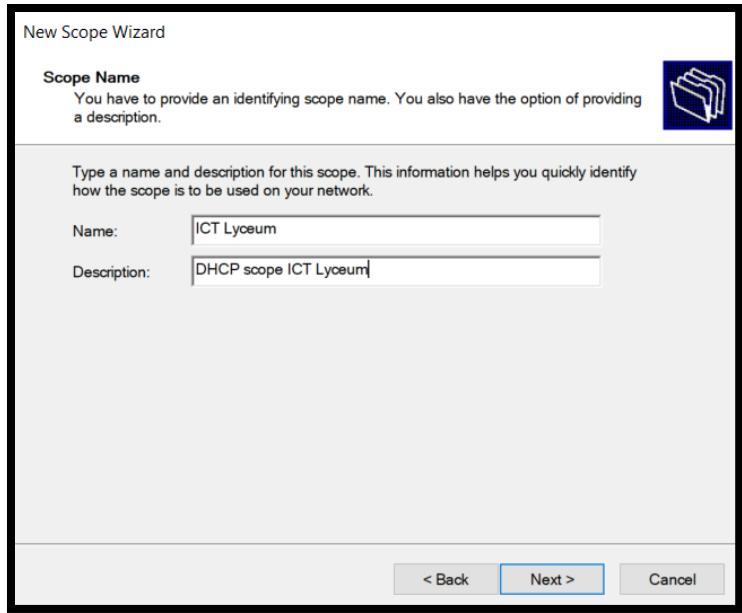
We beginnen door met de rechter muisknop te klikken op IPv4, aangezien we op dat niveau de DHCP willen gaan uitdelen (ook wel ‘uitrollen’ genoemd). We kiezen hier in het menu voor **New Scope** en dan wordt de zogeheten '**New Scope Wizard**' gestart.

De DHCP-Scope

De DHCP-scope is eigenlijk simpel gezegd ‘het bereik aan adressen die we willen gaan uitdelen aan onze DHCP-clients’. Hierbij is het belangrijk dat we niet alleen een IP-adres naar de **‘dynamische hosts’** gaan sturen, maar ook enkele belangrijke opties. Je smartphone of iPad/laptop heeft in de meeste gevallen namelijk niet heel veel aan alleen een IP-adres. Uiteraard zijn er uitzonderingen, maar in onze omgeving is het belangrijk dat we het totaalplaatje gaan rond sturen, anders kan onze client namelijk (Windows 11) geen verbinding maken met het opgebouwde ICTLYCEUM.DC domein.

Om te beginnen gaan we deze nieuwe scope een naam geven. In principe kan dit alles zijn, maar vaak is het nuttig om hem een begrijpelijke naam mee te geven. Je kunt er namelijk voor kiezen om meerdere DHCP-scopes op één enkele DHCP-server te configureren. Op dat moment is het bijvoorbeeld erg onhandig als je geen idee hebt wat voor naam je aan welke scope hebt gegeven.

In onze omgeving kiezen we de naam ‘ICT Lyceum’, erg toepasselijk voor nu. Daarnaast kun je, onder de scope naam, een korte omschrijving zetten. Dit kan erg handig zijn wanneer iemand (of jij zelf) de omgeving moet beheren tijdens bijvoorbeeld een vakantie of wisseling van baan. Die voeren we ook netjes in. Je mag uiteraard zelf een logische omschrijving plaatsen of je neemt die van de volgende afbeelding gewoon over.



In de volgende stap gaan we gelijk starten met eigenlijk de belangrijkste stap in dit proces; de '**address-range**'.

Voordat we dit gaan invullen, gaan we hier even goed over nadenken. Het is namelijk erg belangrijk dat je dit in een keer goed doet, aangezien het in een productieomgeving niet raadzaam is deze aan te passen nadat hij live is gegaan en in gebruik is.

We beginnen even weer bij het begin; de eerste twee servers.

Waarom? Nou, kijk;

We hebben tenslotte de AD01 het IP-adres **192.168.101.11** gegeven. De AD02 heeft IP-adres **192.168.101.12**. Dit betekend dat we de adressen **192.168.101.1 t/m 192.168.101.10** vrij hebben én de adressen **192.168.101.13 t/m 192.168.101.254** (192.168.101.255 is natuurlijk écht het eindadres, maar dit is de 'broadcast' en telt dus niet mee in de scope. Dit laatste adres kan overigens nooit worden uitgedeeld/ingesteld).

Het broadcast adres is het enige adres in je IP-range welke op elk niveau de waarde 1 heeft (8x). Die adres wordt ook wel omschreven als het 'gegevensverspreidingsadres', hij kan alle adressen in de range namelijk bereiken.

Als we goed gaan kijken naar de twee vrije 'ranges' dan spreekt het voor zich dat we in onze situatie voor de grootste range zullen gaan, dus **192.168.101.13 tot 192.168.101.254**. We hebben dan namelijk 241 vrije adressen en anders hebben we er slechts 10. Je kunt je voorstellen dat, zelfs in een klein bedrijf, 10 IP-adressen voor 10 apparaten dus wel wat weinig zijn.

Stel je hebt 5 werknemers, met elk een laptop, een mobiel en bijvoorbeeld een tablet, dan zit je als snel op 15 benodigde IP adressen, dus dan zitten we al vast met die 10.

Maar goed, dan is de vraag, beginnen we gelijk met het uitdelen van de **192.168.101.13** of nemen we daarin wat vrije ruimte om meerdere IP adressen handmatig/static uit de delen. Want stel er komen nog een of twee servers bij?

Om die redenen is het altijd raadzaam om een beetje spelend te hebben in je scope. Je kunt dit heel groot maken, maar het belangrijkste is dat je er altijd over nadenkt wat logisch is.

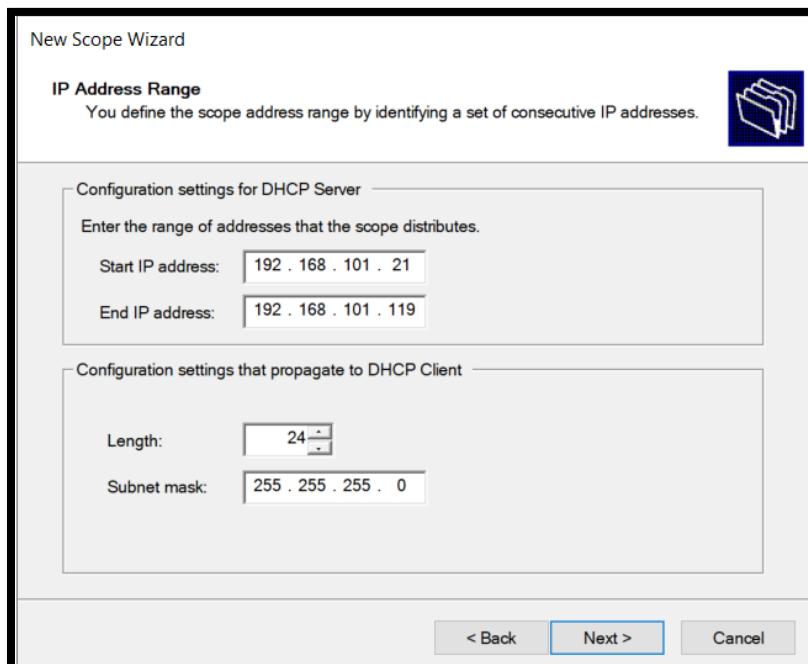
In onze omgeving, waar een extra server niet uitgesloten zal zijn, gaan we er voor kiezen om de adressen tot én met **192.168.101.20** vrij te houden. Wat inhoud dat we dus kunnen gaan uitdelen vanaf **192.168.101.21**. Op die manier kunnen we dus **192.168.101.13 t/m 192.168.101.20** zelf indelen op eventuele nieuwe servers, printers of bijvoorbeeld een Wireless Access Point.

Het begin hebben we dan, maar tot hoever gaan we dan... Dat is de tweede vraag. Het is vaak raadzaam om 'zoveel mogelijk' ruimte aan te nemen, maar dan ook weer niet onnodig veel. Altijd een lastige taak. Gelukkig kun je hem altijd uitbreiden (tot uiteraard max. *.254) dus daarin hebben we een beetje spelend. In deze reader-omgeving kiezen we om op deze server te gaan tot **192.168.101.119**. Deze is server is dus straks in staat om totaal **98** IP-adressen uit te delen. Dat moet meer dan genoeg zijn om te beginnen.

Om te zorgen dat we ook de komende jaren nog vooruit kunnen, gaan we straks óók op de AD02 een DHCP-server inrichten. Deze heeft als primair doel om te zorgen voor fouttolerantie, of ook wel redundancy, net zoals bij de AD DS dus. Mocht server AD01 uitvallen, dan kan de AD02 net als met de Active Directory, deze rol eenvoudig overnemen.

Een andere mooie bijkomstigheid is natuurlijk, dat we op de AD02 de range gaan uitbreiden. Mocht AD01 dan niet uitgevallen zijn, maar de IP-range is 'op', dan kan men alsnog verbinding krijgen met het netwerk via de AD02. Maar eerst even de AD01 afmaken voor we daar mee bezig gaan natuurlijk.

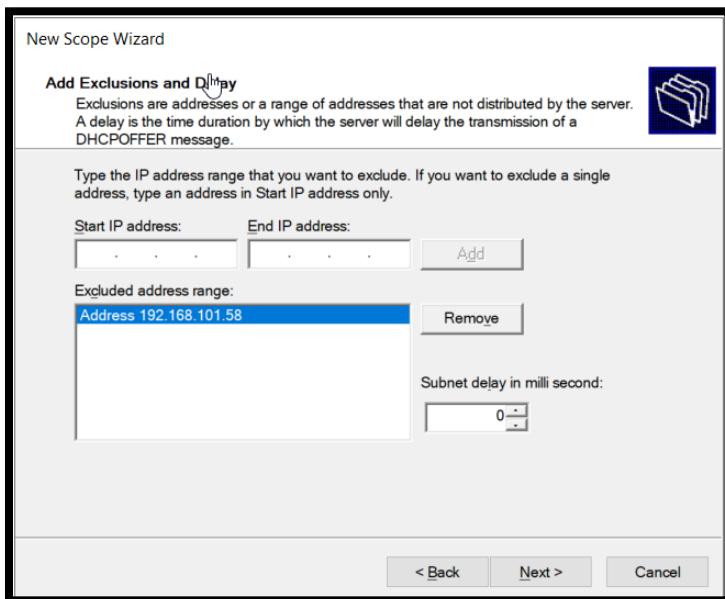
We hebben nu dus de adressen uitgekozen, dus daarmee gaan we snel verder. De range die we dus besloten hebben in te voeren is **192.168.101.21 tm 192.168.101.119**:



Het subnet laten we ongemoeid, het subnet mask past namelijk bij de gekozen range.

In de volgende stap kunnen we een eventuele uitsluiting invoeren. Stel dus dat we in ons netwerk een vaste printer hebben die we niet kunnen of willen aanpassen op IP **192.168.101.58**, dan geven we die hier op. Op die manier wordt hij uitgesloten van de DHCP-range en voorkom je problemen.

met een dubbel IP in je netwerk. Deze fictieve printer gaan we dus uitsluiten van de scope. Je voert het IP adres hier in en kiest voor **ADD**. Dit adres doet nu dus **niet meer mee in je scope**:



Technisch gezien kun je er dus óók voor kiezen om in je DHCP-range te kiezen voor 192.168.101.13 t/m 192.168.101.119 en daarna 192.168.101.13 t/m 192.168.101.20 uit te sluiten.

We kiezen voor **Next**, in dat scherm gaan we een heel belangrijke instelling doen. Namelijk de duur van de lease, ofwel; hoelang mogen de apparaten gebruik maken van de uitgedeelde adressen?

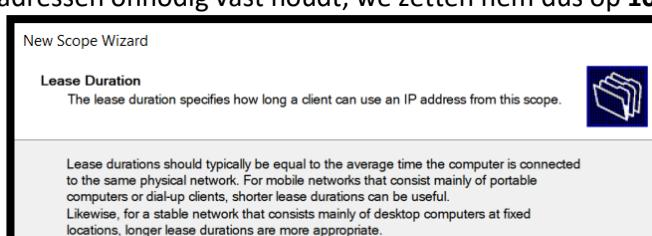
Microsoft heeft er ooit voor gekozen om de standaard leasetijd op **8-dagen** te zetten. Dit is een erg rare keuze geweest eigenlijk. Stel je namelijk eens voor dat er een werknemer is die 1x per week, dus om de 7-dagen, op de zaak komt om te werken. Dan betekend dat bij een leasetijd van 8-dagen dat deze persoon voor **áltijd zijn IP adres vast houdt**, totdat hij op vakantie gaat bijvoorbeeld en dan dus meer dan 8-dagen afwezig is. Op die manier gebeurt het natuurlijk al heel snel dat je geen bruikbare (lees: **vrije**) adressen meer kunt uitdelen, simpelweg omdat ze allemaal vast gehouden worden.

Deze leasetijd zetten we dus in de praktijk **nooit** op 8-dagen, maar vaak op zo'n **8 tot 12 uur**, een gemiddelde werkdag. Zet je hem op 10 uur, dan is het niet zo dat je netwerk verbroken wordt na deze tijd, maar ongeveer een half uur van te voren gaat je DHCP-server controleren of je nog aanwezig bent, zonder dat jij daar als gebruiker iets van merkt.

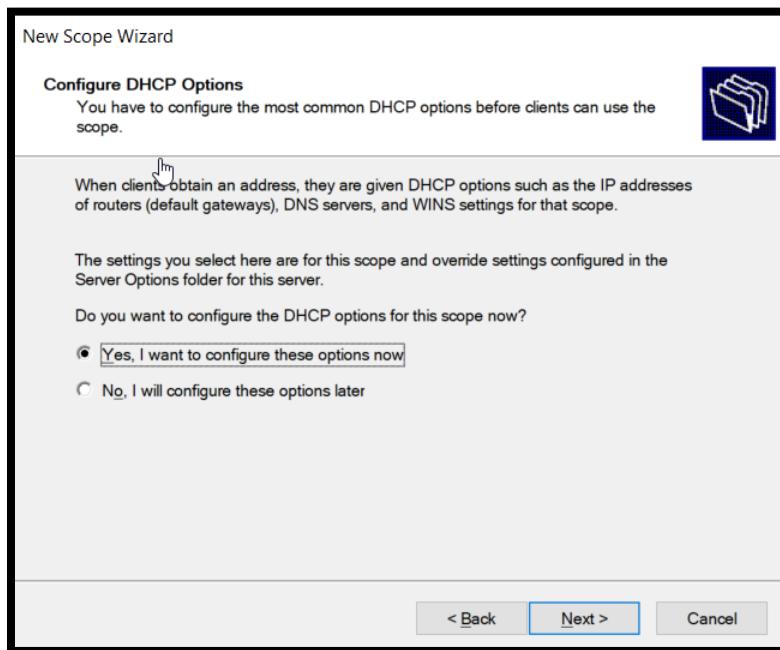
Hiervoor wordt het broadcastadres (***.*.*.255**) gebruikt, die roept op dat moment alle apparaten in het netwerk aan; krijgt hij reactie zet hij een 'vinkje' (denkbeeldig) en zo niet, dan weet hij dat je apparaat uit/weg is. Je kunt je voorstellen dat dit, als je deze tijd dus te kort instelt (laten we zeggen 2 minuten), je enorm veel en onnodig broadcast verkeer op het netwerk aanwezig is. Dit kan verzorgen voor vertraging of pakketten die niet goed of niet op tijd aankomen.

Is je apparaat nog aanwezig, dus reageert hij, dan wordt je adres verlengd met weer 10 uur. Ben je (al) weg, dan wordt het adres vrijgegeven en kan een ander 'dynamische host' dat IP-adres weer krijgen via de scope.

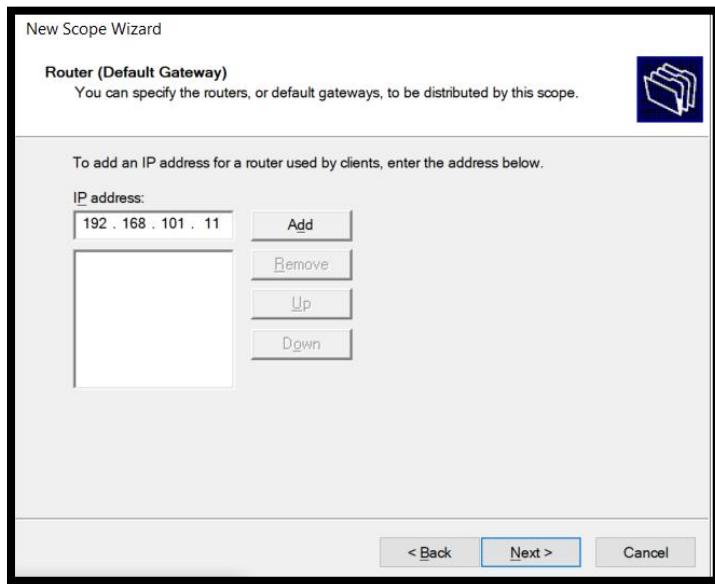
Op die manier heeft men er overdag geen last van, maar voorkom je dat je op den duur al je adressen onnodig vast houdt, we zetten hem dus op **10 uur**.



In de volgende stap gaan we de reeds eerder besproken opties toevoegen aan de scope, we gaan hier de router/default gateway (de weg naar ‘buiten’ dus) instellen en we geven aan welke DNS-servers er uitgedeeld moeten worden. We kiezen dus voor **Yes, I want....**

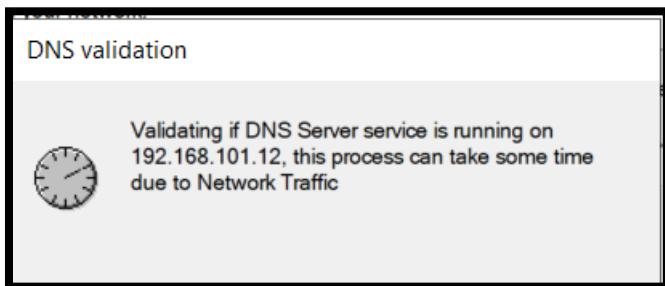


Om te beginnen moeten we de **Router** opgeven. De router hebben we natuurlijk reeds op de AD01 geïnstalleerd en dus geven we aan dat dit dan ook onze router is. Vergeet hierbij niet om op **Add** te drukken voordat je op **Next** klikt, anders voegt hij hem niet daadwerkelijk toe.

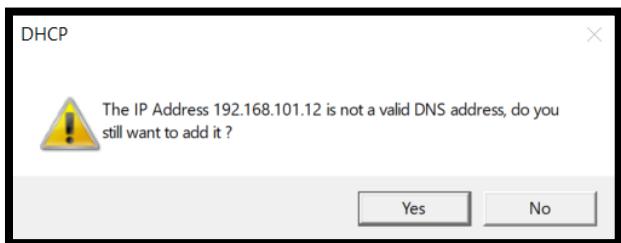


In de volgende stap zorg je ervoor dat de DNS-gegevens allemaal kloppen die je mee wilt geven. Standaard voert de wizard hier al wat gevonden gegevens in. Zorg ervoor dat je van beide servers de IP-adressen hiervan invoert en dat de naam klopt met je domeinnaam.

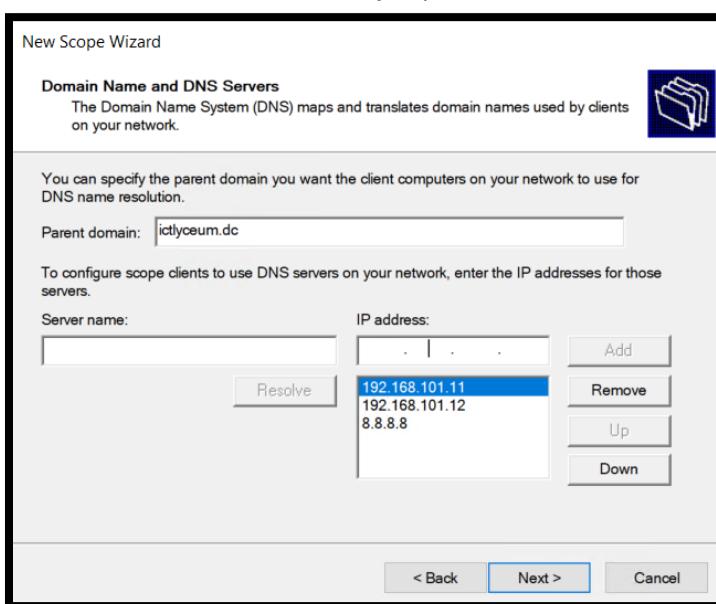
Mocht er hier nu maar 1 IP-adres staan, voer dan handmatig even je tweede (server) in. Wanneer je overigens handmatig een DNS-server toevoegt, dan checkt de server **altijd** even of dit daadwerkelijk ook een DNS-server is:



Mocht dit namelijk dan niet zo zijn krijg je hier een waarschuwing van. Mocht je dan namelijk een typefout hebben gemaakt kun je dit tijdelijke herstellen, maar het kan ook zijn dat deze server bijvoorbeeld tijdelijk uit staat. Op dat moment kun je er gewoon voor kiezen om toch dit adres te gebruiken.

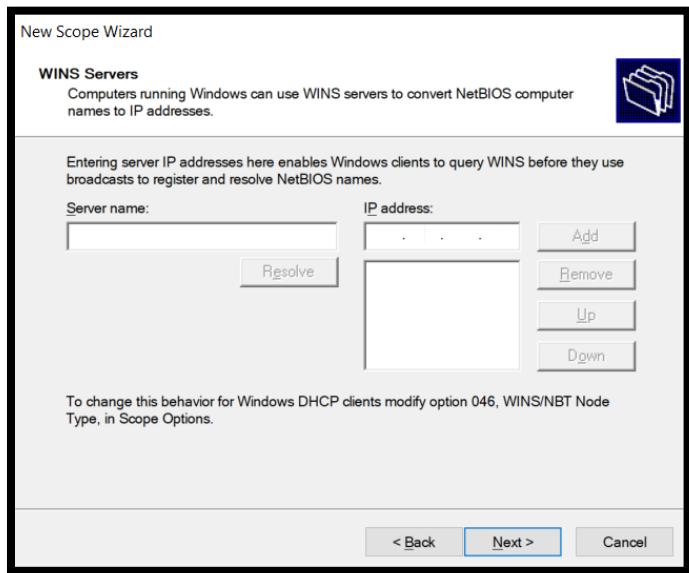


Uiteindelijk moeten in deze stap de adressen **192.168.101.11**, **192.168.101.12** én (voor de zekerheid) **8.8.8.8** komen te staan vóórdat je op **Next** drukt.

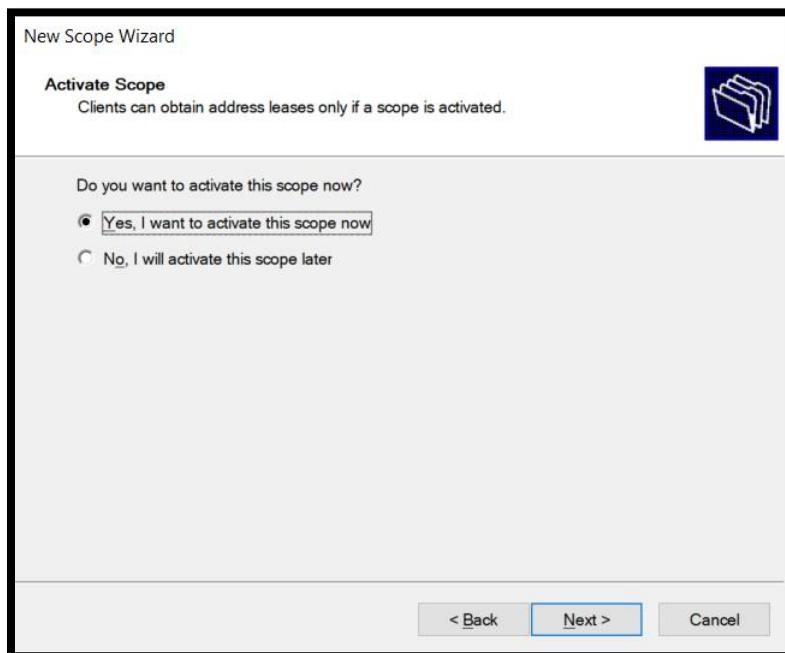


Wanneer dit allemaal klopt kies je voor **Next** en dan komen we bij de laatste configuratiestap, de **WINS** servers. WINS is een heel oud protocol (*pré-2000*) welke NETBIOS-namen om kan zetten in IP-adressen.

Echter gebruiken we dit protocol niet meer in de nieuwere omgeving en dus zorgen we dat deze opties **geheel leeg** zijn voordat we weer **Next** drukken:

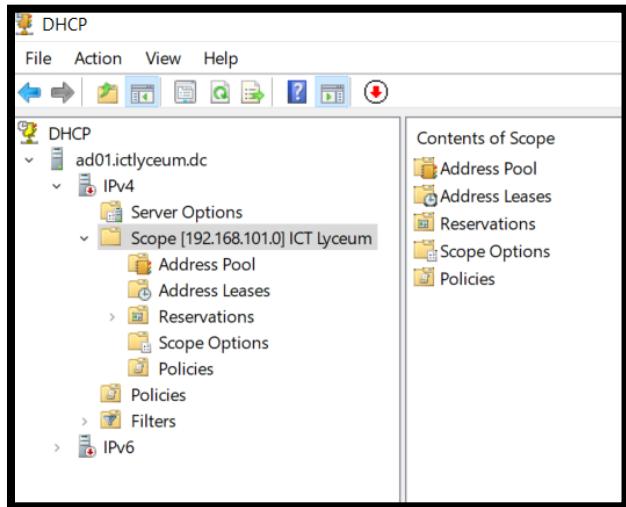


Vervolgens zijn we aangekomen bij de laatste stap van de DHCP-scope; Willen we de scope activeren of niet. In deze omgeving willen we dat graag. Het kan natuurlijk voorkomen dat je in een bestaande omgeving mét reeds een DHCP-server, een nieuwe DHCP-server aan het configureren bent en dat je uiteindelijk wilt switchen. Op zo'n moment zet je hem nog niet actief, maar nu doen we dat zoals gezegd wel.



Je kiest voor een laatste keer voor **Next** en daarna voor **Finish**. Je scope staat nu helemaal klaar voor gebruik.

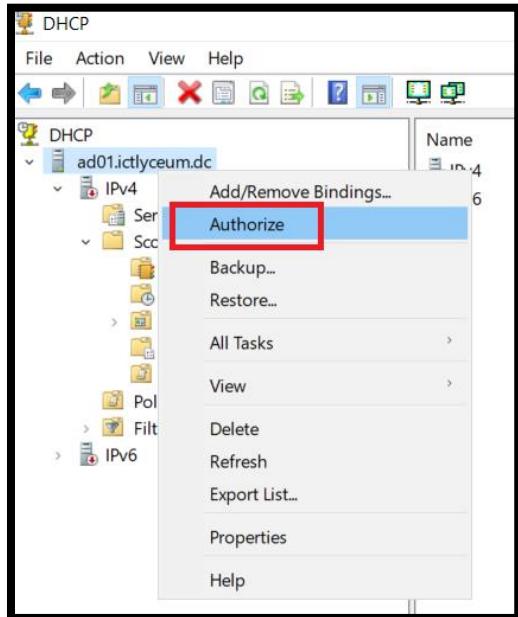
Hij is echter nog steeds down (rode pijl naar beneden), dus hij doet het op dit moment nog niet.



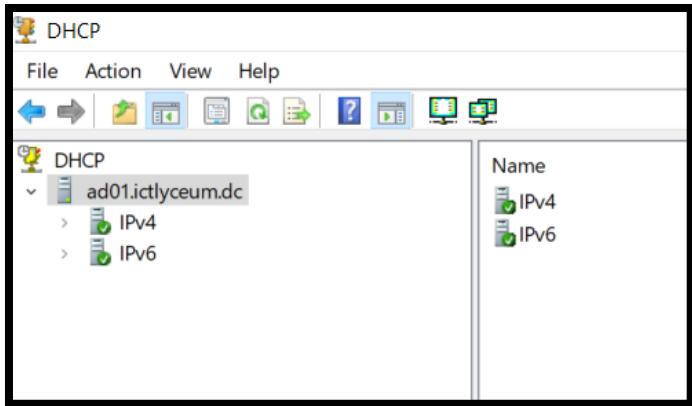
Dit komt omdat we eerst nog moeten 'toe staan' dat deze server daadwerkelijk DHCP mag uitdelen over ons domein. Dit kan alleen gedaan worden door een domein beheerder. Gelukkig zijn wij nog altijd ingelogd als **ictlyceum\administrator**, dus mogen we dit zelf uitvoeren op dit moment.

In sommige andere omgevingen heb je wellicht minder rechten en moet dit dus gedaan worden door iemand met meer rechten op dat moment, wellicht je leidinggevende bijvoorbeeld.

Maar omdat wij dit dus nu wél mogen, klikken we met de rechter muisknop op de **ad01.ictlyceum.dc** bovenin, onder het kopje DHCP en dan kiezen we voor **Authorize**;



Wanneer je dit gedaan hebt, vernieuw je deze MMC-omgeving (**Action -> refresh** of de refresh knop onder het woordje **Help**) en dan moet alles er netjes **up** en dus **groen** uit zien zoals dit:



Ook je DHCP-scope is nu alweer helemaal klaar én actief!

Je kunt nu even rustig de mappen bij langs lopen om te controleren of alles klopt.

Hier zien we bijvoorbeeld onze 'pool', ofwel de range van adressen, waarbij je ziet dat **192.168.101.58** is uitgesloten van de pool:

A screenshot of the Windows DHCP Management console. The left pane shows the 'IPv4' scope under 'ad01.ictlyceum.dc'. The right pane displays a table with three columns: 'Start IP Address' (192.168.101.21), 'End IP Address' (192.168.101.119), and 'Description' (Address range for distribution). Below this, another row shows '192.168.101.58' with a red crossed-out icon, labeled 'IP Addresses excluded from distribution'.

Bij het mapje **Address Leases** staat nu niets, maar zodra we daadwerkelijk IP-adressen hebben uitgedeeld dan zullen we deze hier gaan vinden incl. de bijhorende machine-/hostnaam.

A screenshot of the Windows DHCP Management console. The left pane shows the 'IPv4' scope under 'ad01.ictlyceum.dc'. The right pane is a table titled 'Address Leases' with columns: 'Client IP Address', 'Name', 'Lease Expiration', 'Type', and 'Unique ID'. A message at the top right says 'There are no items to show in this view.'

Opruimen van snapshots?

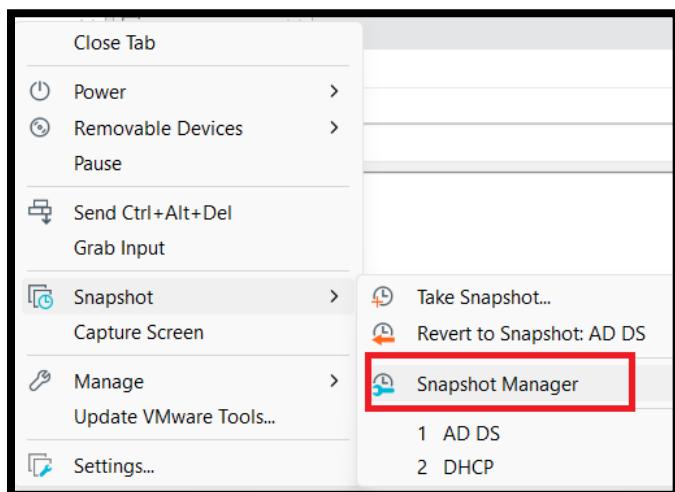
We kunnen er weer voor kiezen om een snapshot te maken, maar omdat we er inmiddels al een paar hebben wordt de omgeving hier steeds een stukje langzamer van. Dát is zo n moment waarop je moet gaan kiezen; vertrouw ik het en gooi ik mijn vorige versies weg, want alles is goed blijven draaien óf bewaar ik ze toch nog even voor de zekerheid?

Die keuze moet je altijd zelf goed beoordelen en vooraf natuurlijk even uitgebreid testen of alles daadwerkelijk nog werkt zoals het zou moeten.

In deze omgeving hebben we steeds doorgewerkt dus als het goed is, kunnen we probleemloos de snapshots verwijderen en daarna direct een nieuwe gaan maken. Zo kunnen we niet meer heel ver terug, maar kunnen we wél terug naar **dit** specifieke moment, waarop dus alles (nog) goed werkt.

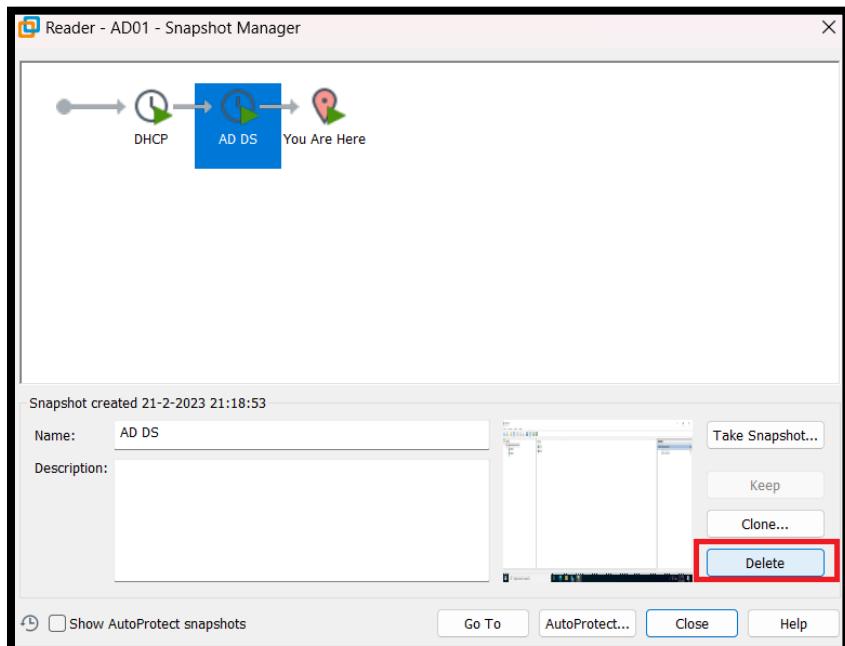
Omdat we onze servers als Domain Controllers hebben gekoppeld, is het belangrijk om van beide servers zo n beetje op hetzelfde moment een nieuwe snapshot te maken om eventuele problemen te voorkomen. Het is niet gezegd dat het altijd voor problemen zorgt, maar we nemen het zekere voor het onzekere.

Om de oude snapshots weg te gooien, klikken we met de rechtermuisknop op onze VM en kiezen we voor **Snapshot -> Snapshot Manager**.



Via de Snapshot manager kun je eenvoudig terug gaan naar een vorig punt, maar we kunnen hem dus ook gebruiken om al onze herstel punten te gaan verwijderen.

Dit doen we eenvoudig door een oude versie te selecteren en te kiezen voor **Delete**.



Nadat ze allemaal weg zijn, maken we even een nieuwe snapshot, dan kunnen we weer rustig verder werken en hebben we toch de zekerheid van een goed herstelpunt wanneer het mis gaat tijdens een stap.

Doe hetzelfde bij de AD02 om dus zoals gezegd problemen te voorkomen wanneer je onverwachts terug moet naar een moment.

Installatie en configuratie DHCP op AD02

We gaan de vorige stappen, dus het installeren van de Role DHCP en het configureren van de DHCP-range nogmaals doen, maar dit keer op de server AD02. Dit wordt zoals eerder al beschreven ook een DHCP-server voor ons netwerk.

De stappen zijn vrijwel gelijk, echter moeten we alleen de IP-range wat gaan aanpassen zodat deze server zonder problemen kan meehelpen of kan overnemen.

Je stelt op de AD02 het volgende in:

Scope-naam: **ICT Lyceum**

IP-range: **192.168.101.120 t/m 192.168.101.219**

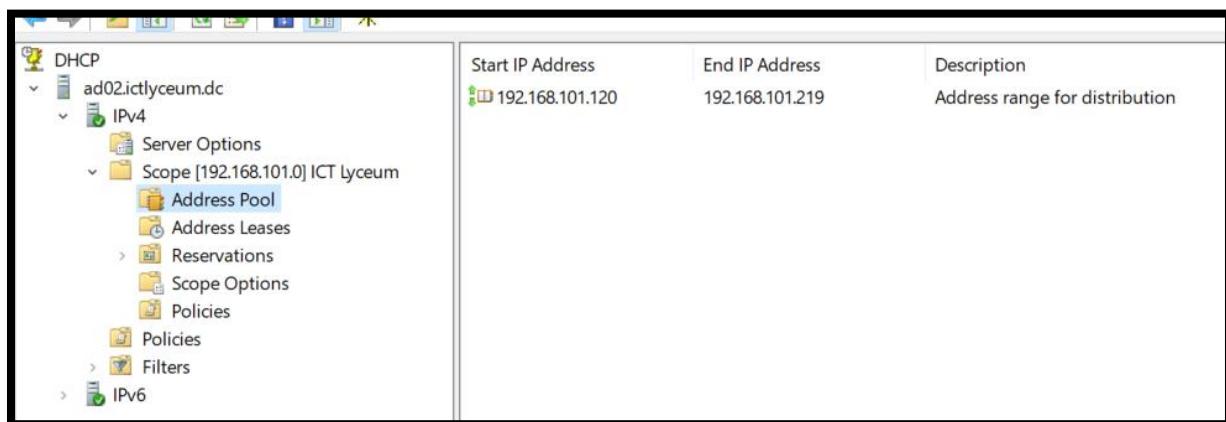
Exclusion: **LEEG (de printer, 192.168.101.58 , valt namelijk al buiten deze range)**

Router: **192.168.101.11**

DNS-servers: **192.168.101.11 en 192.168.101.12**

WINS: **LEEG**

Vervolgens activeer je de scope én zorg je ervoor dat de AD02 óók geautoriseerd is om DHCP uit te mogen delen. Je zult dan zien deze ook deze groen (**up**) is na je configuratie. Controleer ook bij deze server even of alles klopt zoals je het hebt ingesteld door de mapjes bij langs te lopen.



Nu we een redundante (dus dubbel uitgevoerde) AD DS én DHCP-server hebben klaar gemaakt, is het tijd om te gaan testen of alles eigenlijk wel écht werkt. Dit gaan we doen door een workstation/client te installeren en toe te voegen aan ons **ICTLYCEUM.DC** domein.

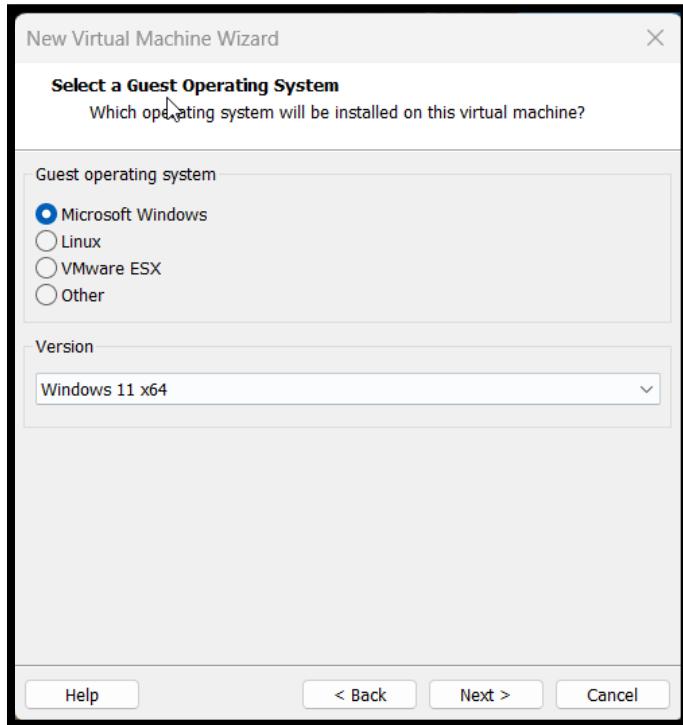
Wat hiervoor erg belangrijk is, is dat deze installatie van de client nooit een **HOME**-versie mag zijn, maar minimaal een **Windows Professional** versie, ofwel de zakelijke versie. De **HOME**-versie kan namelijk simpelweg niet worden gekoppeld aan een domein aangezien die optie is uitgeschakeld.

De volgende versies kunnen wel gekoppeld worden:

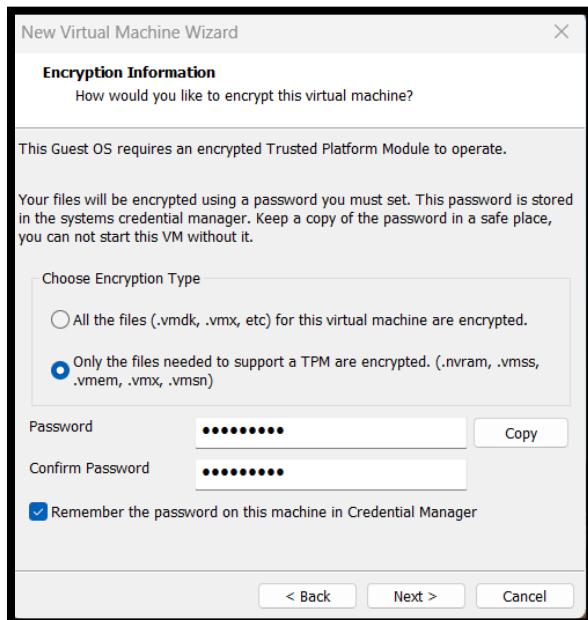
- Windows **Pro**
- Windows **Education**
- Windows **Enterprise**

Denk hier dus altijd bij na tijdens bijvoorbeeld de installatie óf aanschaf van een zakelijke laptop/computer.

Configuratie en installatie Windows Client



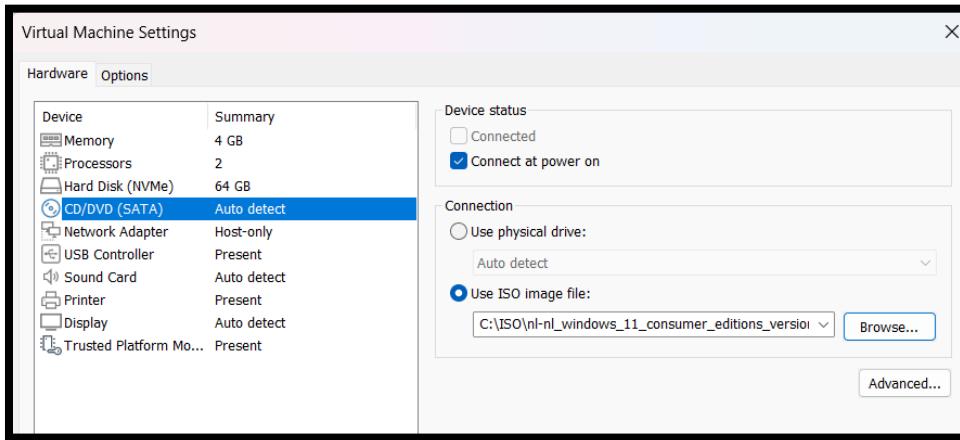
Om encryptie, welke nodig is om Windows 11 te kunnen installeren, in te schakelen is een wachtwoord benodigd. Deze stel je eenvoudig in wanneer je de **New Virtual Machine Wizard** opstart. Je kunt gewoon de default-settings behouden, als wachtwoord gebruiken we wederom **Welkom01!**



Onder settings. zetten we de netwerkadapter op **Host-Only**. Dit is noodzakelijk omdat we straks natuurlijk willen dat onze client (de Windows 11 machine) gekoppeld kan worden met ons domein via de Windows Servers.

De CD/DVD - **ISO** verwijst uiteraard naar de Windows 11 ISO.

Wanneer je dit allemaal juist hebt ingesteld zou dit er ongeveer zo moeten uit zien



DHCP binnen VMware Workstation Pro

Deze client VM heb je voor dit moment helemaal goed staan, dus die zouden we kunnen gebruiken. Het is alleen zo dat we nog één heel belangrijke wijziging moeten uitvoeren binnen VMware zelf, voordat we écht aan de slag kunnen met deze client.

VMware heeft namelijk een ingebouwde DHCP-server geconfigureerd binnen VMware Workstation Pro, welke standaard aan staat voor alle netwerken (dus Host-Only, NAT, Bridged etc.).

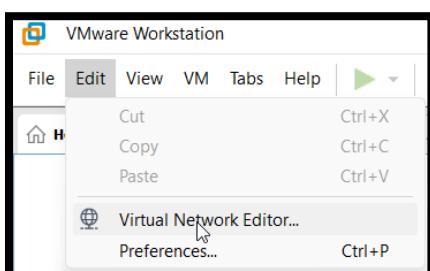
Dit is nodig omdat je anders bijvoorbeeld op je kaal geïnstalleerd machine nooit een werkende internetverbinding gaat krijgen, simpelweg doordat je geen IP-instellingen toegewezen krijgt, op natuurlijk APIPA na (169.254.*.*).

Eigenlijk een heel mooi en goed bedacht systeem dus. Het is echter zo dat Microsoft Server met DHCP het niet fijn vindt wanneer er meerdere verschillende (dus niet Microsoft versies laten we maar zeggen) DHCP-servers draaien binnen een netwerk. Dit is natuurlijk omdat je anders mogelijk verschillende netwerken/IP-ranges door elkaar heen gaan sturen in een netwerk, je kunt je voorstellen dat dat niet wenselijk is.

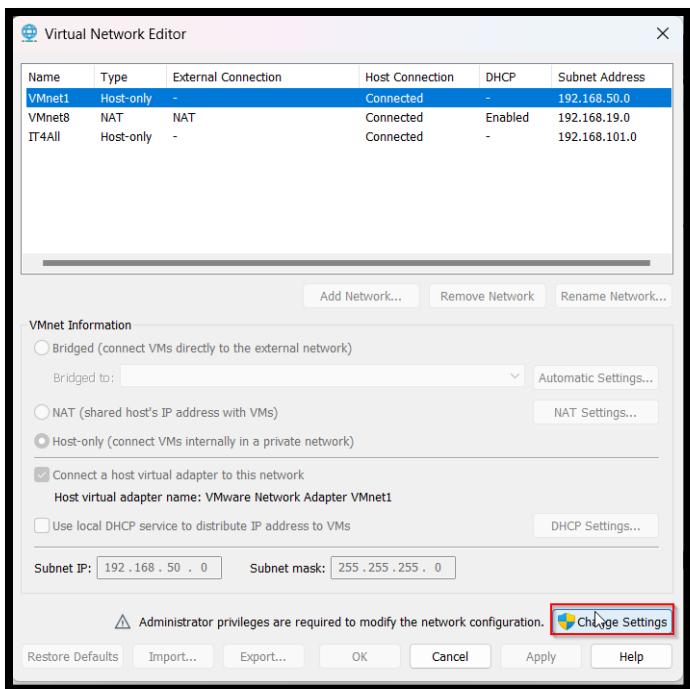
Omdat er dus blijkbaar vanuit VMware Workstation Pro óók al een DHCP-server draait in het Host-Only netwerk, schakelt Microsoft zijn DHCP-servers uit om te voorkomen dat dit bovenstaande dus gebeurt. Mocht je dan je Windows Client opstarten, krijg je geen IP-adres van een van de zojuist configurerde DHCP-servers, maar van VMware zelf. En de kans dat die IP-range overeenkomt met de door ons geconfigureerde adressen is uiteraard zeer klein..

We moet er dus voor zorgen dat we de DHCP in VMware Workstation Pro, op de Host-Only adapter, gaan uitschakelen.

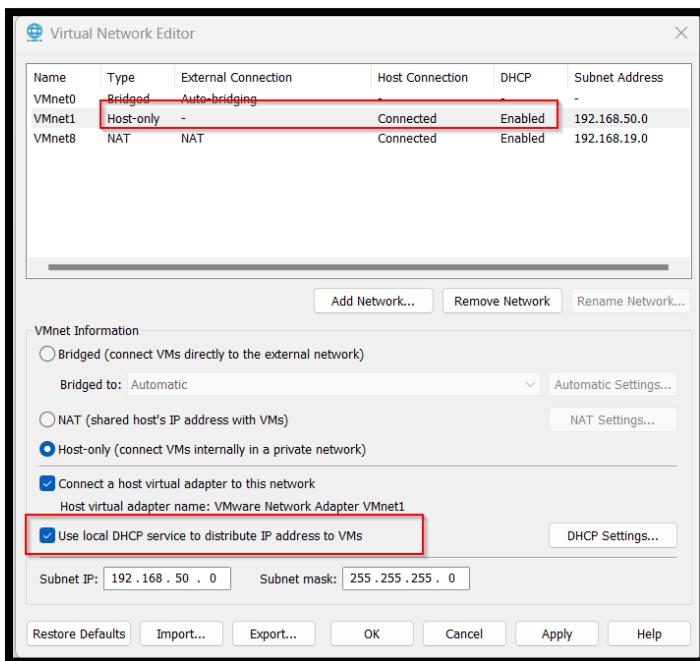
Open VMware Workstation Pro en kies links bovenaan voor **Edit -> Virtual Network Editor..**



Vervolgens kiezen we in de Virtual Network Editor **rechts** onderaan voor **Change Settings**



In de pop-up die dan verschijnt zie je achter de **Host-Only** adapter die wij gebruiken voor onze machines staan dat DHCP op **Enabled** staat.



Zoals gezegd moet deze voor de Host-Only adapter **NIET** zijn ingeschakeld, dus we zetten links onderin het vinkje uit. Let hier wel goed op, dat je er zeker van bent dat je eerst de Host-Only adapter selecteert bovenin het scherm en **dán** past het vinkje uitschakelt. Op de NAT-adapter moet deze functie namelijk weer **wél** ingeschakeld blijven, anders heb je geen internet op de AD01 (omdat we hierop zoals je weet een tweede netwerkadapter hebt ingesteld die op NAT staat!).

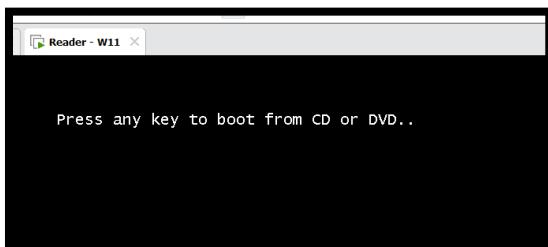
Installatie Windows 11

Nu de instellingen in VMware goed staan gaan we beginnen met de daadwerkelijke installatie van Windows 11, we noemen dit ook wel de Client installatie.

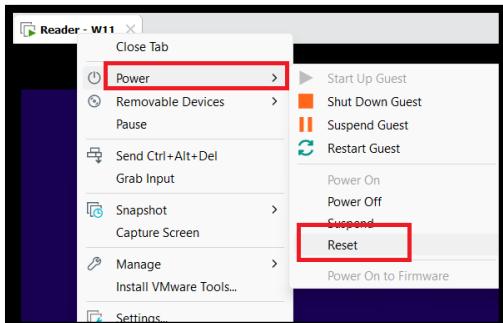
We zetten deze aangemaakte VM aan en zorgen dat we de het VMware scherm activeren door er met de muis direct in te klikken. Op het moment dat er gevraagd wordt om op een willekeurige knop te drukken, druk je op de spatie. De installatie zal dan beginnen.

In deze omgeving installeren we de client bewust in het Nederlands, aangezien dit in de praktijk ook vaak zo is. De servers waarop wij als IT specialisten werken zijn altijd in het Engels, maar onze collega's en klanten werken gewoon op een 'normaal' besturingssysteem en dus is die (vaak) in het Nederlands.

De installatie is vrijwel identiek aan de installatie van Windows Server.



Mocht je te laat zijn, druk je even op **ctrl+alt** (tegelijk) zodat je los komt uit deze console-sessie en reset je de machine even zodat je het nogmaals kunt proberen.

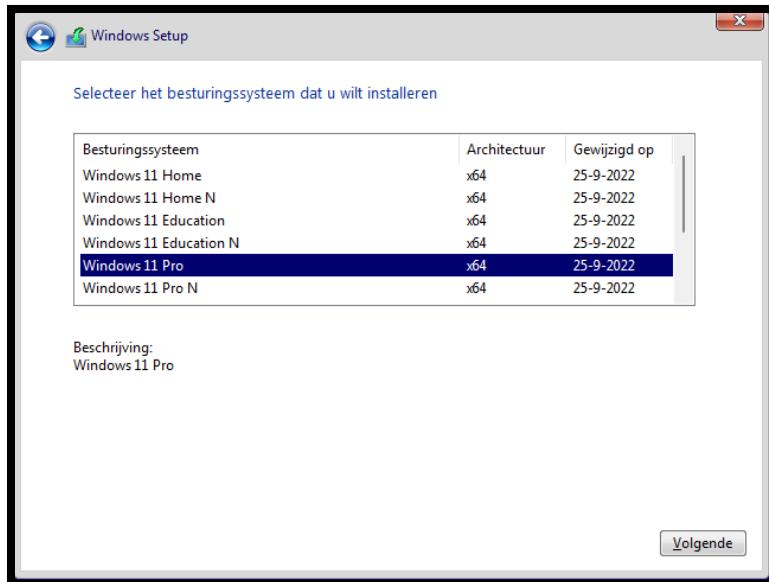


Wanneer hij uiteindelijk doorgaat met de installatie, kies je de gewenste taal en ga je door naar de volgende stap gevuld door **Nu Installeren**.



Omdat we ook bij de clientinstallatie geen gebruik maken van de licentiecode, kiezen we ook hier logischerwijs voor ‘Ik heb geen productcode’, net als bij de installatie van de servers dus eigenlijk.

Bij de installatie kiezen we, zoals reeds eerder uitgelegd, voor een Windows versie met Pro óf Education er achter en daarna kiezen we voor **Volgende**. Zoals je ziet is de Enterprise versie is op deze ISO niet aanwezig.

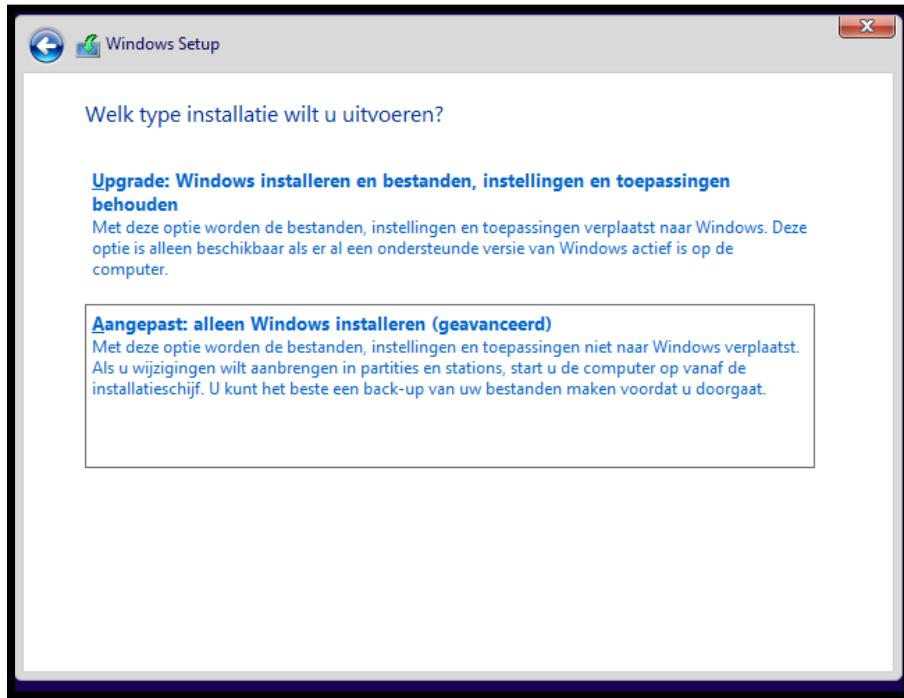


We gaan uiteraard akkoord met de licentievoorwaarden, anders kunnen we niet verder

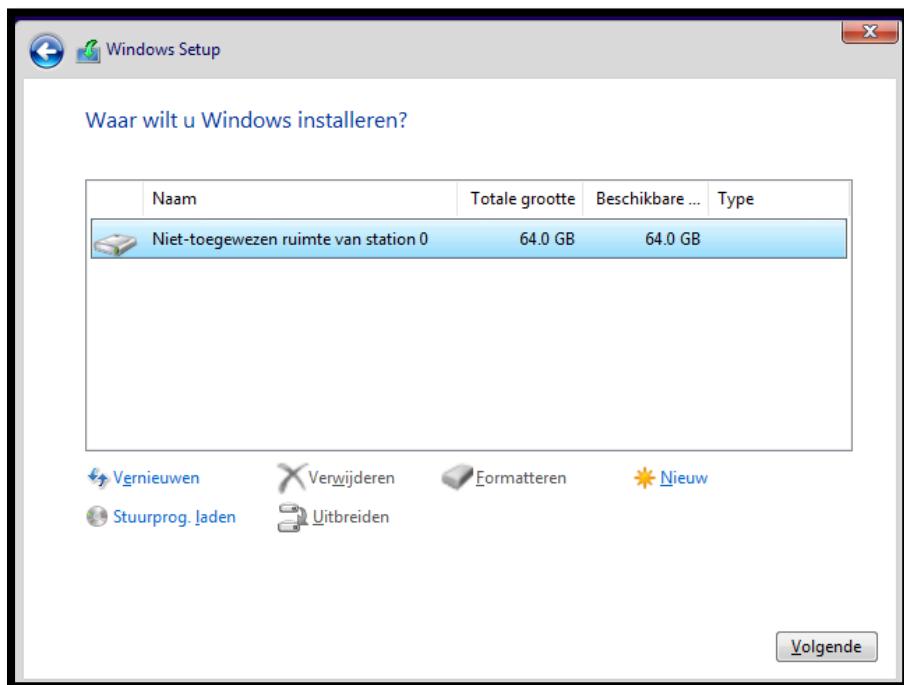


En daarna kies je eigenlijk **altijd** voor de **Aangepaste** installatie. Bij deze client-installatie is het namelijk net zoals bij de installatie van de Windows Server-versies; er is geen vorige versie dus

kunnen we simpelweg niet voor Upgrade kiezen.



We hebben in de laatste stap slechts één harddisk, dus hoeven we hierbij geen keuze te maken en kiezen ervoor om de installatie te gaan beginnen door op Volgende te drukken.



Nadat de installatie voltooid is, moeten we nog wat basisinstellingen goed zetten. De wizard doorloopt deze met je zodat je voor jezelf de beste keuzes kunt maken.

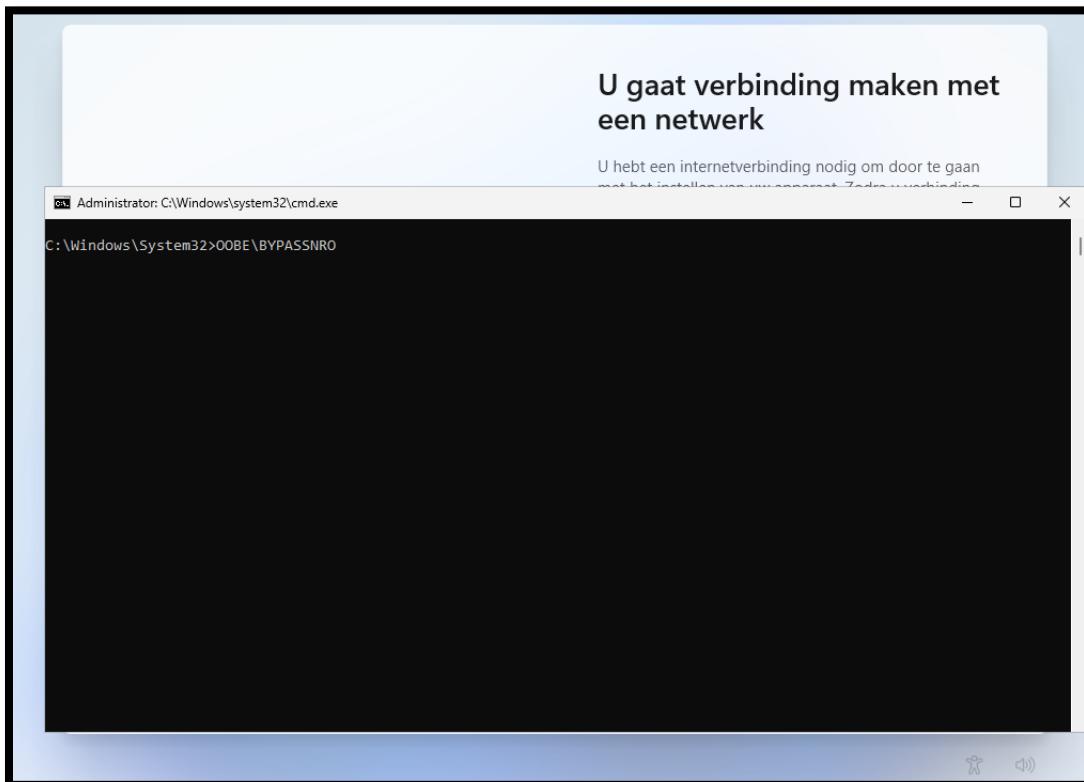
Uiteindelijk kom je op een punt dat je een gebruiker moet toevoegen aan de Azure-cloud van Microsoft. Uiteraard willen ze graag dat je hier inlogt met een Microsoft account en is het verplicht om een internetverbinding te hebben. Om deze reden hebben wij sowieso natuurlijk onze machine

reeds op Host-Only gezet, maar alsnog gaat de configuratie niet verder totdat je een internetverbinding regelt volgens de wizard.

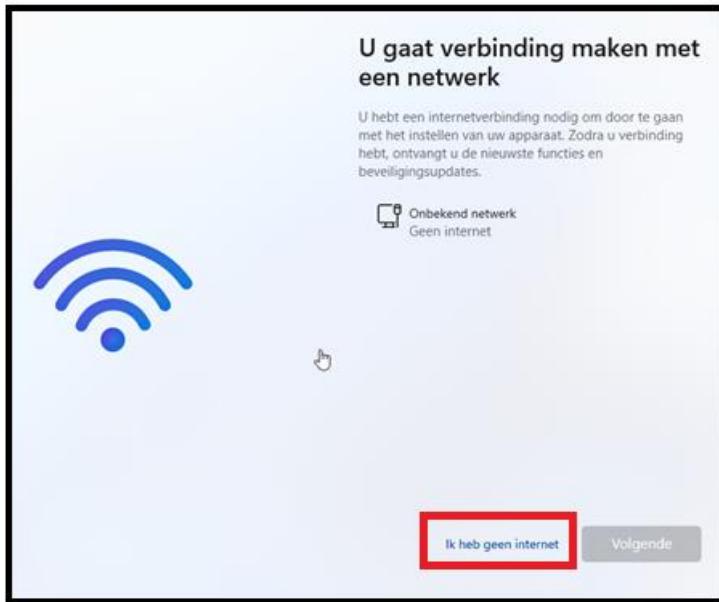
Je ziet dan deze melding en je kunt dus daadwerkelijk niet op Volgende klikken.



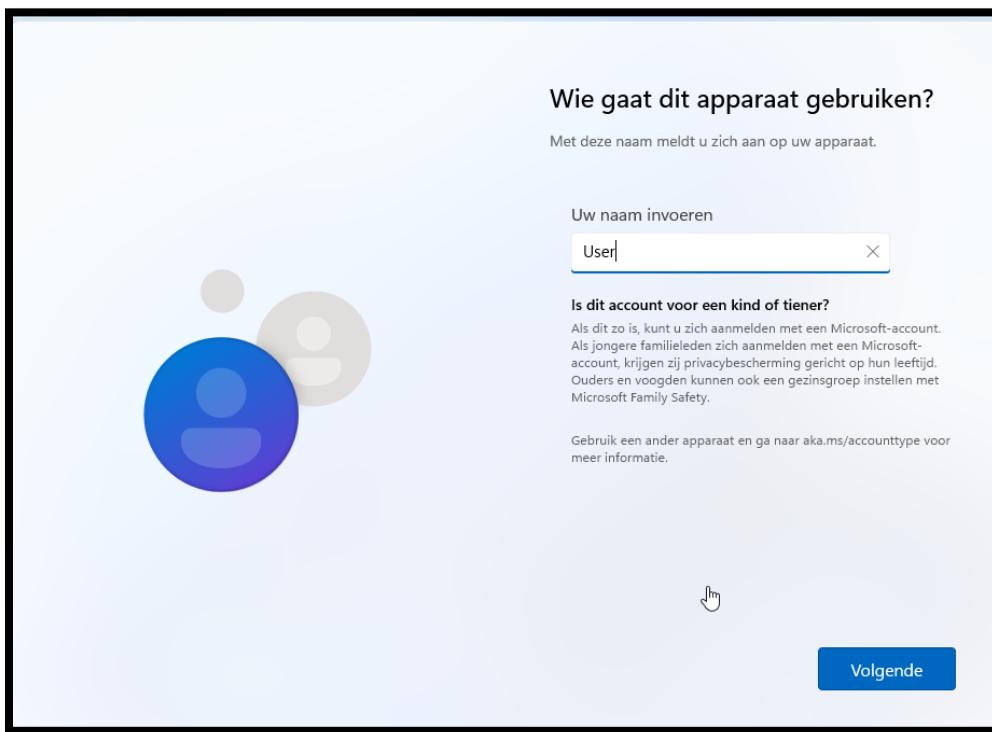
Om verder te kunnen komen zónder internet, gaan we via de command-prompt een commando uitvoeren welke ervoor zorgt dat we toch kunnen gaan inloggen met een lokaal account. We starten hiermee door de **Shift-toets** in te houden en te drukken op **F10** (eventueel **Fn + F10** wanneer nodig). De command-prompt komt dan naar voren. Hierin typen wij: **OOBE\BYPASSNRO** gevuld door **ENTER** (OOBE = Out-Of-the-Box-Experience).



De client wordt dan herstart, in dus de Out-Of-the-Box-Experience, waarbij we wél een lokaal account mogen aanmaken. Je doorloopt dan nogmaals de wizard (taalinstellingen etc) maar nu zal je zien dat je een extra optie erbij hebt gekregen waarmee je aan kunt geven geen toegang tot internet te hebben.



Vervolgens ga je verder met een, volgens Microsoft, 'beperkte installatie' en daarna kun je een lokale gebruiker aan gaan maken voor deze machine. Deze user heeft **geen** wachtwoord nodig.



Je doorloopt dan nog enkele stappen (waar je overigens bijna **Nee** kunt kiezen) en wanneer hij dan uiteindelijk klaar is met de configuratie, moet hij vrijwel direct een IP-adres krijgen van één van onze DHCP-servers. Zorg er dus wel voor dat deze (beide) aan staan en zijn opgestart.

Je merkt in principe meteen of dit goed gegaan is, wanneer je met je muis op het netwerkicoon rechts onderin gaat staan (niet klikken) en dan moet je ons domein zien staan + mogelijk internettoegang. Dit internet krijgt hij natuurlijk via de AD01, Routing and Remote Access.



Als je dit daadwerkelijk ziet, dan weet je dat je DHCP-server goed is ingesteld en dus functioneert.

Toch gaan we voor de zekerheid even kijken via de command-prompt (CMD) of je daadwerkelijk een adres hebt ontvangen van je eigen gemaakte DHCP-servers én uiteraard welke van de twee jou heeft voorzien van de benodigde gegevens.

We drukken hiervoor even met de rechter muisknop op de **Windows-knop** en kiezen voor **Uitvoeren** -> **CMD <enter>**.



In de command-prompt voeren we: **ipconfig /all <enter>** uit en we bekijken de gegevens.

In volgende afbeelding zien we netjes een van de adressen die wij hebben geconfigureerd én bij DHCP-server zie je ook direct van welke server (het IP van de AD01 of AD02) jouw machine heeft voorzien van dit adres.

```
C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-LF6IJQV
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ictlyceum.dc

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : ictlyceum.dc
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-5C-4C-D0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::bcfd:857e%1005:f24e%3(PREFERRED)
IPv4 Address. . . . . : 192.168.101.21(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : vrijdag 24 februari 2023 12:57:27
Lease Expires . . . . . : vrijdag 24 februari 2023 22:57:27
Default Gateway . . . . . : 192.168.101.11
DHCP Server . . . . . : 192.168.101.11
DHCPv6 IAID . . . . . : 100660409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-8A-4C-0F-00-0C-29-5C-4C-D0
DNS Servers . . . . . : 192.168.101.11
                                         192.168.101.12
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth-netwerkverbinding:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 84-7B-57-0A-A3-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

C:\Users\User>
```

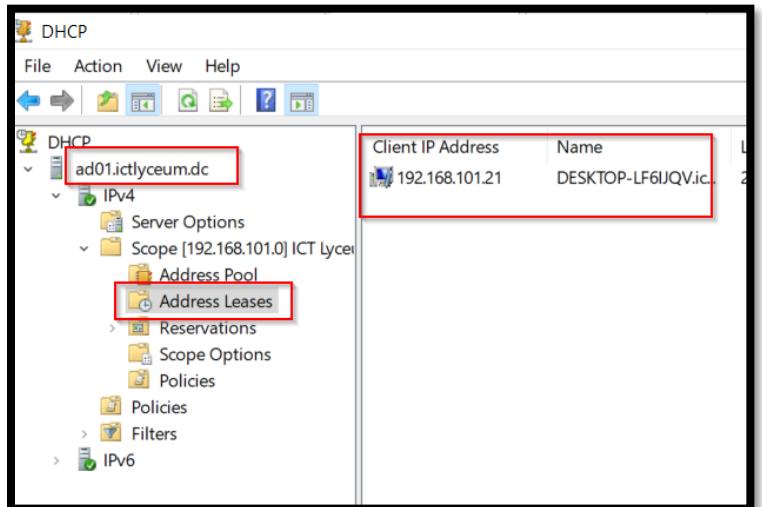
Zoals je ziet is dit het eerste IP-adres wat wij in de lease hebben aangegeven. Bij de AD01 was dit **192.168.101.21** en bij de AD02 was dit **192.168.101.120**

In dit voorbeeld, heb ik een IP-adres gekregen van de AD01 en heb ik dus inderdaad 192.168.101.21 ontvangen.

Mocht je hier nu een heel ander adres zien dan die we hebben ingesteld binnen de DHCP-scope, dan is er mogelijk iets niet goed gegaan met het uitschakelen van DHCP binnen VMware Workstation óf heb je de netwerkadapter niet op **Host-Only** staan. Controleer die twee dan even goed door even een paar stappen terug te gaan in de reader.

Als je wel een goed adres hebt, controleren ook gelijk even op de server **AD01** (en wanneer er bij jou in het overzicht “**DHCP Server – 192.168.101.12**” staat kijk je op server **AD02** natuurlijk), onder **Tools** -> **DHCP** omdat we namelijk hier óók kunnen zien welke lease er bij welke machine hoort.

Dit bekijken we onder het tabblad Address Leases



Zoals hier te zien, matched dit met de lease uit de **ipconfig /all** op de client.

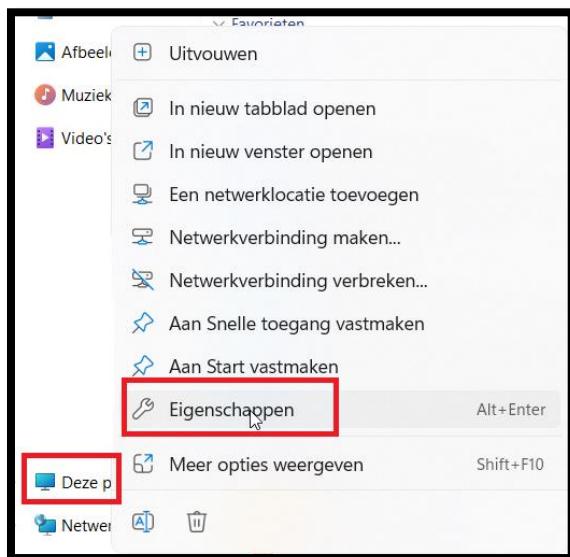
Tevens valt hier op dat de **Name** wel erg raar is, dat komt uiteraard doordat deze nog niet is gewijzigd. Dit moet uiteraard wel gebeuren, want anders kun je later nooit herleiden welke naam nu bij welk workstation hoort.

Wijzigen van computernaam en koppelen aan het domein

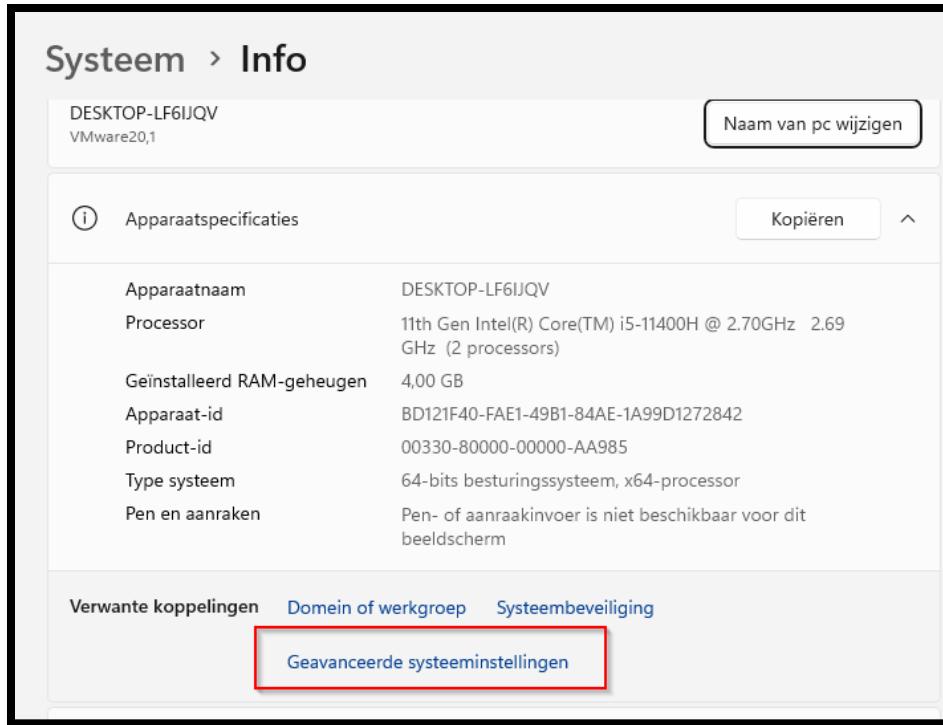
Je gaat nu dus de naam wijzigen van de client naar **WS01** (werkstation 01) en tegelijkertijd hang je dan de client in het domein. Je hebt dit eerder gedaan op de server **AD02** en die stap is vrijwel identiek.

Het grote verschil is natuurlijk wel, dat er in een Windows client versie geen Server Manager aanwezig is waar je even op de naam kunt klikken om deze te wijzigen.

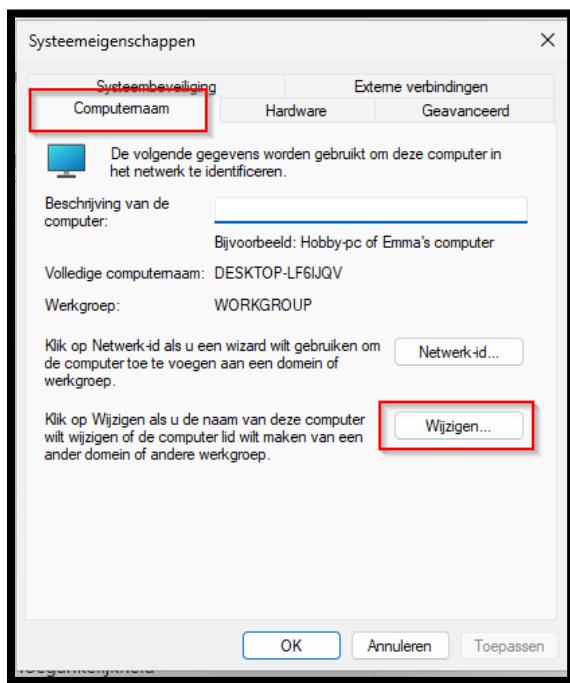
De kortste klap om dit te doen in een client, is door de verkenner te openen (het gele mapje aanklikken dus) en met de rechter muisknop op **Deze PC** te drukken en te kiezen voor Eigenschappen.



Vervolgens kies je in het **Instellingen** scherm voor **Geavanceerde systeemininstellingen**

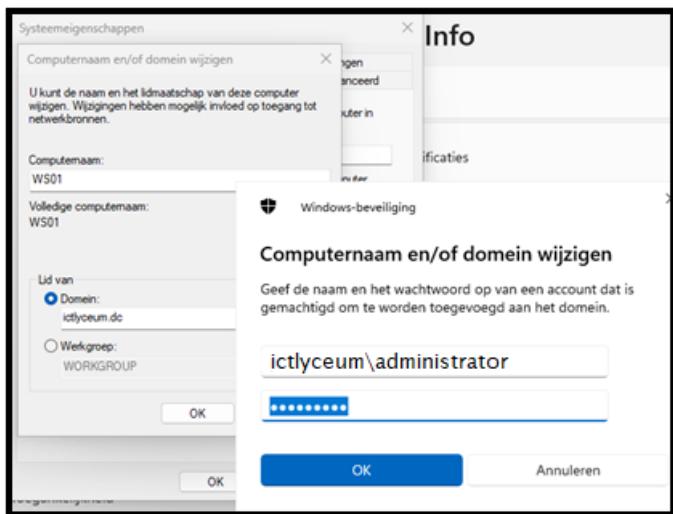


In deze pop-up die je nu te zien krijgt, kies je het tabblad **Computernaam**, daar kies je voor **Wijzigen** en dan kun je daar de naam wijzigen en tegelijkertijd aangeven dat je hem graag aan een domein wilt koppelen.

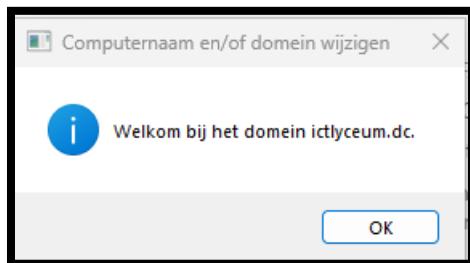


Dit tabblad, **Computernaam** moet je bekend voorkomen. Die is namelijk gelijk als bij het wijzigen van de namen van de servers.

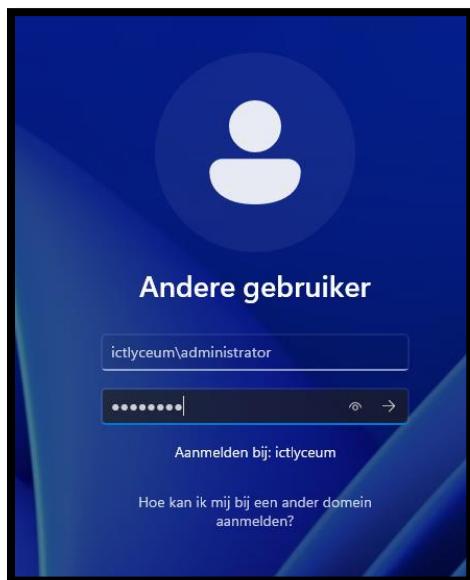
Als je alles juist hebt ingevoerd\gewijzigd, zal je de pop-up zien waarin je de 'credentials' dient op te geven van het domein, net als bij AD02 is dit dus **ictlyceum\administrator + Welkom01!**



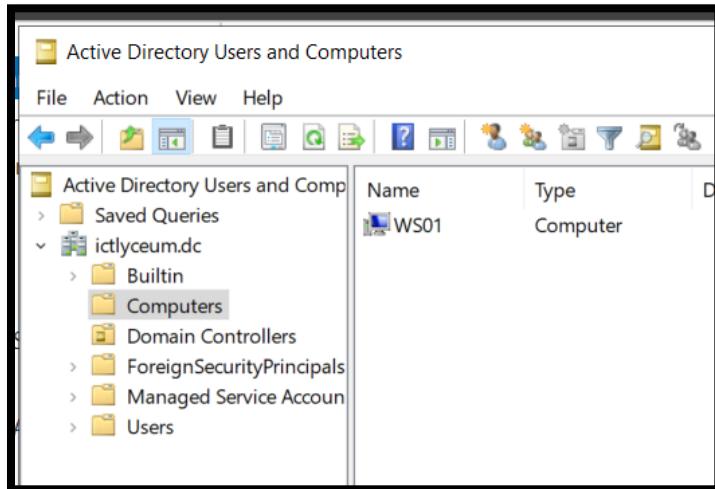
Wanneer dit allemaal in orde is, zie je de reeds bekende welkomstbericht



Herstart nu de client en zorg dat je inlogt op het domein ICTLYCEUM als Administrator (dus als **ictlyceum\administrator**). Wanneer je namelijk als die gebruiker ingelogd bent op de client, heb je feitelijk alle rechten op deze machine aangezien dit account zoals je weet de hoofdbeheerder is van het domein en dus van alle gekoppelde servers/clients.



Wanneer we nu op de AD01 (óf AD02) gaan kijken in de AD DS, in de OU -> **Computers**, dan zullen we onze zojuist aangemelde client daar terug gaan vinden. Op dat moment weet je zéker dat hij correct is aangemeld aan je domein.



Nu de client is gekoppeld én je bent ingelogd als de domain-admin op deze machine, zijn we voor nu klaar met WS01.

We hebben op dit moment een hele mooie basis omgeving neergezet:

- We kunnen inloggen als domeingebruikers op een werkstation (client);
- We routeren via de server zodat alle memberservers én clients voorzien kunnen worden van internet;
- We hebben twee domaincontrollers opgezet, beide met DHCP geconfigureerd;
- We hebben gezorgd dat het domein en de DHCP redundant is opgezet (fout tolerantie).

Nu dus tijd voor de inrichting van ons domein!

We gaan bezig op de AD01 om te beginnen met het opzetten van een organisatie structuur zodat ons domein structuur en overzicht krijgt én we moeten nog enkele instellingen goed zetten op DNS-niveau.

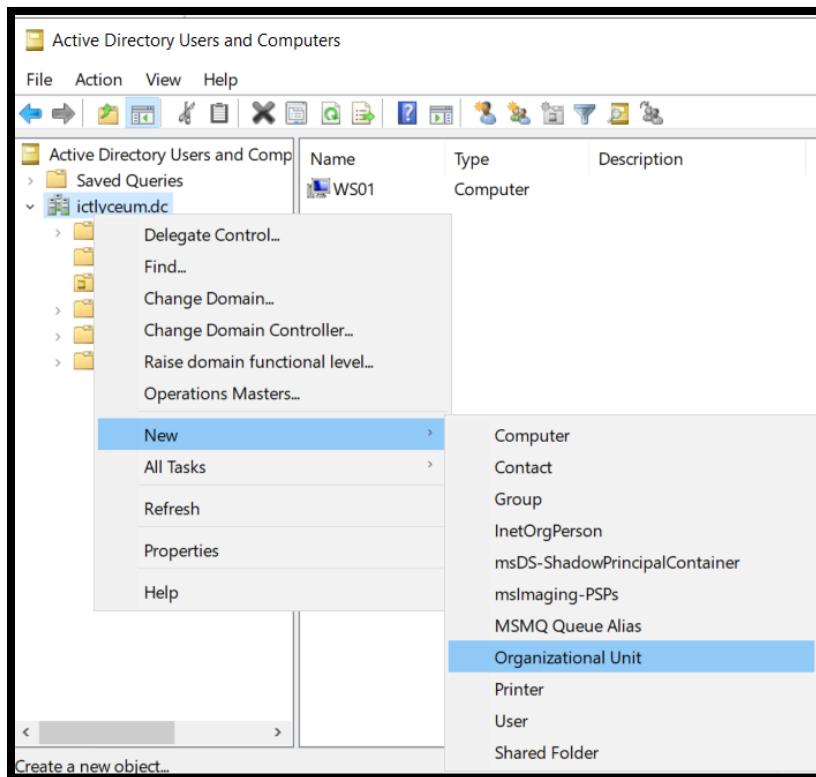
Configuratie AD DS – Organizational Units (OU's)

Om te beginnen gaan we op de AD01 beginnen met het aanmaken van een mappenstructuur, maar dan op domeinniveau. Op deze manier zorgen we ervoor dat een duidelijk en overzichtelijke 'view' krijgen van ons bedrijf. Het is namelijk belangrijk dat je als beheerder een duidelijk overzicht hebt over welke **Organizational Units** er zijn en daardoor natuurlijk wie waar in staan als gebruikers, omdat je dan snel kunt schakelen en mensen snel kunt helpen wanneer er iets gewijzigd moet worden of wanneer je bijvoorbeeld een wachtwoord moet resetten.

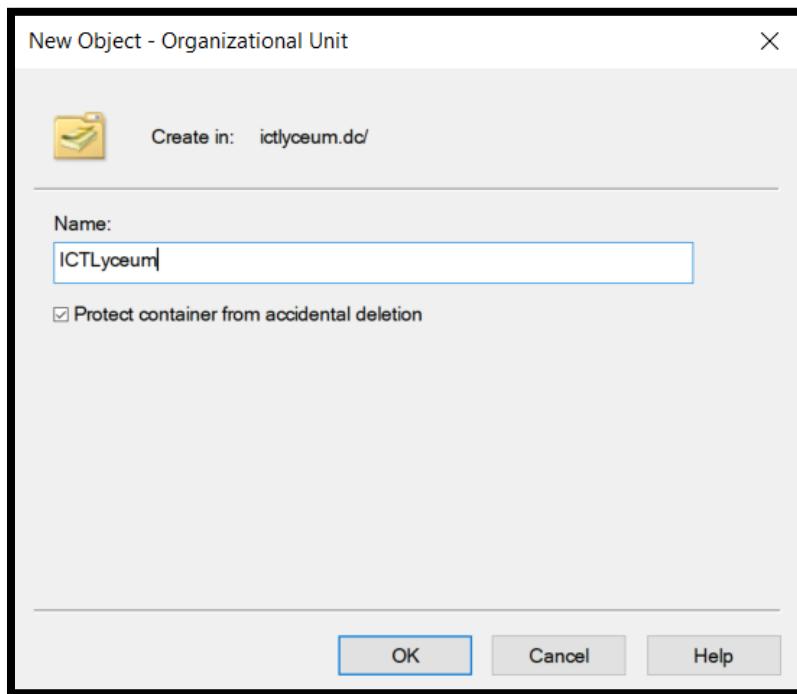
Om hiermee een start te maken, gaan we op de AD01 inloggen als administrator en openen we via Tools -> **Active Directory Users and Computers**.

In dit scherm gaan we op 'top-niveau' beginnen om een top-OU aan te maken. Dit doen we omdat we op deze manier de meest overzichtelijke structuur kunnen gaan opbouwen, ónder deze OU gaan we namelijk verder met bouwen.

Meestal noem je deze eerste **OU** Medewerkers, Afdelingen óf geef je deze de naam van het bedrijf. In dit geval gaan we ervoor kiezen om deze hoofd-OU '**ICTLyceum**' te noemen. We doen dit door met de rechter muisknop te klikken op onze domeinnaam en te kiezen voor **New -> Organizational Unit**



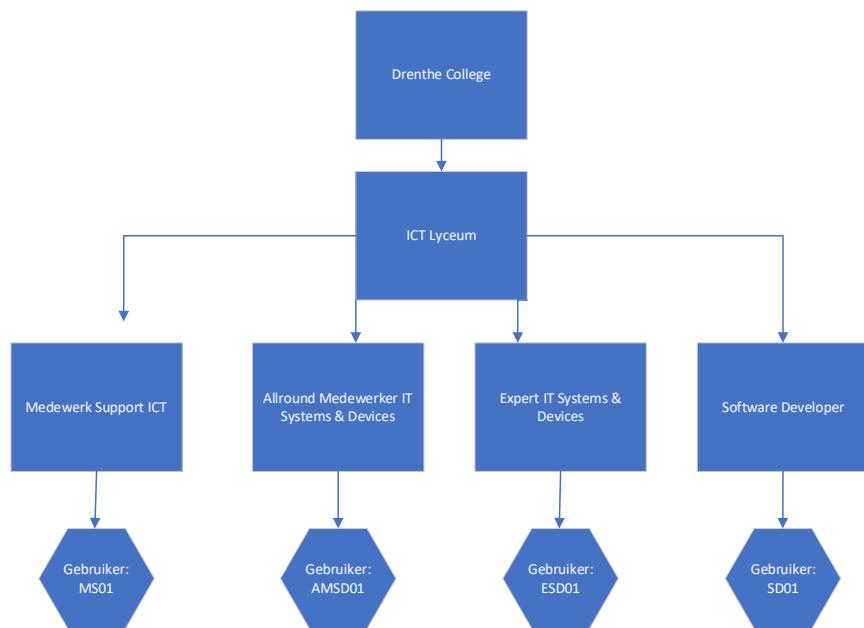
We gebruiken hier dus zoals gezegd de naam **ICLYceum** en het vinkje bij *Protect container from accidental deletion* laten we aan staan.



Dit vinkje voorkomt, zoals het er al staat, dat je per ongeluk deze folder kunt verwijderen.

Tegelijkertijd betekend dit ook gelijk dat je deze folder nu ook niet kunt verplaatsen naar een andere plek, dus daar moeten we zo nog even naar gaan kijken.

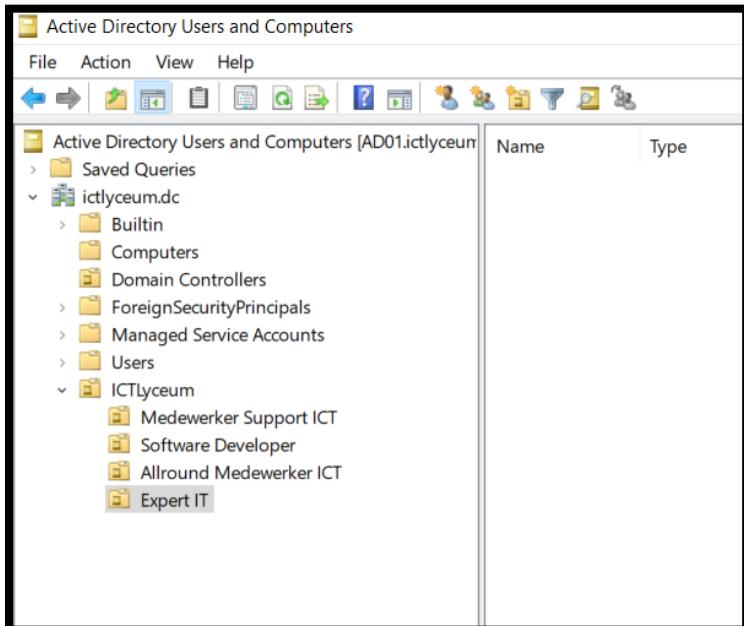
Nadat we dit “top-OU” hebben aangemaakt, doe we ditzelfde nogmaals, maar dan op de zojuist aangemaakte OU. Hierop gaan we nu de OU ‘**Medewerkers Support ICT**’ aanmaken. Eigenlijk gaan we nu dus onze bedrijfsstructuur nabouwen in de AD DS, zoals eerder op pagina 4 besproken is. Als we die nogmaals gaan bekijken, zien we nu dus direct wat onze uiteindelijk OU-structuur moet gaan worden.



We gaan dus onder het **ICTLyceum** (onze top-OU), vier nieuwe OU's aanmaken, enkele moeten we wel even gaan inkorten omdat het anders erg lange namen zijn:

- Medewerker Support ICT
- Allround Medewerker
- Expert IT
- Software Developer

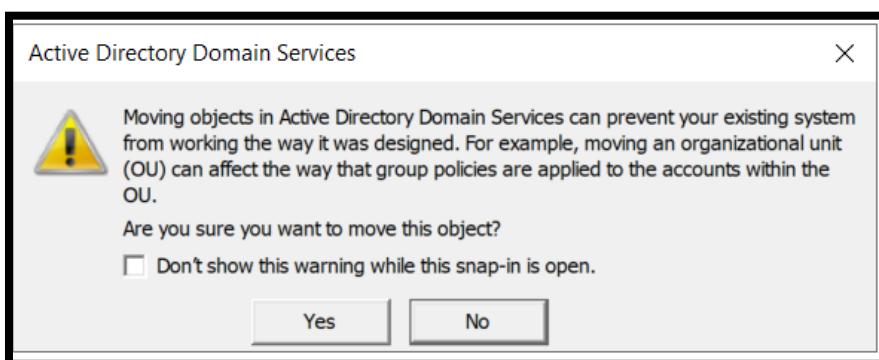
Deze maak je allemaal aan, onder de OU **ICTLyceum** en dit komt er dan uiteindelijk zo uit te zien:



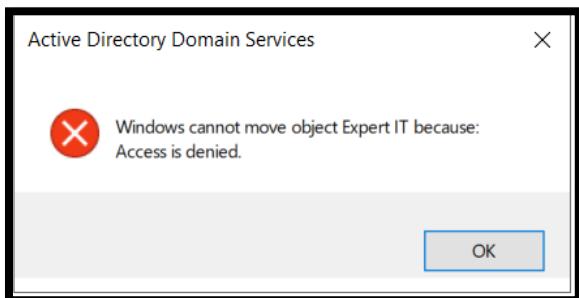
Mocht je nu per ongeluk een mapje (OU) hebben aangemaakt onder een foute OU, dan moeten we deze gaan verplaatsen naar de OU **ICTLyceum**, dit kan normaliter eenvoudig door simpel te slepen met de folder.



Wanneer we de OU van hierboven, *VerplaatsTest* vast pakken en naar boven slepen, komt de vraag of dit een bewust actie is. Hiervoor kiezen we voor **Yes**.



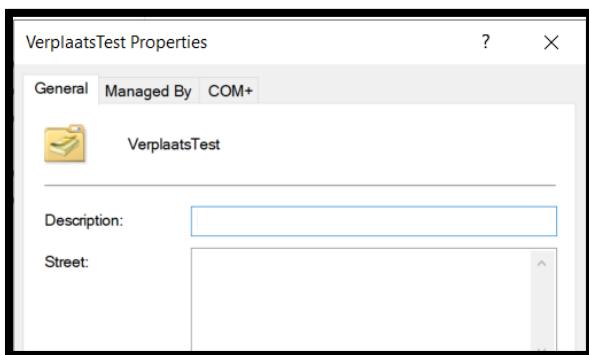
Echter, doordat het vinkje aan staat bij ‘*Protect container from accidental deletion*’ mag dit nu nog niet en krijgen we de volgende foutmelding:



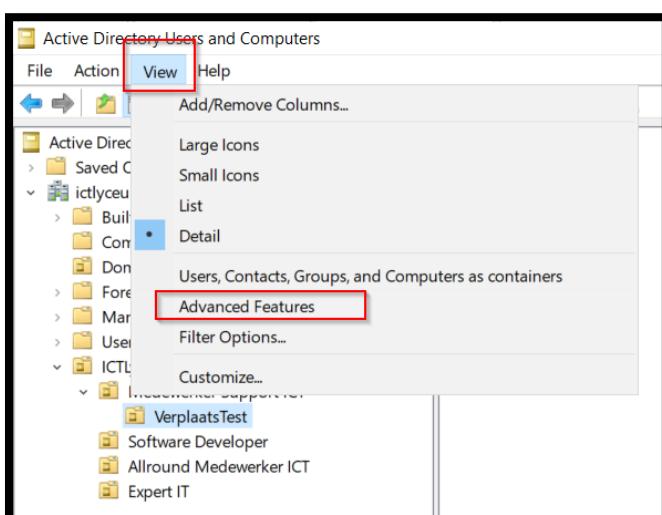
Om dit op te kunnen lossen moeten we er voor gaan zorgen dat we het vinkje kunnen uitschakelen. Dit kan echter alleen maar op een speciale manier. Dit is uiteraard beveiligd zodat men nooit ‘zomaar’ een hele OU kan weg gooien of verplaatsen. Tegelijkertijd een mooi moment om er dus bewust bij stil te staan wanneer je iets aanmaakt of verplaatst.

Dit vinkje zouden we moeten kunnen uitschakelen via Properties (*dit kan door de OU aan te klikken met de rechter muisknop en te kiezen voor Properties*) op de OU die we willen verplaatsen (of verwijderen)..

Echter, als we daar gaan kijken ziet het er uit zoals hieronder en kunnen we deze optie nergens vinden.



Om het vinkje op te vinden, moeten we onze ‘View’ van de *AD DS Users and Computers* gaan aanpassen. Dit doen we eenvoudig door bovenin het scherm van de AD DS op **View -> Advanced Features** te klikken.



Op het moment dat je deze aanklikt, valt je waarschijnlijk direct op dat de OU-structuur van je domein plots veel meer mappen bevat dan dat je oorspronkelijk wist. Hierbij zie je ook gelijk het nut van je aangemaakt top-OU, deze structuur en het overzicht blijft namelijk onveranderd terwijl de rest helemaal verspreid lijkt te zijn nu.

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational ...	Default container for do...
ForeignSecur...	Container	Default container for sec...
ICTlyceum	Organizational ...	
Infrastructure	infrastructureU...	
Keys	Container	Default container for key...
LostAndFound	lostAndFound	Default container for orp...
Managed Se...	Container	Default container for ma...
NTDS Quotas	msDS-QuotaC...	Quota specifications con...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
TPM Devices	msTPM-Inform...	
Users	Container	Default container for up...

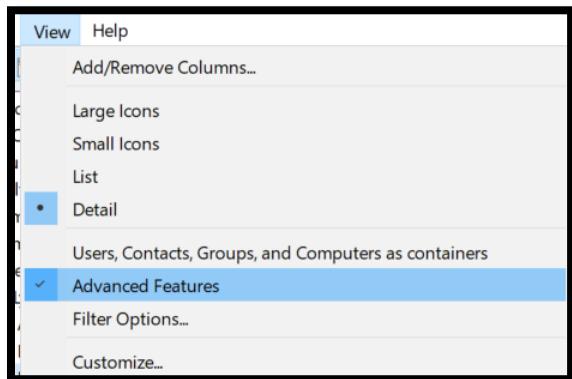
Het activeren van deze ‘Advanced Features’ heeft ervoor gezorgd dat we nu meerdere (extra) opties beschikbaar hebben voor alle objecten in onze AD DS.

Dit kunnen we zien door nu op de OU die we willen verplaatsen wederom te kiezen voor **Properties** en zoals je zult zien hebben we nu heel wat meer opties beschikbaar, waaronder het tabblad **Object**. Deze was er eerst niet, dus klikken we deze aan en daar treffen we het gezochte vinkje aan.

We zetten dit vinkje uit en kiezen voor **Apply/OK**. Nu kunnen we het mapje wél gaan verplaatsen en/of verwijderen. Wanneer je hem hebt verplaatst zet je het vinkje uiteraard weer aan op dezelfde

manier, om te voorkomen dat je hem (ooit) per ongeluk verwijderd.

Nadat dit klaar is, zet je de **Advanced Features** weer uit door er nogmaals op te klikken, zodat je weer de ‘normale’ view hebt.

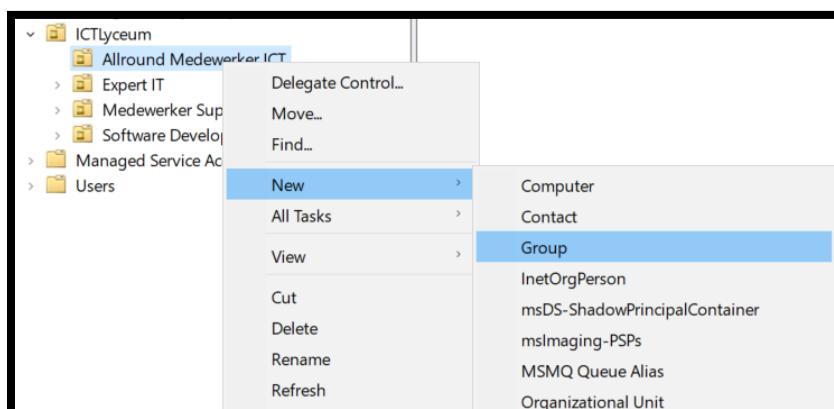


Aanmaken Security Groups

We hebben nu de OU-structuur helemaal klaar en we weten hoe we eventuele fouten kunnen herstellen. Om gelijk verder te gaan met ons bedrijf, gaan we nu we hier toch bezig zijn, verder met het aanmaken van **Security Groups**. Deze groepen hebben we nodig in ons domein, om bijvoorbeeld rechten te geven aan shares en/of om Group Policy Objects (GPO's) aan de juiste groepen te kunnen koppelen.

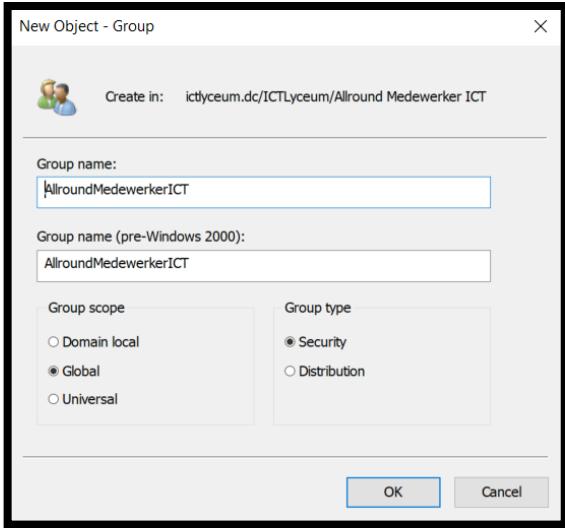
We hebben ze nu niet direct nodig, maar het is wel zo handig dit gelijk even mee te pakken omdat dit een relatief eenvoudige handeling is zonder directe gevolgen.

We gaan dus nu onder iedere OU die we zojuist hebben aangemaakt een beveiligingsgroep aanmaken door in of óp de betreffende OU te klikken met de rechter muisknop en te kiezen voor **New -> Group**



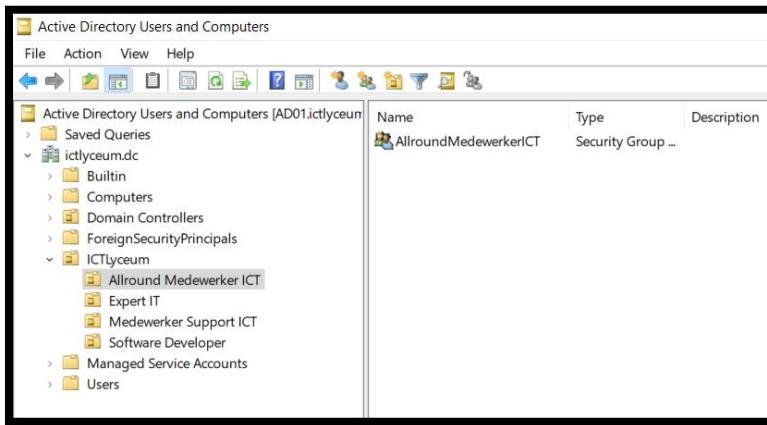
Deze groepen geven we dezelfde naam als onze OU's, maar dan zonder spaties of vreemde tekens.

- AllroundMedewerkerICT
- ExpertIT
- MedewerkerSupportICT
- SoftwareDeveloper



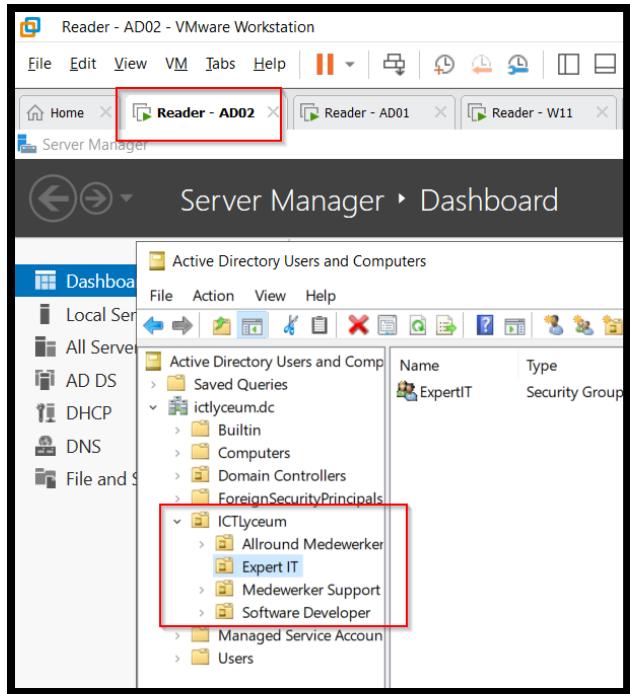
We laten de instellingen verder staan zoals ze standaard worden aangegeven, op Global Security. Op deze manier kunnen we ze gebruiken voor al onze gewenste doelen.

Dit ziet er dan zo uit;



We hebben op deze manier een nette en overzichtelijke organisatie structuur opgezet én we hebben (alvast) de benodigde beveiligingsgroepen aangemaakt. Ons domein krijgt dus al écht vorm op deze manier.

Het mooie is, dat al het werk wat we nu zojuist hebben uitgevoerd, automatisch gesynchroniseerd is naar onze tweede domein controller, de AD02. We gaan hier dus even kijken en zullen zien dat alle OU's én de aangemaakte groepen hier reeds aanwezig zijn.



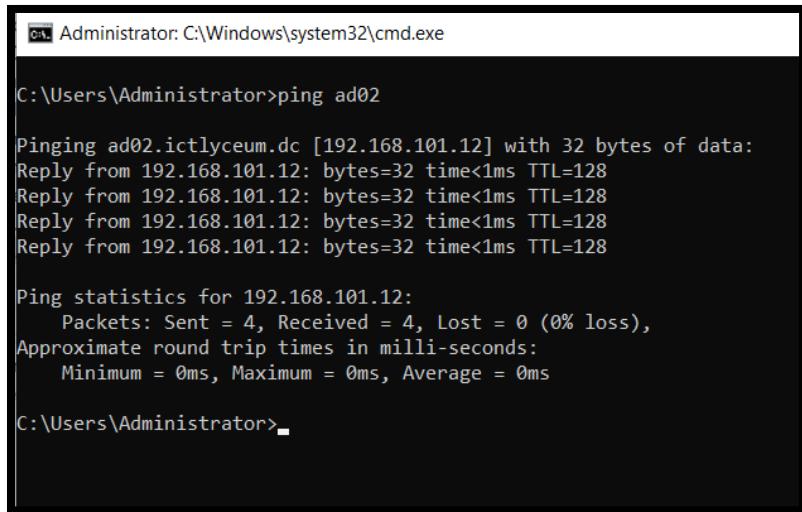
Mocht je de AD02 nu eerst nog moeten opstarten, dan kan het heel even duren (max. 5min) voordat alles verwerkt is.

Het 'enige' wat we nu nog missen, zijn eigenlijk de gebruikers. Die gaan we straks aanmaken zodat we daarmee kunnen inloggen op onze client. Eerst moeten we echter nog zorgen dat onze DNS-zone helemaal correct staat ingesteld, dus daar gaan we nu mee bezig.

Het inrichten van DNS

Het inrichten van de DNS is grotendeels eigenlijk automatisch al gedaan tijdens de installatie van het domein. Standaard werkt de DNS na installatie reeds ‘naar voren’ toe, dit heet de **forward lookup-zone**. Dit wil zeggen dat we dus al kunnen pingen op een server/client-naam en dat de DNS-server deze dan kan omzetten naar een IP-adres.

Gaan we dus even vanuit de Command Prompt (**Run -> CMD**) op server AD01 pingen op naam naar server **AD02**, dan zullen we zien dat we een reactie krijgen met het IP-adres wat bij AD02 past.



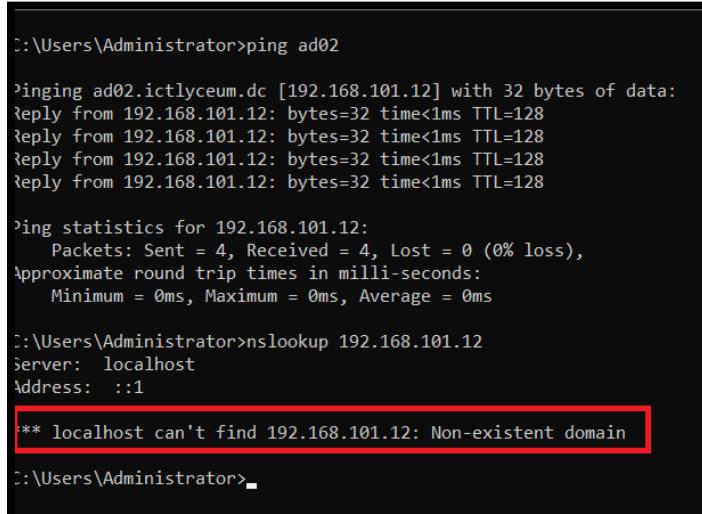
```
C:\Users\Administrator>ping ad02

Pinging ad02.ictlyceum.dc [192.168.101.12] with 32 bytes of data:
Reply from 192.168.101.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.101.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Gaan we echter andersom zoeken, dus van IP naar naam met het commando **NSLOOKUP**, dan herkent onze DNS server de bijhorende naam nog niet. Dit komt doordat we op dit moment alleen nog slechts de forward lookup-zone hebben.



```
C:\Users\Administrator>ping ad02

Pinging ad02.ictlyceum.dc [192.168.101.12] with 32 bytes of data:
Reply from 192.168.101.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.101.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>nslookup 192.168.101.12
Server:  localhost
Address:  ::1

** localhost can't find 192.168.101.12: Non-existent domain

C:\Users\Administrator>
```

Om dit andersom te kunnen bekijken hebben we een ‘**Reverse Lookup-zone**’ nodig.

Om deze aan te maken, moeten we de tool **DNS** openen, via de Server Manager onder Tools. Kijken we in deze tool onder **Forward Lookup Zones** dan zie we dat deze netjes gevuld is met ‘onze adressen en namen’.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[267], ad01.ictlyceum.dc, ho...	static
(same as parent folder)	Name Server (NS)	ad02.ictlyceum.dc.	static
(same as parent folder)	Name Server (NS)	ad01.ictlyceum.dc.	static
(same as parent folder)	Host (A)	192.168.19.129	3/10/2023 2:00:00 PM
(same as parent folder)	Host (A)	192.168.101.12	3/10/2023 2:00:00 PM
(same as parent folder)	Host (A)	192.168.101.11	3/10/2023 2:00:00 PM
ad01	Host (A)	192.168.19.129	static
ad01	Host (A)	192.168.101.11	static
AD02	Host (A)	192.168.101.12	static
WS01	Host (A)	192.168.101.21	3/10/2023 2:00:00 PM

Kiezen we hier echter voor de **Reverse Lookup Zones** dan zien we dat deze nog niet bestaan en dat we deze dus moeten gaan aanmaken.

The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.

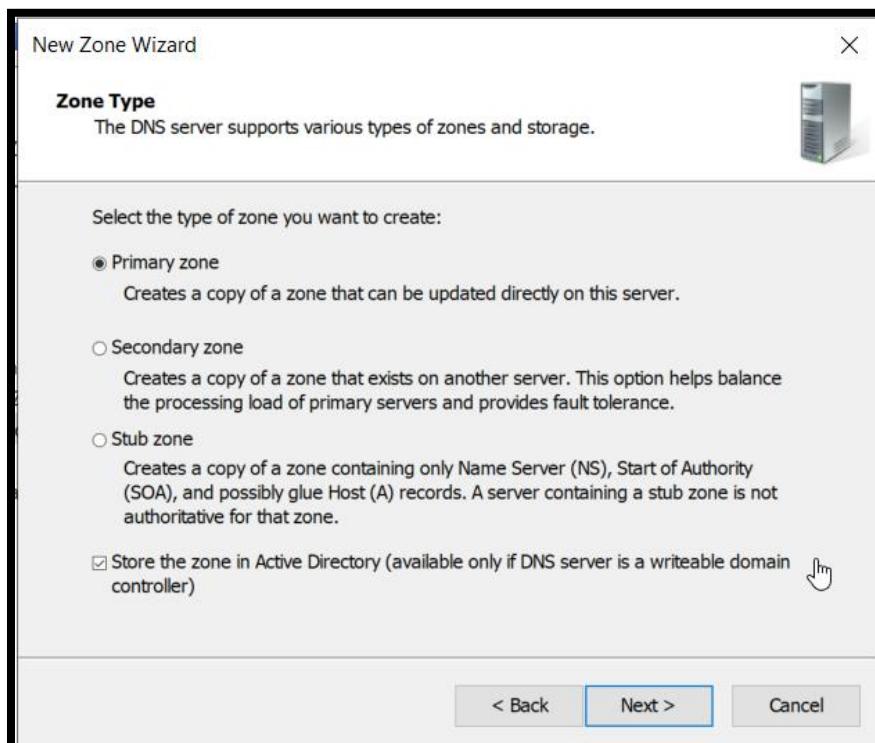
To add a new zone, on the Action menu, click New Zone.

Dit doen we door binnen deze Reverse Lookup Zones te klikken met de rechter muisknop en te kiezen voor **New Zone**

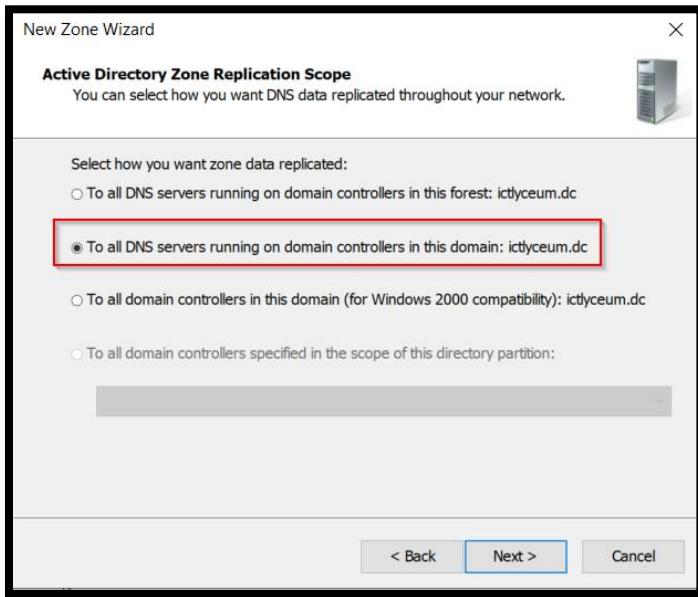
In de wizard die dan naar voren komt kunnen we eigenlijk alle stappen eenvoudig doorklikken via **Next.**



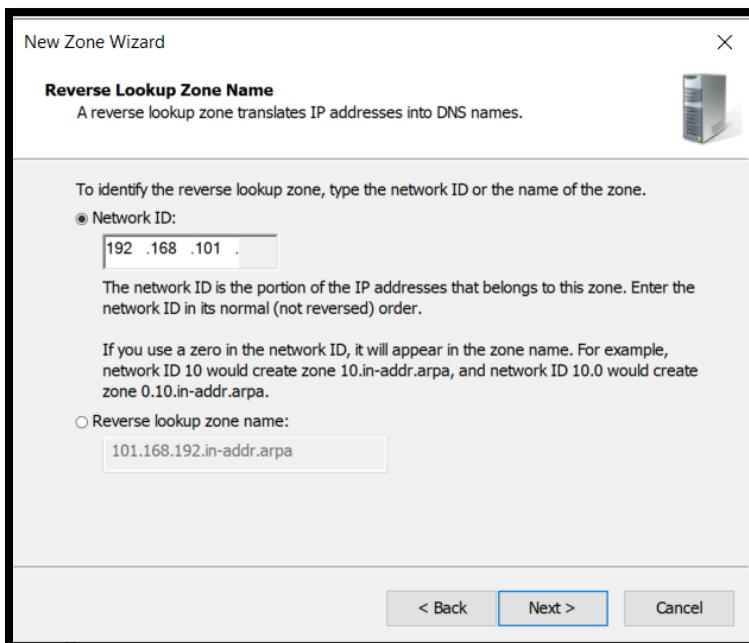
We kiezen namelijk de standaard ingesteld waarden, waaronder de **Primary Zone** (we hebben tenslotte nog geen andere zone, dus een secondary óf stub zone zijn technisch gezien helemaal niet mogelijk) dus kiezen we ook hier weer voor **Next**.



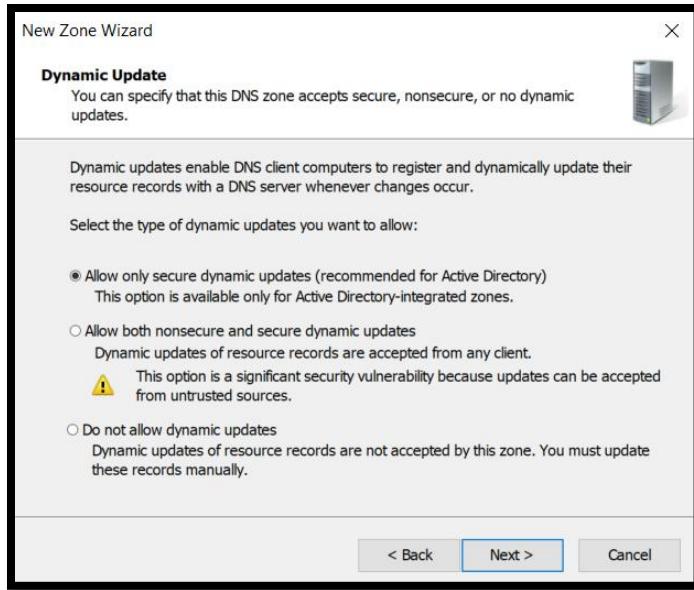
Ook de volgende stap laten we onveranderd, we willen onze nieuwe zone over ons hele domein verspreiden



In de volgende stap kies je voor **IPv4** aangezien we geen IPv6 ingesteld hebben op dit moment. Daarna dienen we ons **Network ID** op te geven, hierin vullen we de basis in van ons IP-adres. Je ziet onderin dit scherm dan ook dat het adres 'reversed' wordt genoteerd als ***.101.168.192**:



Wanneer we wederom op **Next** drukken komen we in het laatste scherm van deze wizard. Hierin doen we wederom **geen wijziging** en daarna kunnen we op **Finish** klikken.



We hebben nu een **Reversed Zone** aangemaakt voor onze DNS zone. Deze zone is echter, zoals je kunt zien, nog 'leeg' en moet dus gevuld worden.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], ad01.ictlyceum.dc, host...	static
(same as parent folder)	Name Server (NS)	ad01.ictlyceum.dc.	static

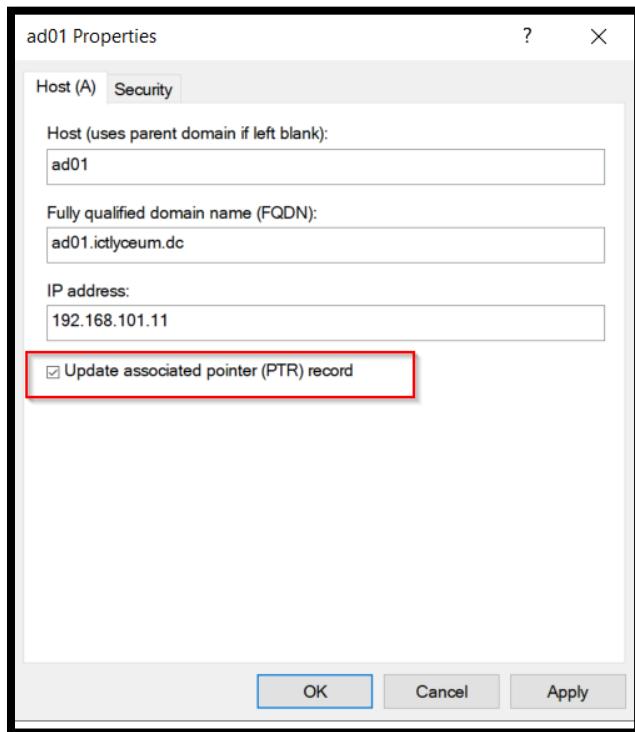
Deze stap moeten we voor de machines die we reeds hebben gekoppeld aan ons netwerk even handmatig doen, nieuwe machines worden vanaf nu automatisch toegevoegd wanneer ze worden gekoppeld met ons domein.

Het handmatig toevoegen doen we door in de **Forward Lookup Zones**, onder ictlyceum.dc de gewenste naam te openen (dubbel klikken of rechter muisknop -> Properties).

We zetten hier bij de AD01, AD02 en WS01 het vinkje aan bij **Update associated pointer (PTR) record** en kiezen dan voor **Apply** en daarna voor **OK**.

Bij server **AD01** zal je zien dat hij bij **beide namen** de PTR aanzet, dit komt aangezien hij twee netwerken heeft, dat is prima.

Mocht er bij een naam reeds een vinkje staan bij deze optie, zet je deze even uit en kies je voor **Apply**. Daarna zet je het vinkje weer aan (wederom gevuld door **Apply**).



Zoals je kunt zien in de **Forward DNS zone**, heeft de AD01 zoals vermeld **twee** DNS-records, simpelweg doordat je hier twee netwerkkaarten hebt toegevoegd (LAN en Internet).

DNS Manager					
		Name	Type	Data	Timestamp
	DNS		_msdc		
	AD01		_sites		
			_tcp		
			_udp		
			DomainDnsZones		
			ForestDnsZones		
			(same as parent folder)	Start of Authority (SOA)	[267], ad01.ictlyceum.dc, ho...
			(same as parent folder)	Name Server (NS)	ad02.ictlyceum.dc.
			(same as parent folder)	Name Server (NS)	ad01.ictlyceum.dc.
			(same as parent folder)	Host (A)	192.168.19.129
			(same as parent folder)	Host (A)	192.168.101.12
			(same as parent folder)	Host (A)	192.168.101.11
			ad01	Host (A)	192.168.19.129
			ad01	Host (A)	192.168.101.11
			AD02	Host (A)	192.168.101.12
			WS01	Host (A)	192.168.101.21

Wanneer je nu de betreffende servers hebt aangevinkt en we gaan wederom kijken bij **Reverse Lookup Zones** zal je zien dat deze nu netjes 'gevuld' is

The screenshot shows the Windows DNS Manager. On the left, the tree view shows a root node 'DNS' with a child 'AD01'. Under 'AD01', there are two main categories: 'Forward Lookup Zones' and 'Reverse Lookup Zones'. The 'Forward Lookup Zones' category contains several sub-zones like '_msdcs.ictlyceum.dc.', 'ictlyceum.dc.', and 'DomainDnsZones'. The 'Reverse Lookup Zones' category contains entries for IP addresses such as '192.168.101.11', '192.168.101.12', and '192.168.101.21'. On the right, a table lists these records with columns for Name, Type, Data, and Timestamp.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[9], ad01.ictlyceum.dc., host...	static
(same as parent folder)	Name Server (NS)	ad02.ictlyceum.dc.	static
(same as parent folder)	Name Server (NS)	ad01.ictlyceum.dc.	static
192.168.101.11	Pointer (PTR)	ad01.ictlyceum.dc.	static
192.168.101.12	Pointer (PTR)	AD02.ictlyceum.dc.	static
192.168.101.21	Pointer (PTR)	WS01.ictlyceum.dc.	3/10/2023 4:00:00 PM

Gaan we nu wederom controleren welke naam, via de **Command Prompt**, bij IP-adres 192.168.101.12 hoort, zullen we zien dat we wél een reactie gaan krijgen. Deze hebben we tenslotte net toegevoegd:

```
C:\Users\Administrator>nslookup 192.168.101.12
Server:  localhost
Address:  ::1

Name:      AD02.ictlyceum.dc
Address:   192.168.101.12
```

Ook de DNS hebben we dubbel opgezet, dus deze is net als zojuist bij de Active Directory Users and Computers inmiddels gesynchroniseerd naar server AD02. We gaan dit ook even bekijken en zullen zien dat hier nu dus ook een **Reverse Lookup Zone** is gecreëerd.

The screenshot shows the DNS Manager window for the 'Reader - AD02' VM. The tree view on the left shows the 'DNS' node with a child 'AD02'. Under 'AD02', the 'Forward Lookup Zones' and 'Reverse Lookup Zones' categories are visible. The 'Reverse Lookup Zones' category contains the entry '101.168.192.in-addr.ar'. A red box highlights this entry.

Nu we de DNS-zone hebben aangemaakt én de OU-structuur hebben opgezet (inclusief de beveiligingsgroepen), is het verstandig om even weer een snapshot te maken van alle machines!

Schijfbeheer en Shares

Nu we kunnen inloggen op onze client en nu we de basis van onze server zo'n beetje klaar hebben, kunnen we verder gaan met het aanmaken van nieuwe schijven op onze server(s). Op deze manier kunnen we straks gaan zorgen dat we data (bestanden) over het netwerk kunnen gaan delen met onze clients en dus onze gebruikers van het ICT Lyceum domein.

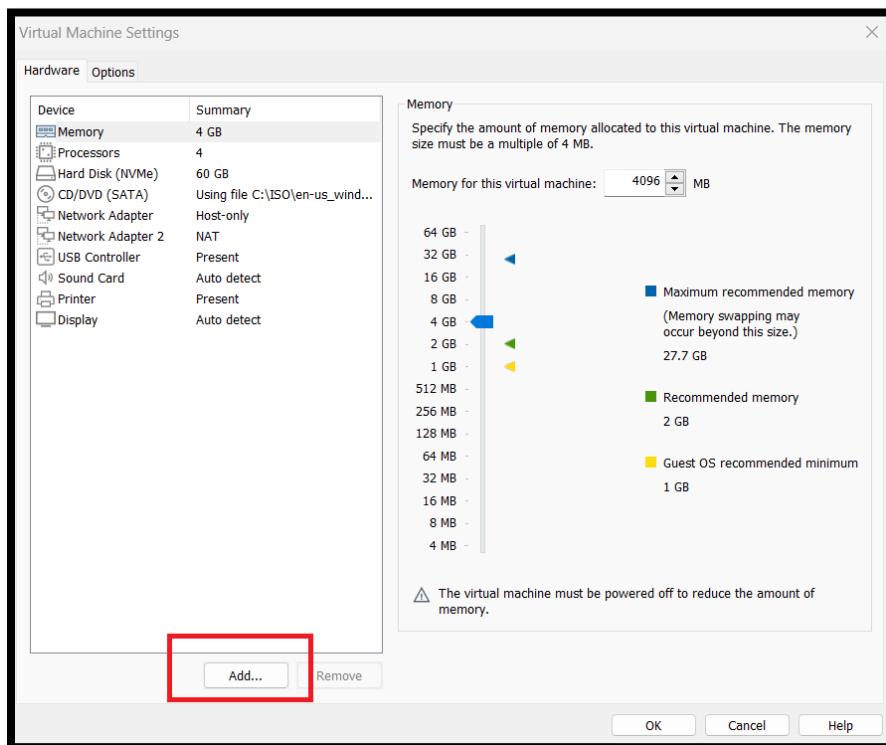
Wat een andere mooie optie is, is dat je er ook voor kunt zorgen dat gedeelde shares kunnen worden beperkt in opslagruimte binnen de server, waarmee je dus kunt voorkomen dat een gebruiker de hele netwerkschijf gaat vol zetten met bijvoorbeeld foto's en filmpjes van de vakantie.

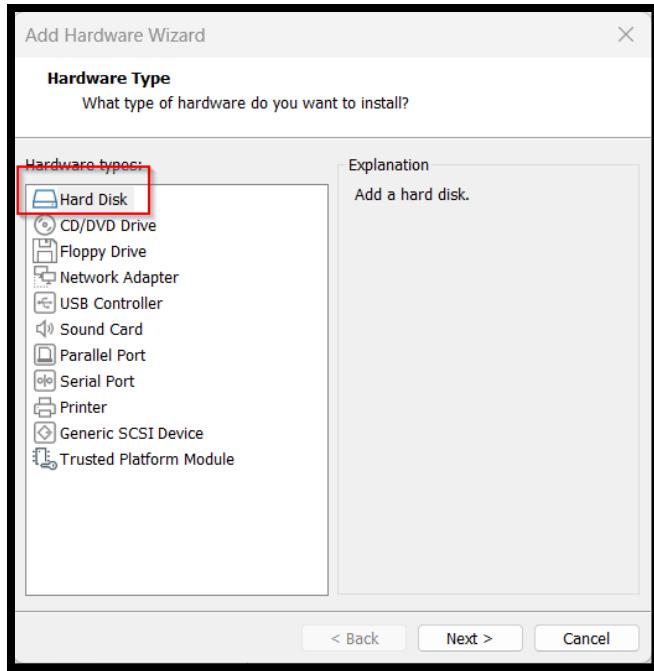
Om hiermee te beginnen gaan we eerst zorgen dat we een aparte schijf toevoegen aan de server waarop we de shares gaan aanmaken. Op deze manier creëer je (wederom) een duidelijke structuur en uiteindelijk beter overzicht over wat/waar staat.

Het aanmaken en koppelen van een nieuwe schijf

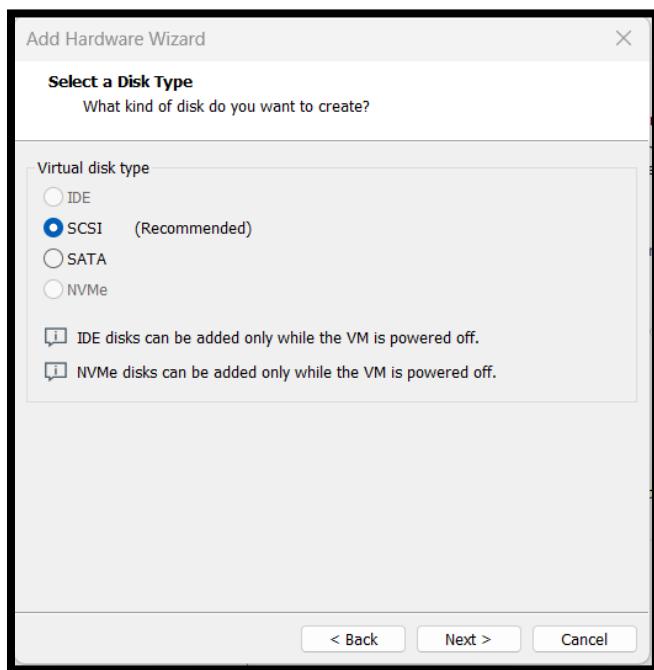
We gaan om te beginnen een schijf koppelen in je VM van 50GB. Die 50GB wordt pas écht gebruikt wanneer je ook daadwerkelijk 50GB aan data op gaat slaan, dus je kunt deze prima toevoegen. Ook wanneer je bijvoorbeeld slechts 30GB aan vrije ruimte hebt op je laptop.

We gaan dus eerst naar de **settings** van de AD01 en kiezen daar voor **Add -> Harddisk**. De machine mag hiervoor overigens aan blijven.



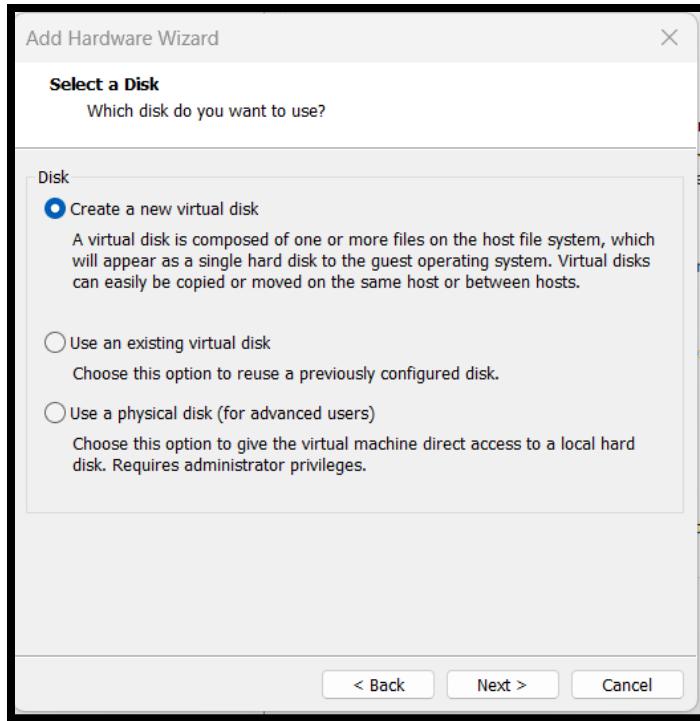


Wanneer je op **Next** drukt zal je zien dat je daar het type v-disk (virtual disk) moet aangeven. Standaard gebruiken we eigenlijk altijd SCSI óf NVMe, die laatste kan echter alleen worden gekozen wanneer de machine uitgeschakeld is, dus nu kiezen we voor het gemak even voor SCSI (spreek je ook wel uit als skoezie).

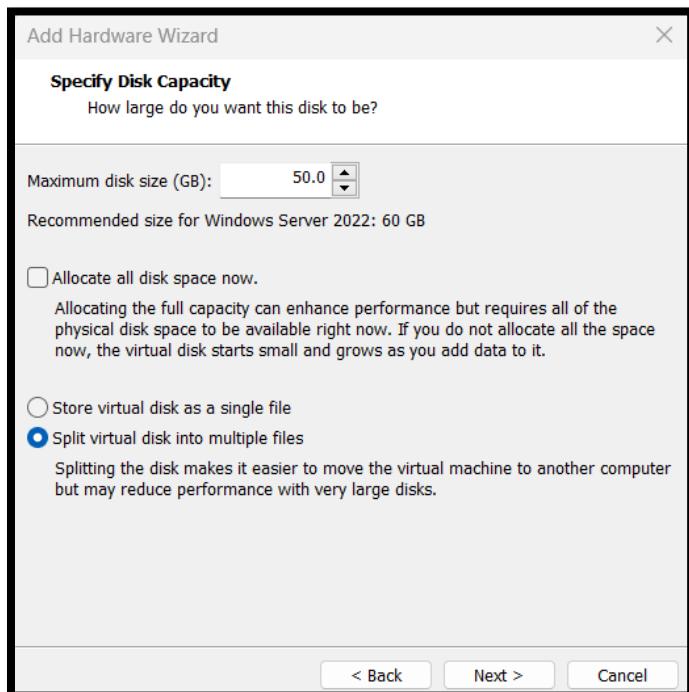


In de volgende stap van deze wizard gaan we opgeven of we een nieuwe óf reeds bestaande schijf willen toevoegen aan deze VM.

In dit geval kiezen we voor de (default optie) eerste. Het is echter wel nuttig om te weten dat je dus eventueel óók kan kiezen om een bestaande disk te koppelen vanuit een andere VM bijvoorbeeld.



In de voor laatste stap van deze wizard moeten we opgeven wat voor formaat we willen hebben, hier doen we dus zoals eerder aangegeven 50GB. Tevens moeten we opgeven of we deze disk in één groot bestand of in meerdere-kleinere-bestanden willen opslaan. Hierin kies je eigenlijk altijd voor de standaard optie; **Split virtual disk into multiple files**.

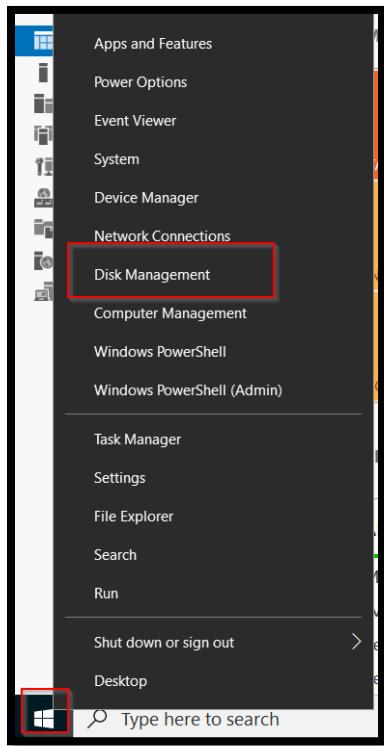


In de laatste stap kun je eventueel nog een naam of locatie wijzigen, maar in principe laten we deze altijd gewoon zoals het is en kiezen we voor **Finish**. De schijf is nu toegevoegd aan je virtuele machine **AD01**, je moet alleen nog even op **OK** drukken in het **Settings** scherm zodat hij het ook gaat opslaan.

Gaan we echter nu kijken in de Verkenner van deze server, zien we daar onze schijf helaas nog niet.

We gaan hem eerst nog moeten configureren zodat hij ook daadwerkelijk gebruikt kan gaan worden. Dit kan op meerdere manieren, waaronder via de Server Manager, echter is de meest overzichtelijke en snelste manier eenvoudig via de **Windows Disk Management-tool**.

Deze gaan we dan nu ook gebruiken. We openen deze door met de rechter muisknop te klikken op het Windows icoon en te kiezen voor **Disk Management**.

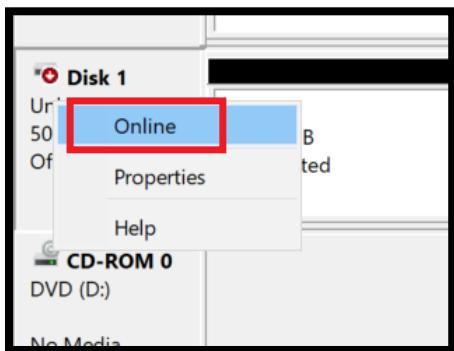


Wanneer we in de Disk Management komen, zal je gelijk zien dat onze nieuw toegevoegde schijf hier klaar staat om gebruikt te worden. Hij is echter nog **Offline** én hij is nog niet geïnitialiseerd.

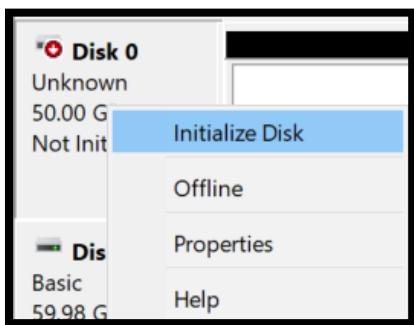
De eerste optie is natuurlijk helder, daarmee is hij offline dus niet beschikbaar óf online en dus wel beschikbaar. Bij de tweede optie gaan we aangeven op welke manier de schijf moet worden geïnitialiseerd, ofwel; wordt deze schijf gebruikt met de partitietabel MBR of GPT.

Bij nieuwe schijven gebruiken we eigenlijk altijd **GPT** (GUID Partition Table). Deze schijven kunnen veel meer opslag hanteren en kunnen beter beveiligd worden. De **MBR** (Master Boot Record) heeft namelijk een limiet van 2TB en wordt veelal alleen gebruikt voor de C-schijf, waarop dus bijvoorbeeld je Windows installatie staat.

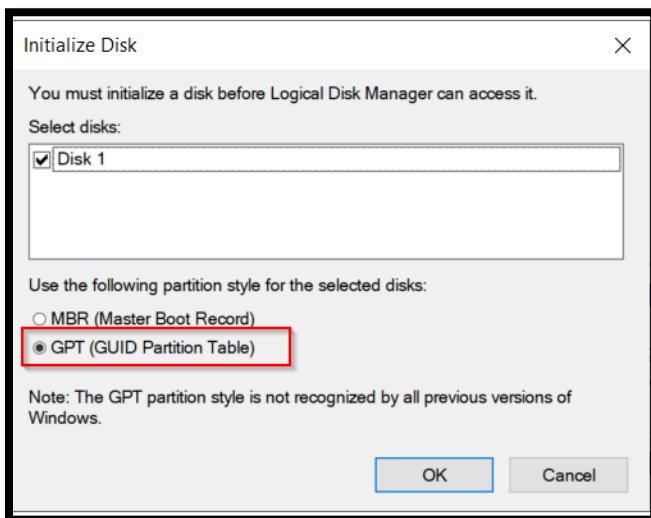
We gaan dus onze 50GB schijf eerst online zetten en vervolgens gaan we hem dus als **GPT** initialiseren. Hiervoor kiezen we onze disk en klikken hierop met de rechter muisknop en kiezen daarvoor **Online**



Vervolgens doen we direct nogmaals rechter muisknop en nu zien we dat we extra opties hebben gekregen. We kunnen hem weer offline zetten óf we kunnen hem dus zoals gezegd initialiseren. We kiezen hier dus voor **Initialize Disk**

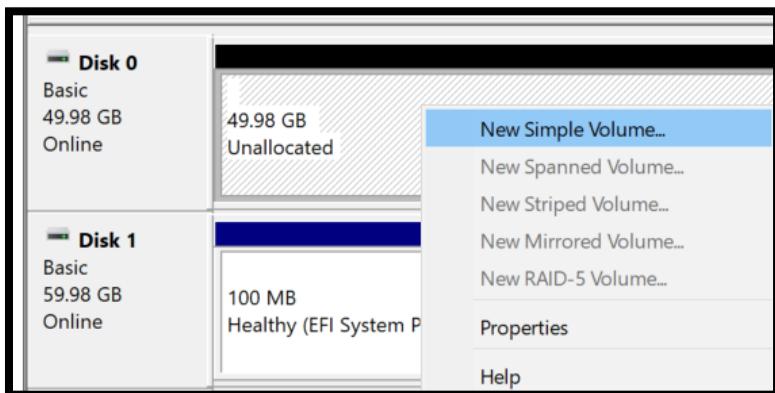


Wanneer we hierop drukken verschijnt er direct een pop-up waarin we moeten gaan kiezen of we MBR of GPT willen gebruiken als partitietabel. We kiezen hier zoals eerder besproken voor **GPT** en kiezen voor **OK**.



We kunnen na deze stap de schijf daadwerkelijk gaan inrichten zodat hij uiteindelijk een schijfletter gaat krijgen in onze verkenner.

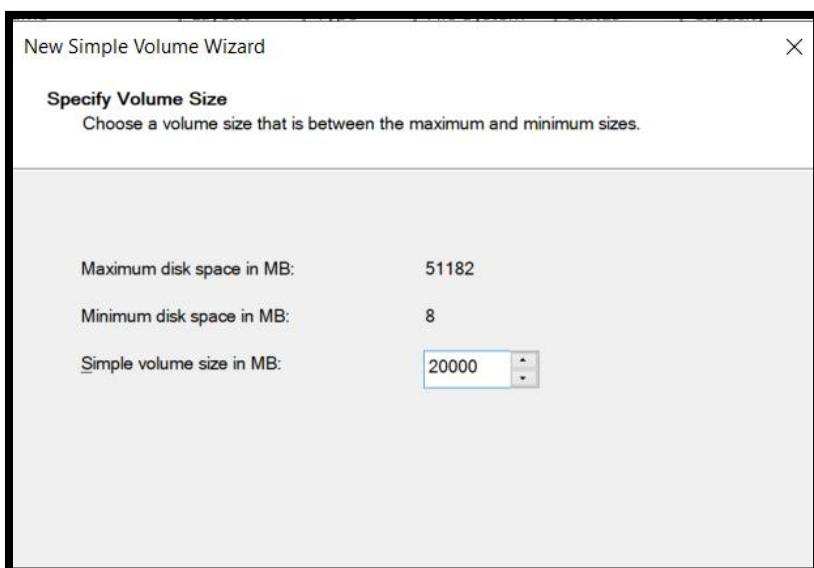
Om dit voor elkaar te krijgen, klikken we dit keer met de rechter muisknop op de (nieuwe) zwarte ‘schijf’ en kiezen we voor **New Simple Volume**. We gaan namelijk een nieuw volume aanmaken in deze schijf.



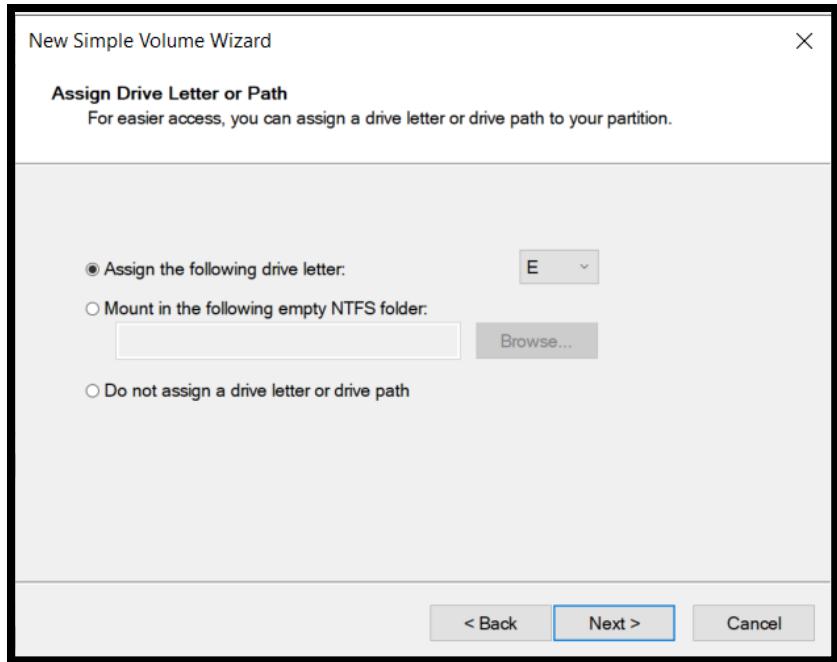
We kunnen er hierbij kiezen om gelijk alle opslag te gebruiken (50GB dus) óf we kunnen de schijf opdelen in kleinere stukjes, zodat we deze later bijvoorbeeld kunnen uitbreiden of zodat we meerdere (virtuele) schijven zichtbaar hebben in de verkenner.

Op dit moment kiezen we voor dit laatste en gaan we beginnen met 2 volumes van 20GB aan te maken. Wanneer we hebben gekozen voor **New Simple Volume** komen we in een Wizard terecht. In het 2^e scherm hiervan dienen we al gelijk op te geven hoe groot dit volume dient te worden in MB's.

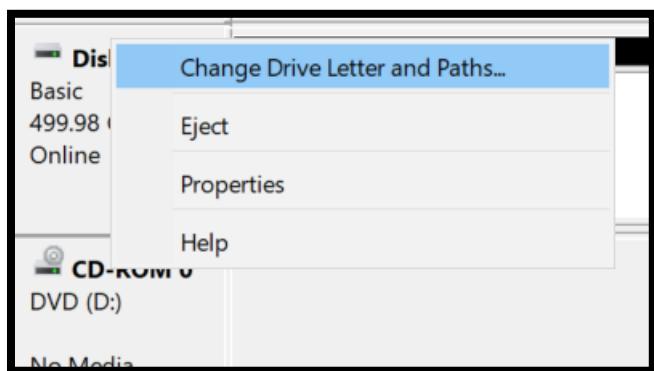
We zien bovenaan staan dat de maximale volume grote **51182 MB** is, 50GB dus ongeveer. Echter willen wij een volume aanmaken van 20GB dus we voeren hier **20000** in, dit is ‘ongeveer’ 20GB. 1GB is 1024MB, dus willen we écht 20GB hebben dienen we hier $20 \times 1024\text{MB} = 20480\text{MB}$ in te geven. Zo nauw komt het echter niet voor volumes en shares dus kiezen we voor 20000 en kiezen we voor **Next**.



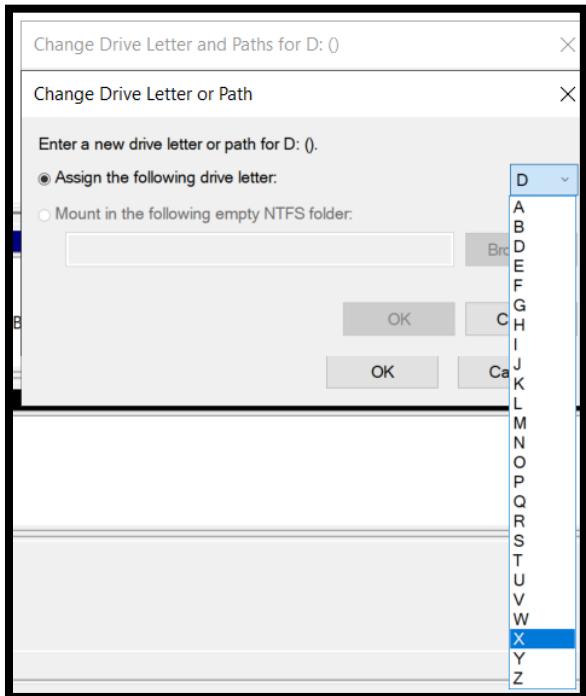
In het volgende scherm kunnen we een schijffletter gaan toekennen. Via het dropdown menu kun je hier de gewenste letter kiezen. Standaard pakt de wizard de eerst volgende vrije letter, in onze geval is dit E: aangezien de DVD-speler de D: in gebruik heeft.



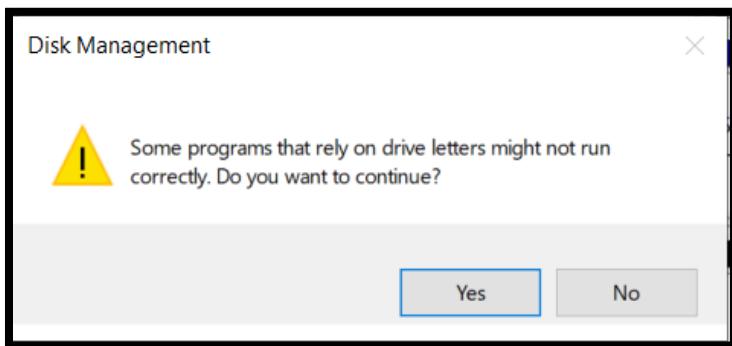
Omdat wij hier graag de letter **D** willen gebruiken, sluiten we de Wizard af via **Cancel** en drukken we met de rechter muisknop op de D-schijf en daar kiezen we vervolgens voor **Change Drive Letter and Paths..**.



We kiezen dan voor **Change** en kiezen dan simpelweg een andere letter, X bijvoorbeeld.



Bij de waarschuwing die je dan te zien krijgt, kun je voor **Yes** kiezen.



Het is wel belangrijk om te onthouden dat wanneer je dit in een praktijkomgeving doet, je **nooit** zomaar een schijfletter mag wijzigen. Er kan namelijk software op draaien die op dat moment verwijst naar de letter D:\ óf er kunnen shares zijn die zijn gekoppeld zijn aan deze drive. Denk dus altijd goed na voordat je dit uitvoert.

Wanneer dit is aangepast, starten we de Wizard opnieuw en kiezen we wederom voor 20000MB om onze schijf van 20GB aan te maken. Nu kunnen we wél voor de letter **D** kiezen. Tevens zorgen we ervoor dat ons volume **snel geformateerd** wordt en dat we bij **File System** kiezen voor NTFS.

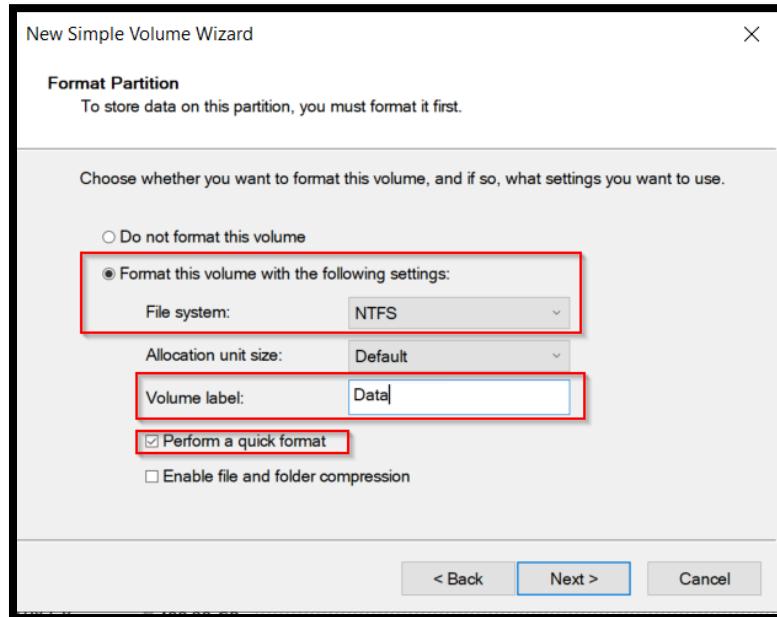
Het volume geven we de naam **Data** mee.

NTFS

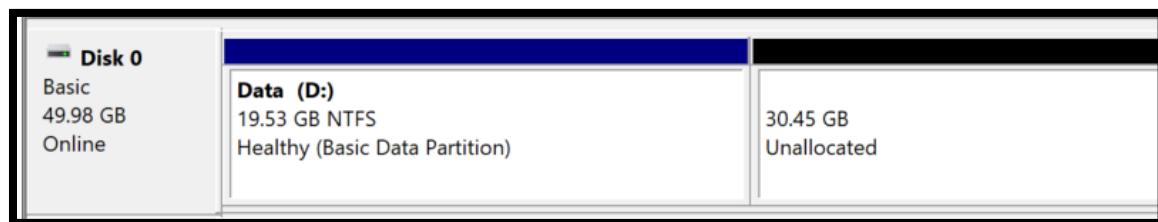
NTFS (New Technology File System) is het meest gebruikte file system wanneer je een Windows Server omgeving opzet. Een belangrijk kenmerk van NTFS is dat deze volumes tot 16TB ondersteund, dat moet dus voor de meeste bedrijven meer dan genoeg zijn. Tevens is het ook tegelijk goed te beveiligen door bijvoorbeeld encryptie.

ReFS

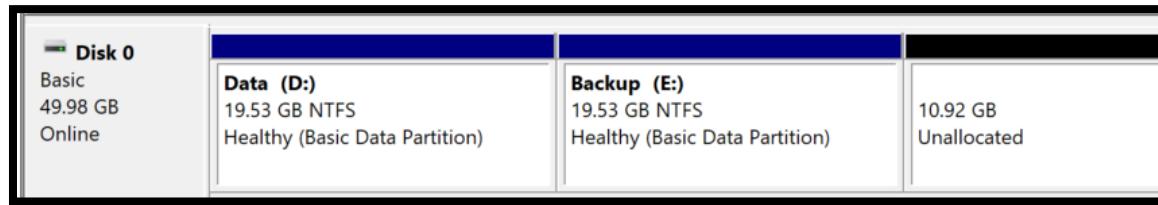
Een ander file system die je mogelijk kunt kiezen is **ReFS** (Resilient File System). Deze ondersteund volumes tot 16EB (ExaBytes) en kan corrupte data automatisch herstellen, echter is deze optie nog niet beschikbaar voor alle besturingssystemen gezien dit een vrij nieuwe technologie is op dit moment. Deze wordt dus ook niet heel vaak gebruikt op dit moment.



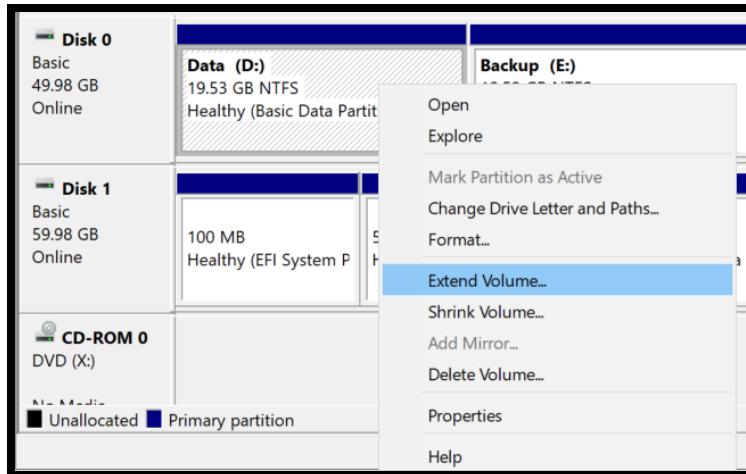
Wanneer je de laatste stappen van de Wizard doorloopt, zal je zien dat je een nieuw volume hebt aangemaakt van ca. 19,53GB en dat er nog iets meer dan 30,45GB ongebruikt is.



Het tweede volume van 20GB gaan we nu aanmaken met dezelfde specificaties, met de letter E en naam **Backup**. Dit ziet er dan uiteindelijk als volgt uit, maar dan voor jullie natuurlijk met de 20GB schrijven:

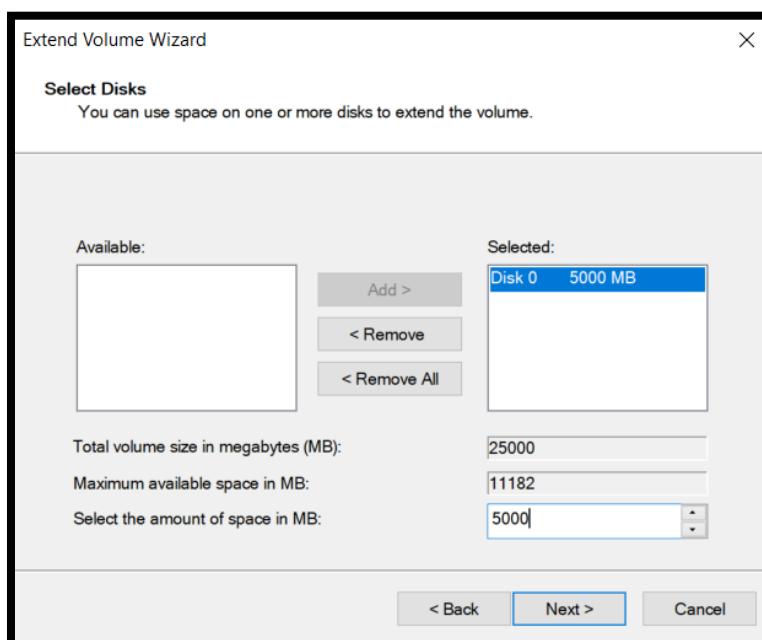


Als dit gelukt is, vergroten we het volume D: met 5GB en verkleinen we het volume E: met 10GB. Dit doe je wederom met de rechter muisknop en door daar te kiezen voor **Expand or Shrink** op de gewenste partitie.

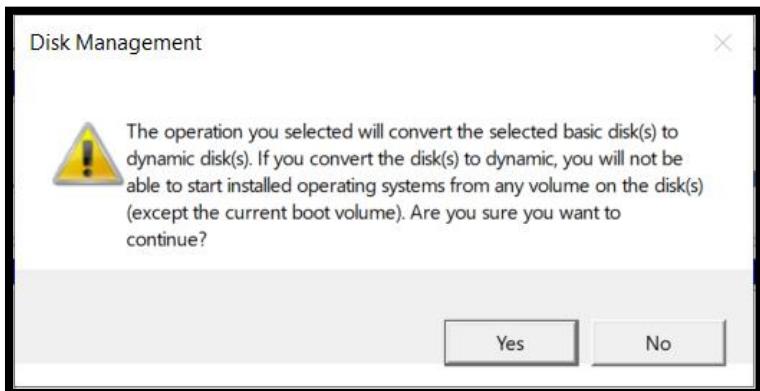


Tijdens het vergroten, zie je altijd hoeveel ruimte er totaal nog beschikbaar is en ook wat de totale volumegrootte wordt na het vergroten.

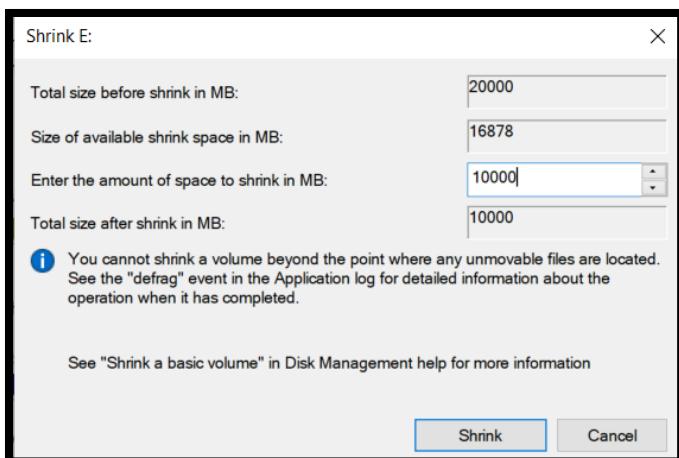
In de afbeelding hieronder zie je bijvoorbeeld dat we het volume met 5.000MB (=ca. 5GB) gaan vergroten en dat dus de totale volumegrootte 25.000MB wordt op dat moment (=ca.25GB).



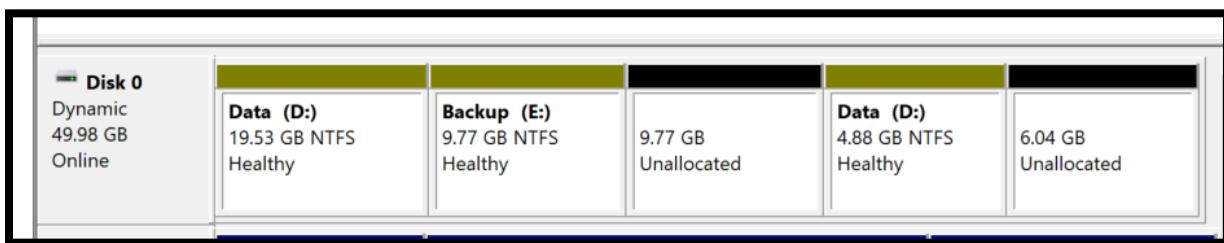
Omdat het niet mogelijk is om een zogeheten **Basic-Disk** te wijzigen, krijg je wanneer je het vergroten (of verkleinen) afrond een waarschuwing te zien:



Wanneer je hier voor **No** kiest, stopt het wijzigen van de schijf en wijzigt er verder niets. Uiteraard willen wij dit wel, dus kiezen we voor **Yes**. Het verkleinen werkt vergelijkbaar. Hier geef je echter natuurlijk aan met hoeveel MB je de schijf wilt laten krimpen en dan laat hij netjes zien wat er over blijft:

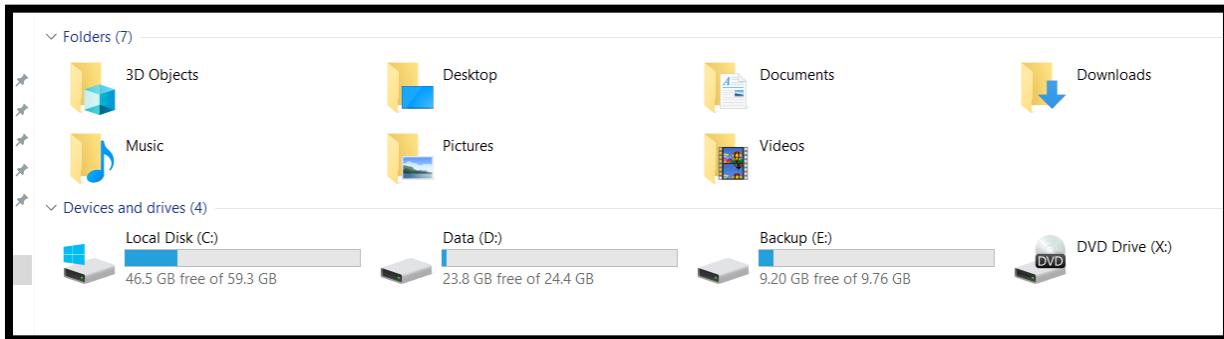


Uiteindelijk moet dit er ongeveer zo uit komen te zien.



Zoals je ziet is het volume D-Data uitgebreid naar totaal 24,41GB (19,53 + 4,88) en is E-Backup verkleind naar 9,77GB. 'Onder water' ziet Windows dit dus als aparte partities, dat is normaal.

In de **Verkenner** ziet dit er gelukkig wel gewoon uit als één D-Data volume van totaal ca. 24,4GB.



De schijven zijn nu aangemaakt en gekoppeld, dus is het tijd om ze te gaan delen door middel van het aanmaken van Shares op het netwerk binnen ons domein.

Het aanmaken van een Share

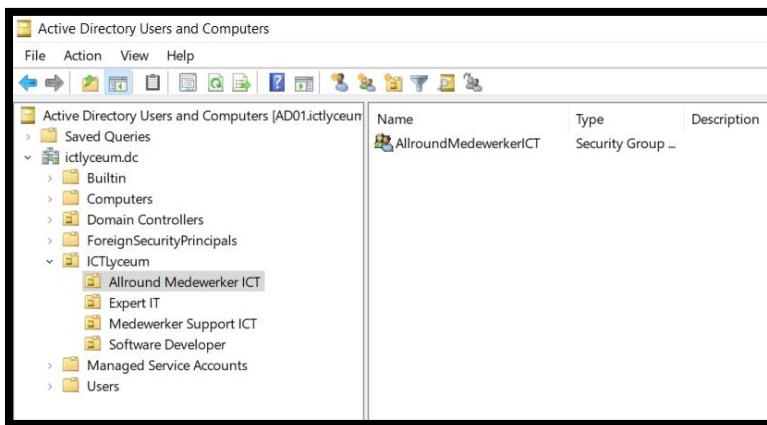
Nu we weten hoe we een extra harddisk aanmaken en koppelen aan de serveromgeving, gaan we ervoor zorgen dat we deze schijf ook daadwerkelijk kunnen gebruiken op het netwerk.

Uiteindelijk is het natuurlijk ons doel om er voor te zorgen dat alle gebruikers op het netwerk straks bij een gedeelde map kunnen komen. Om dit te kunnen realiseren, is het belangrijk om eerst mappen aan te maken. Vervolgens gaan we deze delen (zodat ze dus bereikbaar worden via het netwerk) en daarna gaan we ervoor zorgen dat de mappen goed dicht gezet worden op beveiligingsniveau (met behulp van NTFS-Security rechten). Op die manier zorg je ervoor dat bijvoorbeeld niet iedereen zomaar bij de directie of financiële-data kan komen.

Maar voordat we zover zijn, gaan we eerst de eerder gemaakte OU-structuur namaken in folders op de nieuwe dataschijf (D-schijf).

Het is hiervoor handig dat je even de OU-structuur er weer bij pakt. Op die manier vergeet je niets en kun je snel nieuwe folders aanmaken.

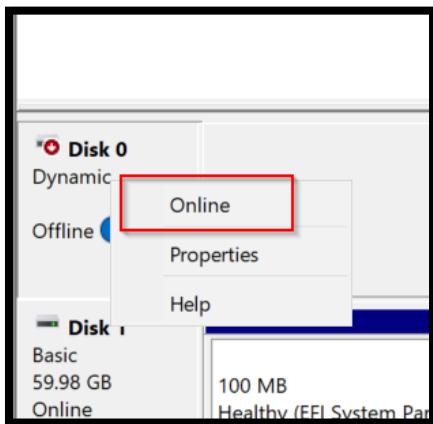
Mijn OU-structuur ziet er zo uit dus die ga ik nabouwen:



Ik begin altijd standaard met een hoofdfolder **Data**. Op die manier is het duidelijk, ook voor andere beheerders, wat er hierin te vinden is. Mocht je zomaar beginnen met mappen aanmaken, dan veroorzaak je eigenlijk gelijk al chaos in je structuur. Dus zetten we, net als in de AD DS, direct een overzichtelijk structuur op.

Nu gebeurd het heel soms wel eens dat een nieuwe partitie/schijf, na een herstart niet meer zichtbaar is onder de Verkenner.

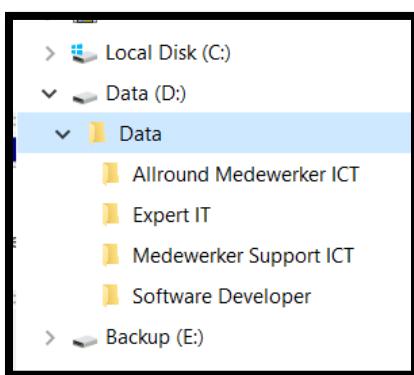
Dit betekend niet dat alle data en instellingen direct verdwenen zijn, maar alleen dat de schijf op dat moment nog **Offline** staat. Erg vervelend, maar je kunt hem snel weer online zetten zodat hij weer bereikbaar is, via **Diskmanagement**. Je klikt dan even met de rechter muisknop op de **Disk0** en kiest dan voor **Online (!). That's all 😊 !**



Je schijf én eventuele partities/mappen en alles zijn dan direct weer zichtbaar en te benaderen.

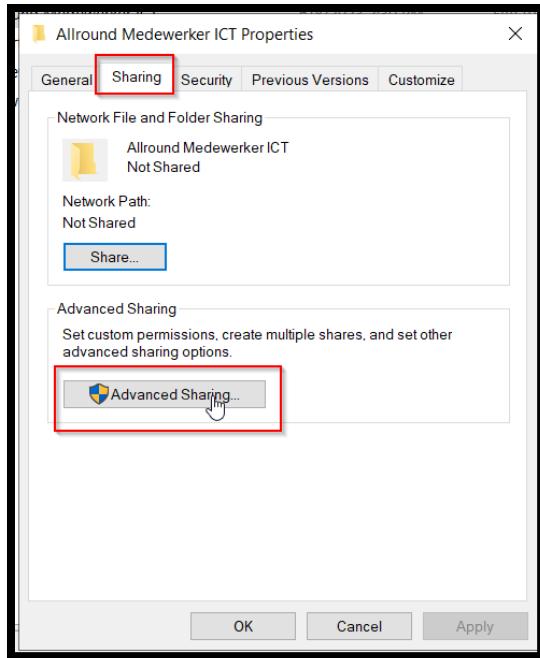
Zoals gezegd gaan we op de D-schijf beginnen met het aanmaken van een map Data. Daaronder maken we de overige mappen uit de AD DS aan.

Uiteindelijk heb je dus, heel eenvoudig, vijf mappen aangemaakt op deze nieuwe schijf:



Na het aanmaken van de mappen, gaan we deze mappen **delen** op het netwerk. Je doet hiervoor **ALTIJD precies hetzelfde**, voor elke share die je maakt. Voor het delen van de map, geef je namelijk het recht aan iedereen (groep **Everyone**) op deze share te lezen en te bewerken. Klinkt wellicht wat vreemd misschien, maar het daadwerkelijk 'dichttimmeren' van de rechten op deze mappen, gebeurt via de NTFS-rechten, door middel van de eerder gemaakte [Security Groups](#).

We beginnen met de eerste map, je kiest eenvoudig voor **Properties** op de folder die je wilt gaan delen en kiest daar voor het tabblad **Sharing**. Daar kiest je voor de knop **Advanced Sharing...**



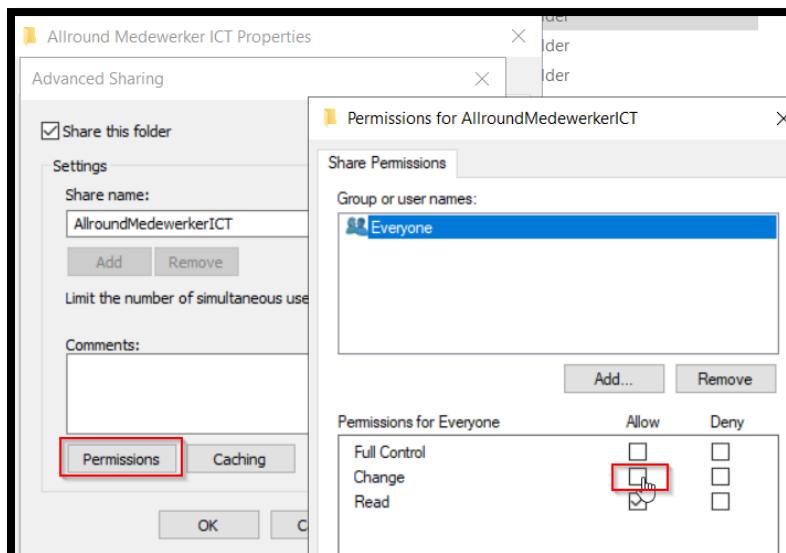
In het opkomende scherm, zet je een vinkje bij 'Share this folder' en desgewenst pas je de naam aan van de share. Het is aan te raden om spaties altijd te verwijderen uit een sharenaam.

Zet je hier achter de share name eventueel een **\$-teken**, betekent dit dat de share verborgen wordt. Hij is dan simpelweg niet zichtbaar wanneer men gaat kijken op het netwerk via de verkenner (bijvoorbeeld via <\\AD01>) maar alleen wanneer het gehele pad wordt ingetypt.

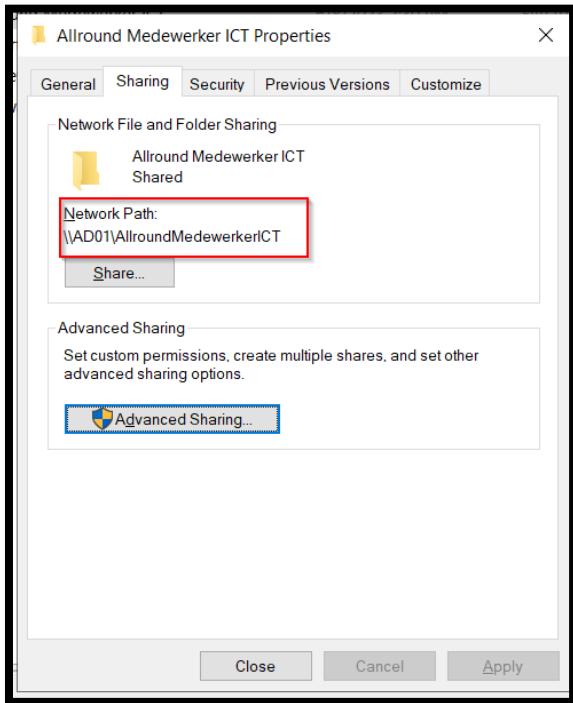
Dit kan erg handig zijn bij het delen van een wallpaper over het netwerk, iets wat wij straks ook gaan doen, dus later gaan we hier daadwerkelijk mee bezig!

Voor nu maken we gewoon een normale share aan. Nadat je de gewenste naam dus hebt gekozen, klik je onderin op de knop **Permissions**. Je ziet daar standaard de groep **Everyone** reeds staan.

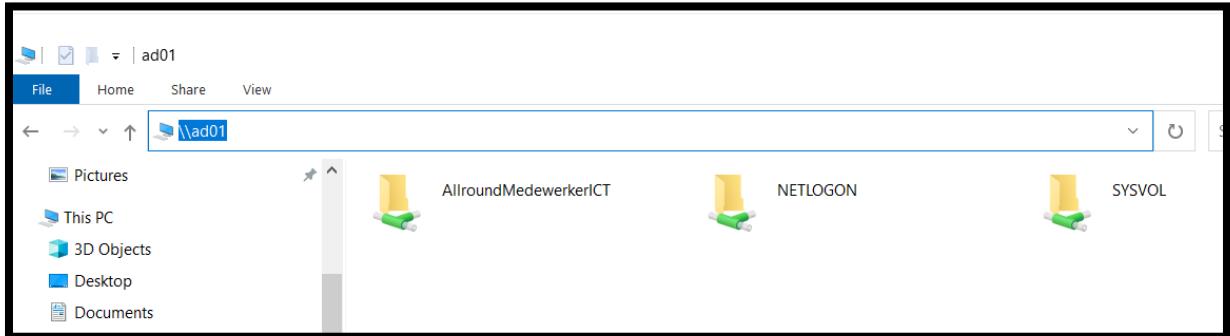
Het enige wat je hier altijd moet doen, is **een extra vinkje plaatsen bij Change**, zodat er uiteindelijk 2 vinkjes staan (**Change/Read**). Meer niet. Je sluit dit scherm vervolgens af via **OK** of **Apply** en kiest daarna weer voor **OK** of **Apply** zodat je weer bij de tabbladen terecht komt van de folder.



Zoals je ziet, is de folder nu daadwerkelijk gedeeld. Het pad zie je bij het tabblad Sharing ook staan.



Wanneer we dit pad nu intypen in de Verkenner van Windows op de AD01, dan zie je dat deze share werkt en benaderbaar is. Type je alleen <\\AD01> in, dan zie je dat deze share er dus netjes is bijgekomen:



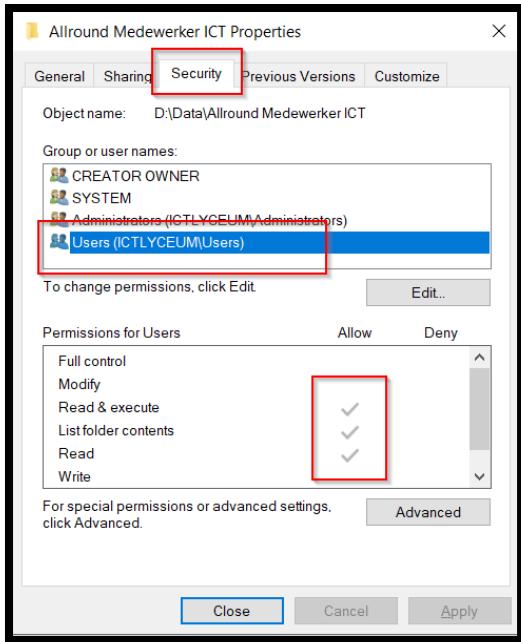
Onze eerste share is dus een feit! Nu moet hij alleen nog even dicht gezet worden, zodat alleen de mensen, die lid zijn van de Security Group AllroundMedewerkerICT, deze folder kunnen benaderen.

Het is belangrijk om te onthouden dat shares in Windows NIET hoofdlettergevoelig zijn. Dus of je nu \\ad01 of \\AD01 intypt, en AllroundMedewerkerICT of allroundmedewerkerict , dat maakt niets uit.

Dit doen we dus via het tabblad Security.

Wanneer je die aanklikt, zie je reeds een aantal ingestelde groepen of gebruikers staan. In de basis zal Windows Server altijd zorgen dat alle domeingebruikers toegang hebben tot een map op de server. Niet heel handig, dus gaan we zorgen dat deze groep (ICTLYCEUM\Users) verwijderd wordt.

Wanneer je deze groep echter aanklikt, valt direct op dat de rechten die zijn ingesteld, 'greyed-out' zijn. Ze zijn dan niet te wissen en/of aan te passen:

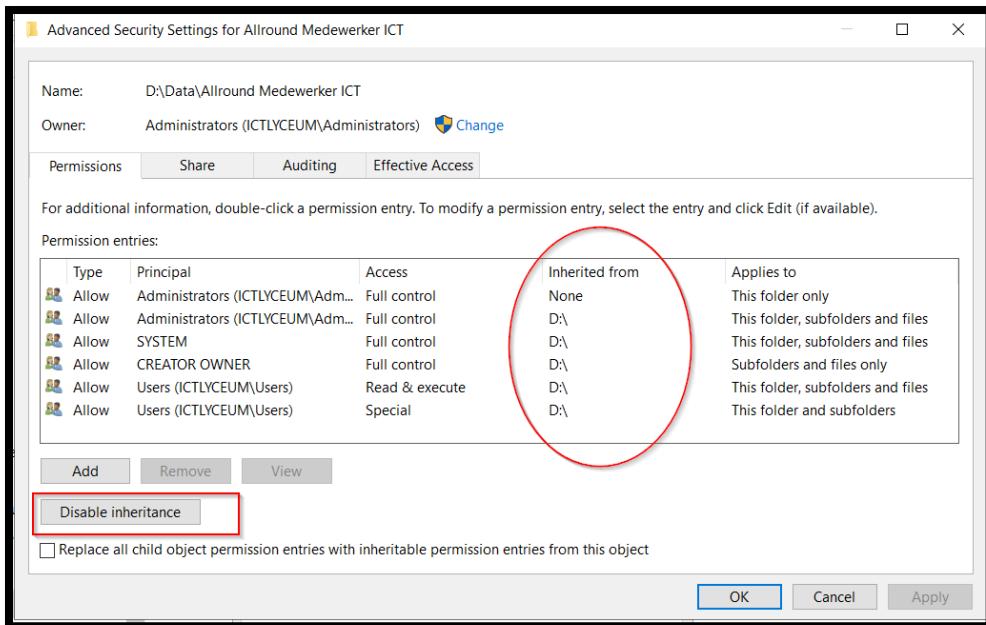


Dit komt doordat deze folder, automatisch, altijd de bovenliggende rechten overneemt. In ons geval dus de map **DATA** óf de D-schijf zelf.

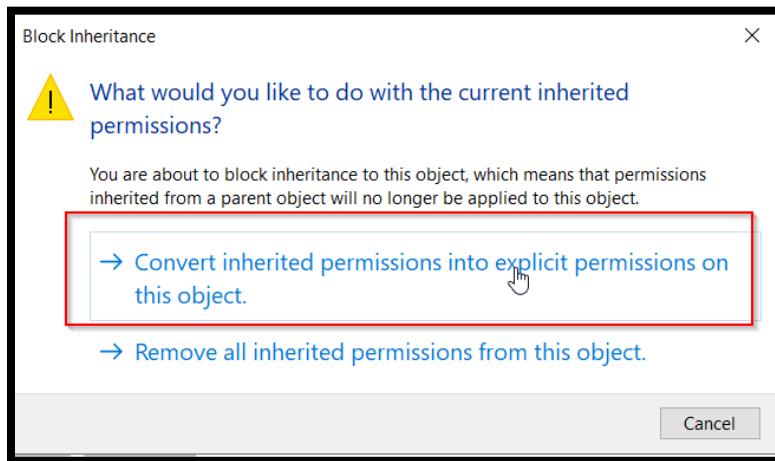
Nu moet men natuurlijk wél in de map **Data** kunnen komen, dus daarop is dit recht in principe prima (zoals je ziet heeft deze groep hier ook **geen** modify rechten), maar voor alle onderliggende mappen is het niet erg veilig.

We gaan dus beginnen met het verwijderen van die bovenliggende rechten. Dit heet binnen Windows ook wel **Inheritance**. Om dit aan te passen, klikken we op de knop **Advanced** in het bovenstaande scherm. Je komt dan in een geavanceerde omgeving terecht waar je rechten kunt toekennen. Dit gaan we hier echter niet doen.

We zien staan dat deze folder, de rechten heeft overgenomen (**Inherited from**) onze D:\ schijf. Gezien we dat dus niet willen, kiezen we links onderin voor **Disable inheritance**



In de Pop-Up die volgt, kiezen we voor **Convert inherited permissions into explicit permissions on this object**.



Kies je hier namelijk voor **Remove All....**, dan zijn alle rechten weg. Er zijn echter enkele belangrijke rechten (waaronder **System**, **Creator Owner** en **Administrators**) die altijd bewaard moeten blijven gezien er anders ook geen back-ups of wijzigingen meer gedaan kunnen worden op deze map/folder.

Na het converten zie je dat de kolom bij **Inherited From** leeg is geworden. Je klikt dan op **OK**.

Inherited from
None

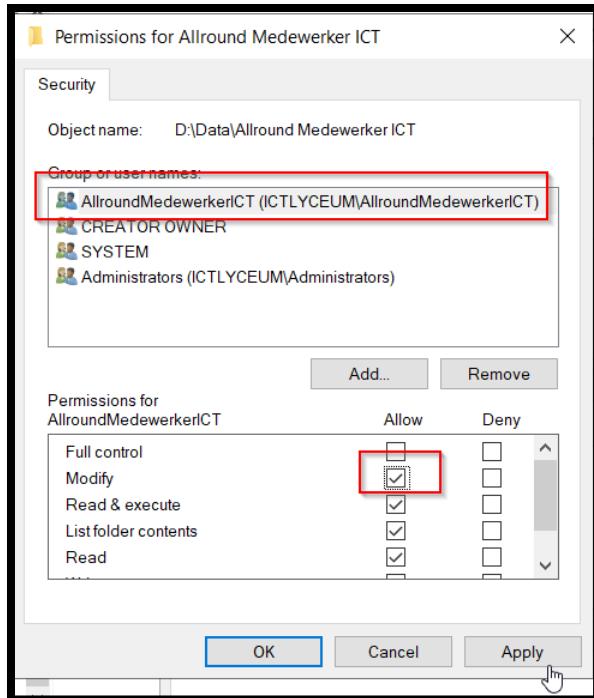
Nu kunnen we daadwerkelijk beginnen met het juist instellen van de rechten op deze folder. Hiervoor klikken we op **Edit**. We zitten hierbij nog altijd onder het tabblad Security van onze folder (!)

In dit schermpje kunnen we heel eenvoudig en snel rechten toekennen. Zoals gezegd kunnen we de standaard groep **Users** gaan verwijderen (vaak **domainname\users** overigens) en gaan we de benodigde Security Group toevoegen.

Je klikt dus simpelweg op de groep **Users** -> gevolgd door **Remove**.

Daarna klik je op **Add..**, dan type je het begin in van de naam in van je Security Group en dan klik je op de knop **'Check Names'**. Type je hier dus het woord **Allround** in, dan zal de AD DS automatisch aanvullen met de gehele naam van de groep. Mochten er meerdere zijn waarmee dit begint, krijg je een pop-up te zien waaruit je kunt kiezen.

In dit geval is er echter maar één groep die zo heet en dus wordt hij automatisch aangevuld. We zetten **bij** deze groep een extra vinkje bij **Modify** en klikken op de knop **Apply** om te bevestigen.



Mocht het nodig zijn dat een andere Security Group ook rechten nodig heeft op deze folder, dan kan dat uiteraard, door deze op dezelfde manier toe te voegen. Het gebeurd vaak dat bijvoorbeeld een Directie ook overal bij wil, maar dan alleen met **Read & Execute** rechten, omdat deze simpelweg niet hoeven te wijzigen. Zodat je het **Modify** vinkje toekent aan de groep, dan betekend dit automatisch ook dat deze mogen **verwijderen**. Let hier dus altijd goed op!

Daarnaast is het zeer belangrijk om te onthouden dat je **nooit** losse gebruikers toevoegt aan een share of rechten. Je maakt hiervoor altijd een (nieuwe) security group voor aan in de AD DS.

Stel je doet dit namelijk niet en je hebt directeur James toevoegt aan onze vier shares, kan James prima de mappen benaderen en zijn spullen opslaan. Helemaal prima! Echter is het zo, dat James het bedrijf gaat verkopen aan Jannes na drie jaar. Er zijn veel mappen toegevoegd, het bedrijf is gegroeid en inmiddels moet jij als beheerder nu 25 shares bij langs om James te verwijderen en Jannes toe te voegen. Niet heel handig, maar goed, het is te doen. Jannes zet het bedrijf goed voort, bouwt internationaal uit en verkoopt het bedrijf na 12,5 jaar weer verder. Nu zijn er echter ruim 500 shares, ruim 16TB aan data en enkele subfolders waar hij ook rechten op heeft gekregen in de loop van de jaren.

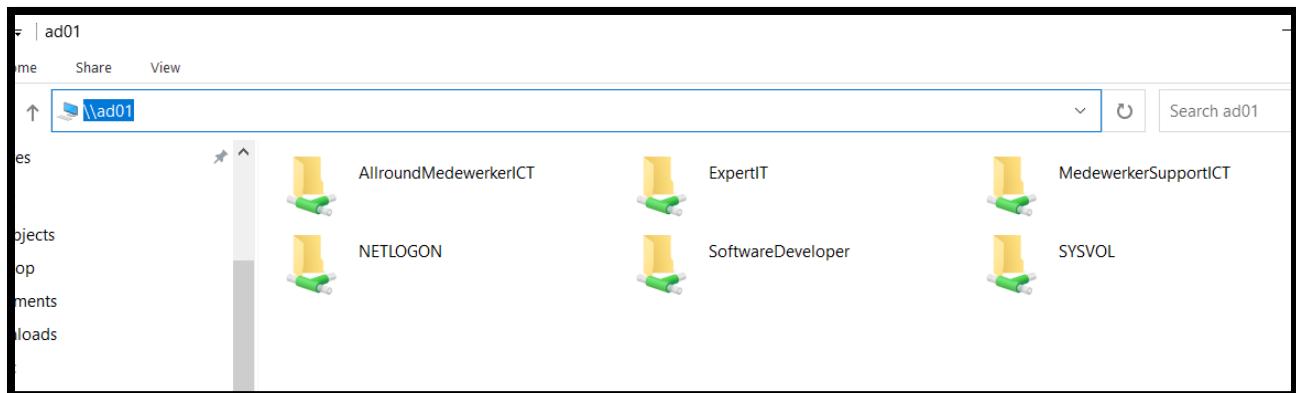
Op dat moment, ga jij als beheerder, nooit meer vinden waar Jannes alles in zat en dus uit moet, laat je hem namelijk ergens zitten, heb je kans op een beveiligingslek en dat mag niet volgens de AVG natuurlijk.

*Stel dat je nu een Security Group **Directie** had gekoppeld aan de vier shares van James, dan had je heel eenvoudig James uit deze groep kunnen gooien en Jannes er in kunnen zetten. Deze groep was dan ook gekoppeld tijdens de groei van het bedrijf aan de andere 496 shares waardoor je dus later na de verkoop door Jannes, in 3 seconden had kunnen wisselen van directeur via de AD DS. Heel simpel en efficiënt. Als beheerder is het altijd belangrijk dat je dit in je achterhoofd houdt. Het moet tenslotte wel goed te managen blijven!*

Even een klein zijsprongetje, maar wel een heel belangrijke!

Je hebt nu de eerste share inclusief alle benodigde rechten helemaal goed ingesteld. Je ziet hem ook in de verkenner, dus dat is top! Nu ga jij ervoor zorgen dat de overige folders ook net worden gedeeld en ingesteld met de rechten. Succes en denk bij de shares aan de spaties!

Wanneer je klaar bent en je gaat op server AD01 of AD02 via de verkenner naar <\\AD01> dan moet je uiteindelijk dit te zien krijgen:

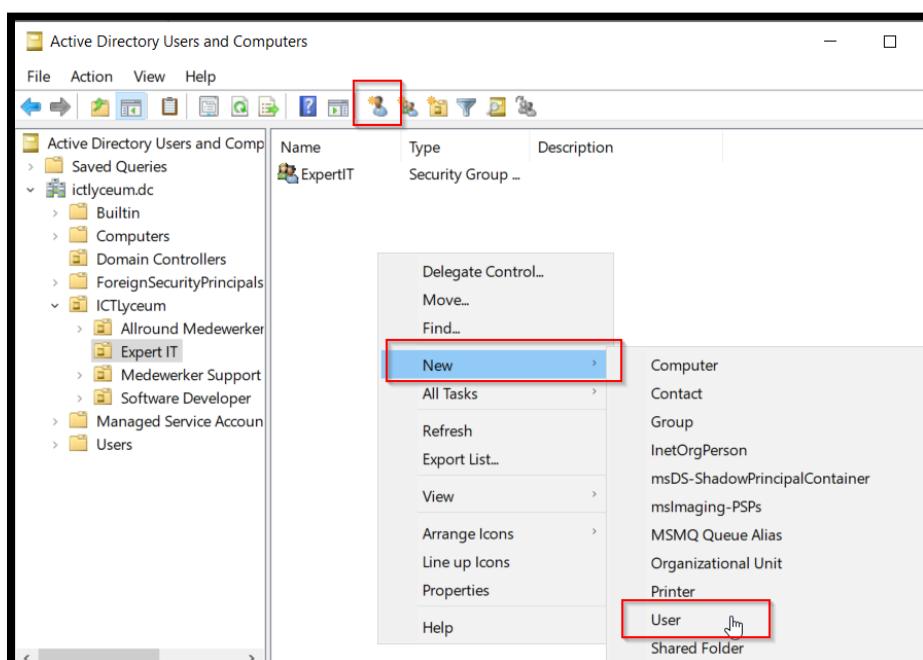


Nu we de shares af én werkend hebben, gaan we ook even kijken of we dit kunnen benaderen via onze client. We gaan hierbij inloggen als iemand die lid is van ExpertIT , zodat we gelijk kunnen zien of de rechten juist zijn ingesteld.

Aanmaken van gebruikers in het domein

Om hiermee te kunnen beginnen, is het noodzakelijk een gebruiker aan te maken in de AD DS. We openen via Tools **Active Directory Users and Computers**. Gezien het feit we willen testen met een Expert IT gebruiker, beginnen we in deze OU met het creëren van een nieuwe user. Na het aanmaken van deze, gaan we hem uiteraard direct koppelen aan de bijhorende Security Group, die is ertenslotte al!

In de juiste OU klik je met de rechter muisknop in het witte vlak óf op het poppetje bovenin de taakbalk. Je kiest in het menu voor **New -> User**:



In dit menu voer je simpelweg de gegevens van deze gebruiker in. In dit voorbeeld heb ik mijzelf genomen als gebruiker. Om het inloggen makkelijk te maken, heb ik ervoor gekozen om mijn (fictieve) personeelsnummer **9876** te gebruiken om in te loggen (bij **User logon name:**)

Jullie gaan je eigenaccount aanmaken met bij User Logon Name je studentnummer!

The screenshot shows the 'New Object - User' dialog box. It contains fields for First name (Jurry), Last name (Pijnaker), and Full name (Jurry Pijnaker). Under 'User logon name', the 'User logon name' field is set to '9876' and the domain dropdown shows '@ictlyceum.dc'. Below it, 'User logon name (pre-Windows 2000)' is set to 'ICTLYCEUM\9876'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Ik had er hier uiteraard ook voor kunnen kiezen om **J.Pijnaker** te gebruiken , of **JurryP** , maar op deze manier voorkom ik ten alle tijden dubbele namen, of namen als **J.Pijnaker2** of **JurryP2**. Is allemaal mogelijk, maar persoonlijk vind ik dit het fijnste/mooiste werken.

Wanneer we hier op Next drukken, moeten we een wachtwoord bedenken. Zoals de hele reder inmiddels kiezen we hier wederom voor **Welkom01!**

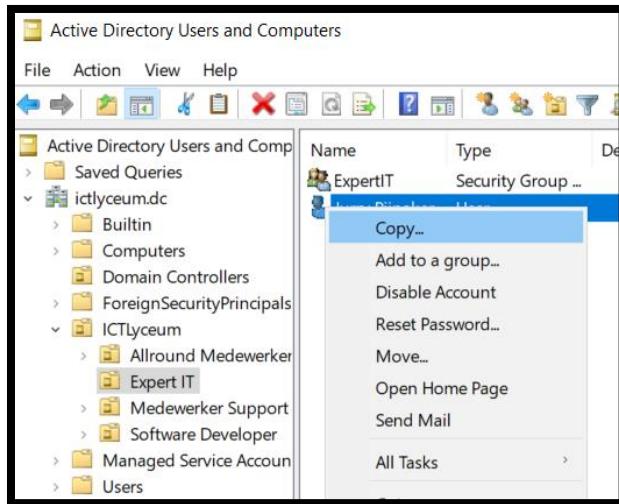
Het vinkje bij **User must change password at next logon** zetten we uit.

The screenshot shows the 'New Object - User' dialog box. It includes fields for 'Password' and 'Confirm' (both containing masked text). Below these are several checkboxes: 'User must change password at next logon' (which is checked and highlighted with a red box), 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Je krijgt nog even kort een overzicht te zien met de naam en inlognaam en dan is de gebruiker aangemaakt.

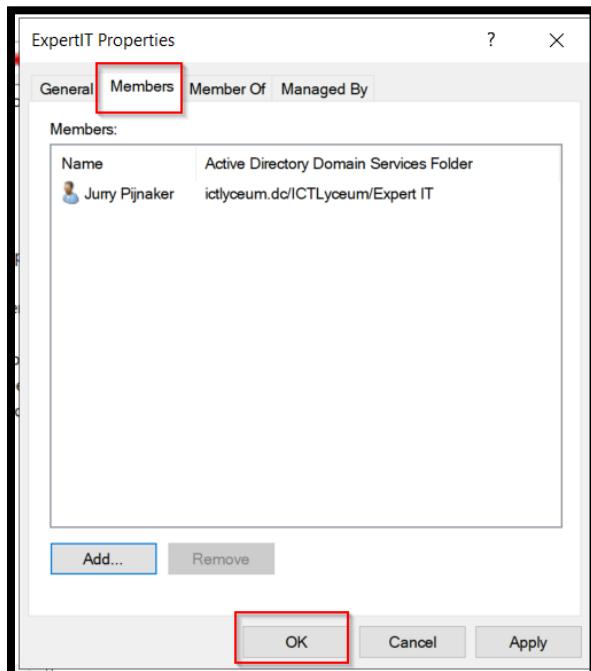
Heb je deze gebruiker nou helemaal klaar en lid gemaakt van de benodigde groepen etc. dan kun je deze gebruiker nu eenvoudig gaan kopiëren. Je klikt dan met de rechter muisknop op de naam en kiest voor **Copy**.

Erg handig wanneer je bijvoorbeeld Profile- en Homepaden hebt opgegeven. Deze neemt hij dan mee en past deze direct aan voor de nieuw aangemaakte gebruiker!



Door nogmaals even met de rechter muisknop te klikken op deze gebruiker en te kiezen voor **Add to a group** kunnen we dit nieuwe account gelijk gaan koppelen aan onze gewenste Security Group.

Ditzelfde kan overigens, door op Properties te klikken op de gewenste Security Group en in het tabblad Members onze gebruikers toe te voegen. De eerste optie (Add to a group) is handig bij 1 of 2 gebruikers. Wil je er meer toevoegen op hetzelfde moment is de tweede optie uiteindelijk sneller.



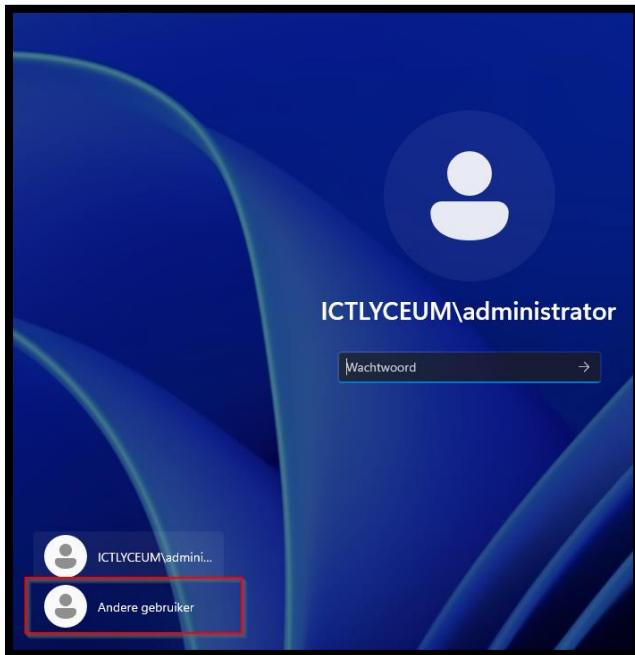
Nadat je op **OK** hebt geklikt, is deze gebruiker lid van de gekozen Security Group.

Zo simpel is het eigenlijk! Maak nu voor elke andere OU ook een gebruiker aan en koppel deze aan de juiste groep!

Inloggen Windows 11 workstation op domein

Nu we diverse gebruikers hebben aangemaakt, gaan we kijken of deze ook daadwerkelijk kunnen inloggen op het domein én natuurlijk of onze shares goed werken.

Wanneer de client is opgestart, kies je links onderin voor **Andere gebruiker**



Je logt vervolgens in met je studentnummer en **Welkom01!**

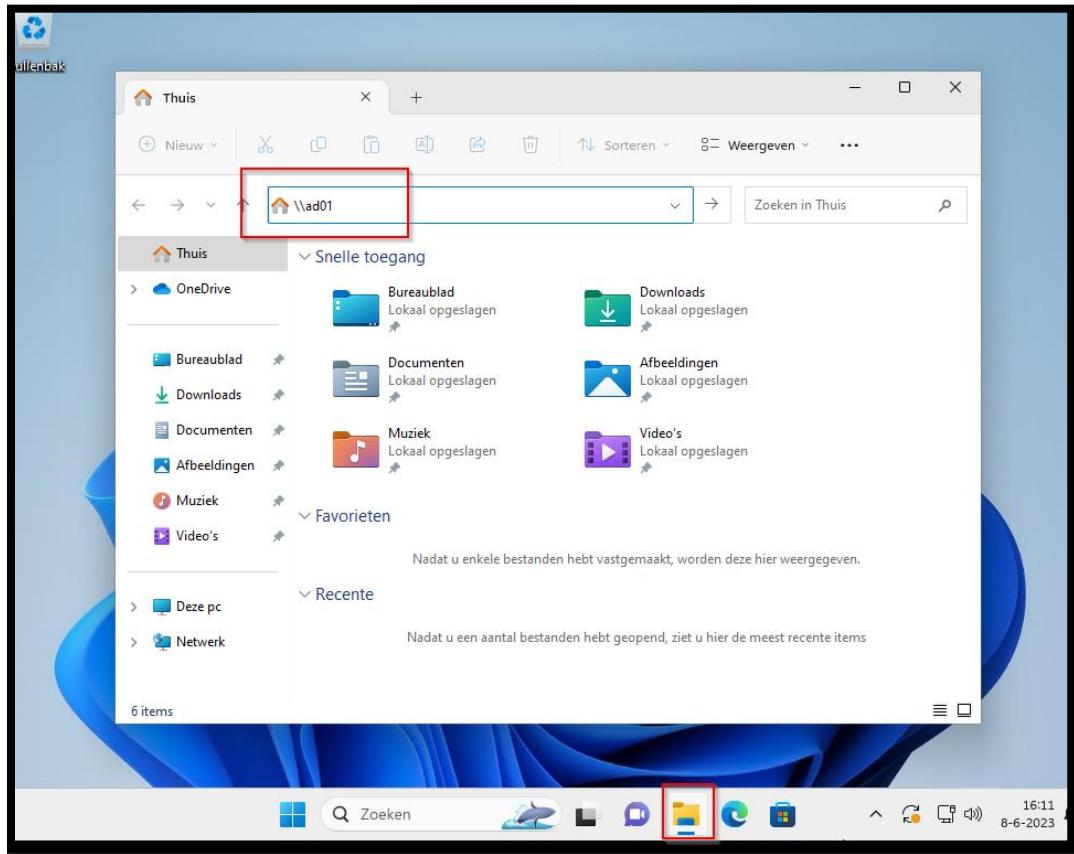
Je zult zien dat hij je nummer netjes koppelt vanuit de AD DS met je volledige naam en dat hij een profiel voor je aanmaakt. Dit kan even duren!



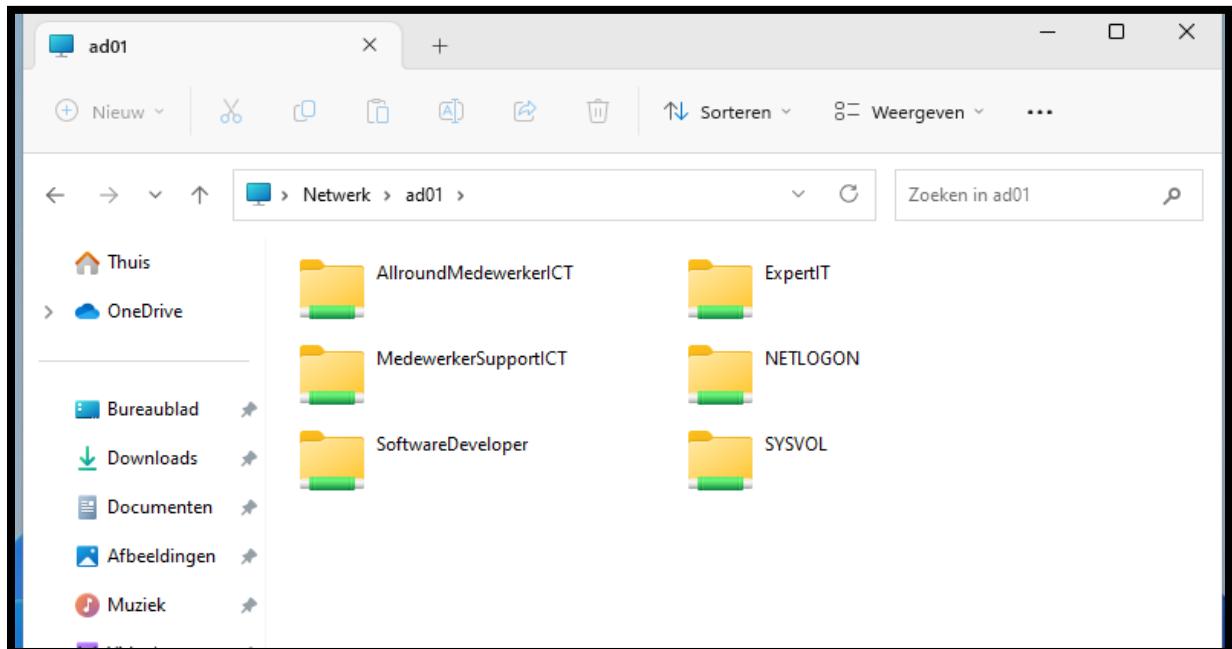
*Mocht je overigens ooit willen inloggen op een Windowsmachine met het administrator account uit je domein. Dien je altijd het domein ervoor te zetten zodat je zeker weet dat je op de juiste manier inlogt. Doe je dat namelijk niet en er bestaat een lokale account met de naam **administrator** dan gaat dat account ten alle tijden voor (!).*

*Dus gebruik altijd **domeinnaam\administrator**, in ons geval **ictlyceum\administrator** dus.*

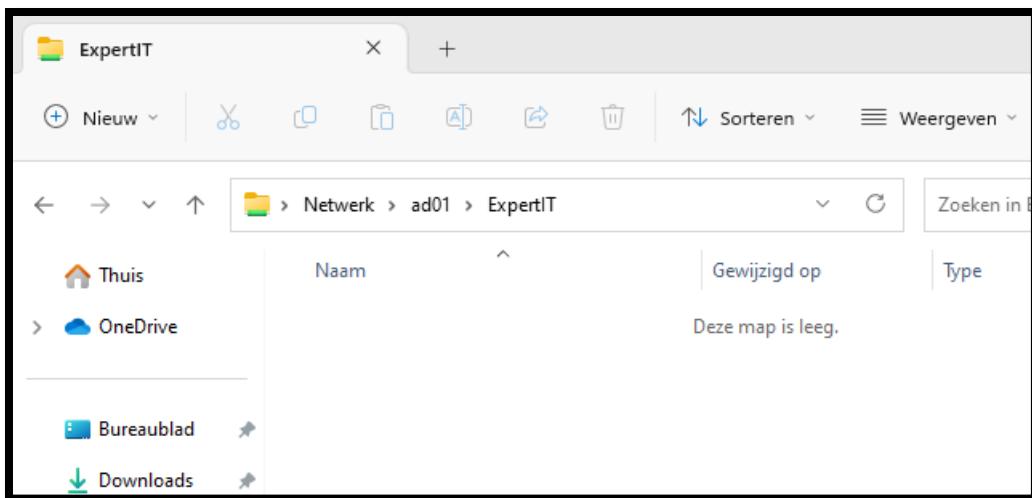
Zodra we zijn ingelogd openen we de verkenner en typen we in de browserbalk **\ad01** gevolgd door **ENTER**



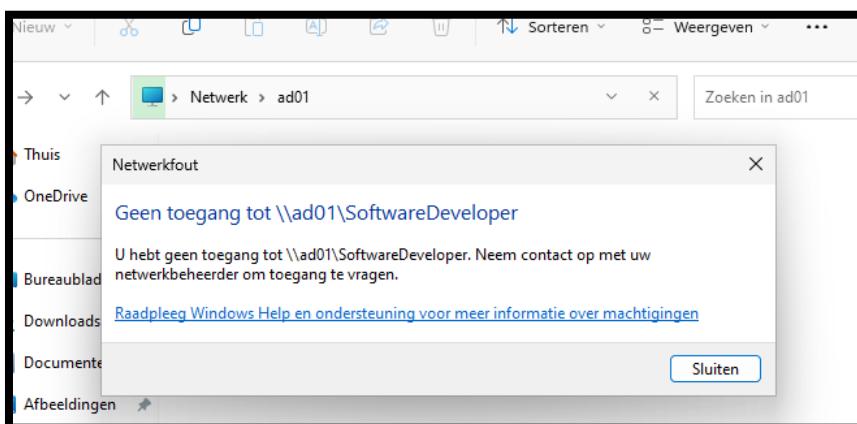
Je krijgt dan alle shares te zien, we zouden echter ALLEEN in de ExpertIT map mogen komen, dit testen we door simpelweg even die map én een andere te openen.



De **ExpertIT** map mag je openen als het goed is:



De **SoftwareDeveloper**- en de **MedewerkerSupportICT**-map niet. Als we een van die willen gaan openen (dubbel klikken) moet hij de onderstaande melding geven, gezien het simpele feit dat we hier geen toegang toe hebben:



Controleer of jij deze melding ook te zien krijgt. Krijg jij dit niet en mag je alle folders in, dan moet je de vorige stappen met rechten (Security tabblad) nog even goed doorlezen en mogelijk aanpassen.

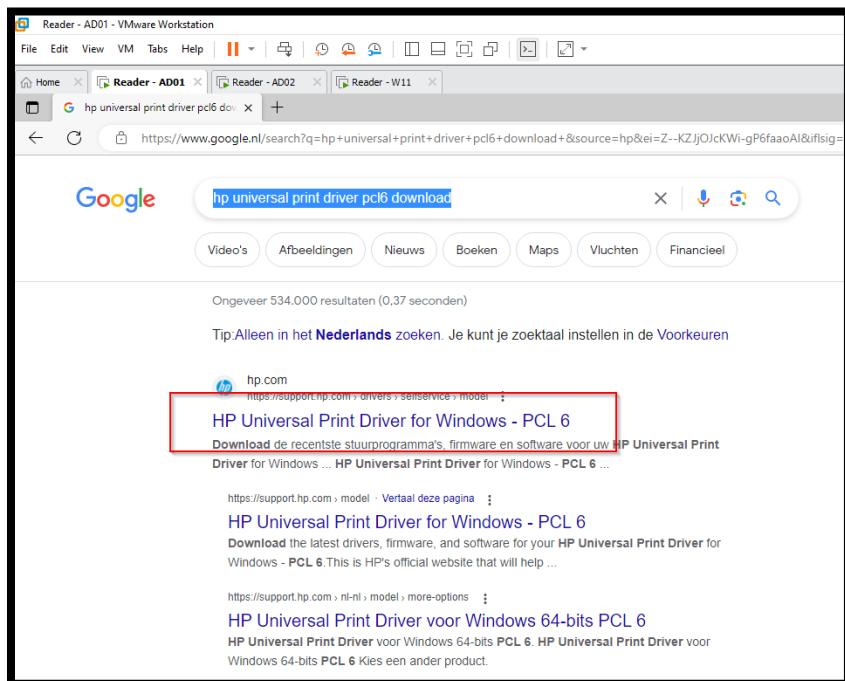
Nu we de folders, shares en rechten hebben aangemaakt, is het verstandig om even weer een snapshot te maken van de AD01! De andere twee hoeven niet perse, daar hebben we tenslotte niets aan gewijzigd!

Aanmaken én delen van een netwerkprinter

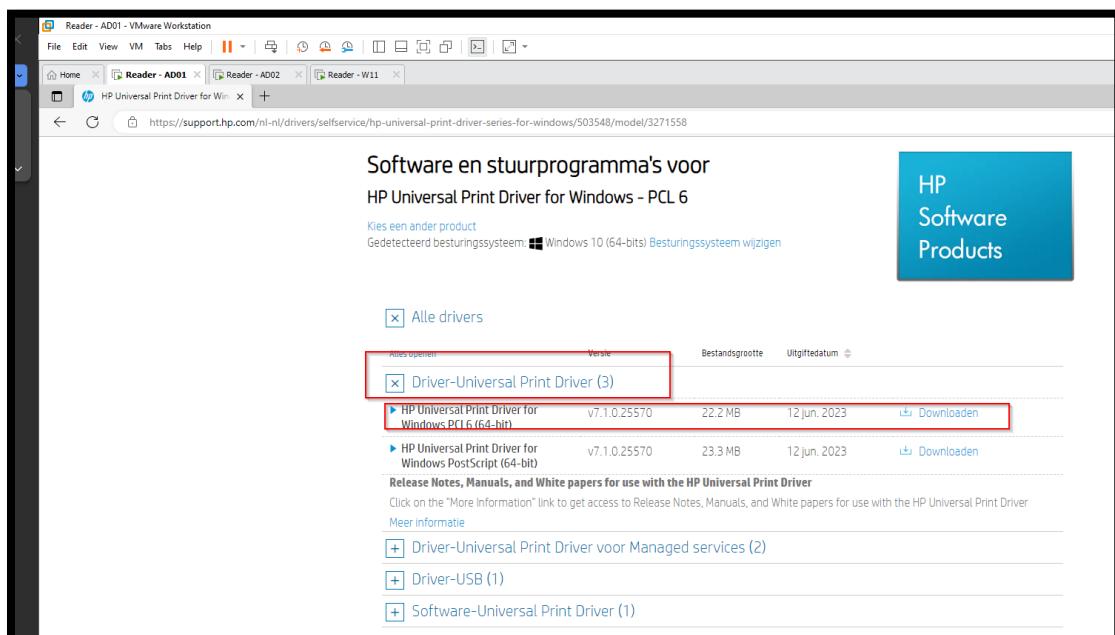
Nu we een netwerkshare hebben aangemaakt en hebben gedeeld, gaan we dit zelfde doen met een printer. Het idee daar achter is dat je snel en eenvoudig je netwerkprinter op die manier, door middel van een GPO (Group Policy Object, gaan we straks mee verder), de printer kunt delen via het netwerk zodat iedereen die dat nodig is die printer kan benaderen.

Om te beginnen hebben we hiervoor even een printerdriver nodig. Deze kunt je het beste downloaden bij de website van HP. Dit gaat dan om de **HP Universal Print Driver PCL6** (of nieuwere).

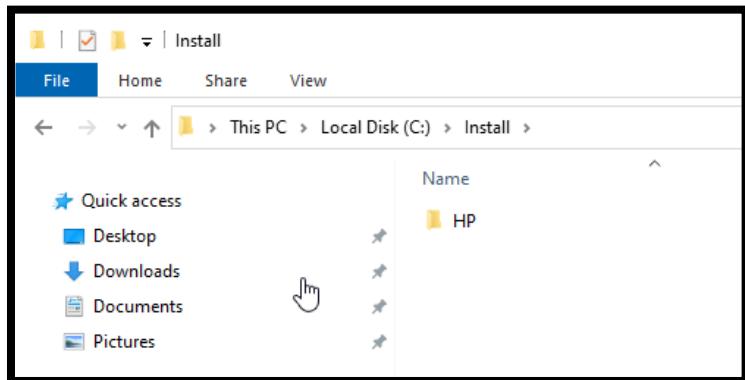
Als je via de AD01 het internet op gaat en dit in Google intypt, kom je er op de meest eenvoudige manier: **hp universal print driver pcl6 download**. Je kunt dan de eerste URL vaak aanklikken.



Je komt dan op de website van HP en kiest daar de nieuwste versie:



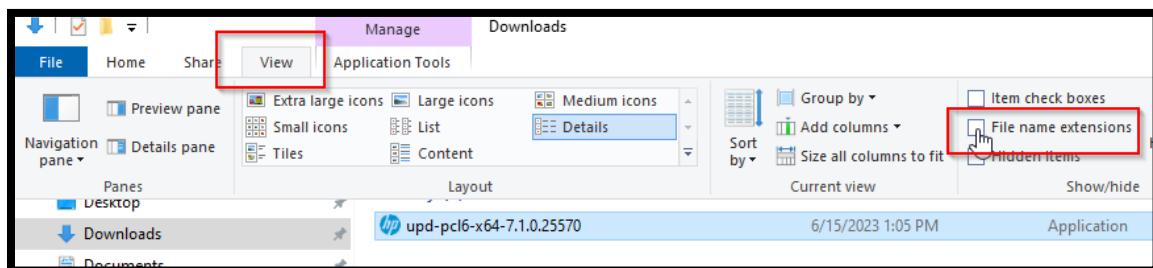
Nadat je dit bestand hebt gedownload, ga je het uitpakken naar een map die je eenvoudig kunt terugvinden. We maken hiervoor op de C:\ schijf van de server een mapje 'Install' aan met dáarin de map HP. Klinkt heel eenvoudig, maar op deze manier weet je altijd precies wat je waar staat en kun je het dus snel terugvinden. Deze Universal Print Driver kun je namelijk gebruiken voor bijna alle HP printers.



Het gedownloade bestand vinden we terug in de map Downloads, hij heet op moment van schrijven:

upd-pcl6-x64-7.1.0.25570.exe (de extensie **exe** betekent overigens **Executable**, wat staat voor 'uitvoerbaar') maar die veranderd vermoedelijk relatief vaak.

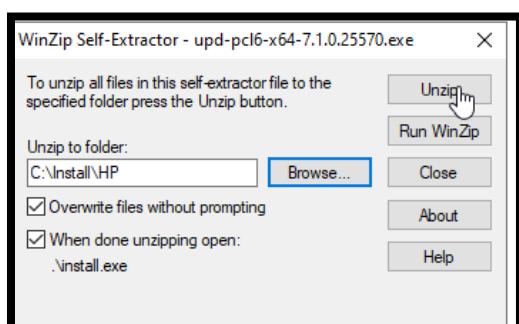
Mocht je overigens, net als in de afbeelding hieronder, niet zien wat de extensie-naam is (dit kan bijvoorbeeld zijn **.com** , **.bat** , **.zip** , **.rar** of **.exe**) dan kun je dit eenvoudig even aanzetten via het tabblad View in de verkenner en vervolgens even een vinkje te plaatsen bij **File name extensions**.



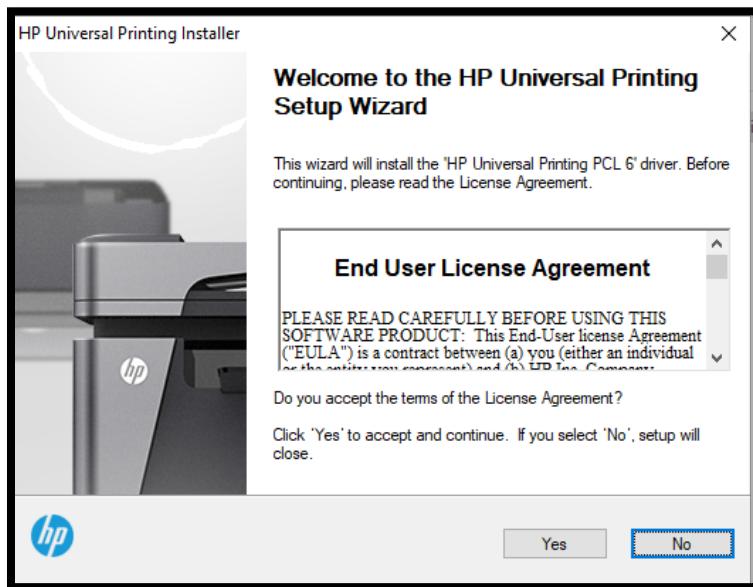
Ik vind het persoonlijk altijd erg prettig om direct te kunnen zien wat voor bestandstype ik heb/ga gebruiken, vandaar deze tip !

Terug naar het uitpakken van het bestand;

Als je het bestand **upd-pcl6-x64-7.1.0.25570.exe** opent, komt er een pop-up met waarmee je het bestand automatisch kunt uitpakken, je verwijst hiermee naar de zojuist aangemaakte folder en klikt op Unzip:

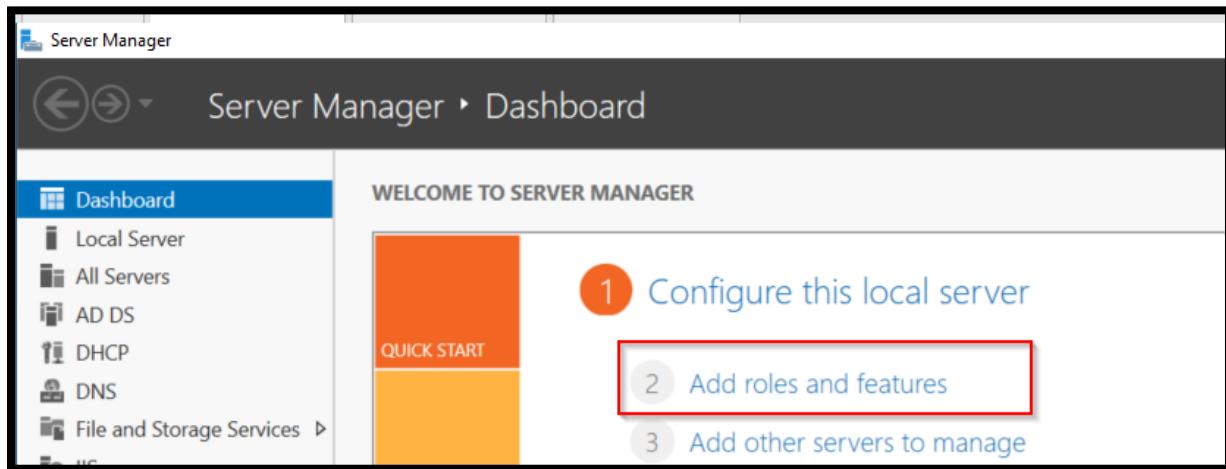


Na het ‘Unzippen’ (ofwel uitpakken) druk je op **OK** en zal er automatisch een HP Setup Wizard starten. Deze gaan we echter direct annuleren, we gaan het namelijk handmatig doen en dus drukken we op **No**.

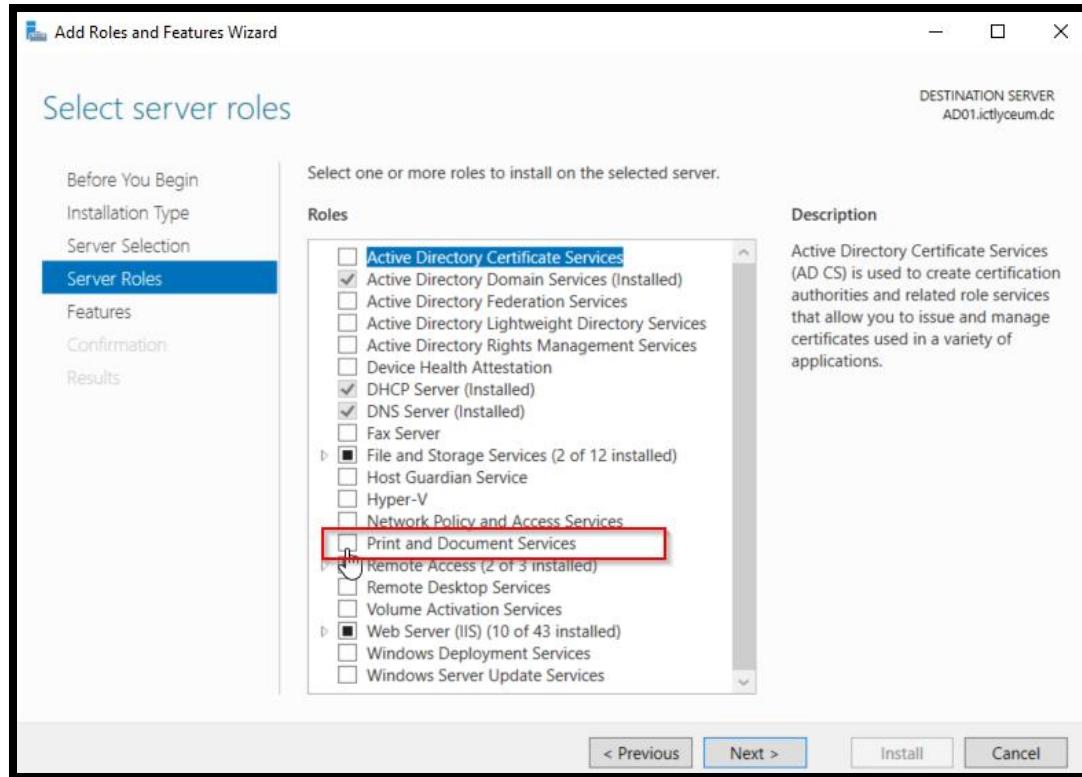


Nu we deze basis klaar hebben installeren we op de server waar we de printer mee willen delen (in dit geval dus de **AD01**) de Role **PrintManagement**.

We gaan dus naar de Server Manager en kiezen voor **Add roles and features** om dit te doen:



De wizard die je te zien krijgt kennen we inmiddels en dus klikken we gelijk door naar Server Roles. In dat lijstje gaan we opzoek naar de role **Print and Document Services**. Deze vink je aan en uiteraard accepteer je daarbij ook de bijhorende **Features**.



In de volgende stap, dienen we op te geven welke specifieke rol we graag willen gaan gebruiken. Hier voor selecteren we alleen Print Server, vervolgens kiezen we voor **Next** gevolgd door **Install**.

The left screenshot shows the 'Select role services' step of the wizard. The 'Role Services' list includes 'Print Server' (selected), 'Internet Printing', and 'LPD Service'. The right screenshot shows the Windows Start Menu with 'Print Management' highlighted.

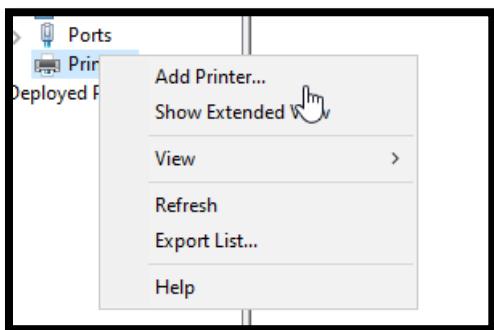
Na de installatie, hebben we onder de knop Tools de rol **Print Management** gekregen, deze openen we.

In deze nieuwe tool kunnen we onze netwerkprinter gaan aanmaken. Uiteraard is deze er niet echt, maar door middel van onze gedownloade drivers en een ‘nep’ IP-adres, kunnen we de realiteit zo goed mogelijk nabouwen. Onze printer, **Printer01**, krijgt IP-adres **192.168.101.20**. We gebruiken .20 aangezien onze DHCP-scope start bij .21 en we daaroor dus geen gezeur krijgen later.

Als we de Print Management hebben gestart, klappen we om te beginnen het menu onder **Print Servers** uit via de pijltjes aan de linkerkant, zodat we een open-menu structuur te zien krijgen. Dat zorgt voor wat overzicht en duidelijkheid.

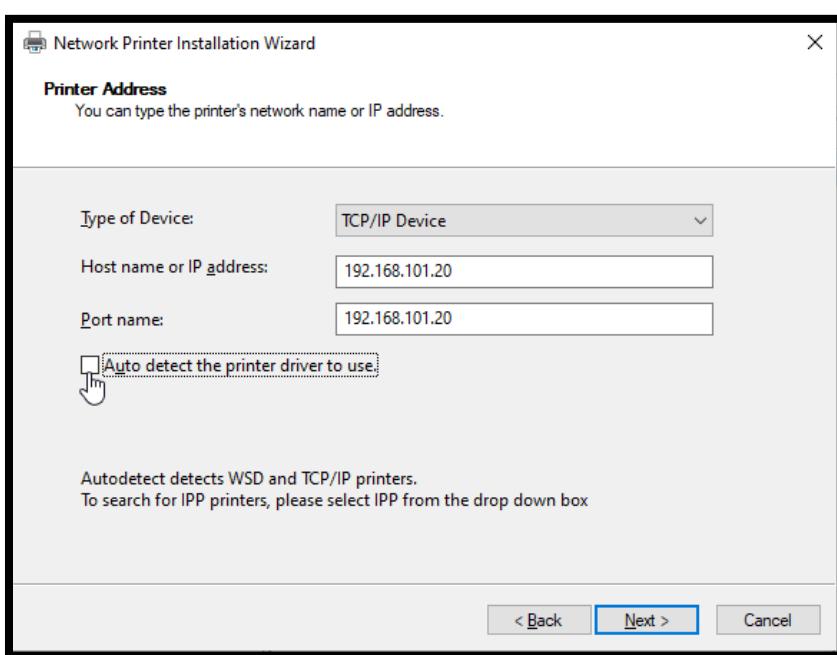
Als we op **Printer** klikken, dan zie we direct al 2 voor geïnstalleerde printers staan, deze zijn standaard van Microsoft om bijvoorbeeld een PDF aan te kunnen maken. We kunnen deze echter niet delen via het netwerk, dus daarvoor moeten we zelf aan de slag!

We klikken met de rechter muisknop op **Printer** en kiezen voor **Add Printer**

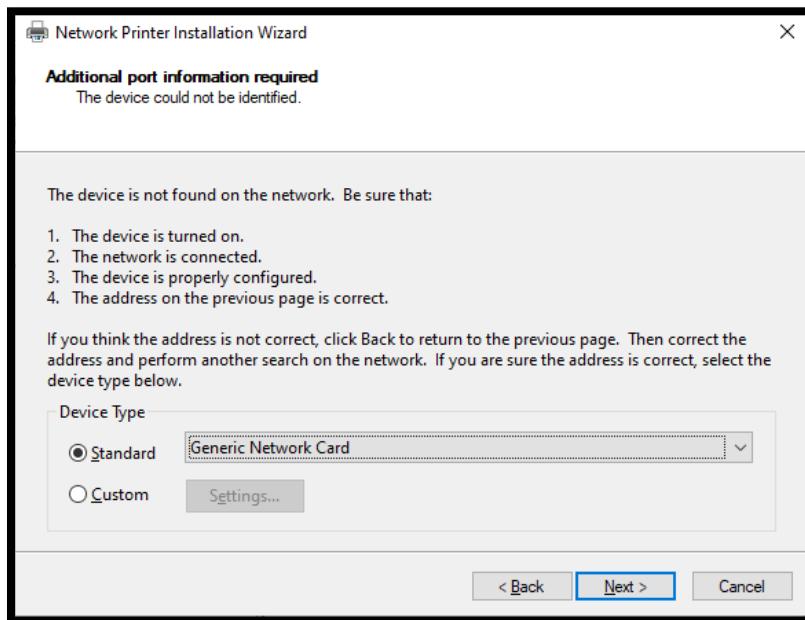


In de ‘Installation Wizard’ laten we de default optie ‘**Add an IPP, TCP/IP, or Web Services Printer by IP address or hostname**’ aangevinkt staan en kiezen we voor **Next**. We gaan zoals gezegd tenslotte een IP-adres opgeven en dus gaan we een TCP/IP-printer installeren.

In het daaropvolgende scherm kiezen we uit het dropdown menu dus voor **TCP/IP Device**, typen we het gekozen IP-adres in én zetten we het vinkje **UIT** bij ‘**Auto detect the printer driver to use.**’ Die moet uit, aangezien hij die printer nooit kan vinden in deze omgeving. Mocht je hem aan laten werkt het wel, maar kan het wel tot 5 minuten duren voordat hij dat zelf ‘door heeft’.



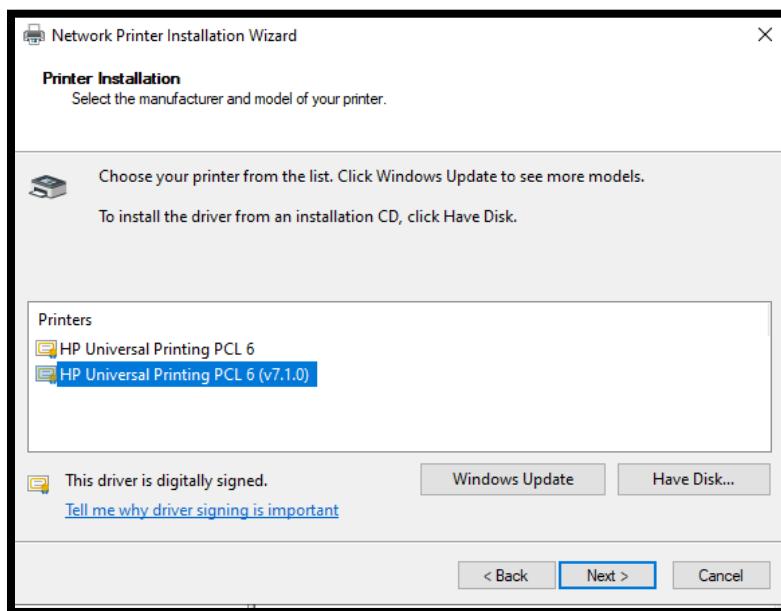
Vervolgens gaat Windows toch even zoeken/pingen naar dit IP-adres om te kijken wat voor device het is. We wachten even, ca. 30 seconden en daarna drukken we op **Next** wanneer er aangegeven wordt dat hij het device niet kan vinden. We veranderen daar verder niets.



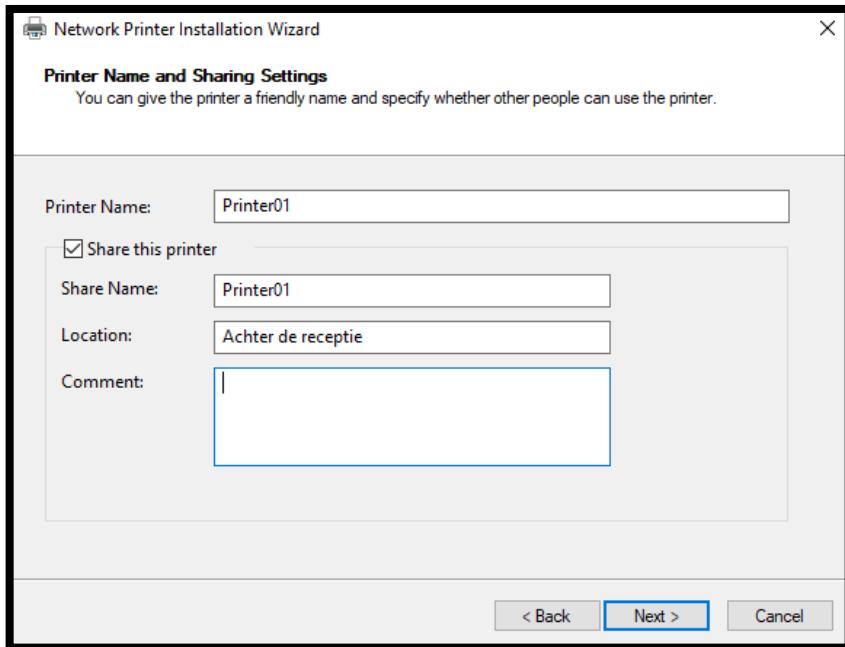
Vervolgens kunnen we aangeven wij zelf een driver hebben voor dit apparaat via **Install a new driver (gevolgd door Next)**.

We kunnen in het scherm daarna kiezen voor de knop **Have Disk...** dus daar klikken we op. In de pop-up die naar voren komt, gaan we via **Browse** naar onze driver map in C:\Install\HP en daarna kiezen we voor **Openen**. Welk bestand hier wel/niet wordt gekozen maakt weinig uit, dus daar hoeven we niet op te letten.

Wanneer je dus op **Openen** hebt gedrukt, gevolgd door **OK**. Zien we daadwerkelijk twee Universal Printing PCL6 drivers staan. Welke je hier kiest maakt weinig uit, men kiest echter meestal voor de nieuwste. Op dit moment van schrijven is dat v7.1.0. Deze selecteren we dus en we kiezen voor **Next**.

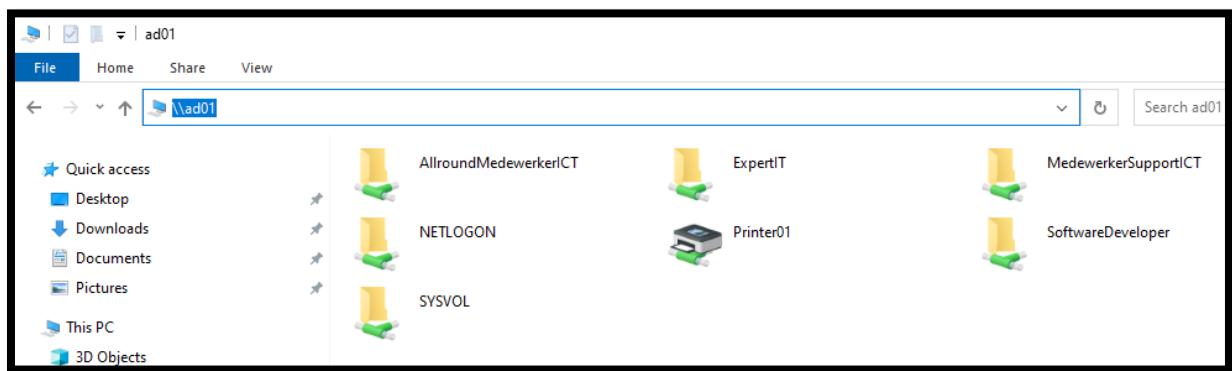


In het scherm daarop dienen we een printernaam mee te geven én een Share Name. Deze laatste naam is de naam die we in het netwerk gaan zien. We maken hier in beide gevallen **Printer01** van zoals eerder gezegd. Bij **Location** kun je eventueel iets nuttigs zetten over de locatie. Men kan dit namelijk zien in de eigenschappen van de netwerkprinter.



Als we alles juist hebben ingevoerd, kies je twee keer voor **Next** en dan zal Windows beginnen met de installatie van je eerste netwerkprinter.

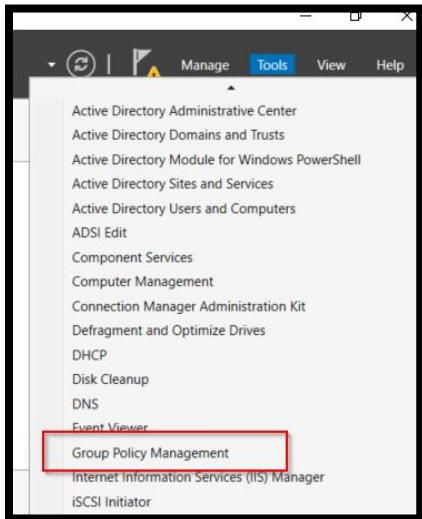
Wanneer hij klaar is en je gaat kijken via de verkenner bij <\\AD01> zal je zien dat er, naast de gemaakte netwerkmappen, nu ook een printer bij staat. Ook deze kunnen we dus vanaf nu gaan delen over het netwerk!



Uitdelen van shares en printers via GPO (Group Policy Management)

Nu we diverse shares hebben aangemaakt met de bijhorende rechten én ook een netwerkprinter hebben klaar gezet voor gebruik, is de volgende stap om deze te gaan “uitrollen” over het netwerk.

Dit gaan we doen via Group Policy Objects. Dit kan altijd gedaan worden via een domeincontroller, met behulp van de Tool **Group Policy Management**.



Group Policies, ofwel **GPO's**, kunnen eigenlijk gebruikt worden om álle binnen een organisatie te beheren in te stellen. Dus of je nu de achtergrond wilt wijzigen, wilt zorgen dat er een ander wachtwoordbeleid geldt of dat je wilt zorgen dat een pc standaard vergrendeld wordt na 5minuten inactiviteit, alles is hiermee in te richten.

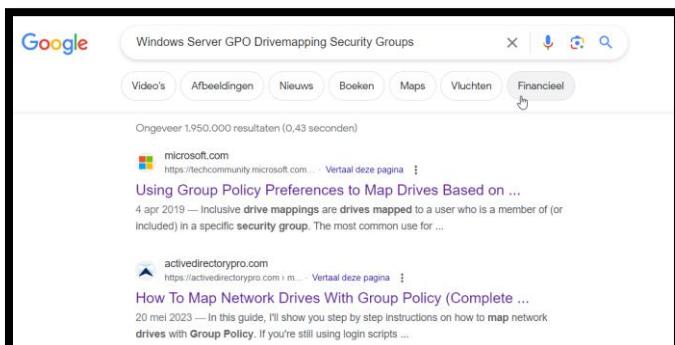
Deze inrichting is eigenlijk relatief eenvoudig, je moet alleen even goed weten wat je waar kunt vinden en hoe je het instelt. Ga je namelijk ‘op de gok’ op zoek naar “een instellingen” dan verdwaal je al snel in de oneindige mogelijkheden.

Een gouden tip die ik wil mee geven is het gebruik van Google en/of ChatGPT op de juiste manier én in het Engels. Ook ik kan, na vele jaren werken met GPO's, nog altijd slechts een heel kleine selectie uit mijn hoofd in 1x vinden en maak nog altijd gebruik van Google of ChatGPT als hulpbron.

In onze situatie willen wij graag gedeelde mappen delen over het netwerk én deze toegankelijk maken voor bepaalde groepen (onze Security Groups). Dan is onze zoekopdracht:

Windows Server GPO Drive mapping Security Groups

In de hits die je dan krijgt, vindt je 9 van de 10x een heldere uitleg inclusief plaatjes over hoe en waar je exact moet zijn.



Gooi je dit vraagstuk in ChatGPT dan zal deze exact uitleggen welke stappen je moet ondernemen. Het is dán echter wel belangrijk om aan te geven welke Windows Server versie je gebruikt, dus als **prompt** geef je dan bijvoorbeeld mee: **how to map drives at Windows Server 2022 GPO with Security Groups**

ChatGPT (Of welke andere AI-bot) geeft je dan een uitgebreide uitleg over hoe dit werkt en waar je moet klikken:

J. how to map drives at Windows Server 2022 GPO with Security Groups

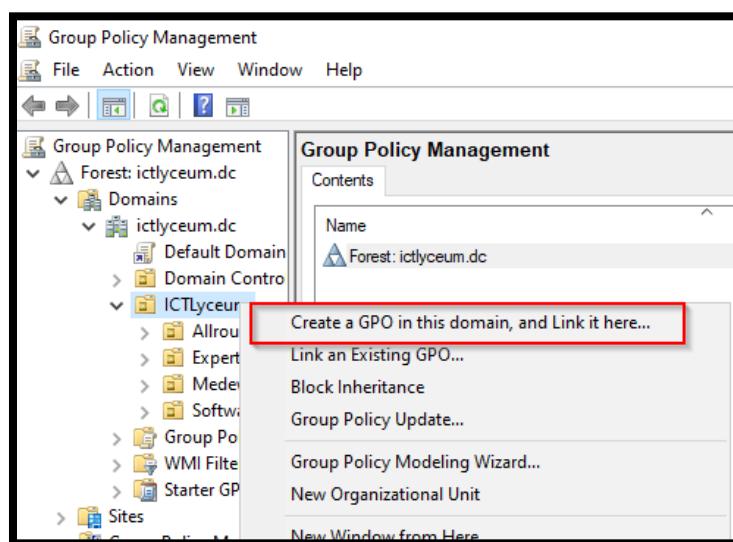
To map drives at Windows Server 2022 using Group Policy Objects (GPO) with Security Groups, you can follow these steps:

1. Open the Group Policy Management console on the Windows Server 2022.
2. Expand the domain and select the Organizational Unit (OU) where you want to apply the Group Policy.
3. Right-click on the OU and select "Create a GPO in this domain, and Link it here." Provide a name for the GPO and click OK.
4. Right-click on the newly created GPO and select "Edit."
5. In the Group Policy Management Editor window, navigate to "User Configuration" > "Preferences" > "Windows Settings" > "Drive Maps."
6. Right-click on "Drive Maps" and select "New" > "Mapped Drive."
7. In the "New Drive Properties" dialog box, configure the following settings:
 - * Action: Select "Update" to update existing mappings or "Create" to create new

Mocht je dus iets willen instellen, even schakelen naar Engels en dan zo op zoek gaan naar de juiste stappen. Voor het instellen van een achtergrond, zoek je dus bijvoorbeeld naar **Windows Server 2022 GPO wallpaper**.

Maar we gaan nu het instellen van de gedeelde mappen regelen. We openen hier dus om te beginnen de **Group Policy Management** onder Tools.

We klappen om te beginnen het hele domein even uit, totdat we onze eigen gemaakte [OU-structuur](#) kunnen zien. Op onze 'hoofd-OU' (ICTLyceum dus) klikken we vervolgens met de rechter muisknop en kiezen voor **Create a GPO in this domain, and Link it here...**

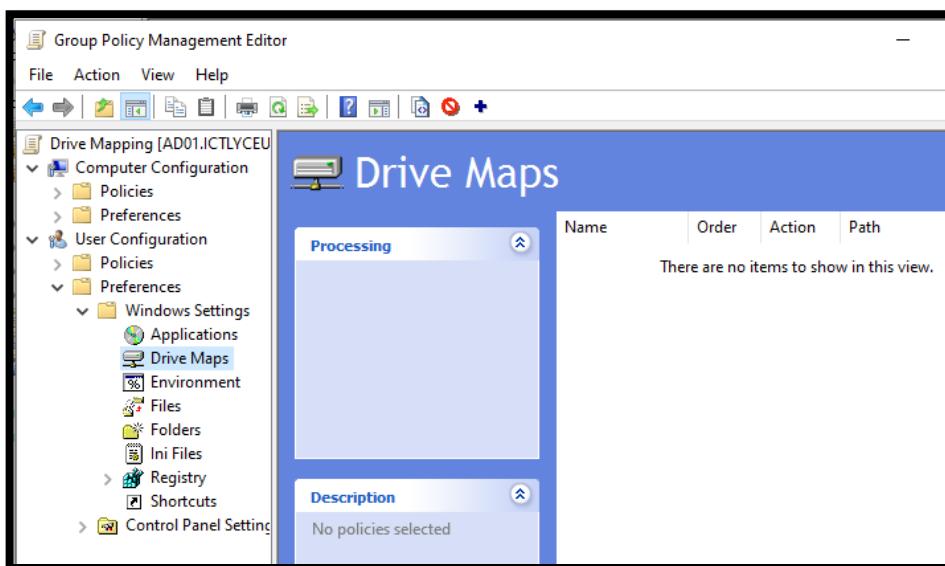


In de pop-up geven we een logische naam op, dus in dit geval **Drive Mapping**. Op die manier kunnen we altijd snel aanpassingen doen of dingen toevoegen aan de juiste GPO zonder te hoeven zoeken.

Je ziet ook dat hij gelijk wordt gekoppeld **ONDER** onze hoofd-OU. Zet je nou de GPO onder het gehele domein, dus rechtstreeks onder **ictlyceum.dc** dan betekend dit dan alle instellingen voor **iedereen** over het gehele domein gelden, dus ook voor de administrators.

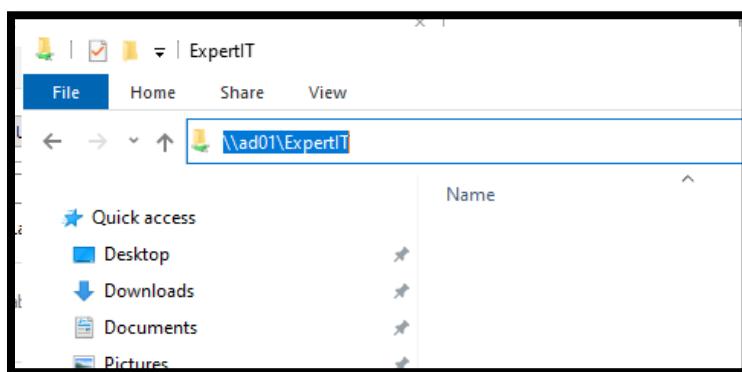
Dat is niet altijd een probleem wanneer je bijvoorbeeld drivemapping doet of een wallpaper gaat uitrollen, maar natuurlijk wél wanneer je er voor zorgt dat je de Command Prompt of USB gaat dichtzetten voor je gebruikers. Op dat moment mogen de beheerders van het domein, jij dus als Administrator, dat ook niet meer. Dus altijd goed opletten waar je ze plaatst!

We kiezen nu voor **Edit (uiteraard rechter muisknop)** op onze nieuwe policy en gaan opzoek naar het stukje Drive Mapping. Zoals ChatGPT hierboven uitlegt, moeten we dat zoeken onder **User Configuration, Preferences, Windows Settings -> Drive Maps:**



In dit scherm, onder **There are no items....** Klikken we met de rechter muisknop en kiezen we voor **New -> Mapped Drive**.

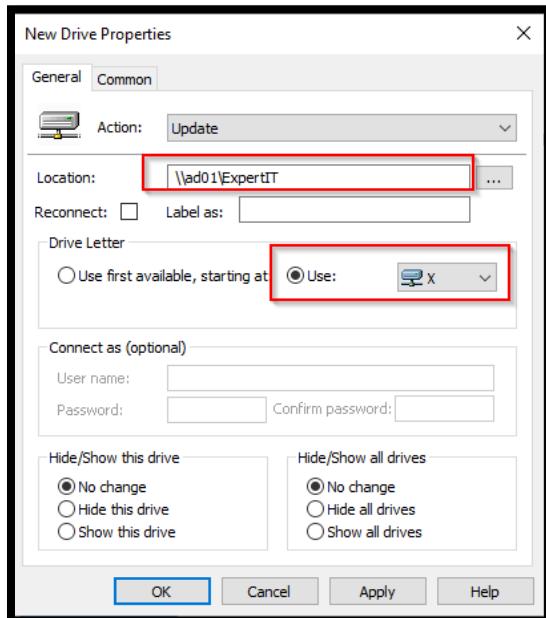
We gaan nu de pop-up invullen met onze eigen gegevens. De Location is onze gedeelde map, dus laten we daar invullen <\\ad01\ExpertIT>. Mocht je hier twijfelen over het exacte pad, open dan even de verkenner en ga naar <\\AD01>. Je ziet dan alle mapjes. Daarvan open je even een en vervolgens kun je bovenin de adresbalk het volledige adres nog even kopiëren 😊 !



Bij Action hoef je in principe niets aan te passen, dus die laten we op **Update** staan. Bij **Labels as:** kunnen we een naam meegeven, maar ook dat is op dit moment niet noodzakelijk. Bij **Drive Letter** gaan we een letter kiezen, dat is wel nodig. Omdat we gaan voor ExpertIT, kiezen we hier voor de optie **Use** en pakken we de letter **X**. Normaliter zou de letter **E** leuk zijn geweest, echter weet je nooit exact of deze reeds in gebruik is door een DVD-speler, een extra HDD of wat dan ook.

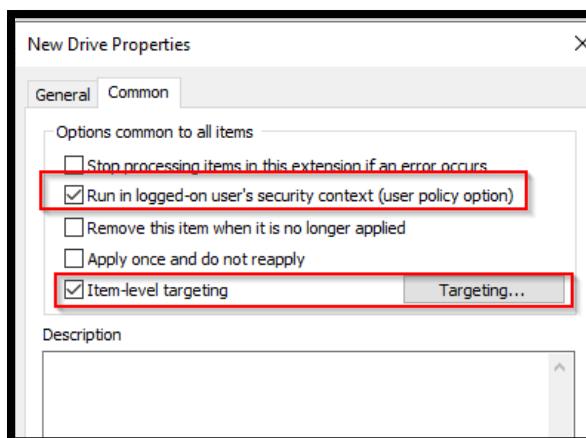
In de ‘regel’ delen we dan ook vaak pas uit vanaf de letter **F**. **A tot en met E blijven dus vrijwel altijd leeg!**

Nadat we dit hebben ingevoerd, ziet dit er dus zo uit;

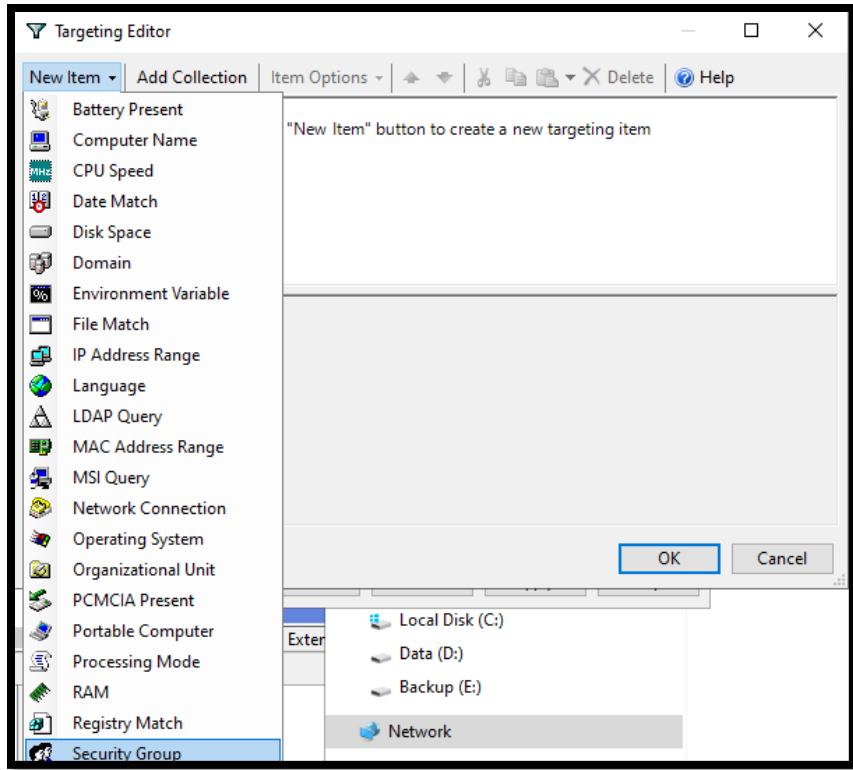


We klikken vervolgens op het tabblad **Common**. Waar we gaan zorgen voor een koppeling met de juiste groep. We willen tenslotte niet dat iedereen deze netwerkschijf straks te zien krijgt.

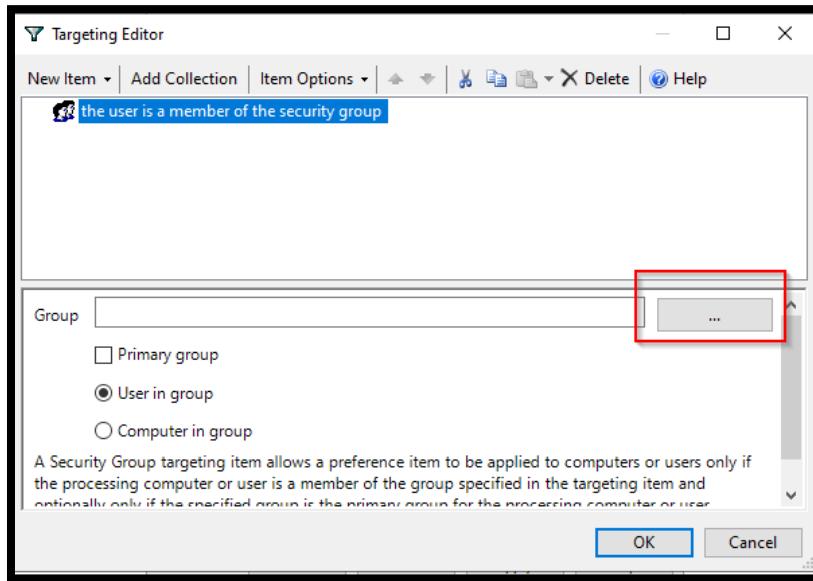
Bij Common zet je altijd een vinkje bij **Run in logged-on user's security context** en bij **Item-level targeting**. Vervolgens druk je dan (uiteraard) op **Targeting...**



Onder dat stukje Targeting zijn enorm veel opties beschikbaar wanneer je kiest voor **New Item**. Wij willen echter koppeling maken met een Security Group, dus die optie kiezen wij hier. Een andere optie kan bijvoorbeeld zijn dat je het per OU gaat koppelen, ook dat is prima!

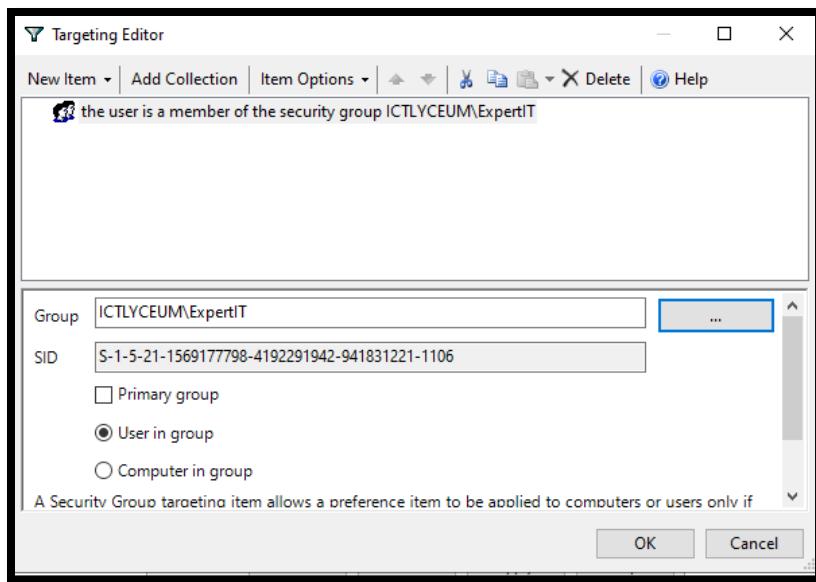


Zodra je op **Security Group** hebt geklikt, dien je op te geven om welke Group dit dan precies gaat. Hier voor klik je even op de drie puntjes aan de rechter kant:



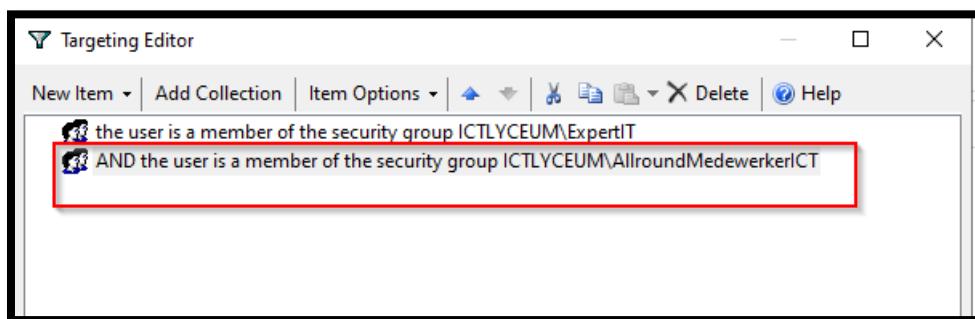
In die pop-up ga je op zoek naar de betreffende groep, in dit geval dus **ExpertIT**. Je kiest voor **Check Names** en vervolgens voor **OK**.

Je zult zien dat hij hem nu heeft aangevuld met je domeinnaam:

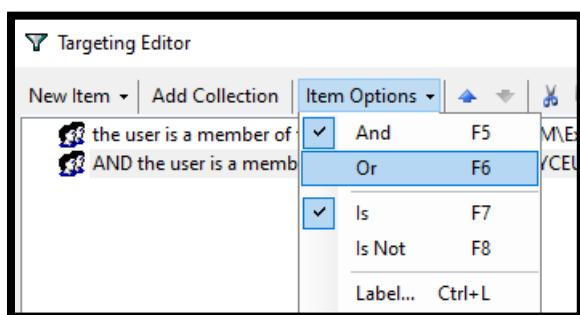


Mocht een andere groep nou óók toegang moeten hebben tot deze drive mapping. Dan kun je nogmaals op **New Item** drukken en wederom kiezen voor Security Group (OF bij gebruik van OU voor Organizational Unit) en daar hetzelfde kunstje doen.

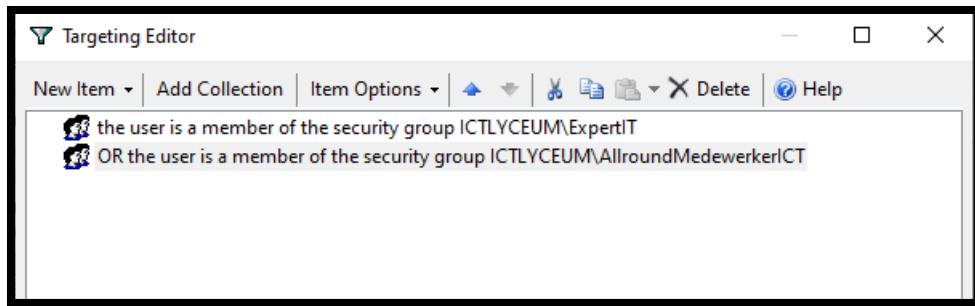
Bij ons is dat niet nodig, maar ik wil dit wel even toelichten omdat hier heel snel een veel gemaakte fout insluipt. Microsoft vult deze tweede groep namelijk altijd aan met de **Item Option AND** waarmee we dus suggereren dat men deze drivemapping pas krijgt wanneer je lid bent van **ExpertIT** ÉN in dit voorbeeld **AllroundMedewerkerICT**



Dit is natuurlijk vrijwel nooit het geval en dus erg belangrijk hier goed op te letten. In dit geval moeten we de **Item Option** (in het midden van dit schermpje) aan gaan passen naar **OR**. Je bent tenslotte lid van ÓF ExpertIT ÓF AllroundMedewerkerICT. Heel eenvoudig, maar wel flink zoeken als je het niet weet!

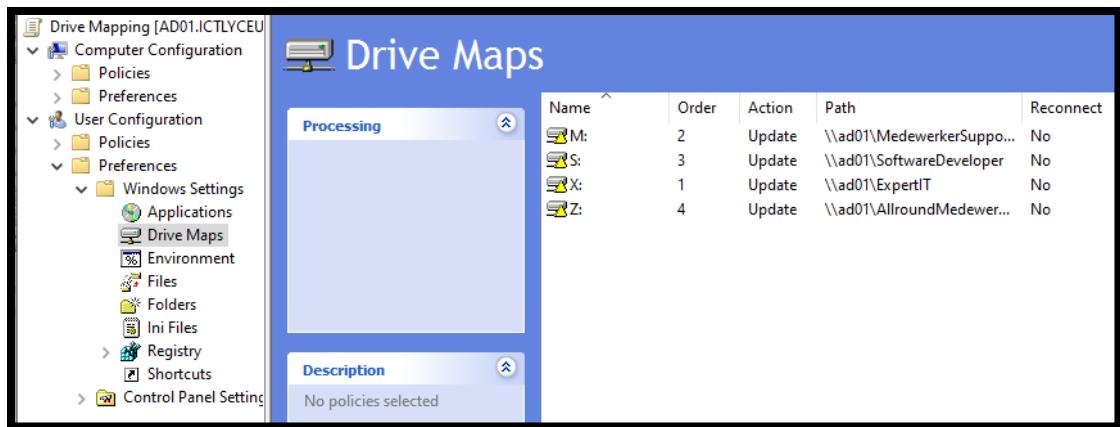


Uiteindelijk ziet het er dan dus **zó** uit met OR en niet met AND:



Maar goed, deze groep verwijder ik en ik kies voor **OK** gevolgd door **Apply/OK**.

De eerste drivemap is nu gemaakt en gekoppeld aan de juiste Security Group. Zorg er nu voor dat je de overige **drie** mappen ook op deze manier gaat uitdelen, zodat het er uiteindelijk zo uit ziet:



De Drive Mapping is nu klaar, wanneer we nu gaan inloggen op onze client kunnen we zien of het ook daadwerkelijk functioneert. Echter gaan we, voordat we dit doen, nog even kijken hoe we onze gedeelde printer kunnen meegeven.

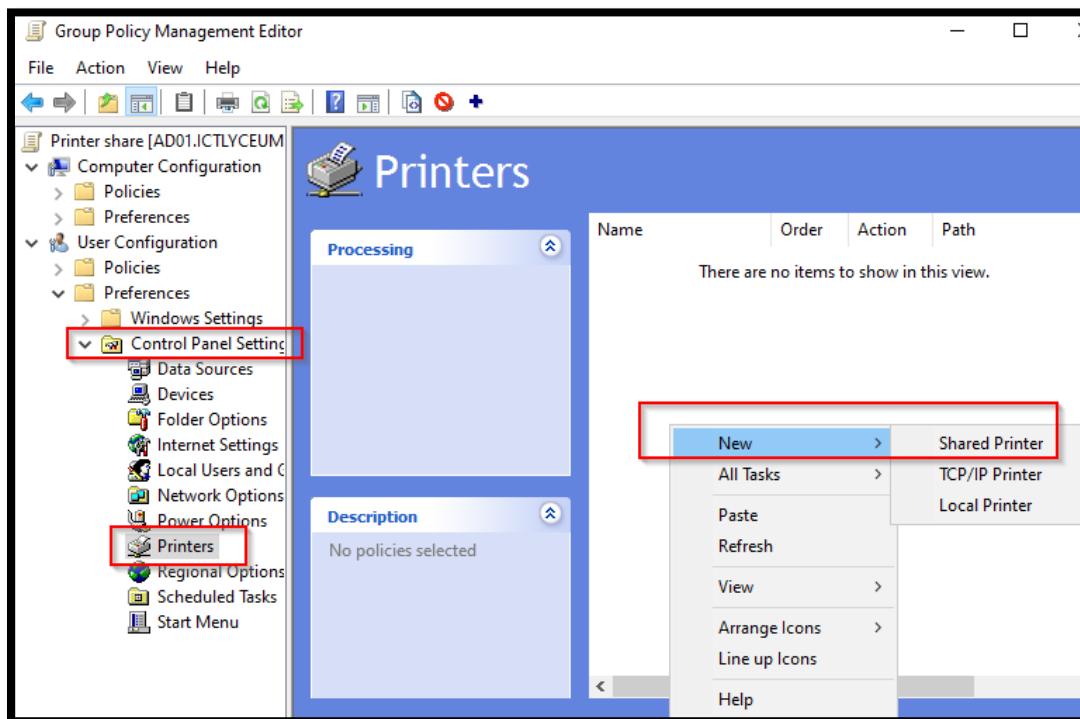
Hiervoor kunnen we wederom ChatGPT of Google vragen waar deze zich bevindt. ChatGPT geeft aan dat we hier moeten zoeken met de prompt: **how to share printers windows server 2022 by gpo under user configuration**. Ik zet hier bewust '*under user configuration*' bij aangezien ik de printer graag onder de configuratie van de gebruikers wil hebben zodat ik deze, wanneer gewenst, aan kan passen per group en eventueel zelfs per gebruikersnaam. Zet ik dat stukje er **niet** bij, dan is het standaard antwoord onder Computer Configuratie, en geldt de policy per computer en dus voor iedereen die daar inlogt.

Het antwoord van ChatGPT in dit geval is:

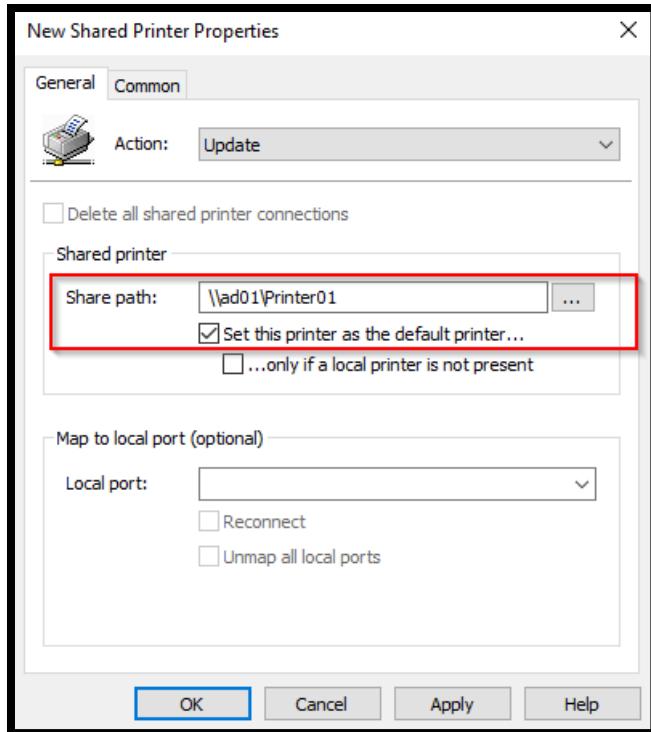
To share printers on Windows Server 2022 using Group Policy Objects (GPO) under the User Configuration, you can follow these steps:

1. Open the Group Policy Management console on the Windows Server 2022.
2. Expand the domain and select the Organizational Unit (OU) where you want to apply the Group Policy.
3. Right-click on the OU and select "Create a GPO in this domain, and Link it here." Provide a name for the GPO and click OK.
4. Right-click on the newly created GPO and select "Edit."
5. In the Group Policy Management Editor window, navigate to "User Configuration" > "Preferences" > "Control Panel Settings" > "Printers."
6. Right-click on "Printers" and select "New" > "Shared Printer."
7. In the "New Shared Printer Properties" dialog box, click on the "Shared Printer Path" field and either browse for the printer or enter the UNC path of the shared printer directly.
8. Configure additional settings as needed, such as setting the printer as the default or

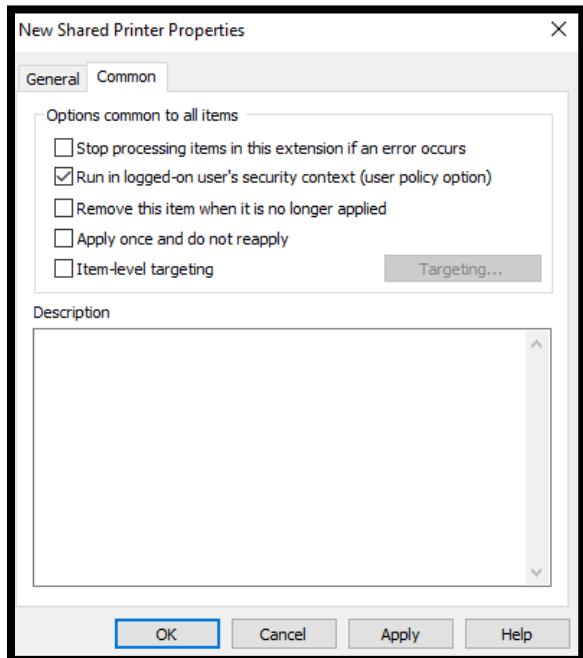
We gaan dus een nieuwe GPO maken met de naam '**Printer share**' (zoals gezegd; om overzicht te behouden) en vervolgens gaan we naar naar dit pad toe wat hier boven omschreven wordt. Daar kiezen we voor Printers en in dat witte vak kiezen we, net als bij de Drive Mapping voor -> New -> Shared Printer



In de pop-up plakken we onze share: <\\ad01\Printer01>, het vinkje bij 'Set this printer as the default printer...' zetten we hierbij aan.

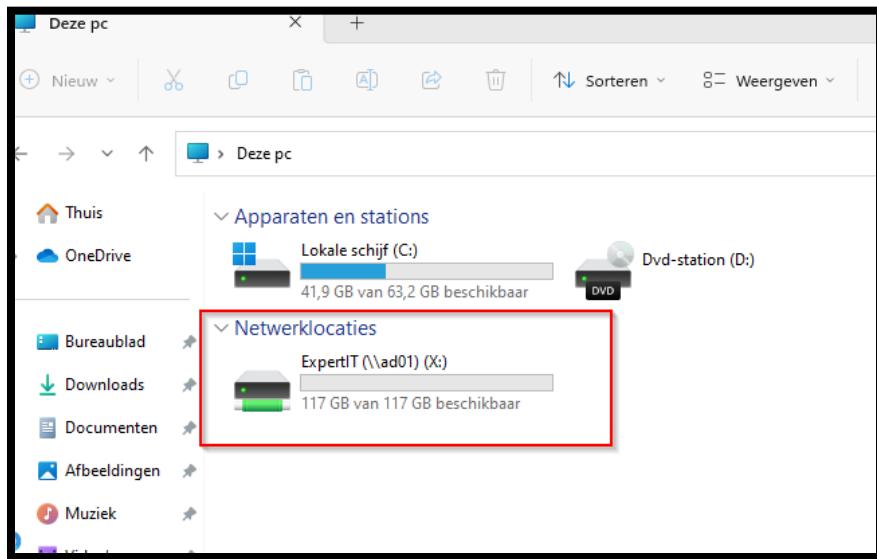


Uiteraard hebben we hier, onder het tabblad Common, wederom dezelfde mogelijkheden om de printer te koppelen aan een Security Group óf OU, echter in dit geval mag iedereen hem hebben dus gaan we dat niet gebruiken. Het enige wat we onder Common even moeten doen, is het vinkje plaatsen bij **Run in logged-on user's security context (user policy option)**



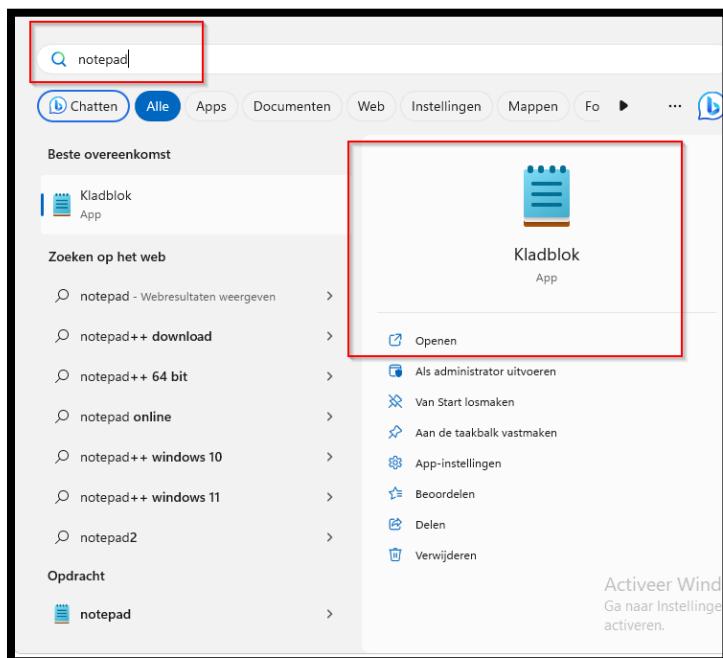
Om te testen of alles goed gaat, gaan we nu inloggen op onze client. We zouden daar dus nu een gedeelde map moeten krijgen én dus een gedeelde printer. Ik ga inloggen met mijn eigen account, die is aangemaakt onder de OU **Expert IT**, dus zou ik de shared drive X moeten krijgen, die verwijst naar de gedeelde map **ExpertIT**.

Na het inloggen openen we de Verkenner (het inmiddels welbekende gele mapje) en als het goed is zie je daar dan dus je gedeelde map staan zoals hieronder te zien is:



Het enige wat hier niet fijn is, is het feit dat hier de volledige schijf toegankelijk is, dus de 'gebruikers' kunnen hier op dit moment 117GB aan data op plaatsen. Dat is uiteraard niet iets wat je wilt in een échte omgeving, dus daar gaan we zo iets aan veranderen door gebruik te maken van Quota's.

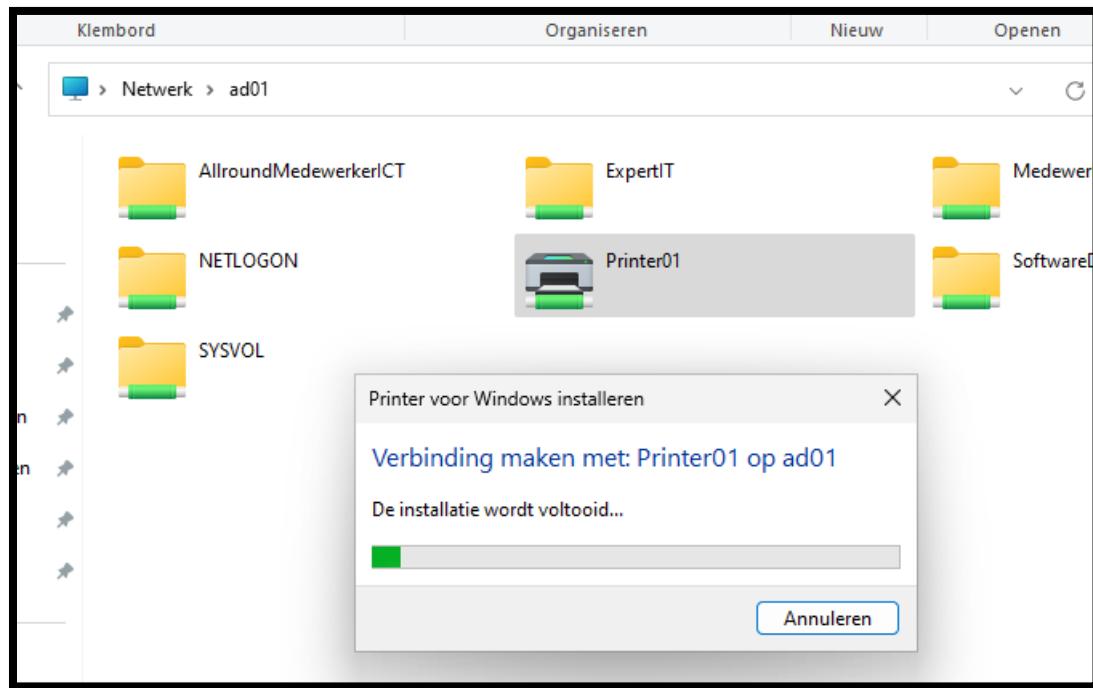
Eerst gaan we nog even controleren of de printer ook netjes gekoppeld is. Je kunt dit natuurlijk op verschillende manieren testen, maar de meest eenvoudige manier is even een Notepad.exe te openen via het Windows-menu en die proberen af te drukken.



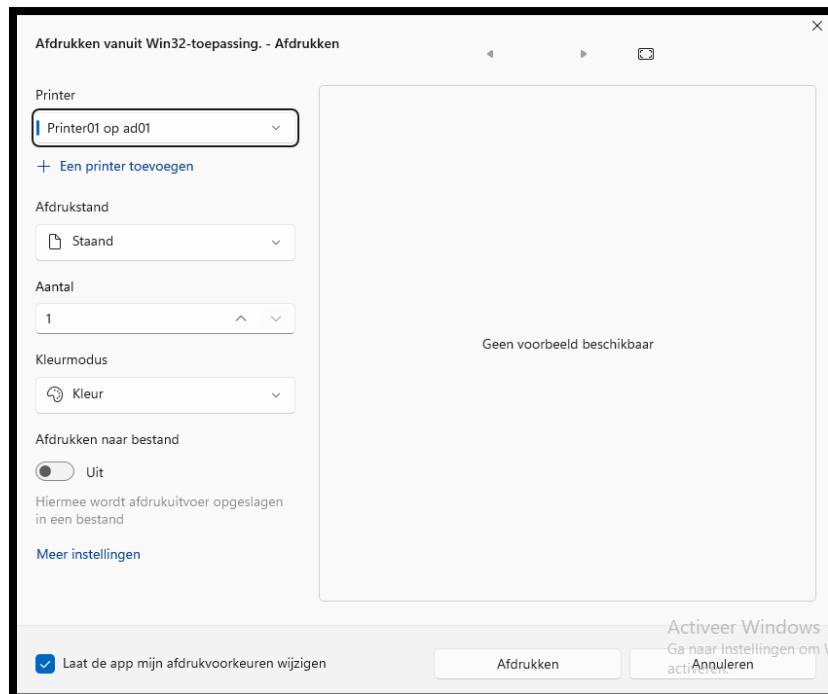
Je zet even iets in dit document, HOI bijvoorbeeld, en klikt op Bestand -> Afdrukken. Je moet dan de printer daar zien staan. Het kan echter voorkomen dat de Windows client de printerdriver niet herkend. Op dat moment kan hij de printer helaas niet automatisch toevoegen voor het gekozen account.

Om dit op te lossen dien je eenmalig in te loggen op de client als domein administrator (dus **ICTLYCEUM\Administrator**) en via de verkenner even dubbel te klikken op de betreffende printer wanneer je gaat naar \\AD01.

Op dat moment zal Windows via de server de benodigde drivers gaan ophalen en installeren, zodat het bij de volgende gebruiker wél goed gekoppeld kan worden. Wanneer je dubbel klikt op de printer, zal je dit in beeld krijgen:



Vervolgens kun je als gebruiker inloggen en heb je deze optie wanneer je wilt afdrukken



Je ziet nu netjes jouw **Printer01** op server **AD01** staan!

Toepassen van Quota's op gedeelde folders

Omdat je als beheerder niet altijd wilt dat alle schijfruimte daadwerkelijk gebruikt kan worden door je netwerkgebruikers, is het verstandig om gebruik te maken van Quota's. Quota's zijn eigenlijk limieten die je kunt plaatsen op een folder, waardoor hij, wanneer deze gedeeld wordt op het netwerk, minder groot lijkt/is dan zijn daadwerkelijke formaat.

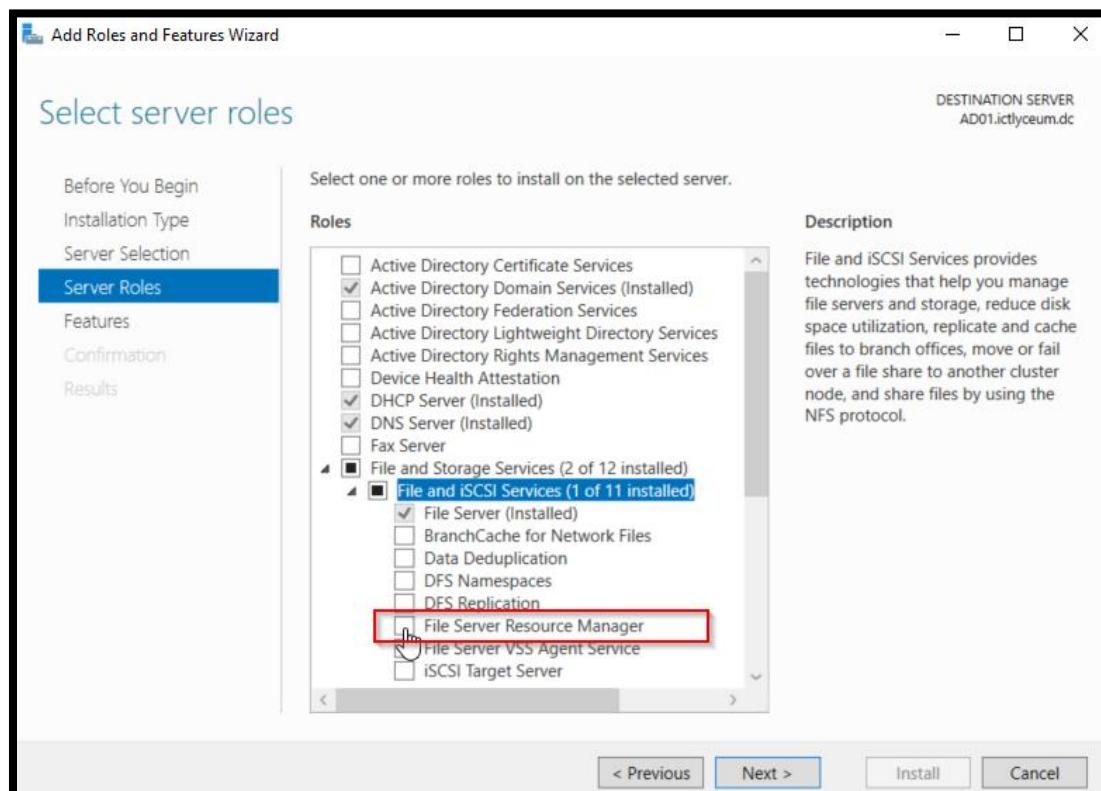
In de stappen hierboven zagen we al dat de gedeelde mappen 117GB beschikbaar hebben voor onze gebruikers. Ideaal dus voor privé foto's, vakantiefilmpjes en noem maar op... Uiteraard is dat niet de bedoeling, maar in de praktijk gaat dat wel zo!

Wanneer men namelijk alle privé data op de server plaatst, moet jij als beheerder ook zorgen dat dit netjes wordt meegenomen in de back-up, jij kunt tenslotte nooit bepalen wat er nu wel of niet belangrijk is voor een back-up, dus neem je eigenlijk altijd gewoon alle data mee.

Om dit dus een klein beetje in de gaten te houden, gaan we onze gedeelde mappen limiteren op 5GB per afdeling. Tevens zeggen we dat de afdeling Software Developer wat meer ruimte nodig is vanwege het enorme aantal scripts wat wordt geupload, die mogen dus een limiet van 10GB hebben.

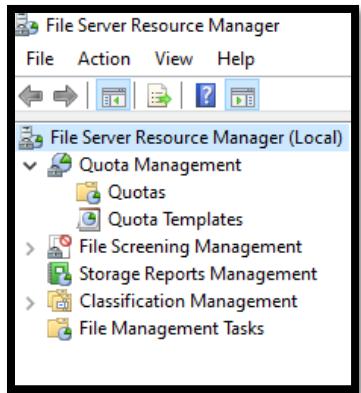
Om dit te realiseren maken we gebruik van de tool: **Fileserver Resource Manager**, of ook wel **FSRM** genoemd. Deze tool dien je altijd te installeren op de server waarop je daadwerkelijke folders zijn aangemaakt. Je kunt namelijk niet verwijzen naar een netwerkpad bij het toekennen van een quota, maar dus enkel naar een 'fysiek pad'.

Onze shares staan op dit moment op de server **AD01** dus hierop gaan we wederom, via Server Manager, een nieuwe rol installeren. Jullie weten inmiddels hoe dit werkt, maar deze zit wat verstopt; je vind hem hier:



Uiteraard installeer je hier wederom óók de bijhorende Features.

Na de installatie gaan we via de Server Manager naar Tools -> Fileserver Resource Manager. We klappen hier aan de linkerzijde Quota Management uit. Zoals je hier ziet, kun je met deze tool óók bestanden blokkeren op je netwerk via File Screening, maar dat is iets wat je later zelf kunt gaan uitproberen in een project bijvoorbeeld.

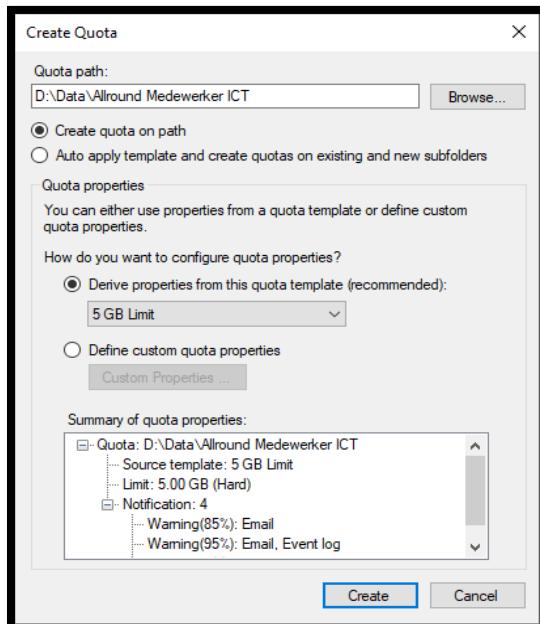


Wanneer je Quota Management hebt uitgeklapt, zie je dat je hier zelf eenvoudig quota-templates aanmaken onder **Quota Templates**. Dit gebruik je wanneer je bijvoorbeeld heel specifieke eisen of vreemde quota's als 2,75GB hebt.

Voor de gangbare quota's kun je gewoon gebruik maken van reeds bestaande templates. Voor onze omgeving kunnen we nu gewoon gebruik maken van de 5GB en de 10GB templates. Dus wij klikken met de **rechter muisknop** op het woord Quota's en kiezen voor **Create Quota**.

Via de knop **Browse...** blader je nu naar de specifieke folder waarop je een quota wilt zetten, in mijn geval kies ik dan de eerste en dat is: **D:\Data\Allround Medewerker ICT**

Ik laat tevens het balletje bij '**Create quota on path**' aan staan, omdat ik wil dat **alleen** dit specifieke pad een quota gaat krijgen en omdat hij mijn quota's bij eventuele andere mappen onder de map **Data** mogelijk anders gaan zijn (zoals dus bij Software Developer het geval gaat zijn).



We klikken op **Create** en we zien dat de Quota is aangemaakt!

Je zet nu dus puur en alleen een quota op de folder “**D:\Data\Allround Medewerker ICT**”, meer niet. Het nadeel van deze stap, is dat je hem voor elke folder moet gaan toepassen (dus nu ook nog bij ExperIT, Software Developer en bij Medewerker IT).

Quota Path	% Used	Limit	Quota Type	Source Template
Source Template: 5 GB Limit (1 item)				
D:\Data\Allround Medewerker ICT	0%	5.00 GB	Hard	5 GB Limit

Je ziet ook gelijk dat het Quota Type op **Hard** staat. Dit houdt in dat, wanneer de 5GB is aangetikt, er niets meer kan worden geplaatst op deze schijf. Hij zit écht vol.

Had je hier, dan in de template wel te verstaan, gekozen voor **Soft**. Dan kun je, ondanks hij de 5GB aan data had bereikt, gewoon rustig doorwerken, je krijgt dan enkel een waarschuwing. Altijd even goed opletten dus! Want eigenlijk heb je zogezegd weinig aan die Soft-quotas, die zijn dus vooral mentaal een barrière.

Ga je nu bijvoorbeeld een quota aanmaken bij persoonlijke (home) folders van gebruikers, want daarbij heeft tenslotte iedereen dezelfde limieten, dán kun je het balletje zetten bij **Auto apply template and create quotas on existing and new subfolders**.

Bij die tweede optie hoef je deze stap namelijk slechts 1x in te stellen en zorgt de FSRM ervoor dat elke onderliggende map automatisch de 5GB als quota krijgt, ook bij het aanmaken van een extra nieuwe map! Eigenlijk wel ideaal dus, tenzij je 1 folder net even iets anders wilt gaan instellen.

Vaak wordt die tweede optie dus alleen gebruikt bij persoonlijke folders/homedrives. Mochten wij nou aan het begin **niet** hebben gezegd dat de folder Software Developer een andere quota moest hebben, hadden wij die 5GB quote eenmalig moeten plaatsen op de map **D:\Data** en had elke onderliggende map automatisch een quota gehad van 5GB, zo simpel is dat...

Wanneer je dat zou doen, dan zou het er zo uit gaan zien (let op het ***-teken** bij het pad)

Quota Path	% Used	Limit	Quota Type	Source Template
Source Template: 5 GB Limit (5 items)				
D:\Data*	---	5.00 GB	Hard (Auto Apply)	5 GB Limit
D:\Data\Allround Medewerker ICT	0%	5.00 GB	Hard	5 GB Limit
D:\Data\Expert IT	0%	5.00 GB	Hard	5 GB Limit
D:\Data\Medewerker Support ICT	0%	5.00 GB	Hard	5 GB Limit
D:\Data\Software Developer	0%	5.00 GB	Hard	5 GB Limit

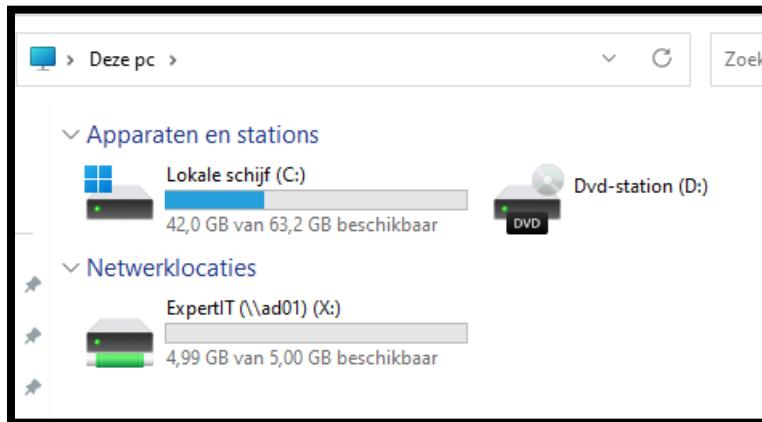
Hier vult hij elke nieuwe map zelfstandig aan en heb je er dus geen werk van ! Het is in deze dus alleen **niet** mogelijk om ‘even’ een uitzondering te maken voor Software Developer. Wat dus wel kan bij het aanmaken van individuele quota’s.

Zorg ervoor dat je alle aangemaakte mappen nu gaat limiteren op 5GB en de Software Developer op 10GB.

Uiteindelijk moet dit er dus zo uit gaan zien:

Quota Path	% Used	Limit	Quota Type	Source Template
Source Template: 10 GB Limit (1 item)				
D:\Data\Software Developer	0%	10.0 GB	Hard	10 GB Limit
Source Template: 5 GB Limit (3 items)				
D:\Data>Allround Medewerker ICT	0%	5.00 GB	Hard	5 GB Limit
D:\Data\Expert IT	0%	5.00 GB	Hard	5 GB Limit
D:\Data\Medewerker Support ICT	0%	5.00 GB	Hard	5 GB Limit

Gaan we even snel terug naar de Client en openen we daar de verkenner (opnieuw/refresh) dan zie je dat de quota per direct wordt toegepast op de gekoppelde share(s):



Uitdelen van achtergrond en instellen van beveiliging via GPO

Nu we via de GPO drive mappings hebben uitgedeeld is het een kleine stap naar de wallpaper. Het is zoals eerder benoemd dus mogelijk om alle instellingen van de computers binnen je netwerk via de GPO aan te passen, dus uiteraard ook de achtergrond en een deel van de beveiliging van de werkstations.

Instellen achtergrond via GPO

Om dit uit te voeren moeten we slechts drie dingen doen:

Stap 1 – Een share maken waarin de achtergrond staat en welke voor iedereen bereikbaar is

Stap 2 – Een achtergrond maken

Stap 3 – De wallpaper-optie vinden en instellen in een (nieuwe) GPO

Stap 1:

Om te beginnen gaan we een nieuwe share maken in onze D:\Data\ map op de server, waarin we straks onze achtergrond(en) kunnen plaatsen. De map gaan we gelijk delen maar we laten de NTFS-rechten (tabblad security) zoals het is. Standaard mogen, zoals je weet, alle domeingebruikers

namelijk in een nieuwe map, dus dat is in dit geval ideaal, we willen hem tenslotte voor ‘iedereen’ gaan toepassen!

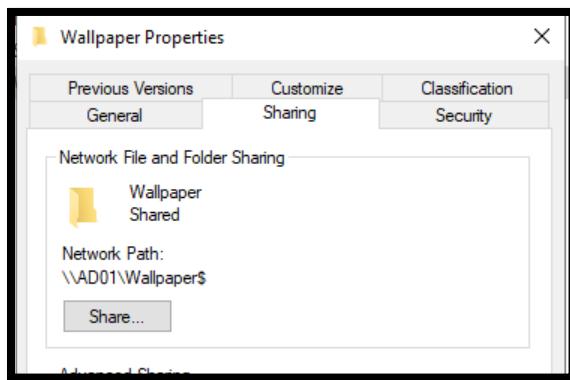
De nieuwe map noemen we **Wallpaper** en de share krijgt dezelfde naam, MAAR we voegen hier het **\$-teken** achter, zodat deze share ‘hidden’ (verborgen) wordt wanneer men op het netwerk gaat kijken.

De sharename wordt dus letterlijk: **Wallpaper\$**

Deze share is dus standaard niet te zien wanneer men via de verkenner naar <\\AD01> gaat, maar enkel toegankelijk wanneer je hem volledig intypt. [\\AD01\\Wallpaper\\$](\\AD01\\Wallpaper$) dus..

De share rechten zijn, zoals altijd; **everyone -> read + write** (In theorie zou in dit geval enkel **read** ook kunnen, er wordt tenslotte niets in deze map geschreven via het netwerk, maar laten we het uniform houden en gewoon de basisregel toepassen met **read + write**).

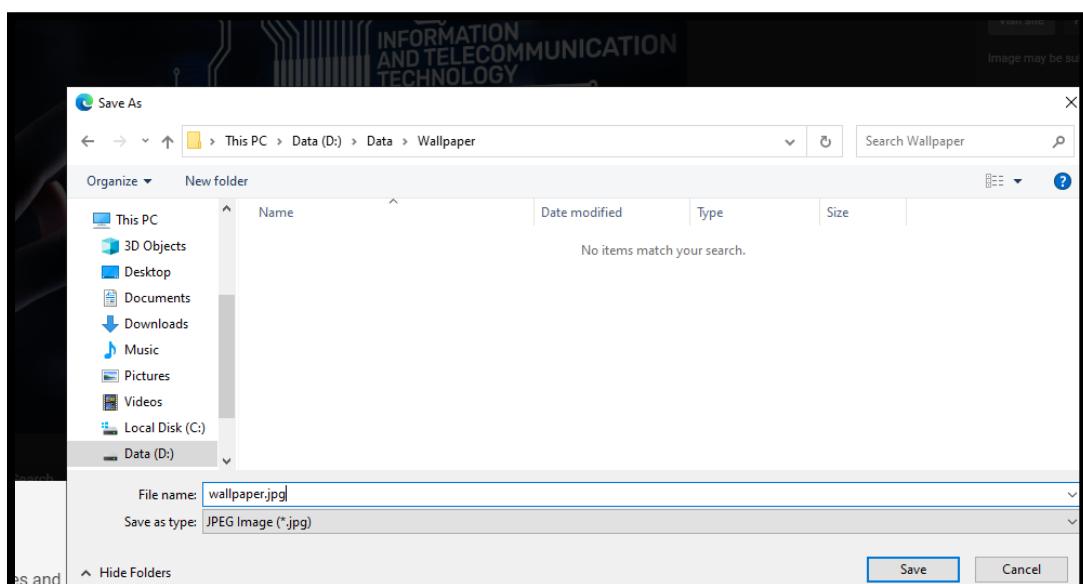
We hebben dan deze share als het goed is aangemaakt:



Stap 2:

Om even heel eenvoudig te starten kun je op internet een afbeelding gaan zoeken die bij je past óf je gaat een maken via MSPAINT op de server en je slaat hem op als **wallpaper.jpg**

Ik duik even op het internet en zoek op afbeeldingen “ICT”, en pak een willekeurige jpg foto. Deze slak ik op in de zojuist aangemaakte map in D:\Data\Wallpaper als **wallpaper.jpg**



Stap 3:

We gaan een nieuwe GPO aanmaken onder onder hoofd-OU, deze noemen we **Wallpaper** en dan moeten we opzoek gaan naar de juiste setting. Dit kunnen we uiteraard weer via Google óf ChatGPT vinden:

The screenshot shows a search result from a platform called J. The title of the result is "How to windows server 2022 gpo wallpaper". The content starts with a green circular icon containing a white gear symbol. The text reads: "To set the wallpaper using Group Policy Objects (GPO) on Windows Server 2022, follow these steps:" followed by a numbered list of 8 steps.

1. Open the Group Policy Management console on the Windows Server 2022.
2. Expand the domain and select the Organizational Unit (OU) where you want to apply the Group Policy.
3. Right-click on the OU and select "Create a GPO in this domain, and Link it here." Provide a name for the GPO and click OK.
4. Right-click on the newly created GPO and select "Edit."
5. In the Group Policy Management Editor window, navigate to "User Configuration" > "Policies" > "Administrative Templates" > "Desktop" > "Desktop."
6. Double-click on the "Desktop Wallpaper" policy on the right-hand side pane.
7. In the "Desktop Wallpaper Properties" window, select the "Enabled" option.
8. In the "Wallpaper Name" field, enter the full path of the image file you want to set as the

Nu is het wederom belangrijk om de juiste zoekterm op te geven. Als je namelijk **niet** meegeeft in de prompt bij ChatGPT of in Google dat je de afbeelding wilt benaderen via een netwerkshare, krijg je een uitleg die verwijst naar bijvoorbeeld C:\Wallpaper\Wallpaper.jpg zoals hierboven.

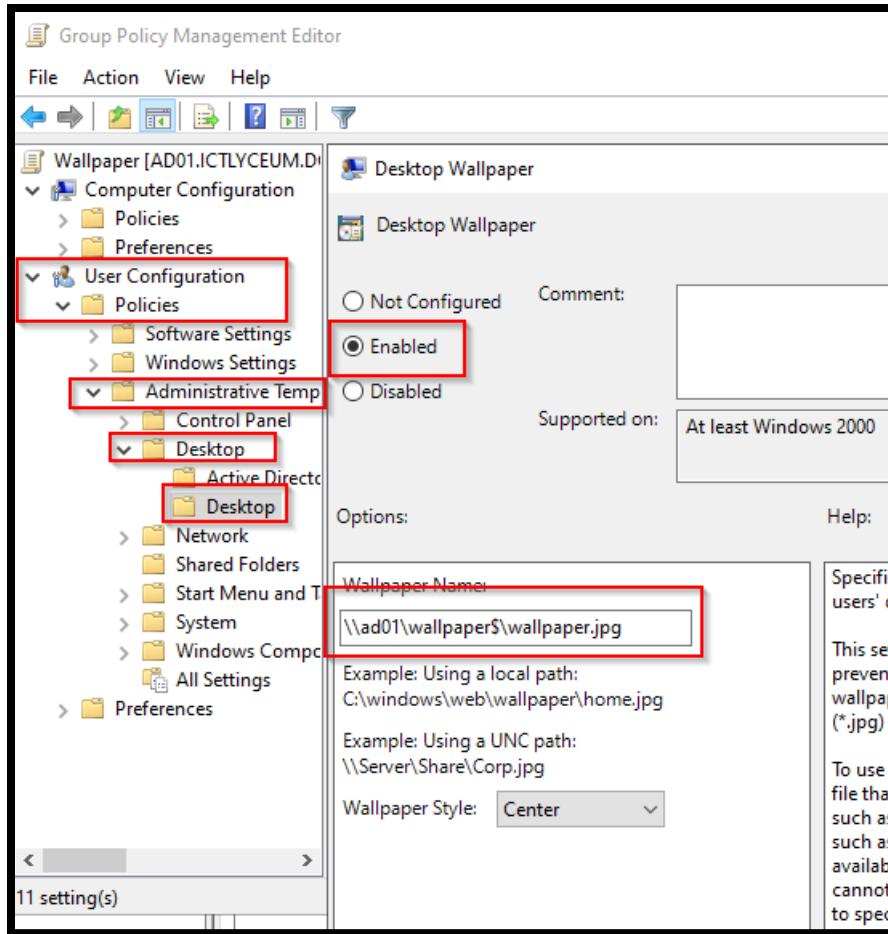
Daarmee zeg je dus eigenlijk in je policy dat voor elk workstation geldt, dat de achtergrond gevonden kan worden op de C-schijf van die betreffende machine, in het mapje **Wallpaper** en dat de naam **Wallpaper.jpg** is.

Je kunt natuurlijk al wel raden dat er nergens een workstation is die exact dat mapje en dat bestandje heeft op de C-schijf. Het is daarom altijd belangrijk om te zorgen dat je dus verwijst naar een goed bereikbare netwerkshare, precies zoals wij die gemaakt hebben.

Dus het padnaam is [\\AD01\Wallpaper\\$\wallpaper.jpg](\\AD01\Wallpaper$\wallpaper.jpg) in onze situatie.

We zoeken dus het bovenstaande configuratiedeel even op en voeren deze daar exact zo in, inclusief dus het \$-teken! We hebben daar nog de optie om de afbeelding gecentreerd te plaatsen, volledig scherm vullend te doen en noem maar op, maar voor eerst laten we heb standaard even op **Center** staan.

Mocht je overigens twijfel aan je volledige padnaam, typ het even volledig in bij de verkenners van je server, druk op ENTER en dan opent hij, als het klopt, de afbeelding die je hebt opgeslagen. Je weet dan zeker dat je share klopt!



We kiezen voor **Apply/OK** zodat de wijzigingen zijn opgeslagen en gaan gelijktijdig de Command Prompt even uitschakelen. Deze tool is als beheerder natuurlijk erg handig en makkelijk voor het pingen/ip controleren, maar ‘normale’ gebruikers hebben hier uiteraard weinig mee te zoeken én het kan een potentieel beveiligingsrisico zijn!

Client beveiliging via GPO

We maken nu, voordat we de wallpaper gaan testen, even snel een nieuwe GPO aan en deze noemen we **Client Security**.

We gaan hierin de Command Prompt (Start -> Uitvoeren -> CMD) uitschakelen, we voorkomen dat men het register mag bewerken, we zorgen ervoor dat de C-schijf op de werkstations niet meer zichtbaar is voor onze gebruikers, toegang tot het Configuratievenster wordt ontzegd én we gaan zorgen dat USB-sticks niet gebruikt kunnen worden op de computers.

Door simpelweg deze vijf basisopties dicht te zetten, voorkom je als beheerder al heel veel problemen. Je kunt je uiteraard wel voorstellen hoeveel “zooi” er op USB-sticks kan staan. Vaak staan daar auto-run tooltjes bij op, die op hun beurt weer de command prompt óf het register proberen op te starten, dus zo voorkomen we veel gezeur achteraf!

We gaan eerst weer opzoek naar de instellingen, dit is inmiddels bekend hoe we dit doen. Wanneer je ze gevonden hebt, ga je ze direct configureren in je nieuwe GPO. Al deze opties ga je vinden onder User Configuration/Policies/Administrative Templates.

Als je alles hebt gevonden, en dat kan best even zoeken zijn naar de juiste termen, dan moet je ongeveer dit hebben staan wanneer je op **Settings** drukt binnen je gekozen GPO (bij de foutmelding van Internet Explorer met het STOPBORD in beeld kun je afsluiten door op **Close** te drukken) :

Policy	Setting	Comment
Prohibit access to Control Panel and PC settings	Enabled	
Prevent access to registry editing tools	Enabled	
Prevent access to the command prompt	Enabled	
All Removable Storage classes: Deny all access	Enabled	
Hide these specified drives in My Computer	Enabled	

Zoals je ziet hebben we de volgende instellingen gedaan:

Hide these specified drives in My Computer – Restrict C drive only

All removable Storage classes: Deny all access

Prevent access to the command prompt – Enable

Prevent access to the registry editing tools – Enable

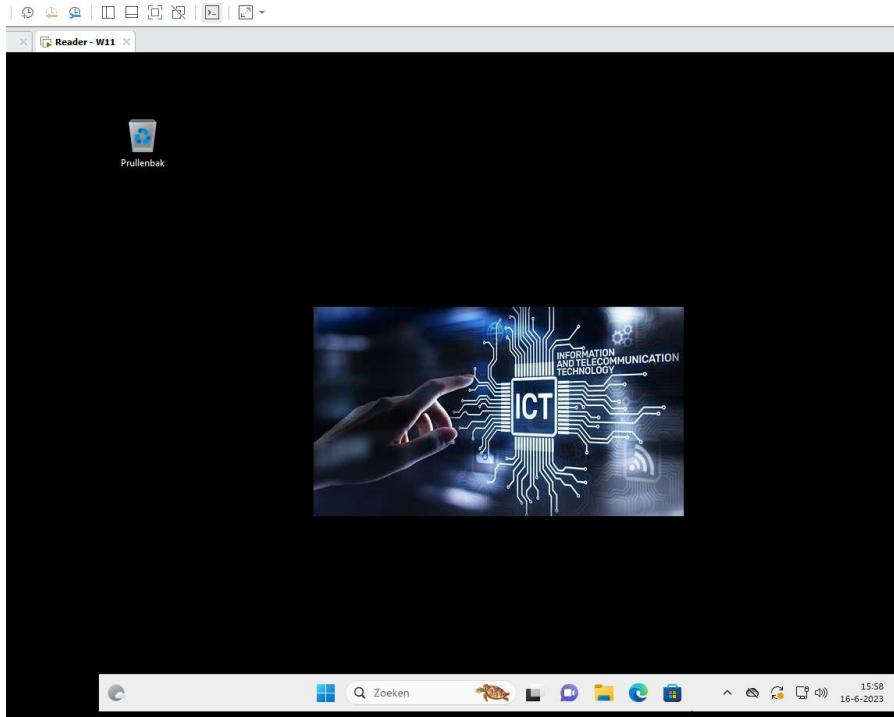
Prohibit access to Control Panel and PC settings - Enable

Zoals je hebt gezien, zijn het allemaal USER CONFIGURATION settings. We hebben deze, bewust, onder de hoofd-OU geplaatst, wat dus inhoudt dat, als je als domeinadministrator op dit werkstation in gaat loggen, dus feitelijk met een account welke **NIET** onder het hoofd-OU of een daar onderliggende OU geplaatst is, deze instellingen niet gelden op dat moment.

De gebruikers hebben er dus "last" van, maar de domein administrator niet.

Nu we al die instellingen gedaan hebben, gaan we eens inloggen op de client om te zien wat er gebeurt!

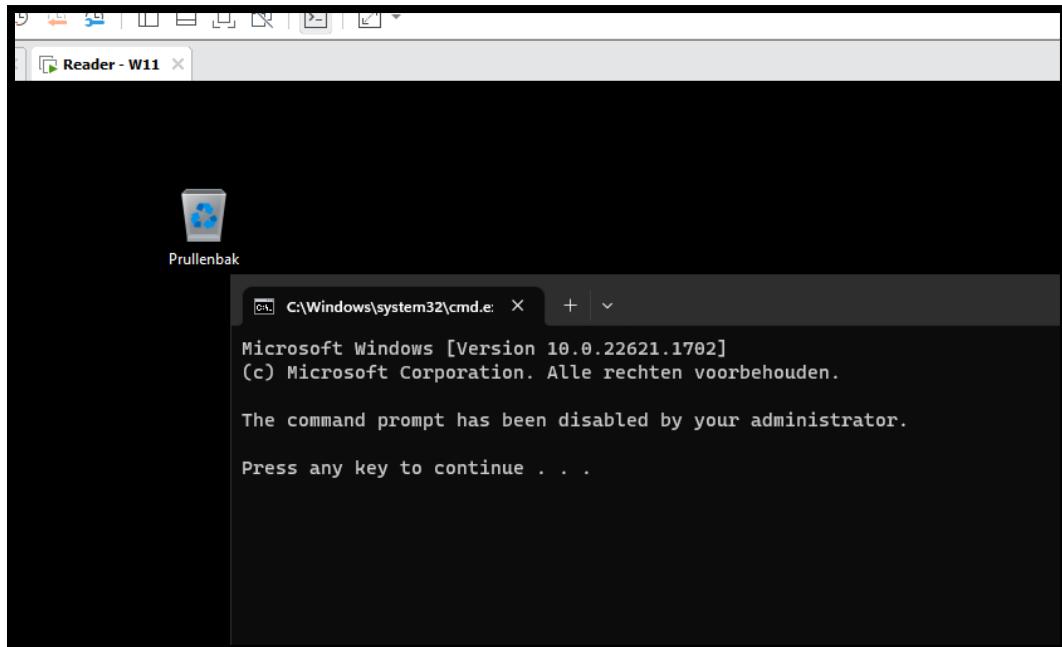
Zoals verwacht, heeft hij netjes de afbeelding verwerkt in de achtergrond!



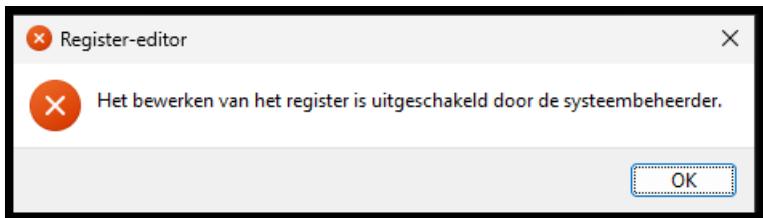
Mocht je nu een zwarte achtergrond hebben, dan klopt mogelijk toch je pad niet óf heb je niet de juiste rechten. Controleer dan even of je de bovenstaande (opgegeven) wallpaper.jpg kunt openen in de verkenners van je client. Je weet dan gelijk wat er eventueel mis is.

Mocht je namelijk geen toegang hebben, is er iets fout gegaan bij het inrichten van de share/de rechten hiervan. Eenvoudig op te lossen vaak dus 😊 !

Voeren we vervolgens via de Windows knop (rechter muisknop) -> Uitvoeren: CMD in, wordt dit netjes geblokkeerd:



En hetzelfde geldt voor Uitvoeren; RegEdit:



Als laatste kunnen we nog even proberen of we het Configuratiescherm mogen openen, maar gelukkig mag dit ook niet meer:



We kunnen dus wel stellen dat deze policy goed zijn werk doet! De basisbeveiliging én de achtergrond zijn dus gelukt!

Log als test nu nog even in als **ICTLYCEUM\Administrator** om te controleren of je met dát account bijvoorbeeld wél de command prompt mag gebruiken. Als het goed is ervaar je hiermee gelijk het grote voordeel van de OU-structuur en de kracht die je als beheerder van het domein hebt !

We zijn nu aan het einde van deze reader. Met deze basis heb je een heel mooie omgeving gemaakt die je, in principe, als basis kunt gaan gebruiken voor toekomstige omgevingen.

De reader kun je altijd even teruglezen bij het bouwen van een omgeving en op den duur zal je ontdekken dat je steeds meer stappen uit je hoofd gaat kunnen doen.

Omdat we toch weer redelijk wat hebben gewijzigd op de AD01 is het verstandig een snapshot te maken. Aangezien het echter de 'zoveelste' is, kunnen we ervoor kiezen om eerst alles te verwijderen (aangezien het allemaal goed functioneert tot dit punt) en direct daarna een nieuwe snapshot te maken. Op die manier blijft het systeem (relatief) snel en blijft het overzichtelijk qua aantal snapshot!

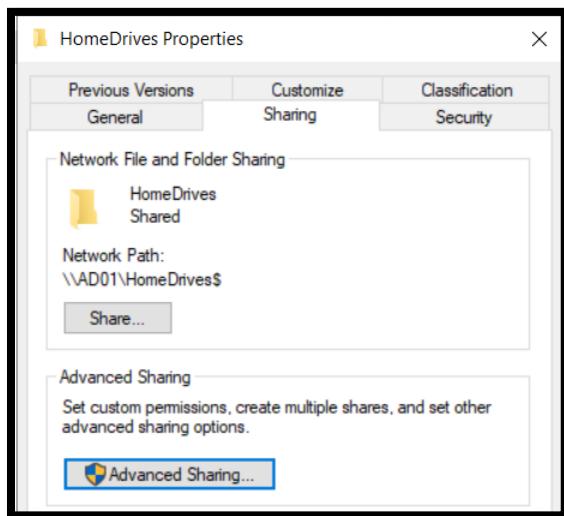
User Home Folders

Omdat iedereen tegenwoordig steeds meer “eigen” data heeft, wat niet overal kan/mag worden opgeslagen vanwege bijvoorbeeld de AVG, is het belangrijk dat gebruikers een **persoonlijke schijf** krijgen.

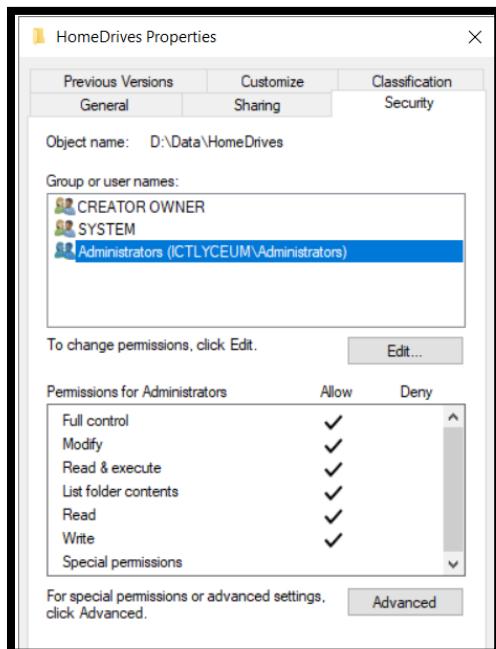
Dit is een relatief eenvoudige actie, maar eerst moet je hiervoor de rechten van de shares en NTFS-rechten goed zetten.

We beginnen hiermee door simpelweg even een share aan te maken op de D schijf, welke we **HomeDrives** noemen.

We zorgen ervoor dat deze schijf verborgen is voor de (standaard) verkenner:



Vervolgens zorgen we ervoor dat bij **Security** de rechten als volgt ingesteld worden:



Zoals je ziet zijn de Domain Users allemaal weg en hebben de **Domain administrators** -> **Full Control**.

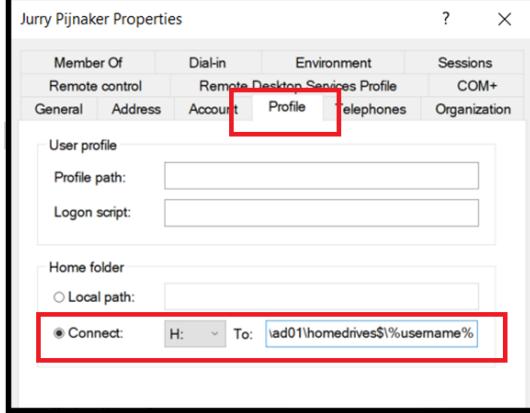
Wanneer je vervolgens de koppeling goed zet in de **AD DS**, dan maakt Windows Server zelf een persoonlijke map aan én zet deze de rechten goed voor de betreffende gebruiker.

Wanneer het om slechts één persoon gaat, dan doe je het volgende:

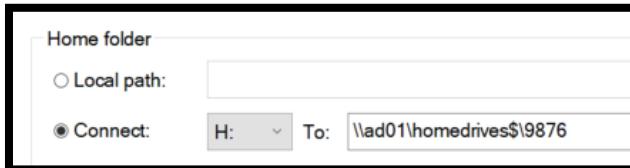
Open op de gewenste gebruiker de Properties en ga naar **Profile**. Daar zet je onder **Home folder -> Connect H:** (van Home) To: de volledige sharename + de toevoeging: **%username%**

Windows vult deze dan automatisch aan met de gebruikersnaam van de betreffende gebruiker.

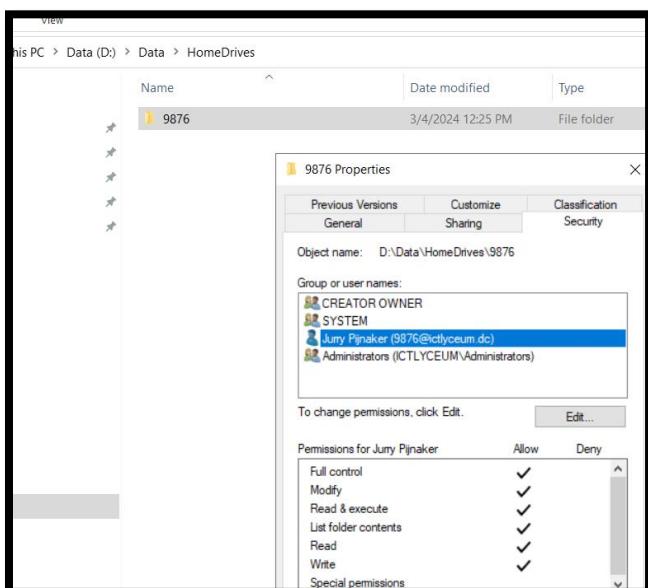
In dit voorbeeld zetten we hier dus concreet neer: **\ad01\homedrives\$\%username%**



Druk je dan op **Apply** dan zie je dat hij de username aanpast:



Tegelijkertijd maakt hij hiervoor een map aan in de verkenner met deze rechten:

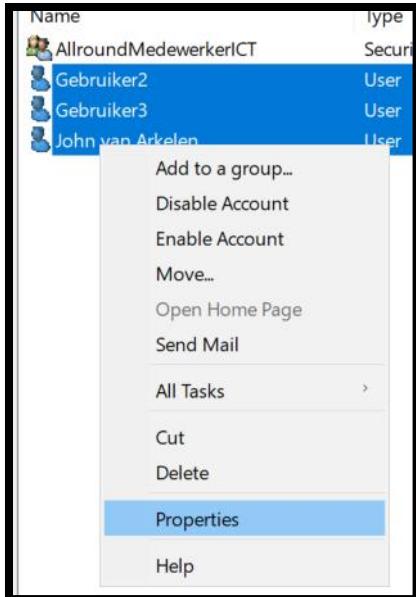


Zoals je dus ziet, heeft alleen de betreffende gebruiker de rechten nu op deze folder. Daarnaast uiteraard de Administrator-groep ook, voor het maken van back-ups bijvoorbeeld.

Let op: De **Homefolders** is de éénige uitzondering waarbij je dus op een folder een **gebruiker** i.p.v. een **Security Group** koppelt!

Wanneer het om meerdere personen uit een OU tegelijkertijd gaat, dan doe je het volgende:

Selecteer de gewenste gebruikers (d.m.v. CTRL bijvoorbeeld) en kies **Properties**



Vervolgens kun je onder **Profile** dezelfde stappen opgeven als hierboven besproken:

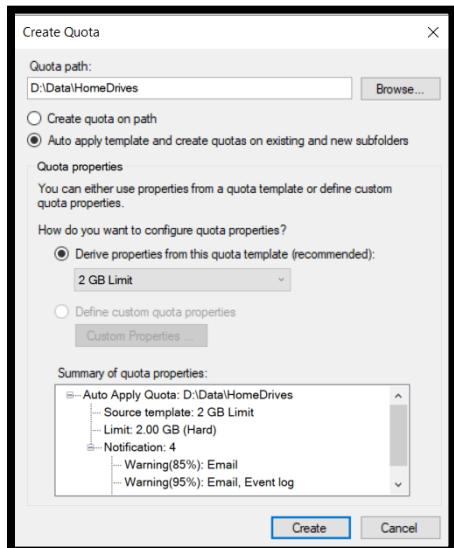
A screenshot of the 'Properties for Multiple Items' dialog in Active Directory. On the left, there's a tree view of the Active Directory structure. In the center, three users are selected: AllroundMedewerkerICT, Gebruiker2, and Gebruiker3. A right-click context menu is open over them. On the right, a dialog box is open with tabs for General, Account, Address, Profile (which is highlighted with a red box), and Organization. The 'Profile' tab contains fields for 'User profile': 'Profile path:' (unchecked), 'Logon script:' (unchecked), 'Home folder' (checkbox checked and highlighted with a red box), and 'Local path:' (radio button unselected). Below these, there's a 'Connect:' section with a dropdown set to 'H:' and a text input field containing '\\ad01\homedrives\$\%username%'. This 'Connect:' section is also highlighted with a red box.

Op deze manier kun je dan dus meerdere users tegelijkertijd koppelen aan de homedrives 😊 !

Quota op de homedrives

Enige wat nu nog even moet gebeuren, is het aanmaken van een quota op deze homefolders. Je wilt tenslotte niet dat iedereen de privé filmpjes en foto's op de schijven gaat zetten!

Je zet hierbij een quota (2GB) op de hoofdmap (dus in mijn specifieke geval D:\Data\HomeDrives) en daarbij zorg je dat alle onderliggende mappen de quota meenemen. Dit gaat via de optie '**Auto apply template and create quotas on existing and new subfolders**':



Filter: Show all: 5 items				
Quota Path	% Used	Limit	Quota Type	Source Template
Source Template: 2 GB Limit (5 items)				
D:\Data\HomeDrives*	---	2.00 GB	Hard (Auto Apply)	2 GB Limit
D:\Data\HomeDrives\5432	0%	2.00 GB	Hard	2 GB Limit
D:\Data\HomeDrives\9876	0%	2.00 GB	Hard	2 GB Limit
D:\Data\HomeDrives\gebruiker2	0%	2.00 GB	Hard	2 GB Limit
D:\Data\HomeDrives\gebruiker3	0%	2.00 GB	Hard	2 GB Limit

Hij maakt nu, door de wildcard (*) achter de share (D:\Data\HomeDrives*), automatisch voor elke nieuwe gebruiker een quota aan met 2GB zoals hierboven te zien is.

Instellen Shadow Copies – ook wel “Backups”

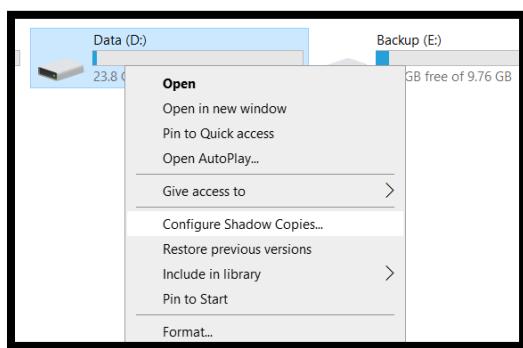
Een eenvoudige manier om snel en makkelijk te beheersbare “back-ups” te maken, is het instellen van Shadow Copies. Een Shadow Copy is eigenlijk een soort versie-beheer. Je hebt dus de optie om van elk bestand wat je aanmaakt en bewerkt, een oude versie te behouden zodat je snel en makkelijk terug kunt naar de vorige versie.

Dit is bijvoorbeeld ideaal wanneer eindgebruikers vaak vragen om “even het bestandje van vanochtend terug te halen”. Ze kunnen dit namelijk zelf!

Het instellen doe je op de hoofdpartitie. Dus op de D-schijf in onze omgeving. Je kunt daar eenvoudig een schema instellen, waarmee je bijvoorbeeld elke 2 uur, tussen 08:00 en 17:00 een kopie maakt.

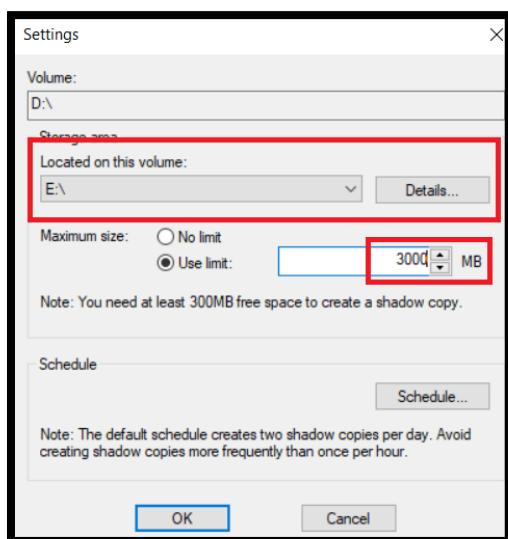
Deze kopie wordt overigens **alleen** gemaakt van bestanden die gewijzigd zijn. Wanneer er niets wijzigt blijft de kopie-map dus als het ware leeg, want er zijn geen oudere bestanden.

Wanneer we op de **D-schijf** klikken met de rechter muisknop, kunnen we kiezen voor **Configure Shadow Copies...**



Het is mogelijk om de Shadow Copies op een andere schijf op te slaan, zodat je data-schijf niet vol loopt met back-ups en dat is nu nét de reden dat wij een E-schijf met label ‘**Backup**’ hebben aangemaakt. We beginnen dus met het wijzigen van de opslaglocatie, dit doe je door de D-schijf te selecteren en te kiezen voor **Settings**.

We zetten hem dus op de E:\ en zetten het limiet, om te beginnen, op 3000MB.



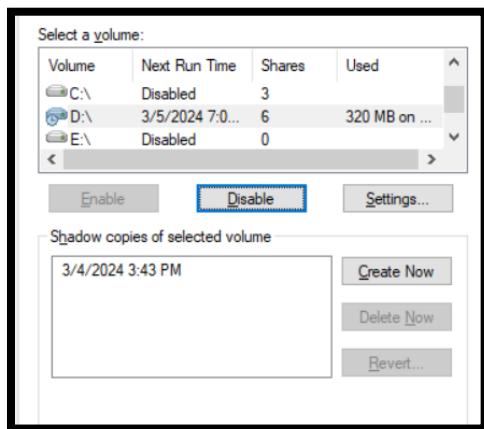
Vervolgens kies je voor **OK**.

Vervolgens kiezen we, wanneer D-schijf nog geselecteerd staat, voor **Enable**.

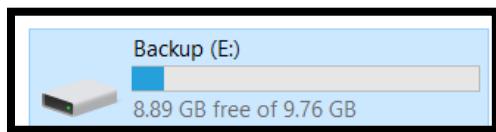
Bij de pop-up die verschijnt, te kiezen voor **Yes**. We gaan tenslotte straks zelf een eigen schema aanmaken hiervoor, dus die is niet relevant.



Je ziet dat hij dát moment direct een Shadow Copy aanmaakt:



Je ziet nu ook dat van je E-schijf er een gedeelte van je vrijeruimte verdwijnt. Je zult daar echter geen data zien staan omdat het besturingssysteem dit verbergt.

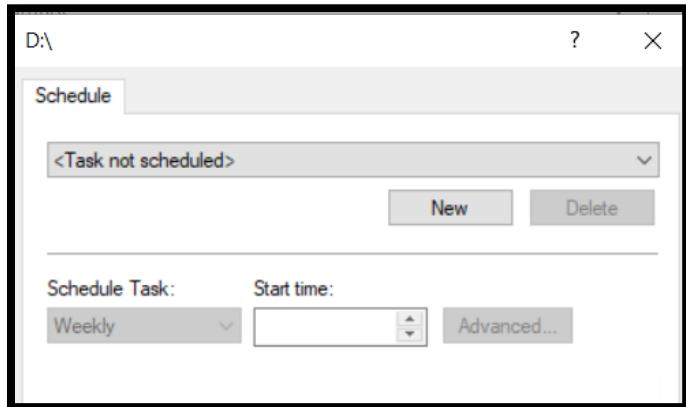


Nu dit is ingesteld, gaan we het schema inrichten, om dus te bepalen hoe vaak hij dit moet gaan doen. Een mooi schema vind ikzelf altijd om elke 2 uur een kopie te laten maken. Dit is bijvoorbeeld zo ingesteld bij onze examenomgeving.

Om dit te doen gaan we weer naar **Settings** en kiezen we nu voor **Schedule**. Dit had natuurlijk ook in 1x gekund, bij het aanpassen van de opslaglocatie, maar op deze manier is het duidelijker te zien wat je precies doet.

Om te beginnen gaan we de huidige (standaard) twee schema's even verwijderen, dit is eenvoudig te doen door het selecteren van het schema en te kiezen voor **Delete**

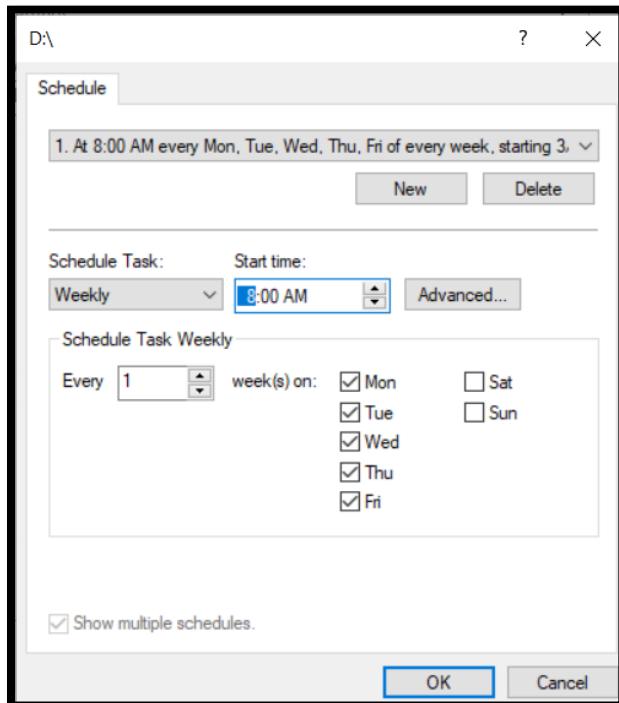
Nu deze twee weg zijn, kunnen we gaan beginnen met het instellen van onze eigen schema's , dat doe je uiteraard via **New**



We gaan er even vanuit in dit voorbeeld dat ons bedrijf maandag t\m vrijdag, van 08:00uur tot 17uur werkt.

We beginnen dus door de **Daily** naar **Weekly** te zetten, waardoor we dan dus eenvoudig de werkdagen kunnen aanvinken. Uiteraard is de Starttijd dan dus om 08:00uur. In het weekend hoeft hij niets te doen.

Dan ziet dit er in de basis zo uit:

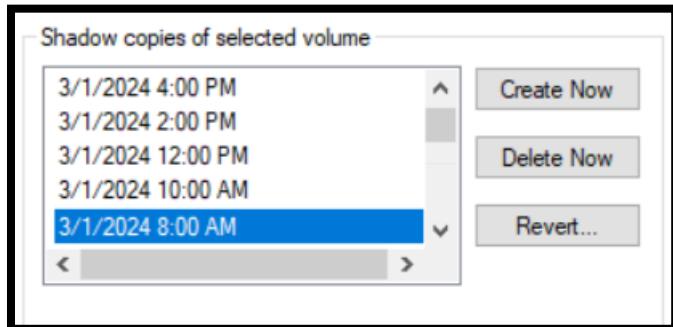


Nu dit goed staat, kiezen we voor **Advanced**, zodat we kunnen aangeven hoe vaak hij de actie moet uitvoeren.

We kiezen ervoor om het schema voor 8uur lang, elke 2 uur te laten uitvoeren.

Dit houdt dus concreet in dat het schema vanaf 's morgens 08:00uur, 8 uur lang draait. Dus tot 16uur voor het gemak. Tijdens deze tijden voert hij elke 2 uur de kopie-actie uit.

Je krijgt dan dus deze tijdstippen als "back-up":

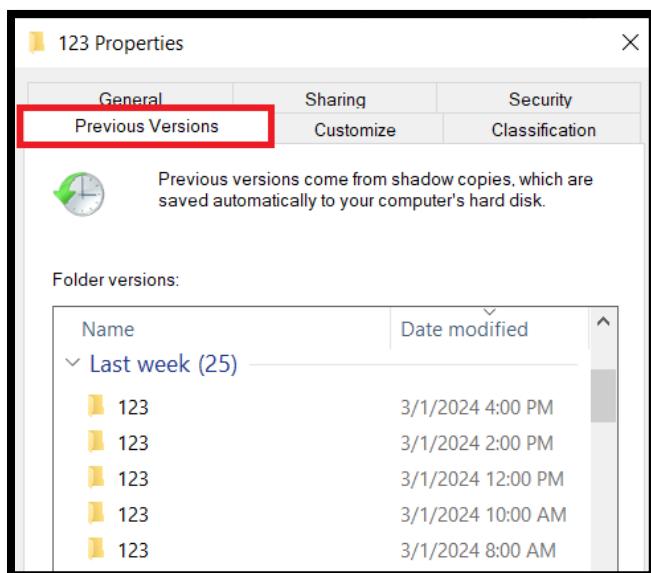


Deze is ideaal, waardoor men bij een fout/verlies dus nooit verder hoeft dan 2uur daarvoor.

Voorwaarde is **uitehaar** wel dat het bestand met regelmaat is opgeslagen 😊

Terughalen van Shadow Copies

Wanneer men nu iets terug wilt halen, van bijvoorbeeld 12uur, kunnen ze op hun client eenvoudig naar de betreffende map gaan. Daar met de rechter muisknop in drukken en kiezen voor **Previous Versions** (vorige versies). Daarin kan men eenvoudig en snel zelf gaan kijken en de gewenste data kopiëren naar een bepaalde map



Testen Previous Versions

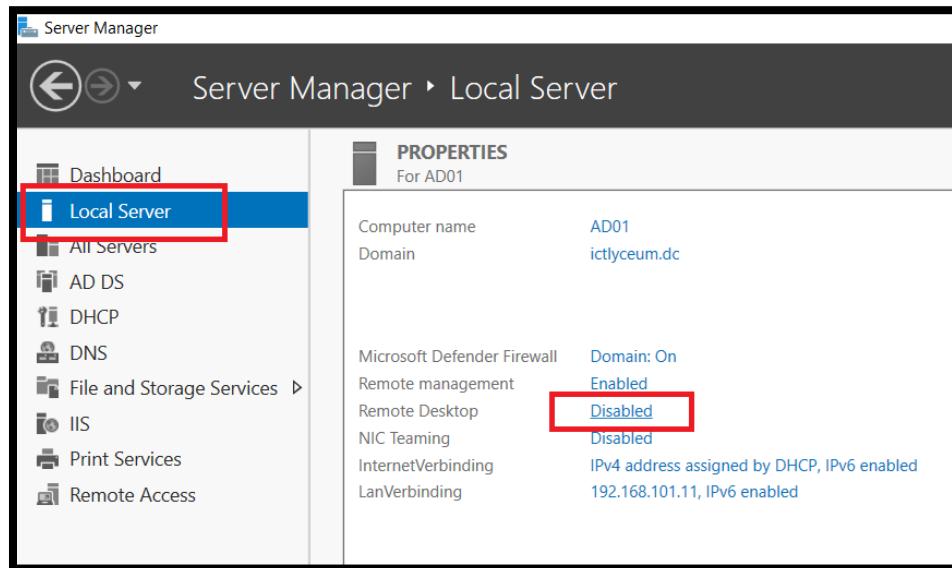
Nu dit allemaal werkt en is ingesteld, ga je via je Windows Client een bestand aanmaken in de persoonlijke homefolder. Ga hier eens mee bezig en kijk eens wat er gebeurt als je hem op bepaalde tijden wijzigt en probeer dit vervolgens (na 2uur bijvoorbeeld) terug te zetten, als 'gebruiker', via Previous Versions.

Remote Desktop

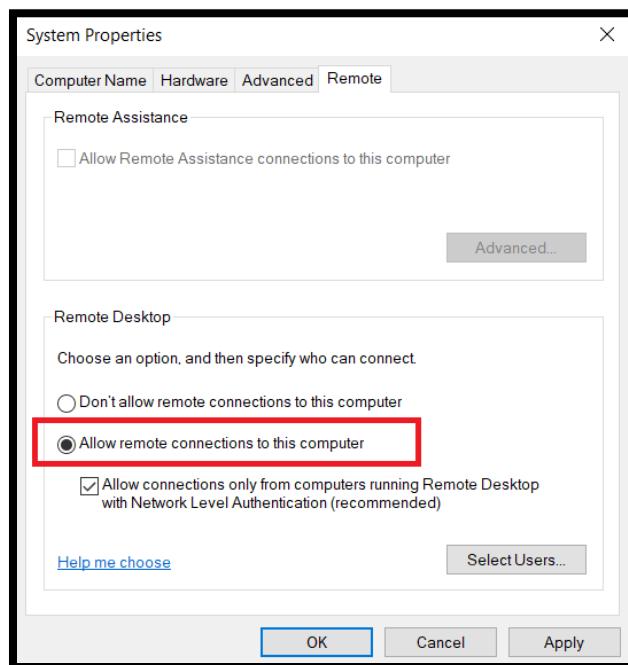
Om de Windows Server makkelijk te beheren, is het fijn om gebruik te maken van de ingebouwde Microsoft Remote Desktop-tool. Deze zit in principe in alle Windows Client versies met Pro en/of Education.

Het is hiervoor nodig om 1 kleine optie in te stellen bij je Windows Server en dat is Remote Desktop.

In de ServerManager klik je op Local Server en vervolgens op het woordje **Disabled** naast Remote Desktop



Hierbij zet je het **balletje** van Don't allow.... naar -> Allow remote connections to this computer.

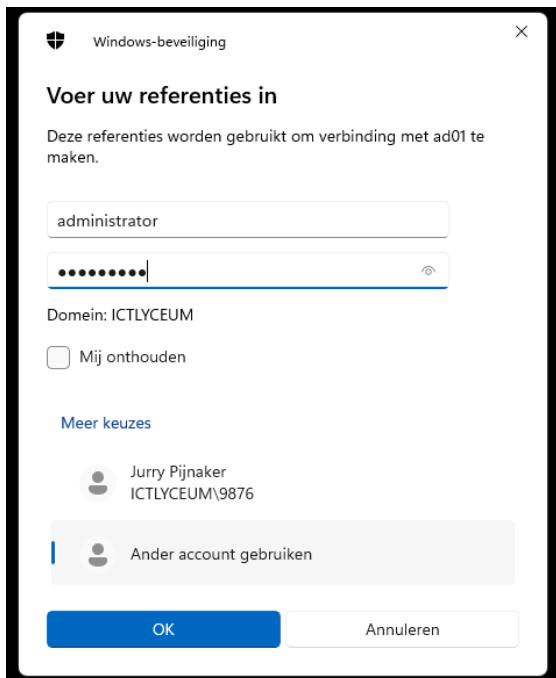


Onder **Select Users...** kun je eventueel nog aparte gebruikers kiezen, maar standaard hebben de Domain Admins op dit moment nu rechten om Remote Desktop te mogen starten naar deze machine.

Ga je dan kijken in de Windows Client machine en voer je het commando **MSTSC** uit via RUN, start de Remote Desktop-tool op. Je kunt dan op basis van IP of DNS-naam verbinden met de machine.



Na het inloggen (ictlyceum\administrator) :



Wordt de verbinding opgebouwd en kun je dus de server(s) beheren vanaf je eigen werkstation!