

# **De opbouw van een bedrijfsomgeving**

Ferranti Computer Systems nv ~Silta

---

Opleiding: Elektronica-ICT

Academiejaar: 2018-2019

Student: Kevin Van de Vyver

Stagementors: Wesley Swartele, Peter De Baerdemaeker

Stagebegeleider: Serge Horsmans

# Woord vooraf

Ik heb de keuze gemaakt om een opdracht te zoeken in verband met netwerking en infrastructuur, omdat dit me het meest interesseert. Zo kwam ik terecht op het bedrijf **Ferranti** wegens een zeer intrigerende opdracht, een compleet fysiek en virtueel bedrijf opstarten van A tot Z.

Het bedrijf Ferranti bestaat uit 3 deelbedrijven; Mecom, Frontforce en Silta. Voor mijn stage ben ik terechtgekomen bij Silta. Het bedrijf is gelegen in het Antwerpse havengebied en telt zo'n 300 tal medewerkers. De Silta afdeling stelt een 20 tal mensen tewerk. Er is enige interactie tussen de verschillende deelbedrijven.

Een bijkomende reden waarom ik deze opdracht gekozen heb, is om te zien of mijn interesse meer richting netwerking gaat of infrastructuur. Door al de verschillende technieken en toepassingen die hiervoor gebruikt worden, zal ik alvast een goed idee krijgen wat me het meeste boeit. Ook zal ik al een goede basis hebben om later te kunnen starten op een bedrijf.

Na een periode van 15 weken hard werken heb ik mijn stage volbracht. Deze opdracht heb ik tot een goed einde gebracht, mede dankzij de aangebode hulp van het personeel van Ferranti. Vooral de heren Wesley Swartele en Peter De Baerdemaeker hebben mij veel kennis bijgebracht. Ook wil ik Ronnie Dibbaut bedanken om mij te betrekken bij meetings, events, ...

Verder bedank ik alle Silta medewerkers voor de aangename ontvangst en begeleiding die ze me hebben gegeven. Steeds kon ik met al mijn vragen bij jullie terecht. Ik heb enorm veel van jullie bijgeleerd en het was een plezier om met jullie te kunnen samenwerken. Ook wil ik de AP lectoren bedanken voor mijn begeleiding.

Mijn stage was een boeiend leerproces en heeft bijgedragen aan mijn persoonlijke ontwikkeling en zelfvertrouwen.

Bedankt allemaal,  
Kevin

# **Samenvatting**

Tijdens de stage was er de mogelijkheid om alle ICT facetten van een bedrijf te leren kennen door een fictief bedrijf op te zetten in een omgeving. Deze omgeving zal Silta achteraf gebruiken om demo's te geven bij klanten, producten te testen of situaties te simuleren.

Eerst voerde ik een uitgebreid onderzoek uit naar de designs van het bedrijf, zowel op het vlak van netwerk als infrastructuur. Vervolgens ontwikkelde ik een high performing en high available serveromgeving (DELL), gebruik makende van enkele veelvoorkomende applicaties (Azure, Hyper-V, fileserver, printserver, domaincontroller, DNS, DHCP, Office 365, Citrix XenApp & Windows Server 2019, ...).

Noodsituaties worden opgevangen door middel van constante monitoring (OMS) en back-ups (VEEAM).

# Inhoudsopgave

## Table of Contents

De opbouw van een bedrijfsomgeving.....	1
Ferranti Computer Systems nv ~Silta .....	1
Woord vooraf .....	1
Samenvatting.....	2
Inhoudsopgave .....	4
De opbouw van een netwerk infrastructuur .....	6
1 Inleiding .....	6
2 Onderzoek .....	9
2.1 Infrastructuur design.....	9
2.2 Netwerk design.....	10
3 Configuraties .....	11
3.1 Hardware (RAID, OS installatie, iDRAC).....	11
3.1.1 Server 1 + Server 2 .....	11
3.1.2 Server 3 .....	14
3.2 Netwerk.....	15
3.2.1 Firewall .....	15
3.2.2 Switch .....	16
3.2.3 Servers .....	18
3.3 Toepassingen .....	19
3.3.1 Domaincontroller.....	20
3.3.1.1 Installatie primary domaincontroller (DC_1) .....	20
3.3.1.2 Installatie backup domaincontroller (DC_2) .....	23
3.3.2 Group policies.....	26
3.3.2.1 Configuratie default browser (DC_1) .....	26
3.3.2.2 Configuratie browser startpagina (DC_1) .....	27
3.3.2.3 Configuratie drive mapping (DC_1) .....	31
3.3.3 DNS .....	34
3.3.3.1 Installatie DNS (DC_1) .....	34
3.3.4 DHCP .....	36
3.3.4.1 Installatie DHCP (DC_1).....	36
3.3.5 Printserver .....	38
3.3.5.1 Installatie printserver (PS_1) .....	38
3.3.6 Fileservers (DFS).....	41

3.3.6.1 Installatie fileservers .....	41
3.3.7 Citrix.....	46
3.3.7.1 Configuratie VDA (Citrix-1, Citrix-2) .....	47
3.3.7.2 Configuratie Delivery controllers (Citrix-d1, Citrix-d2) .....	48
3.3.8 Veeam .....	51
3.3.8.1 Configuratie VEEAM (Backup) .....	51
3.3.9 Replication .....	55
3.3.9.1 Configuratie (Server1) .....	56
3.3.9.2 Installatie (Server3) .....	57
3.3.10 DMZ .....	58
3.3.10.1 Configuratie (Server2) .....	59
3.3.11 NetScaler .....	61
3.3.11.1 Configuratie (NetScaler Virtual Appliance) .....	61
3.3.12 Azure AD Connect.....	69
3.3.12.1 Installatie (AD_connect) .....	69
3.3.13 Multi-factor Authenticatie .....	73
3.3.13.1 Configuratie MFA.....	74
3.3.14 Secure wireless .....	75
3.4 Powershell .....	76
3.4.1 Domaincontroller (PS_AD) .....	76
3.5 Besluit .....	80

# De opbouw van een netwerk infrastructuur

## 1 Inleiding

Veel bedrijven doen steeds meer beroep op virtualisatie. Het is haast niet meer weg te denken in grote en succesvolle bedrijven. Waarom meerdere fysieke servers gebruiken om rollen op te splitsen in plaats van één server met daarop meerdere virtuele machines. Het is efficiënt, schaalbaar en redundant.

Het bedrijf *Ferranti Computer Systems nv* bood hierbij de perfecte opdracht aan, een bedrijf opstellen van A tot Z. Het doel van deze opdracht was een high performing en high available serveromgeving (DELL) op te stellen. Deze omgeving zal Silta later gebruiken om demo's te geven aan klanten, producten te testen of situaties te simuleren.

Om alvast een idee te geven wat er in deze scriptie aan bod komt van technologieën, volgt volgende opsomming:

- windows server 2019,
- domaincontroller,
- group policies,
- dns,
- dhcp,
- printserver,
- fileservice,
- citrix,
- replication,
- dmz,
- netscaler,
- veeam,
- azure ad connect,
- multi-factor authentication.

Het is begrijpelijk dat bepaalde technologieën niet direct bekend zijn. Deze zal ik toelichten in de bijlage.

## Domaincontroller

De domaincontroller zorgt voor centraal beheer van de rechten van alle users en computers in het domein, wat handig is voor grote netwerken. Zonder domaincontroller zou de administrator op iedere PC afzonderlijk gebruikers moeten aanmaken en vervolgens de bijhorende rechten toewijzen.

## Group policies

Met group policies kan de administrator instellingen en configuraties van gebruikers en computers beheren. Dit kan je onder andere gebruiken om de startpagina van de browser aan te passen, rechten aan bepaalde schijven en/of mappen op de computer toe te kennen en standaard templates voor documenten toe te wijzen..

## DNS

DNS regelt de netwerkconfiguratie. Deze zet IP-adressen om naar namen en omgekeerd. Zodoende hoeft men geen IP-adressen van de servers te onthouden, maar kan je gebruik maken van de servernamen.

## DHCP

DHCP kan je instellen om dynamisch IP-adressen uit te delen aan computers, evenals de correcte DNS instellingen. De DHCP server wijst IP-adressen toe vanuit een pool en zijn herbruikbaar wanneer een computer wordt uitgeschakeld.

## Printserver

De printserver zal de beschikbare printers in het domein op het netwerk aan de gebruikers beschikbaar stellen. Zo kan iedereen die op het domein zit van alle printers gebruik maken. De printserver zorgt ook voor de installatie van de noodzakelijke printerdrivers.

## Fileserver

Met een fileserver kan je 1 of meerdere gedeelde netwerkfolders configureren. Dit is handig om bestanden uit te wisselen tussen gebruikers en vergemakkelijkt het backuppen van de data.

## Citrix

Citrix is een technologie die je kan gebruiken om desktops en/of applicaties te publiceren. Dit is een handige tool om applicaties centraal beschikbaar te stellen voor gebruikers of om toegang tot applicaties te beperken (werknemers in administratie hebben toegang tot andere applicaties dan in productie). Applicaties worden op de server beheerd en gestart, het is niet nodig om deze op de afzonderlijke PC's te installeren.

## Veeam

Veeam is een applicatie die automatische back-ups maakt volgens voorgedefinieerde scenario's. In geval van falen van een server kan je snel op een werkende back-up terugvallen.

## Replication

Met replication kan je de VM's (virtuele machines) die niet high available zijn, toch failoveren. Dit betekent dat wanneer er een VM defect raakt, deze meteen wordt overgenomen door een andere VM. Om replicatie te bekomen, gaat men één fysieke server instellen als een replica server. Dit betekent dat je VM's kan "kopiëren" naar deze server. Wanneer de originele VM uitvalt, zal de replica server de gekopieerde VM aanzetten en gebruiken. Voor de eindgebruiker is dit proces volledig transparant. Hij merkt niet dat hij op een andere machine zit te werken.

## DMZ

DMZ staat voor demilitarized zone. Dit is een zone die zich bevindt tussen het interne en externe netwerk. Deze zone wordt meestal gebruikt als extra security laag, omdat hierin de publieke toepassingen van het netwerk komen. Op deze manier is het niet nodig om de externe gebruikers toegang tot het interne netwerk te geven, terwijl ze toch de noodzakelijke netwerkdiensten kunnen benaderen.

## RODC

RODC is de afkorting van read-only domaincontroller. Deze heeft net dezelfde functionaliteiten als een normale domaincontroller, maar kan niet schrijven. Dit betekent dus dat de rodc geen gebruikers kan aanmaken, permissies kan wijzigen, ... Vanwege de schrijflimitaties wordt deze vooral gebruikt in een DMZ, omdat er geen gevaren zijn moet deze gecompromitteerd worden.

## Netscaler

De netscaler is een toepassing die je kan gebruiken om de Citrix applicaties beschikbaar te stellen voor zowel interne als externe gebruikers. Deze netscaler heeft een grote impact op de performantie, beveiliging en schaalbaarheid van de application delivery.

## RAID

Redundant array of independent disks, afgekort door RAID is de benaming voor verschillende methodes die betrekking hebben op data-opslag op harde schijven. Hierbij wordt de data ofwel verdeeld over meerdere schijven (striping) of opgeslagen op meerdere schijven (mirroring). Je kan ook beide opties combineren met elkaar. De keuze hiervan hangt af van de toepassing waar je het voor gebruikt. Toepassingen die snel moeten zijn, gebruiken meestal een RAID 0 terwijl betrouwbare toepassingen gebruik maken van RAID 1 of 5.

## iDRAC

De iDRAC (Dell Remote Access Controller) is een management tool om servers vanaf afstand te beheren. Met de iDRAC browser kan je de servers heel goed monitoren, zo kan je de logs van de server zien, de ventilatoren, CPU, geheugen en nog veel meer.

## VPN

VPN of virtual private network kan je zien als een privé netwerk binnen een groter netwerk. Hiermee maak je onder andere een connectie naar de netwerkomgeving van de demo-omgeving.

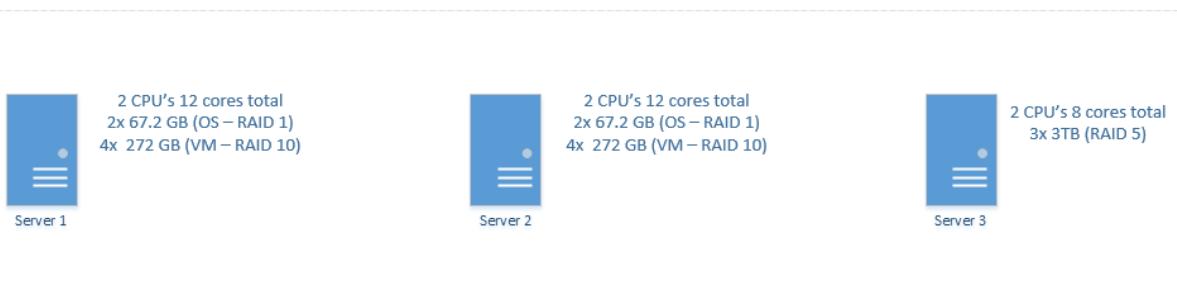
## 2 Onderzoek

In dit hoofdstuk zal ik de benadering van het project verder uitgeleggen. Om een project tot een goed eind te kunnen brengen, is het essentieel om eerst de designs te maken. Dit zal later heel wat problemen voorkomen in verband met installaties en netwerk configuraties.

### 2.1 Infrastructuur design

In de demo omgeving zijn er 3 fysieke servers ter beschikking om alle toepassingen over te verdelen. De servers waren nog niet opgebouwd. Dit wil zeggen dat ik moest nadenken over de grootte van het geheugen, de harde schijven en in welke RAID configuratie deze het best geïnstalleerd werden. Aangezien de omgeving gebackupped en gemonitord wordt, is er hiervoor een fysieke server aan toegewezen. Deze server heeft het meeste opslagruimte nodig omdat alle data van de back-ups hier opgeslagen zal worden. Om deze reden zitten er huidig 3 schijven in van ieder 3TB. De server is geconfigureerd met een RAID level van 5 om dataverlies tegen te gaan moet er een schijf niet meer werken. De overige 2 servers worden gebruikt om de virtuele machines op te zetten en zijn vooral performantie gericht, hierdoor moeten ze snel kunnen lezen en schrijven. De performantie gerichte servers bevatten elk 2 schijven van 68 GB in mirror (RAID 1) waar het operating systeem op draait en 4 schijven van 136 GB met striping en mirror (RAID 10).

Tekening 1:



## 2.2 Netwerk design

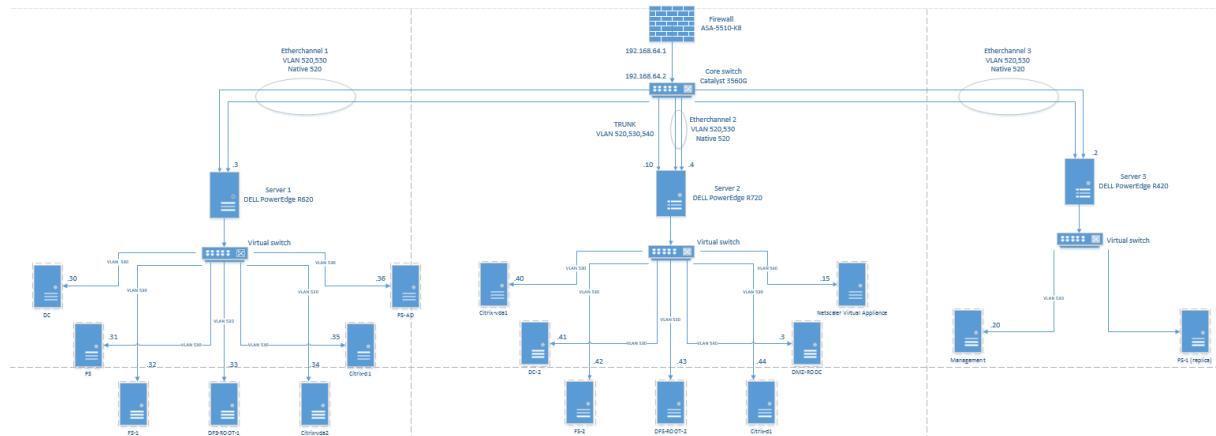
Eens het infrastructuurontwerp vast lag, kon er begonnen worden aan het netwerkdesign. Primaire voorwaarde was dat de omgeving high-available moest zijn. Op netwerkvlak waren er 3 servers (Dell Poweredge R420, Dell Poweredge R620, Dell Poweredge R720), een layer 3 switch (Cisco Catalyst 3560G) en een firewall (ASA-5510-K8) ter beschikking. Om te beginnen werden de subnets uitgewerkt voor het opdelen van het netwerk. Er zijn 8 subnets (VLAN's) beschikbaar:

- |  |                   |
|--|-------------------|
| • VLAN 510: Interconnect firewall/switch | (192.168.64.0/23) |
| • VLAN 520: Fysieke servers              | (192.168.66.0/23) |
| • VLAN 530: Virtuele servers             | (192.168.68.0/23) |
| • VLAN 540: DMZ                          | (192.168.70.0/23) |
| • VLAN 550: Nog ter beschikking          | (192.168.72.0/23) |
| • VLAN 560: Nog ter beschikking          | (192.168.74.0/23) |
| • VLAN 570: Management                   | (192.168.76.0/23) |
| • VLAN 580: Nog ter beschikking          | (192.168.78.0/23) |

Om het netwerk high available te maken, kan je gebruik maken van etherchannels (2 fysieke links als één logische link). Als er één van de twee links defect raakt, zal al het verkeer zich verplaatsen over de andere link.

Op de servers is een externe virtuele switch geconfigureerd (deze maakt gebruik van de fysieke netwerk adapter) om te kunnen communiceren met de andere systemen (andere fysieke servers, externe PC, ...).

Tekening 2:



### 3 Configuraties

In dit hoofdstuk zal ik beschrijven welke configuraties er zijn gebeurd en hoe deze precies zijn geconfigureerd.

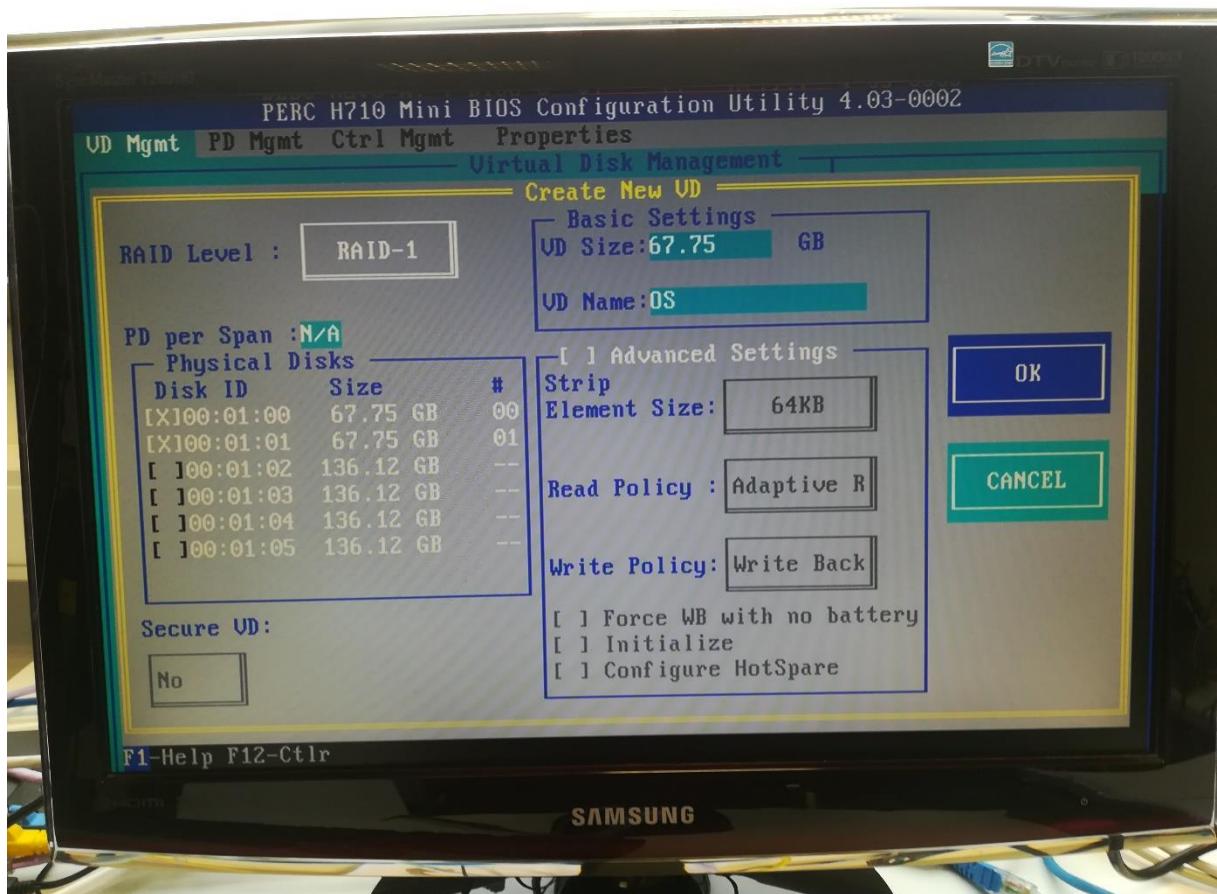
#### 3.1 Hardware (RAID, OS installatie, iDRAC)

##### 3.1.1 Server 1 + Server 2

Aangezien servers 1 en 2 exact dezelfde configuratie hebben, zijn deze samengenomen in dit onderdeel. Beide maken gebruik van een RAID 1 (mirror) level waar het operating systeem opstaat, hierdoor blijft het OS intact al is er een schijf defect. Ook hebben de servers een RAID 10 (striping + mirror) level waar de virtuele machines op draaien.

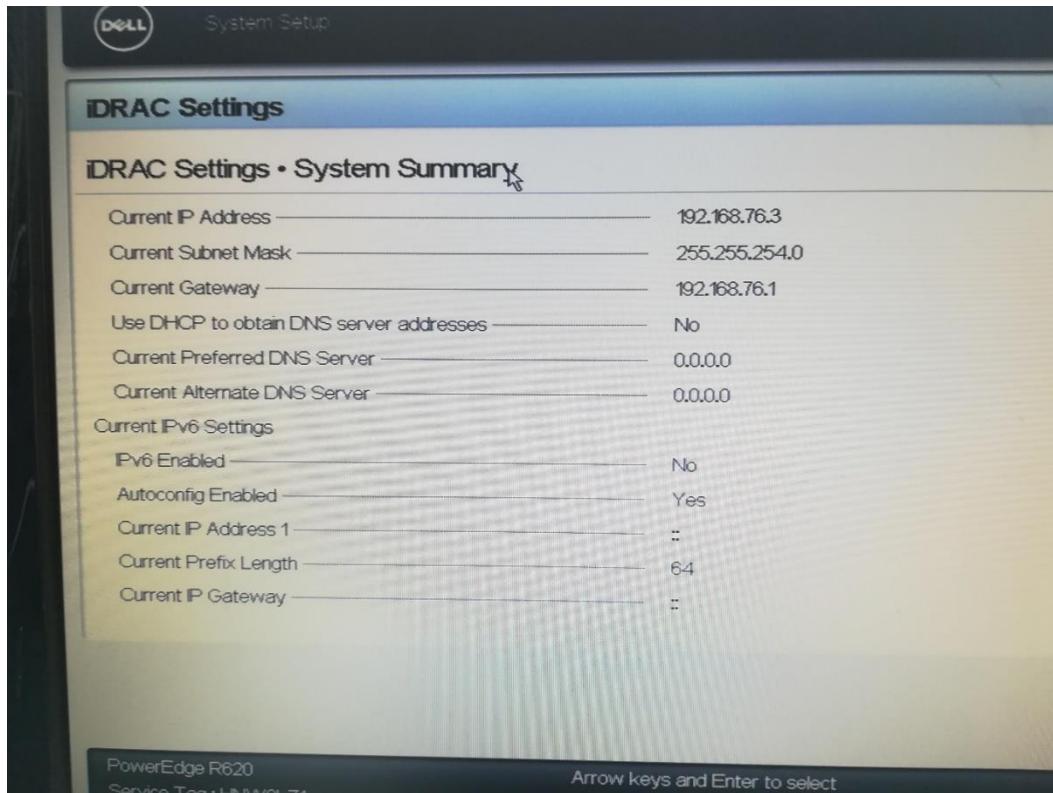
Hieronder vind je een foto van de RAID configuratie van de servers.

Tekening 3:



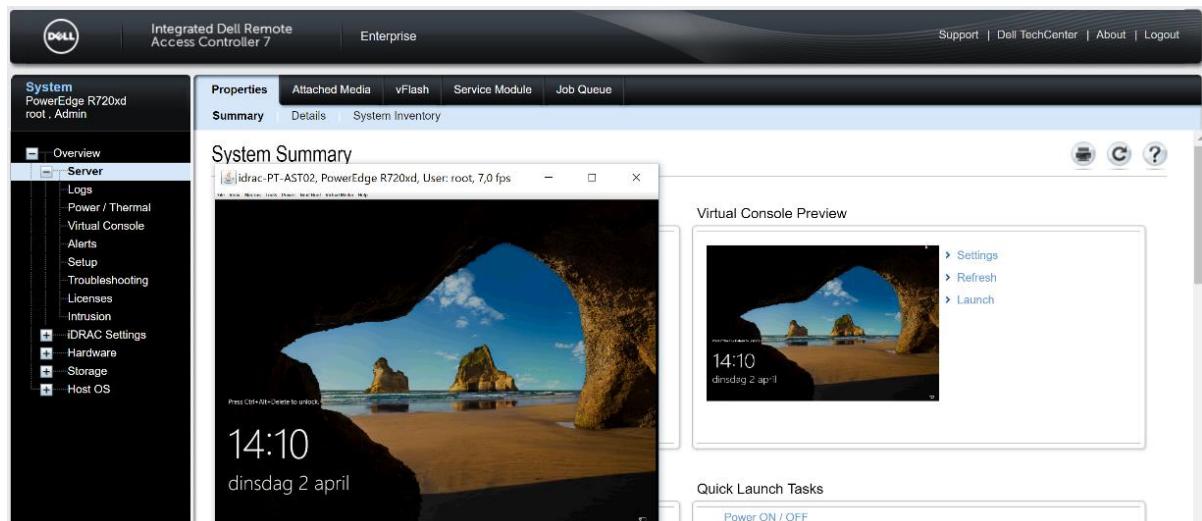
In de system setup van de servers zijn de iDRAC instellingen gemaakt zodat we vanop afstand aan de servers kunnen, zelfs wanneer de server uitgeschakeld is of nog geen besturingssysteem heeft.

Tekening 4:



Dit vergemakkelijkt de installatie van de servers. Servers staan steeds ergens in een datacenter, en dit is niet noodzakelijk in de buurt van je werkplek. Het is niet de bedoeling om een USB-stick of DVD in de server te steken om het besturingssysteem of software te installeren, alles moet vanop afstand via het netwerk kunnen gebeuren. Met iDRAC kan je via de browser connecteren met de server en kan je op die manier aanpassingen maken. Je kan er ook de console starten zodat je het opstarten van de server kan monitoren.

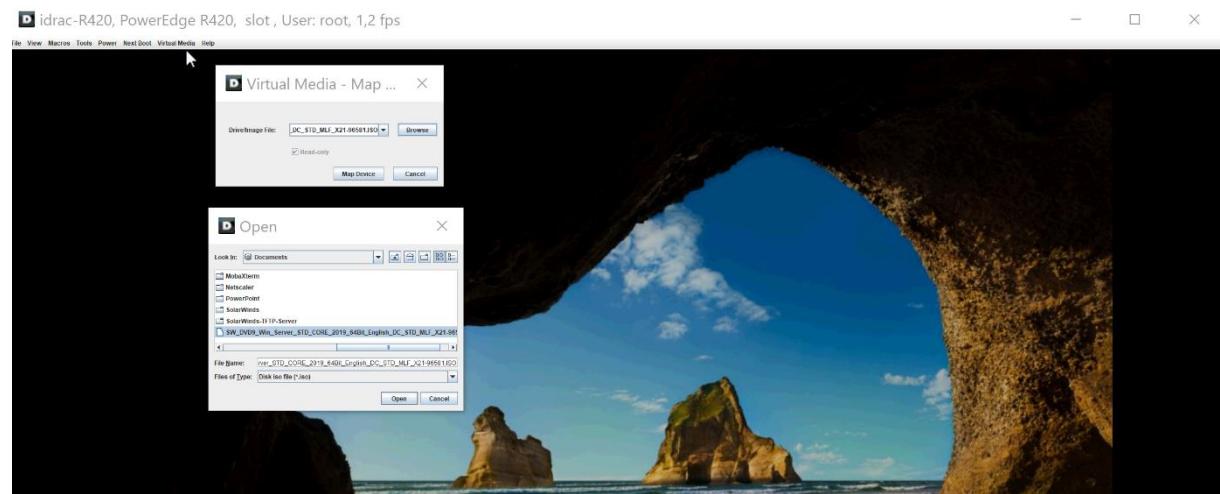
Tekening 5:



Als operating systeem is er besloten om windows server 2019 te gebruiken. Hieronder volgt er een korte uitleg hoe je deze via de iDRAC interface kan installeren.

Om een operating systeem te installeren heb je de ISO van het product nodig. Eens je die hebt, kan je die gebruiken in de iDRAC console om de installatie te starten. In de menubalk navigeer je naar virtual media. Daar heb je de optie om een ISO-bestand als een virtuele CD/DVD te mappen naar je server. Voor de server lijkt het dan alsof er een DVD in een DVD-lezer zit waarvan er opgestart kan worden.

Tekening 6:



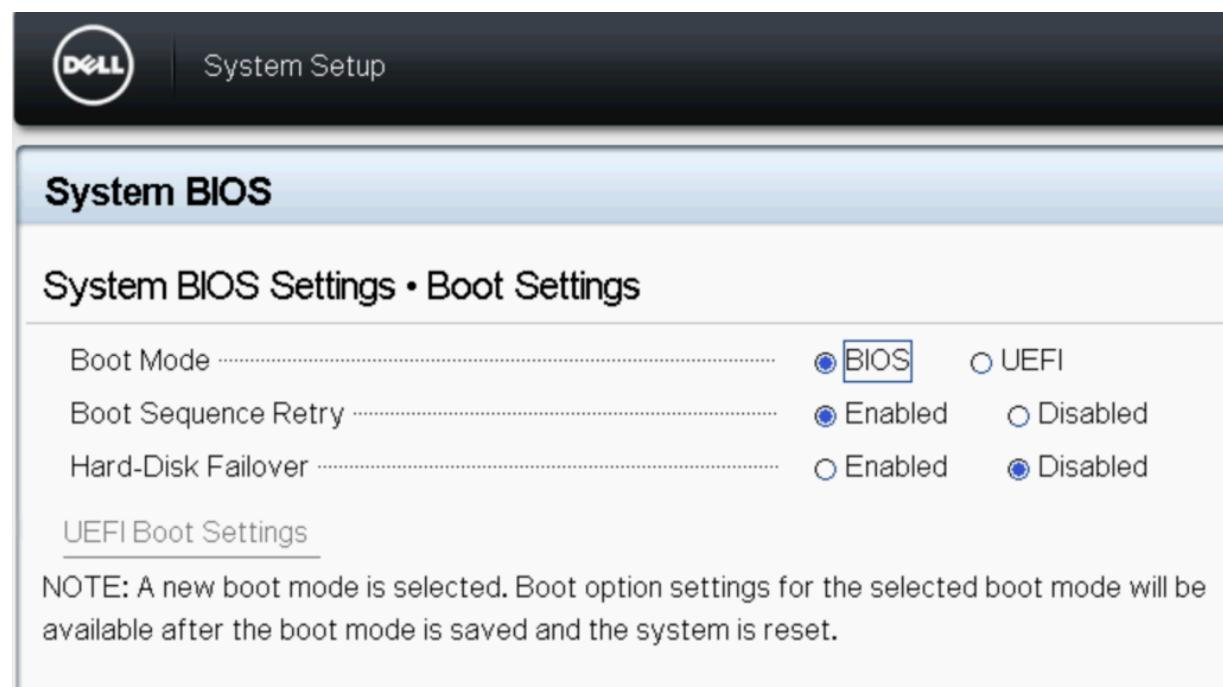
### 3.1.2 Server 3

Deze server wordt gebruikt als back-up en monitoring server. Daardoor heeft deze redelijk wat opslagruimte nodig. Momenteel zitten er 3 schijven van elk 3TB in deze server met een RAID 5 level om geheugenverlies tegen te gaan. Door deze RAID configuratie blijft er een totaal van 5.5TB over om alle data op te kunnen slaan.

Omdat de grootte van de opslagruimte groter is dan 2 TB, moet je de partitionering instellen op GPT (GUID Partition Table) en niet op MBR (Master Boot Record). De redenering hiertoe is dat MBR enkel schijven tot 2 TB ondersteund. Als je dus schijven gebruikt die groter zijn dan 2 TB, zal er dataopslag verloren gaan.

De makkelijkste manier om GPT te gebruiken, is dat je de bootmodus veranderd van BIOS mode naar UEFI mode. Hieronder vind je een afbeelding waar je de boot mode kan veranderen.

Tekening 7:



## 3.2 Netwerk

### 3.2.1 Firewall

De firewall zorgt voor de beveiliging van het netwerk door middel van access lists. Standaard zijn alle 65000 inkomende poorten geblokkeerd. Om communicatie tussen de verschillende toestellen en applicaties mogelijk te maken moet je dus gaten maken in de firewall. Hieronder vind je een screenshot van de firewall die in de demo omgeving geconfigureerd is.

Tekening 8:

Interconnect_ASA (10 incoming rules)						
1	✓ any	192.168.70.0/23	ip	✓ Permit	28	
2	✓ #Internal_Users	any	ip	✓ Permit	0	
3	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	icmp	✓ Permit	0	
4	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	snmp	✓ Permit	0	
5	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_console	✓ Permit	3	
6	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_browser	✓ Permit	133	
7	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	Remote/Desktop	✓ Permit	1	
8	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	Citrix	✓ Permit	0	
9	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	SQL_TCP	✓ Permit	0	
10	✓ #VPN_Users	#VLAN510_VLAN520_VLAN530_VLAN...	SQL_udp	✓ Permit	0	
management (0 implicit incoming rules)						
Global (1 implicit rule)						
1	any	any	ip	Deny		Implicit rule

Het netwerk 192.168.70.0/23 is de DMZ zone en laat alle services toe aan alle gebruikers. Aangezien de DMZ zone een publieke zone is en los van het interne netwerk staat, is dit geen enkel probleem. Enkel VPN gebruikers hebben toegang het interne netwerk.

Om ervoor te zorgen dat het netwerk binnen de firewall bereikbaar is voor gebruikers buiten de firewall, zijn er static routes nodig.

Tekening 9:

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options	
Interconnect_ASA	0.0.0.0	0.0.0.0	192.168.254.49	1	None	
ASA_LAN	192.168.66.0	255.255.254.0	192.168.64.2	1	None	
ASA_LAN	192.168.76.0	255.255.254.0	192.168.64.2	1	None	
ASA_LAN	192.168.68.0	255.255.254.0	192.168.64.2	1	None	
ASA_LAN	192.168.70.0	255.255.254.0	192.168.64.2	1	None	

Belangrijk is dat elk subnet dat je gebruikt, hier terecht komt. Anders zal niemand buiten de firewall met dat subnet kunnen communiceren.

### 3.2.2 Switch

De switch die in de demo omgeving gebruikt wordt, is een layer 3 switch. Dit betekent dat de switch zowel op data layer laag als op netwerk laag kan werken. Op de switch zijn enkele VLAN's aangemaakt die gebruikt worden in de omgeving.

Een VLAN is een groep IP-adressen (eventueel op verschillende switches) die worden samengenomen en zo een virtueel LAN vormen. Meerdere VLAN's kunnen naast elkaar bestaan op dezelfde switch. Deze VLAN's zorgen voor een segmentering van het netwerk, zo kunnen de gebruikers van het ene VLAN geen rechtstreekse informatie sturen naar de gebruikers van een andere VLAN. Hieronder vind je enkele voordelen van VLAN's:

- Een broadcast is beperkt tot het VLAN waar die zich in bevindt. Zeker in grotere netwerken is dit een must, omdat er anders door de vele broadcasts geen bandbreedte meer beschikbaar is voor de data die je eigenlijk wil gaan verzenden.
- Als er gebruikers van VLAN veranderen, kan men deze wijzigen door enkel de switchconfiguratie aan te passen en hoeft men geen kabels te versteken.
- Omdat VLAN's onderling geen informatie kunnen uitwisselen, kunnen de betrouwbare gebruikers gescheiden worden van de onbetrouwbare.

Vooral om de laatste reden wordt er gebruik gemaakt van VLAN's.

Tekening 10:

```
interface Vlan1
  ip address 192.168.78.1 255.255.254.0
!
interface Vlan520
  ip address 192.168.66.1 255.255.254.0
!
interface Vlan530
  ip address 192.168.68.1 255.255.254.0
!
interface Vlan540
  ip address 192.168.70.1 255.255.254.0
!
interface Vlan570
  ip address 192.168.76.1 255.255.254.0
!
ip default-gateway 192.168.64.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.64.1
```

Deze VLAN's zijn de verschillende subnets voor de fysieke servers (VLAN 520), de virtuele machines (VLAN 530), het DMZ netwerk (VLAN 540) en het management netwerk (VLAN 570). De ip route zorgt ervoor dat alle destination adressen die de switch niet kent, doorgestuurd worden naar de firewall.

Om routing mogelijk te maken tussen de VLAN's op een layer 3 switch, moet je de routing aanzetten.

Tekening 11:

```
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
ip routing
```

Om ervoor te zorgen dat de netwerkverbindingen een hoge beschikbaarheid hebben kan je gebruik maken van port-channels. In principe laat je de switch denken dat er 1 logische link is terwijl er 2 fysieke kabels aanwezig zijn. Hierdoor gaat de switch nog steeds het verkeer kunnen doorlaten voor in het geval dat er 1 kabel of switchpoort defect geraakt.

Tekening 12:

```
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk native vlan 520
switchport trunk allowed vlan 520,530
switchport mode trunk
!
interface Port-channel2
switchport trunk encapsulation dot1q
switchport trunk native vlan 520
switchport trunk allowed vlan 520,530
switchport mode trunk
!
interface Port-channel3
switchport trunk encapsulation dot1q
switchport trunk native vlan 520
switchport trunk allowed vlan 520,530
switchport mode trunk
!
interface GigabitEthernet0/1
no switchport
ip address 192.168.64.2 255.255.254.0
```

De kabels van de switch naar de management poorten van de servers zijn op access mode gezet, hierdoor laat deze alleen verkeer toe naar VLAN 570.

Tekening 13:

```
interface GigabitEthernet0/18
switchport access vlan 570
switchport mode access
!
interface GigabitEthernet0/19
switchport access vlan 570
switchport mode access
!
interface GigabitEthernet0/20
switchport access vlan 570
switchport mode access
```

### 3.2.3 Servers

De netwerk configuratie van de servers zijn vrij simpel. Het enige waar je zeker rekening mee moet houden is dat je de NIC Teaming (het samennemen van poorten) aanzet om de port-channel te activeren van switch naar server. Als dit niet gebeurd, zal de switch de port-channel niet kunnen maken en dus errors geven.

Tekening 14:

Computer name	Server3	Last installed updates	28/02/2019 11:56
Domain	Virt.com	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Yesterday at 22:30
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Enabled	Time zone	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
vEthernet (vEthernet)	192.168.69.2, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2019 Standard	Processors	Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz, Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz
Hardware information	Dell Inc. PowerEdge R420	Installed memory (RAM)	7.94 GB
		Total disk space	5587.39 GB

Bij het maken van een nieuw team, selecteer je de adapters die geconnecteerd zijn met de switch. Belangrijk is dat als je LACP gebruikt, de Teaming mode zeker op LACP zet en niet standaard op switch independent laat staan.

Tekening 15:

NIC Teaming X

New team

Team name:

Member adapters:

In Team	Adapter	Speed	State	Reason
<input type="checkbox"/>	NIC3	Disconnected		
<input type="checkbox"/>	NIC4	Disconnected		
<input type="checkbox"/>	vEthernet (vEthernet)	2 Gbps		

Additional properties

**Teaming mode:**

**Load balancing mode:**

**Standby adapter:**

**Primary team interface:**

### 3.3 Toepassingen

Om een duidelijker beeld te geven waar elk VM zich bevindt, staat hieronder een afbeelding van alle VM's in de demo-omgeving.

Server 1:

Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Citrix_2	Running	0%	2596 MB	26.03:52:58	
Citrix_d2	Running	0%	5260 MB	26.03:52:56	
DC_1	Running	0%	2604 MB	29.04:45:29	
DFSROOT_1	Running	0%	1686 MB	29.04:45:32	
FS_1	Running	0%	1744 MB	29.04:45:29	
Powershell_AD	Running	0%	1846 MB	18.23:39:31	
PS_1	Running	0%	1978 MB	29.04:45:23	

Server2:

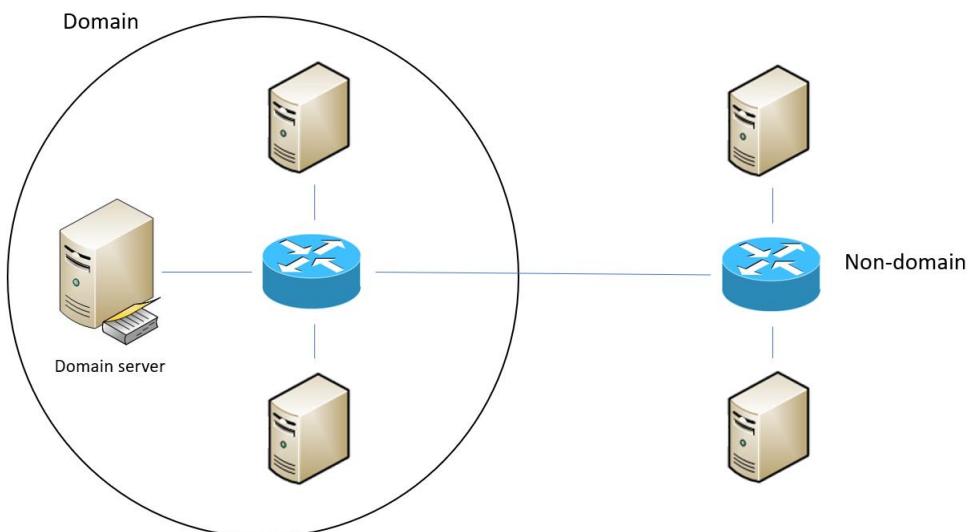
Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Citrix_1	Running	0%	2628 MB	26.03:53:41	
Citrix_d1	Running	0%	6720 MB	26.03:53:39	
citrix_netscale	Running	0%	6448 MB	17.21:34:44	
DC_2	Running	0%	2906 MB	43.02:46:29	
DFSROOT_2	Running	0%	1386 MB	41.02:28:37	
DMZ_RODC	Running	0%	1528 MB	29.02:47:55	
FS_2	Running	0%	2100 MB	41.02:38:34	
NetScaler Virtual Appliance	Running	4%	2048 MB	29.00:16:07	

Server3:

Virtual Machines					
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Azure_connect	Running	0%	2608 MB	6.02:56:15	
Backup	Running	0%	3736 MB	13.01:22:46	
Management	Running	0%	610 MB	1.02:41:01	
MFA_server	Running	0%	1534 MB	1.01:37:14	
NPS	Running	0%	970 MB	00:15:41	
PS_1	Off				
WIN10_Host	Running	11%	962 MB	00:20:37	

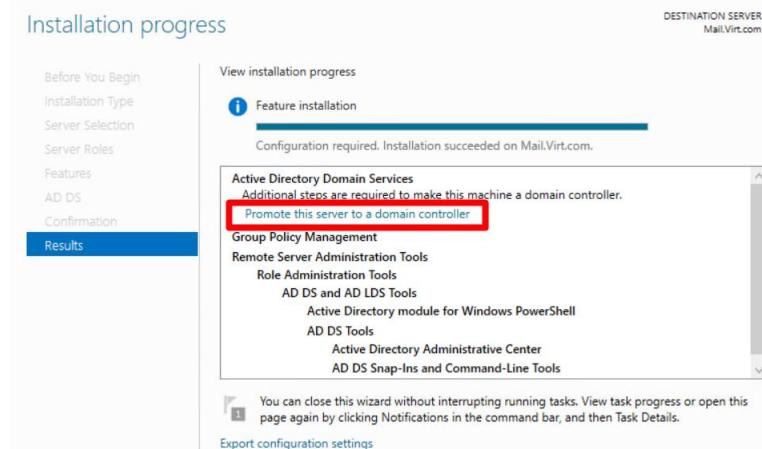
### 3.3.1 Domaincontroller

De domaincontroller beheert de rechten van alle users op het domein, wat handig is voor grote netwerken. Zou je geen domaincontroller gebruiken, moet de administrator op iedere PC de rechten aanpassen.

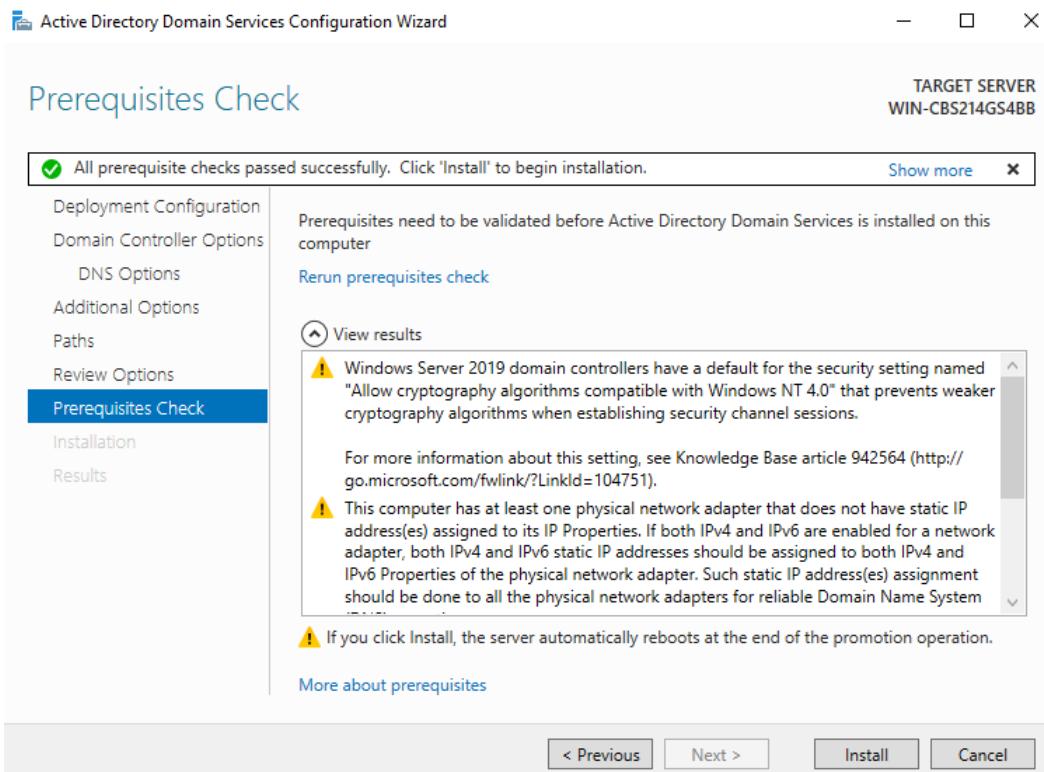


#### 3.3.1.1 Installatie primary domaincontroller (DC\_1)

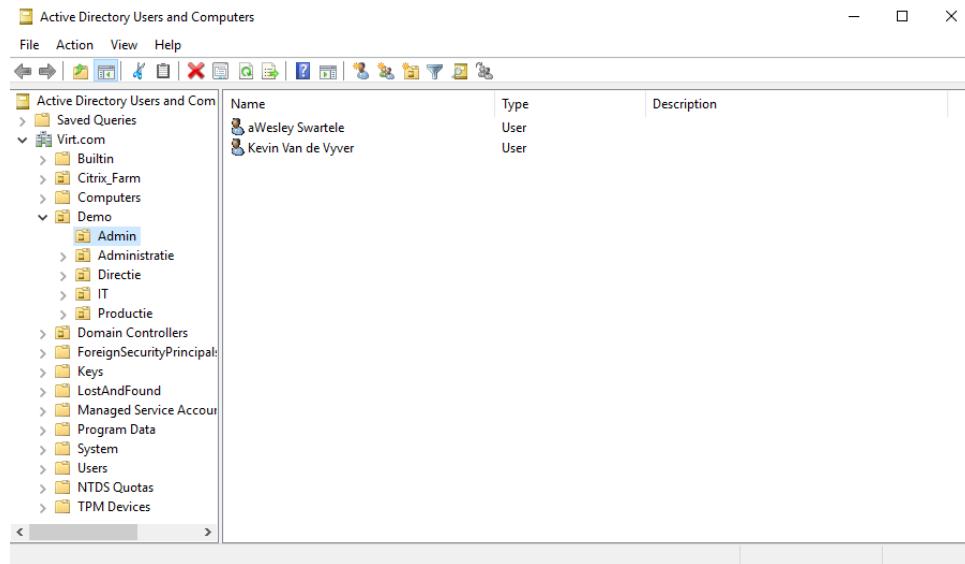
DC\_1 is de primaire domaincontroller en zal een nieuw domein moeten aanmaken. Via de server manager kan je deze rol installeren. De volgende stap na het installeren van de rol is de server promoten tot een domaincontroller.



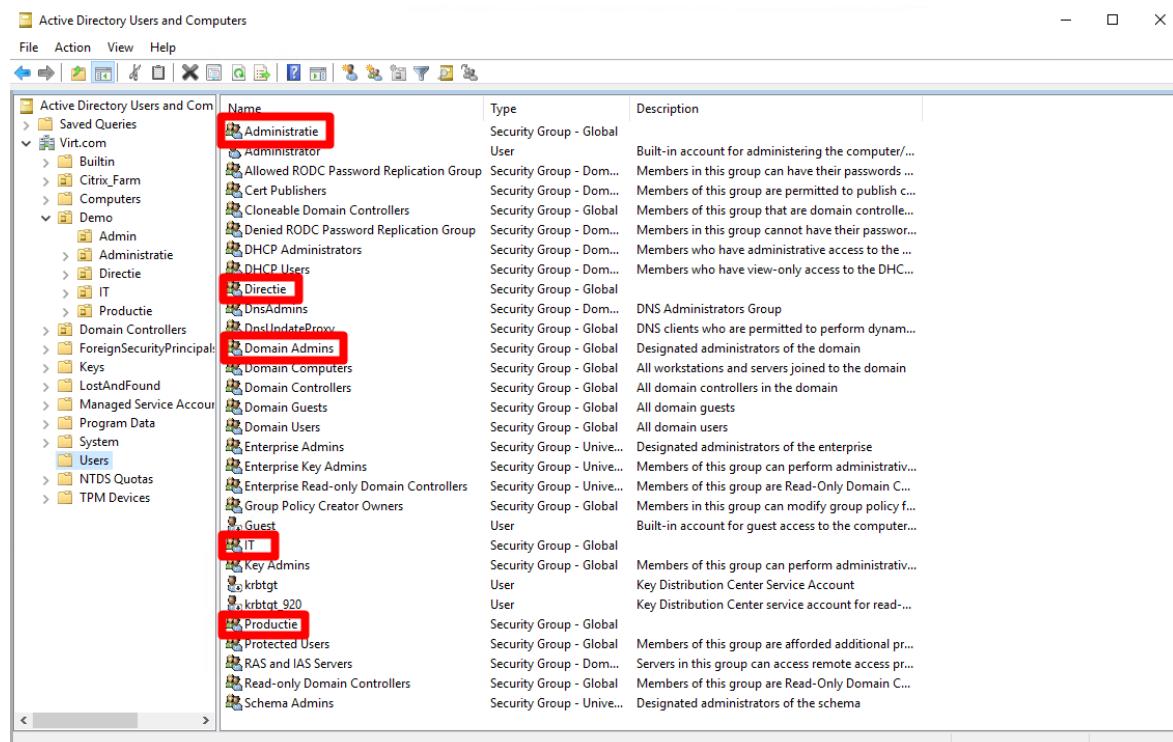
In de configuratie van de domaincontroller voeg je een nieuw domein (forest) toe, stel je een paswoord in om de AD database te kunnen restoren of repareren. Eens de server gepromote is tot een domaincontroller kan de "echte" configuratie beginnen.



Om een domein goed op te starten is het aangeraden om eerst de structuur hiervan op te stellen. Dit zal het werk later wat gemakkelijker maken. Hieronder zie je een afbeelding van de structuur in de demo omgeving. Er zijn verschillende departementen aangemaakt (Admin, Administratie, Directie, IT en Productie). Later kan je group policies toepassen op deze departementen. Meer info over group policies volgt nog.

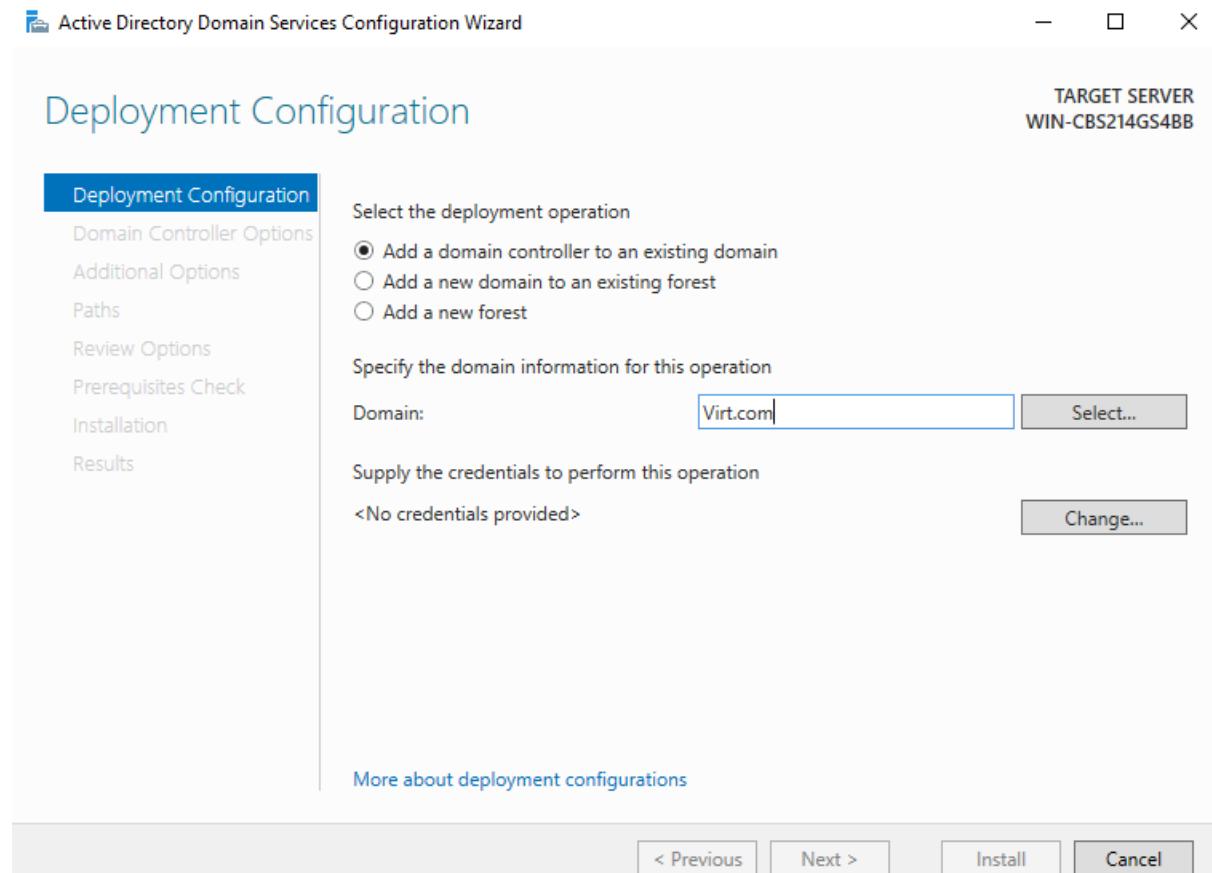


Voor elk departement is er een security groep aangemaakt. Alle gebruikers die tot die groep behoren kan je hieraan toevoegen. Dankzij deze groepen kan je de rechten van de gebruikers instellen op heel het domein. Dit is een veel efficiëntere en snellere manier dan dat je op elke computer individueel de rechten moet aanpassen.

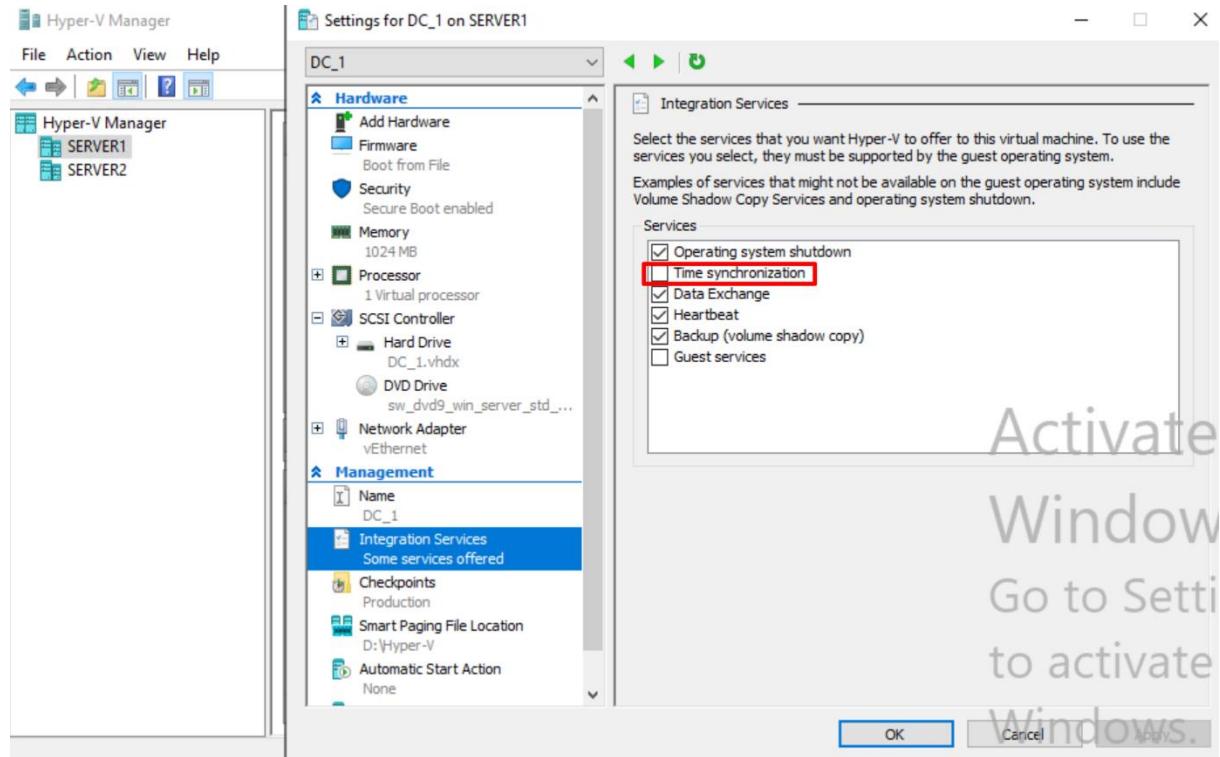


### 3.3.1.2 Installatie backup domaincontroller (DC\_2)

DC\_2 is de backup domaincontroller (BDC), deze zal de taken van DC\_1 overnemen als de VM uitvalt. Om deze BDC in te stellen moet je - net als een primaire domaincontroller - de rol installeren. Eens de rol geïnstalleerd is, moet je deze promoten tot een domaincontroller. In de configuratie is er echter wel een verschil. Nu moet je deze domaincontroller toevoegen aan een bestaand domein. De rest van de configuratie blijft hetzelfde.



In een domein is het belangrijk dat de tijd gesynchroniseerd is tussen alle VM's. Als dit niet het geval is kunnen er problemen optreden. De synchronisatie kan je instellen met de w32tm service, deze staat standaard geactiveerd in een windows server omgeving. Een belangrijke opmerking is dat als de tijd gesynchroniseerd wordt van hypervisor naar VM, je deze uitzet naar de domaincontrollers. Als dit wel aanstaat, zal de domaincontroller de tijd van de hypervisor nemen en niet die van de externe tijdserver. De andere VM's kunnen deze instelling laten aanstaan.



Eerst moet je de server – die als tijdserver dient – identificeren. Meestal is dit de primary domaincontroller. Om deze te vinden, open je een command prompt en gebruik je het commando *net time*.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\kvdvyy>net time
Current time at \\DC.Virt.com is 19/04/2019 13:41:37

The command completed successfully.

C:\Users\kvdvyy>
```

Log nu in op de tijdserver en selecteer een externe tijdserver waarmee je wilt synchroniseren. In de demo-omgeving wordt *time.windows.com* gebruikt als externe tijdserver. Eens deze gevonden is, kan je de delay testen tussen de huidige en de externe tijdserver.

```
C:\Users\kvdvyy>w32tm /stripchart /computer:time.windows.com /dataonly
Tracking time.windows.com [52.166.120.77:123].
The current time is 19/04/2019 13:44:50.
13:44:50, -00.0019472s
13:44:52, -00.0017504s
13:44:54, +00.0014823s
^C
C:\Users\kvdvyy>
```

Om de externe tijdserver te gebruiken, moet je deze instellen in de w32tm config. Dit kan met het volgende commando.

```
w32tm /config /manualealpeerlist:time.windows.com /syncfromflags:MANUAL
```

De laatste stap is de w32tm config updaten en synchroniseren.

```
w32tm /config /update
```

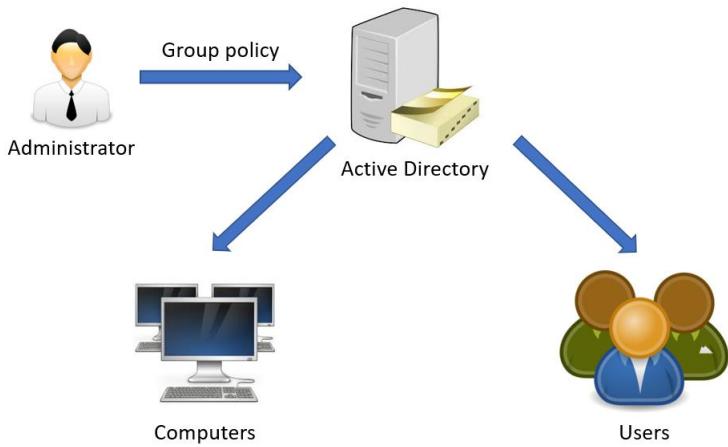
```
w32tm /resync
```

Tot slot moeten de clients nu de primary domain controller gebruiken als tijdserver. Soms gebeurd dit automatisch maar niet altijd. Om manueel de tijdserver aan te passen, kan je het volgend commando gebruiken.

```
net time \\NETTIMESERVER.DOMAIN.com /set /y
```

### 3.3.2 Group policies

Met group policies kan de administrator instellingen en configuraties van gebruikers en computers beheren. Dit kan je onder andere gebruiken om de startpagina van de browser aan te passen, rechten aan bepaalde schijven en/of mappen op de computer toe te kennen en standaard templates voor documenten toe te wijzen.



#### 3.3.2.1 Configuratie default browser (DC\_1)

Om bijvoorbeeld chrome als default browser in te stellen voor bepaalde functies, kan je een bestand downloaden van het internet of je kan ervoor kiezen om er zelf één aan te maken. Enkele voorbeelden van deze functies zijn links of bestanden.

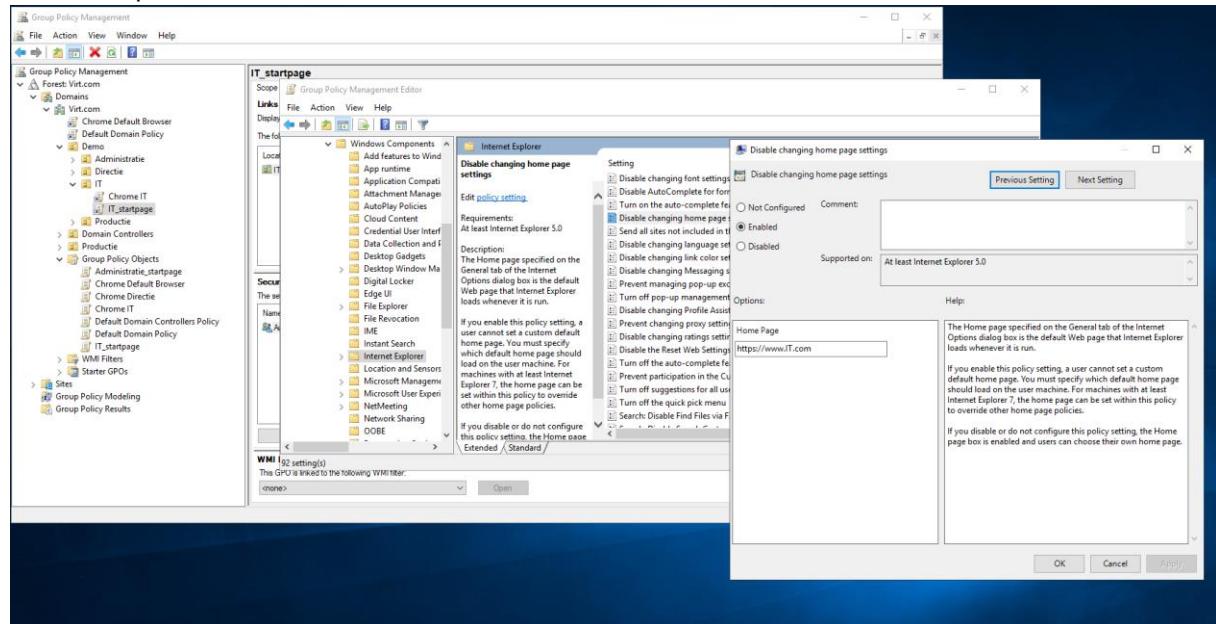
**Uitleggen zelf aangemaakt**

```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
    <Association Identifier=".htm" ProgId="ChromeHTML" ApplicationName="Google Chrome" />
    <Association Identifier=".html" ProgId="ChromeHTML" ApplicationName="Google Chrome" />
    <Association Identifier="http" ProgId="ChromeHTML" ApplicationName="Google Chrome" />
    <Association Identifier="https" ProgId="ChromeHTML" ApplicationName="Google Chrome" />
</DefaultAssociations>
```

### 3.3.2.2 Configuratie browser startpagina (DC\_1)

Met group policies kan je de startpagina van de browser aanpassen. Zo kan je bijvoorbeeld de website van het bedrijf laten openen bij de opstart (dit kan je aanpassen per departement). Dit toepassen voor Internet Explorer is gemakkelijker dan het aanpassen in chrome, waar je een template voor moet downloaden.

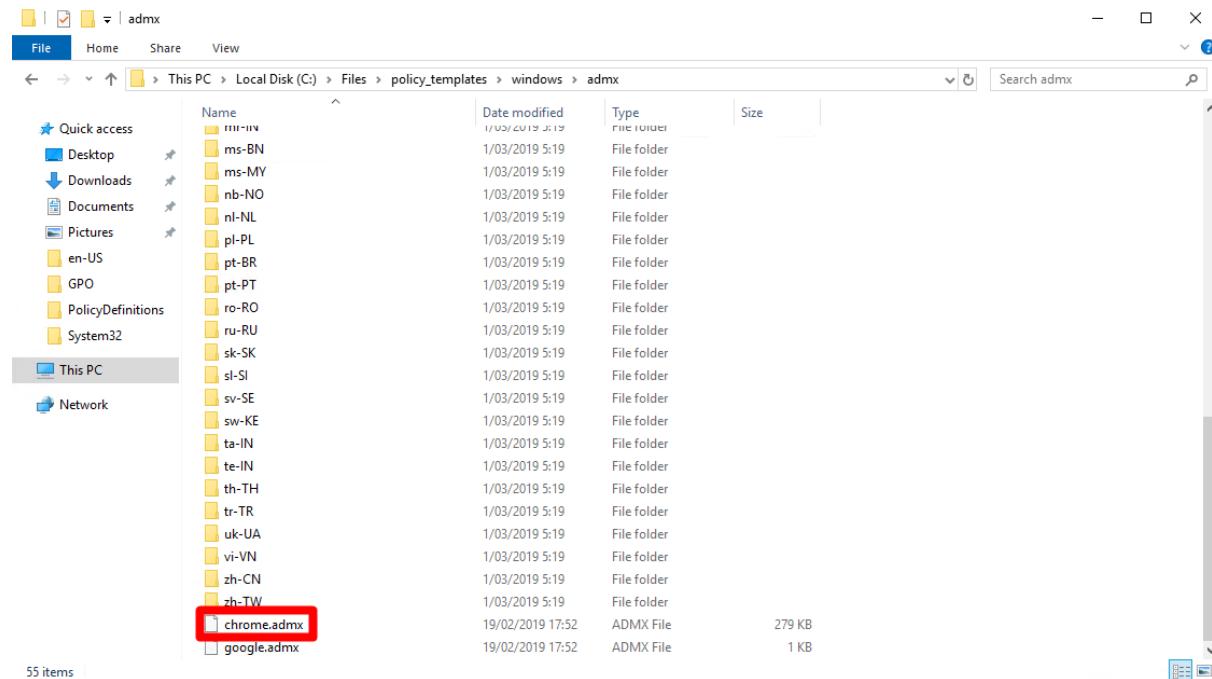
Internet explorer:



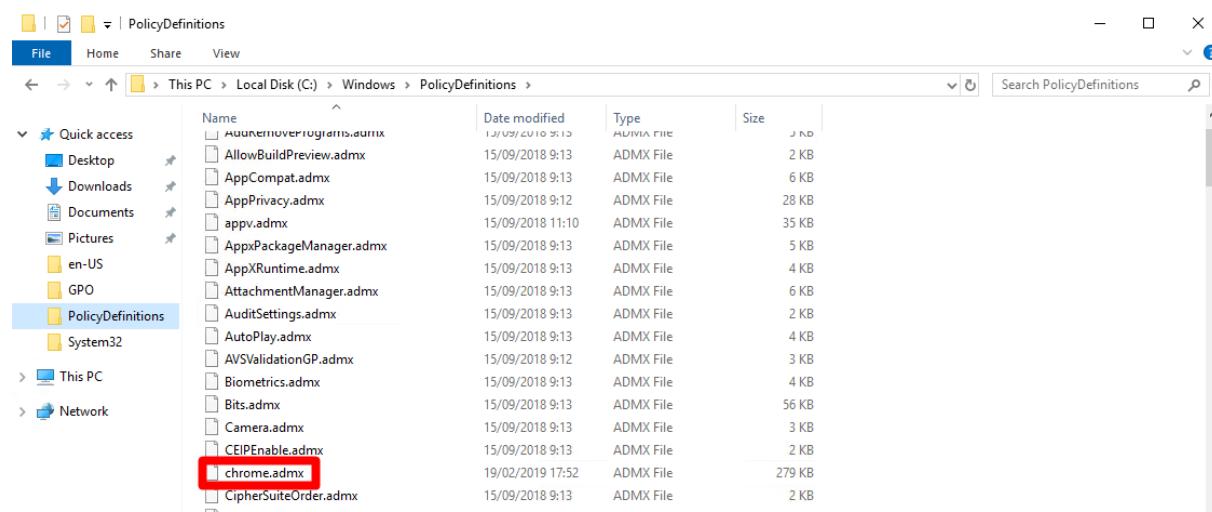
De template die je nodig hebt voor chrome kan je met deze URL halen:  
[http://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](http://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip)

Eens gedownload, unzip je het bestand op de server en navigeer je naar de windows folder. Hier zie je 2 belangrijke folders, namelijk *adm* en *admx*

Om dit te implementeren op windows server 2008 of nieuwer, navigeer ja naar de *admx* folder. Hier kopieer je het *chrome.admx* bestand.

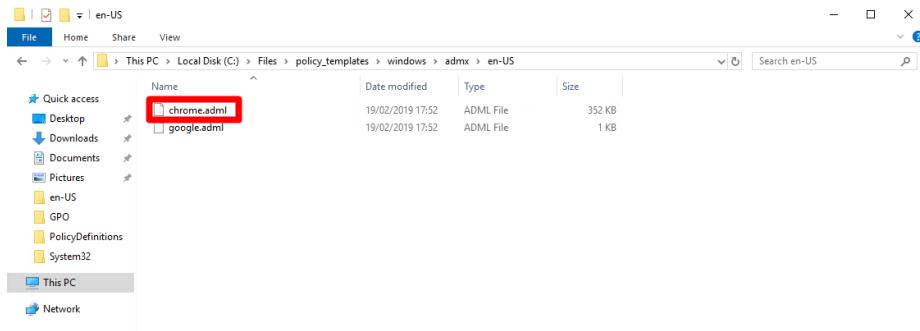


Open een nieuwe verkenner, navigeer naar C:\Windows\PolicyDefinitions en plak het bestand daar.



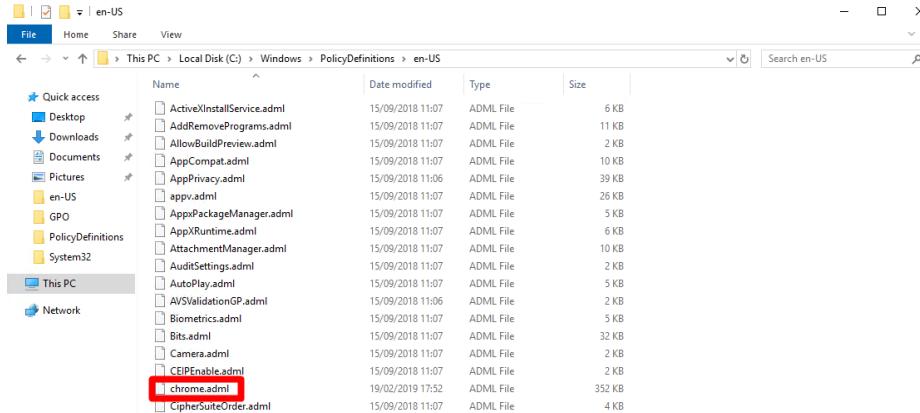
Met de eerste verkenner, open de folder met de juiste taal en kopieer het chrome.adml bestand.

pad



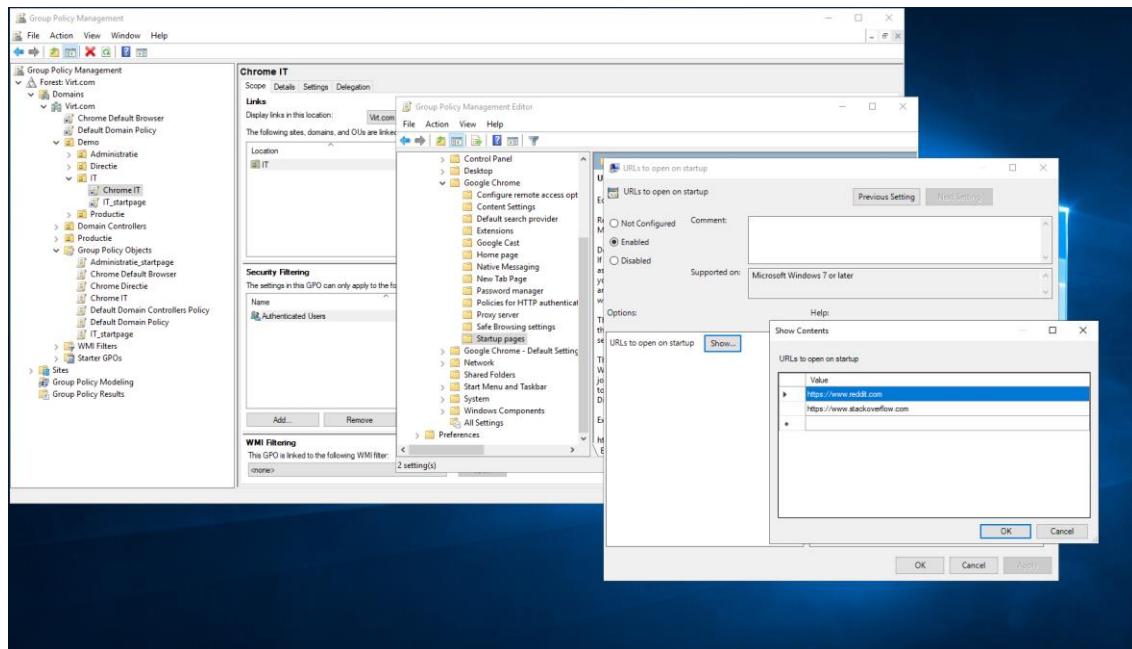
Neem je tweede verkenner terug, open de folder met je taal en plak het .adml bestand in deze folder.

pad



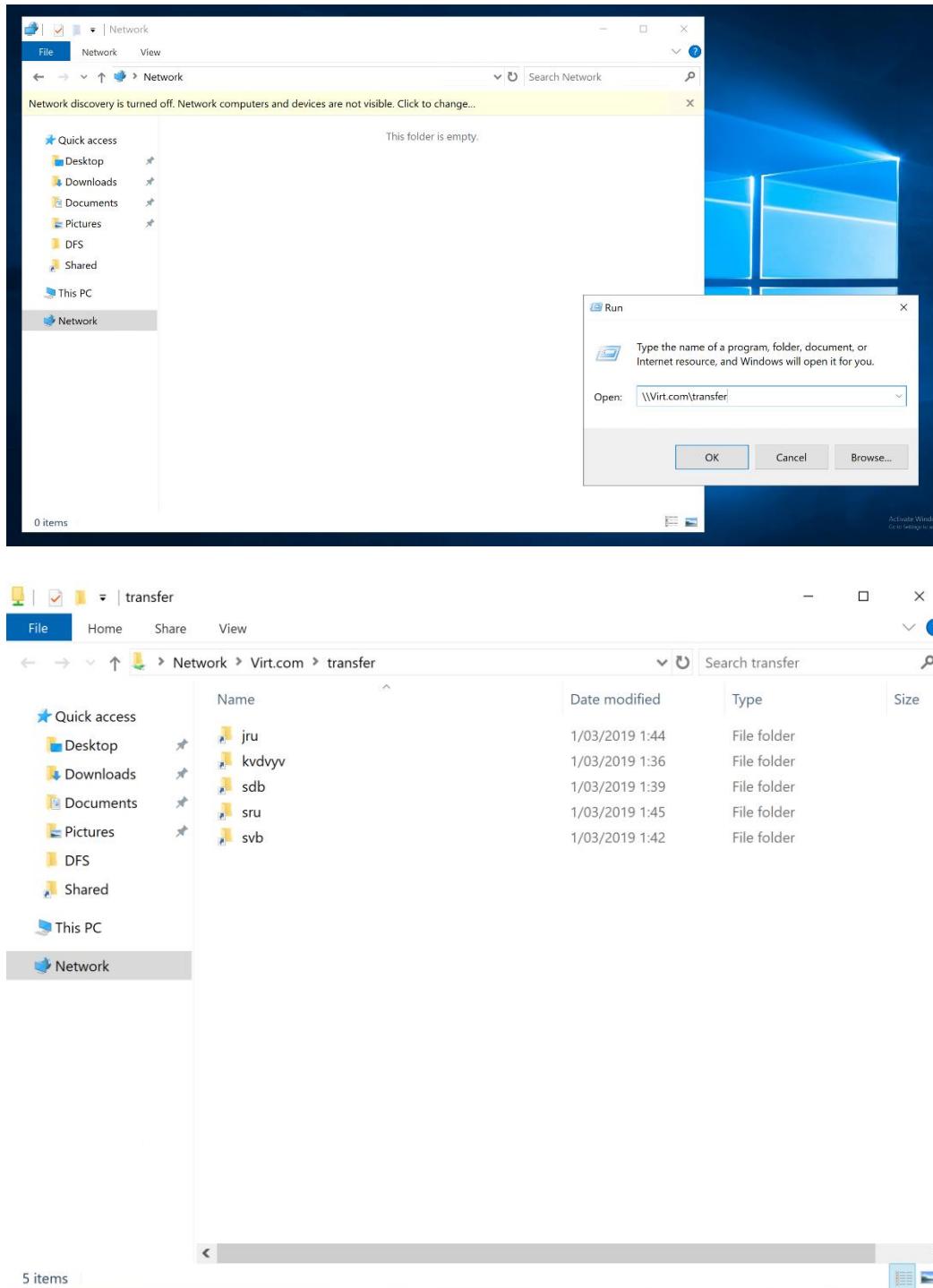
Nadat deze twee bestanden op de juiste plaats staan, zal je in de policy manager een extra folder *Google Chrome* zien staan waar je de policies kan aanpassen.

## Chrome:

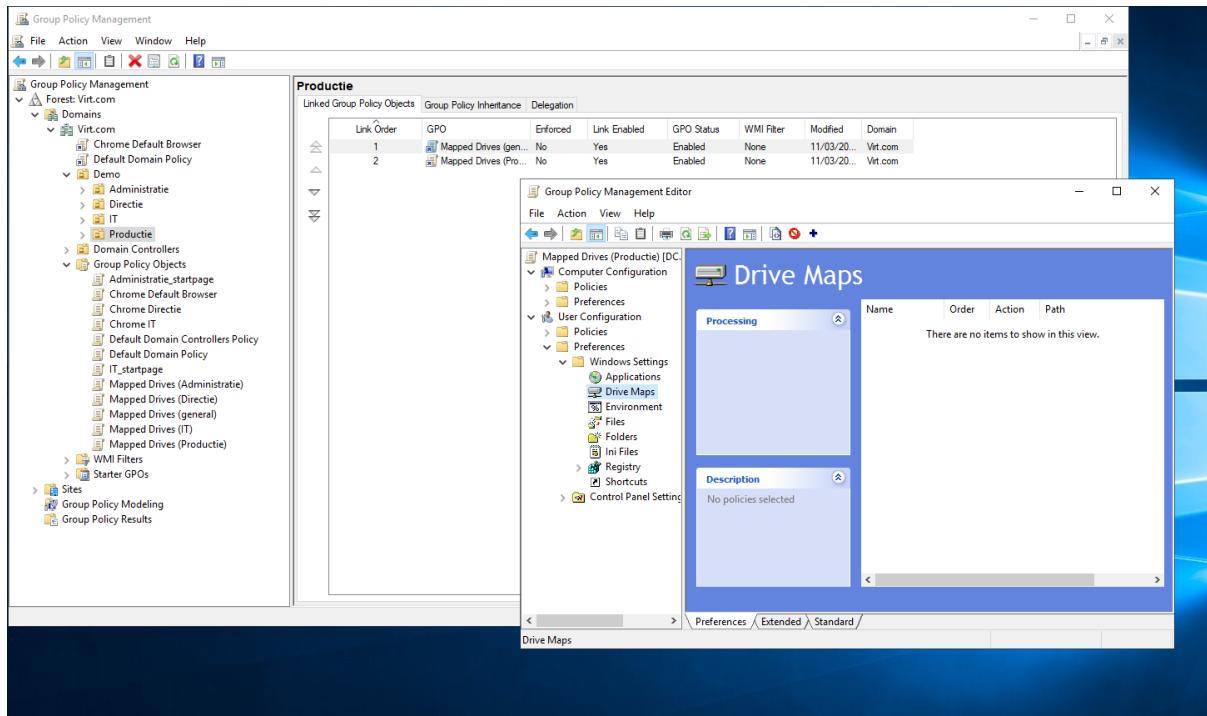


### 3.3.2.3 Configuratie drive mapping (DC\_1)

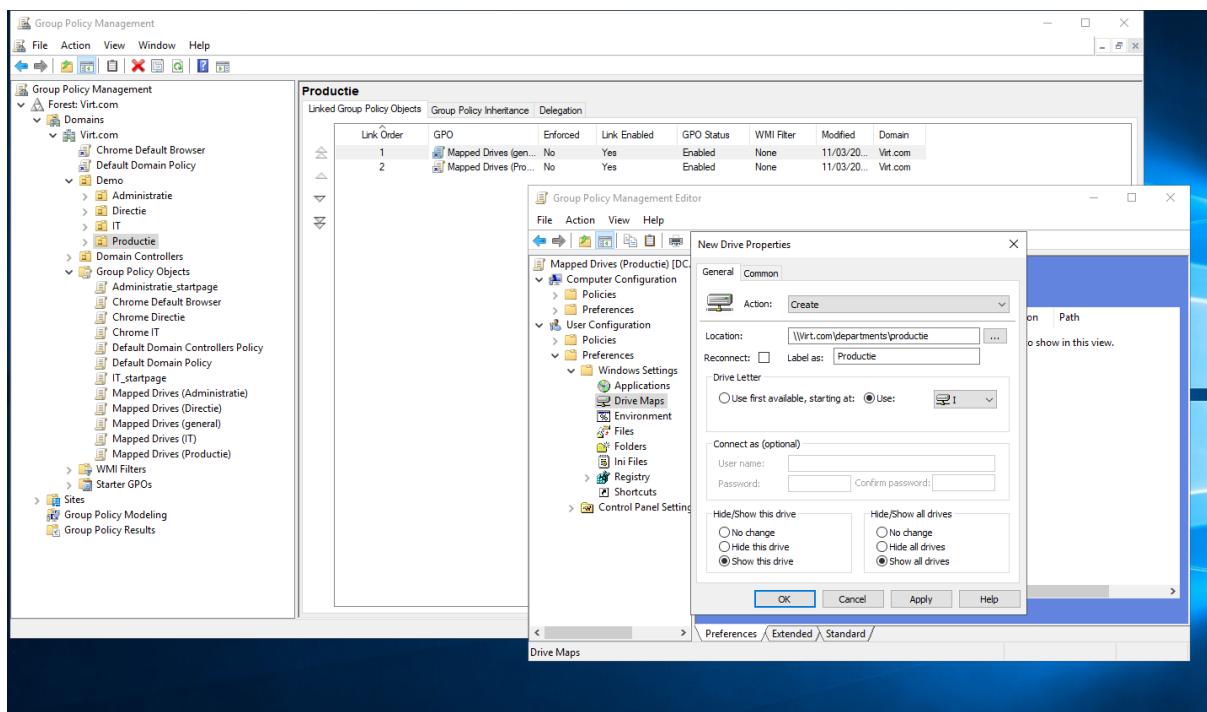
Een ander voordeel van group policies is drive mapping. Hiermee kan je bepaalde netwerkschijven zichtbaar maken voor gebruikers in een domein. Een opmerking hierbij is dat de mappen al beschikbaar waren voor de gebruikers met het run commando, maar dit is niet echt evident.



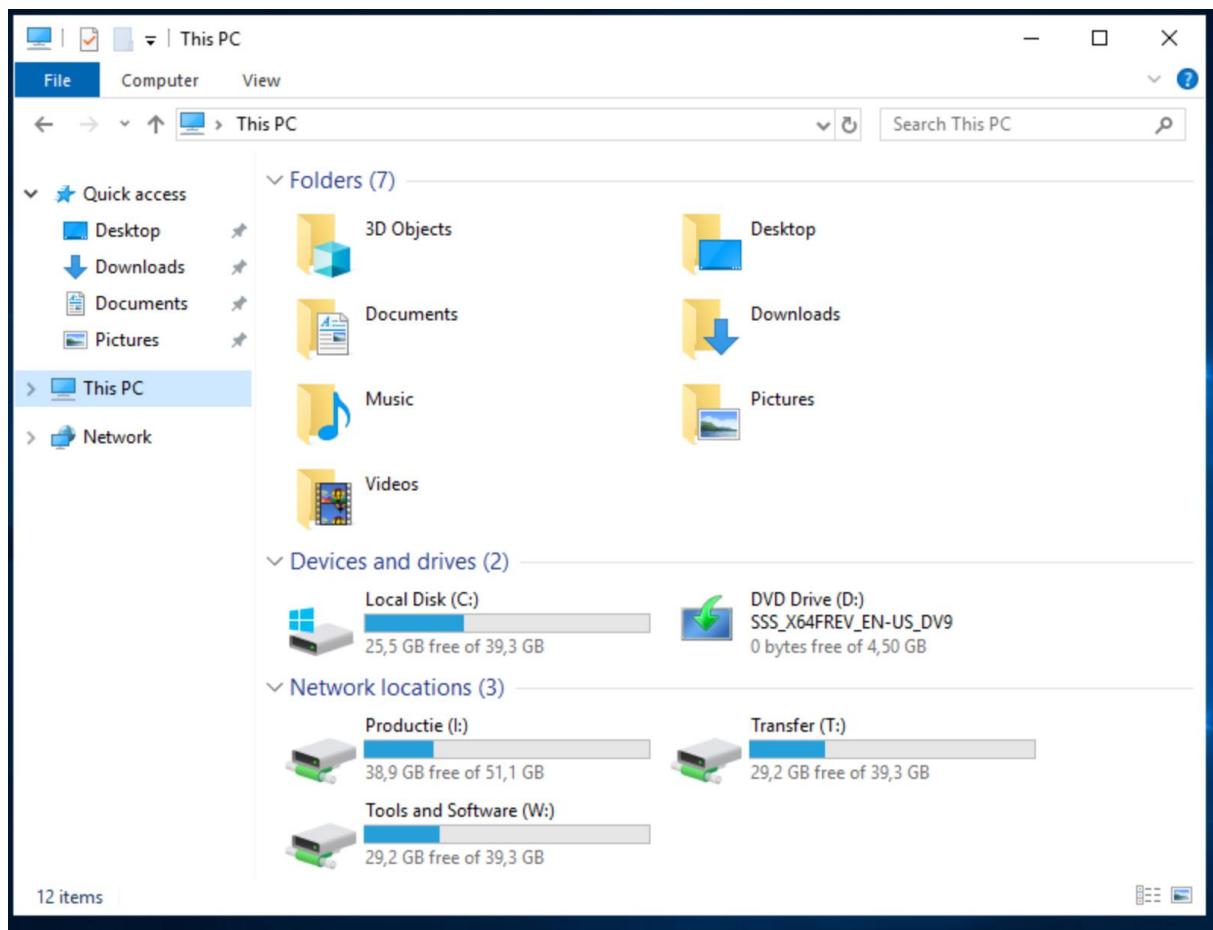
De configuratie van de drive maps doe je als volgt. Navigeer naar de organizational unit (departement) waar je een mapped drive wil maken. Selecteer daarna new GPO. Geef de GPO een naam en navigeer naar User Configuration -> Preferences -> Drive Maps en maak daar een nieuwe mapping aan.



Geef het pad naar de gedeelde netwerkfolder in, geef een naam en een letter naar keuze.



Na het aanmaken van deze group policy kan het departement *Productie* gemakkelijk aan deze schijf geraken. Hieronder vind je een resultaat van het departement.



### 3.3.3 DNS

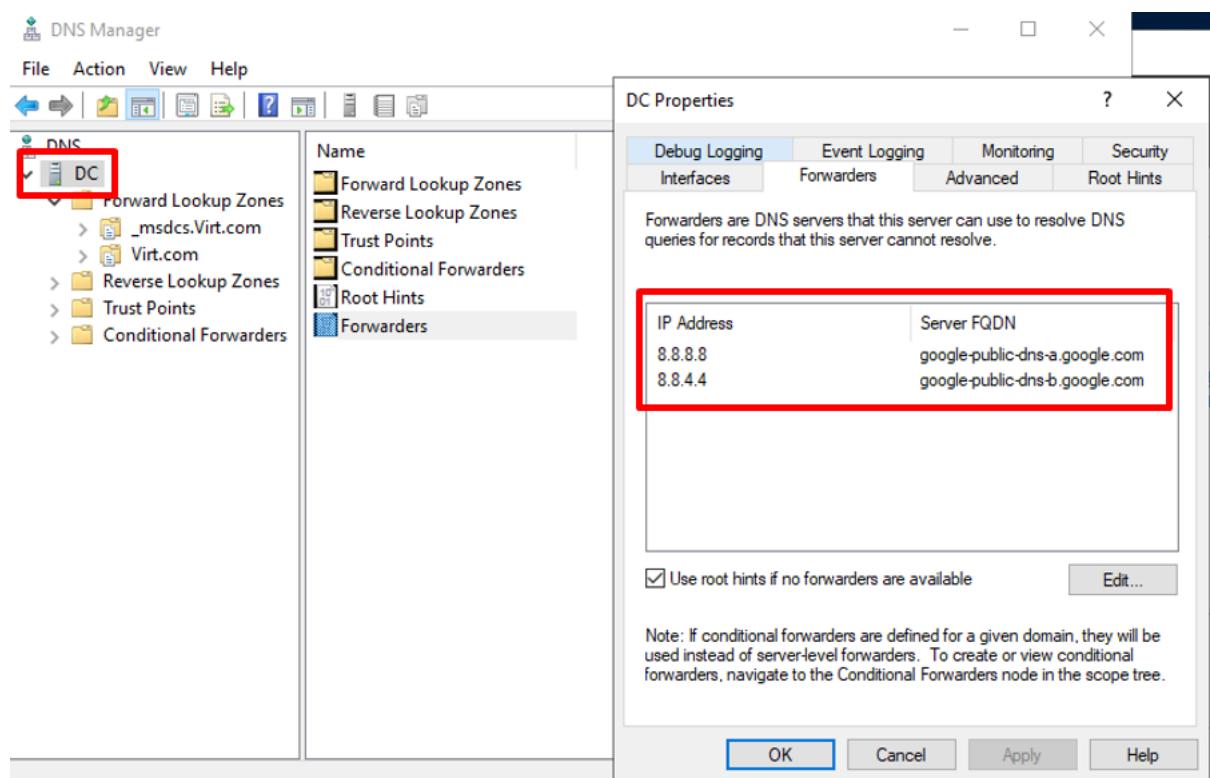
#### 3.3.3.1 Installatie DNS (DC\_1)

Domain Name System, afgekort DNS maakt het mogelijk om op het internet te zoeken naar adresnamen in plaats van enkel IP-adressen. In de demo omgeving is de DNS toepassing samengenomen met de domaincontroller.

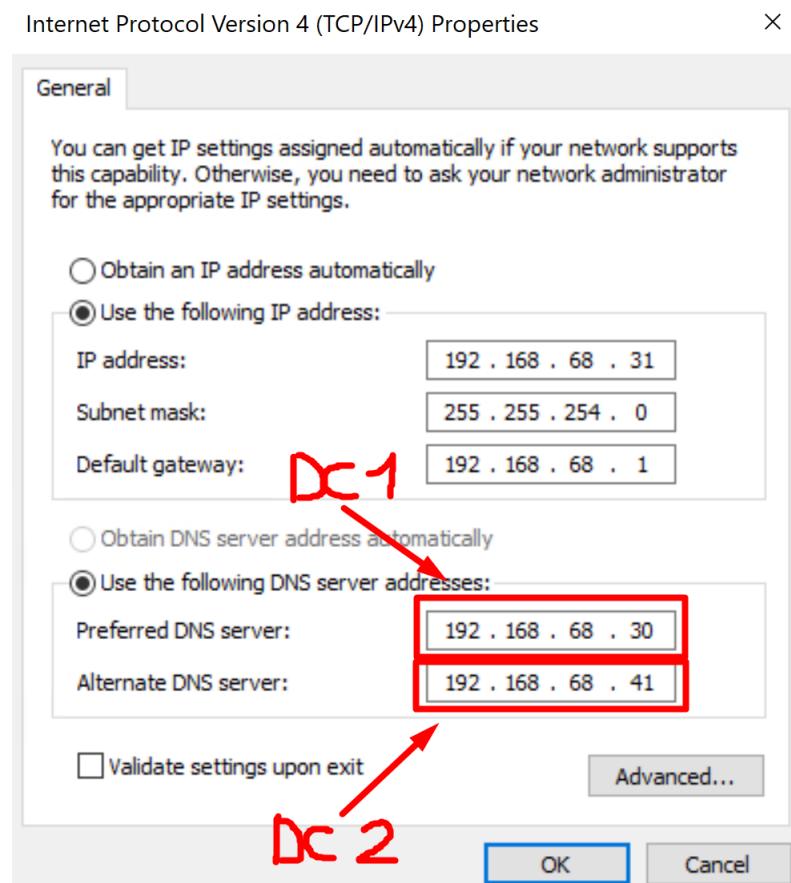
Om te kunnen zoeken met adresnamen, moet je forwarders configureren. Deze forwarders zijn meestal publieke DNS servers, enkele voorbeelden hiervan zijn:

- OpenDNS,
- Cloudflare,
- Google Public DNS,
- Norton ConnectSafe,
- Comodo Secure DNS,
- Quad9
- Verisign DNS.

In de demo omgeving is er gebruik gemaakt van de Google Public DNS (8.8.8.8 en 8.8.4.4).



De demo omgeving maakt gebruik van een PDC (primary domaincontroller) en een BDC (backup domaincontroller). Om ervoor te zorgen dat de DNS blijft werken op de servers en computers moet je beide DNS servers toevoegen in de netwerkinstellingen.

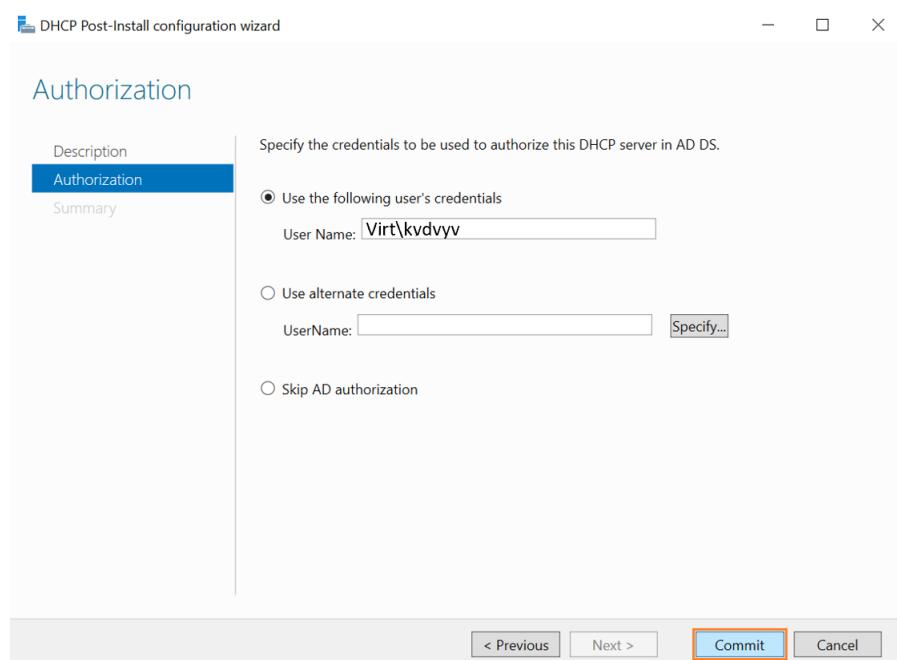


### 3.3.4 DHCP

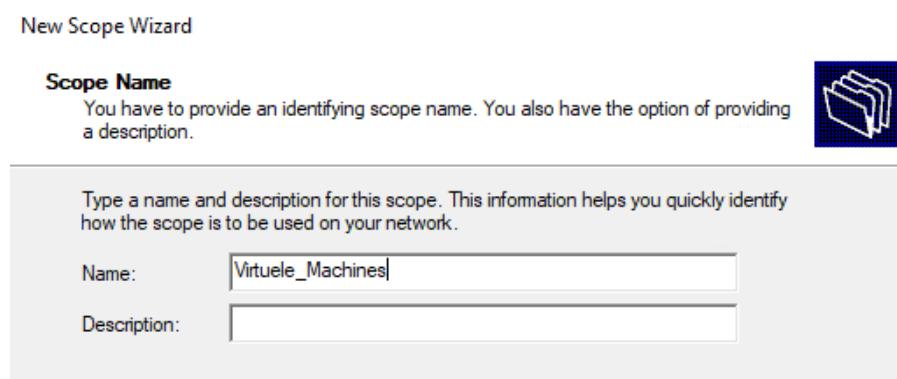
DHCP kan je instellen om dynamisch IP-adressen uit te delen aan computers, evenals de correcte DNS instellingen. De DHCP server wijst IP-adressen toe vanuit een pool en zijn herbruikbaar wanneer een computer wordt uitgeschakeld.

#### 3.3.4.1 Installatie DHCP (DC\_1)

Begin met de rol van DHCP te installeren. Eens deze geïnstalleerd is, kan je de DHCP installatie beginnen. In de setup geef je de inlog gegevens mee van de active directory.



Open nu de DHCP applicatie op de server en maak een nieuwe scope aan, geef deze een naam en eventueel een beschrijving.



De volgende stap is de range instellen van de beschikbare IP-adressen, uitgesloten adressen kan je hierna nog instellen.

New Scope Wizard

**IP Address Range**

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 68 . 110

End IP address: 192 . 168 . 68 . 254

Configuration settings that propagate to DHCP Client

Length:

23 ▾

Subnet mask:

255 . 255 . 254 . 0

< Back

Next >

Cancel

New Scope Wizard

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: \_\_\_\_\_

End IP address: \_\_\_\_\_

Add

Excluded address range:

Remove

Subnet delay in milli second:

0 ▾

< Back

Next >

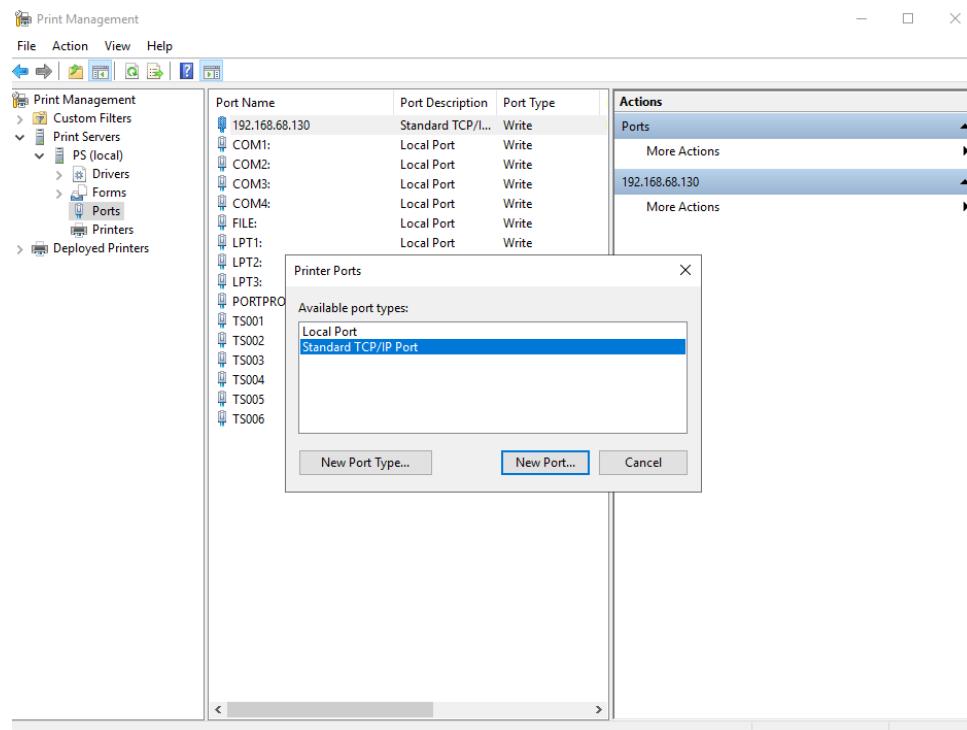
Cancel

Na deze stap kan je de andere DHCP opties ook instellen (default gateway en DNS). Tot slot activeer je de scope en kan je deze gebruiken.

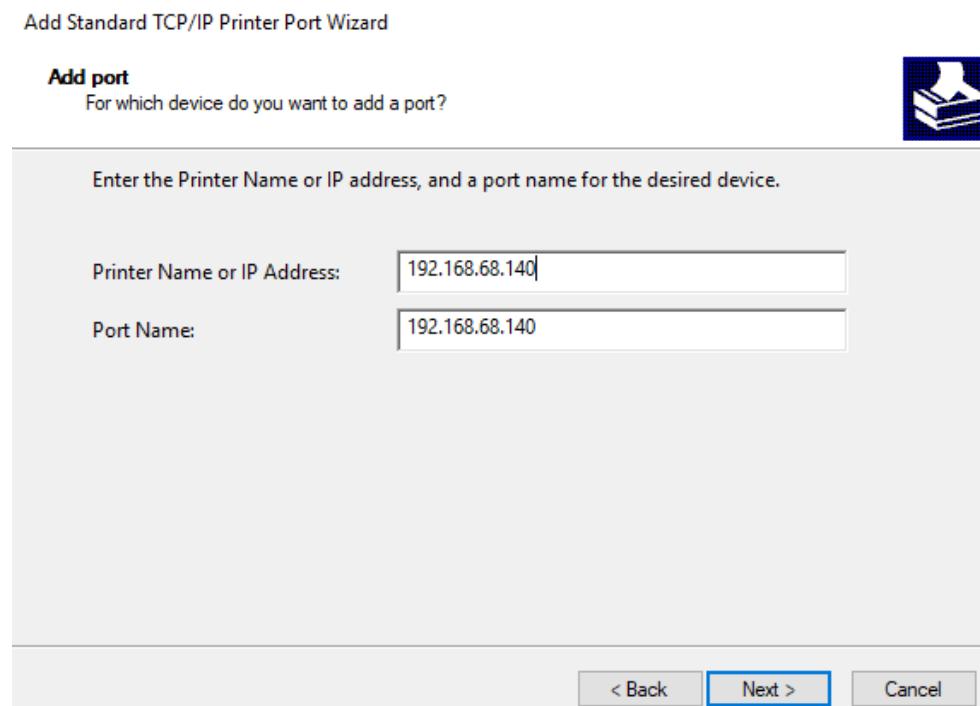
### 3.3.5 Printserver

#### 3.3.5.1 Installatie printserver (PS\_1)

Een printer is één van de meest gebruikte apparaten in een bedrijf en het is dus noodzakelijk om deze toe te voegen aan het netwerk. Om een printer beschikbaar te maken voor het netwerk heb je een poort, een driver en natuurlijk een printer nodig.

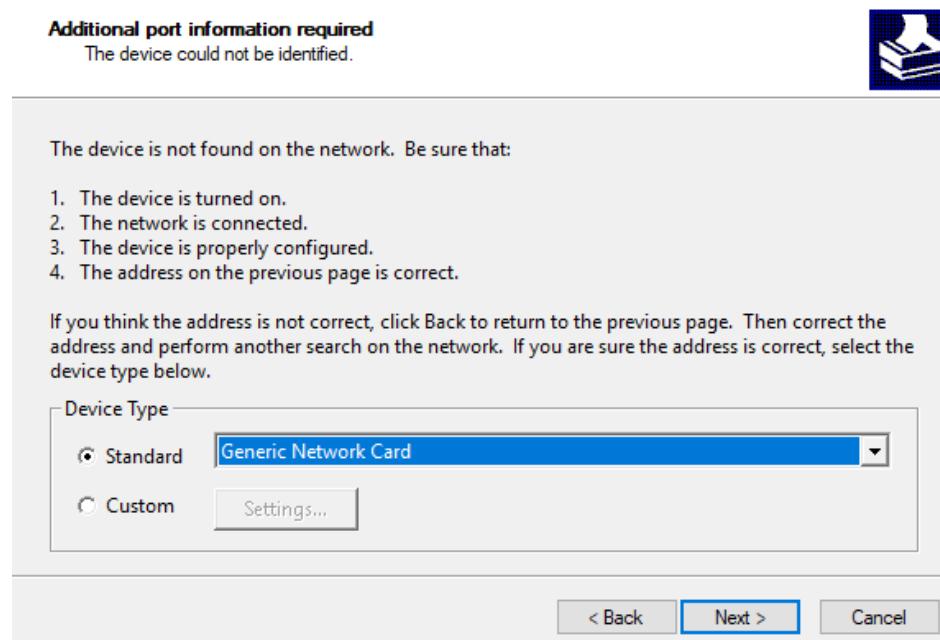


Zorg er voor dat het IP van de gedeelde printer tot een VLAN behoort die toegankelijk is voor de andere servers.

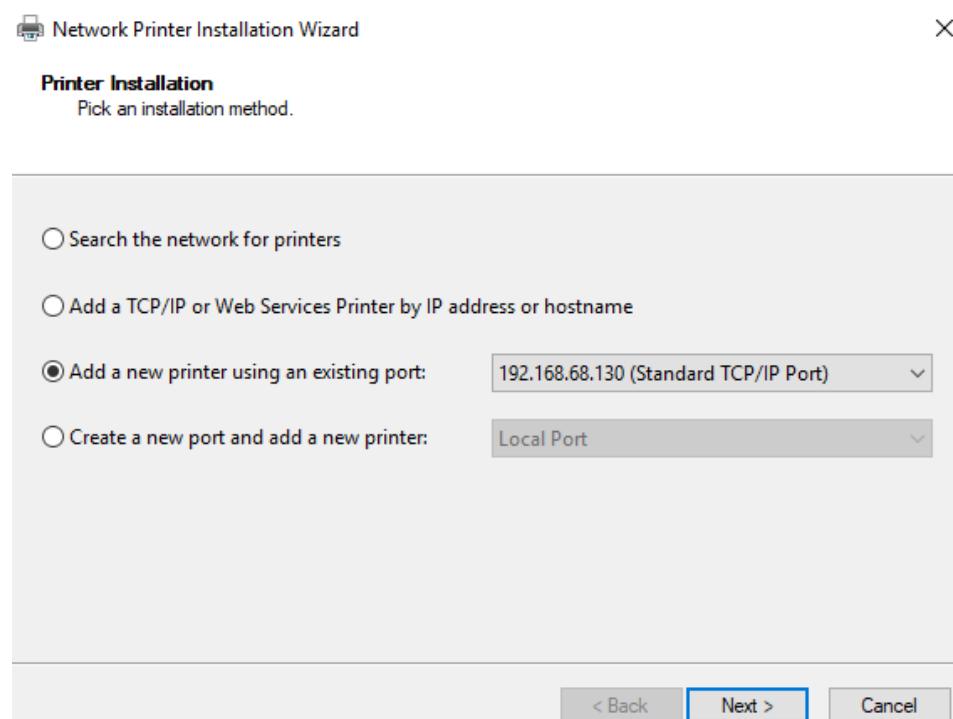


Aangezien dit een demo omgeving is en er geen fysieke printer aan de server is aangesloten, moeten we even creatief zijn. Om toch een simulatie te kunnen maken, kan je een generic network card gebruiken (dit is een virtuele kaart).

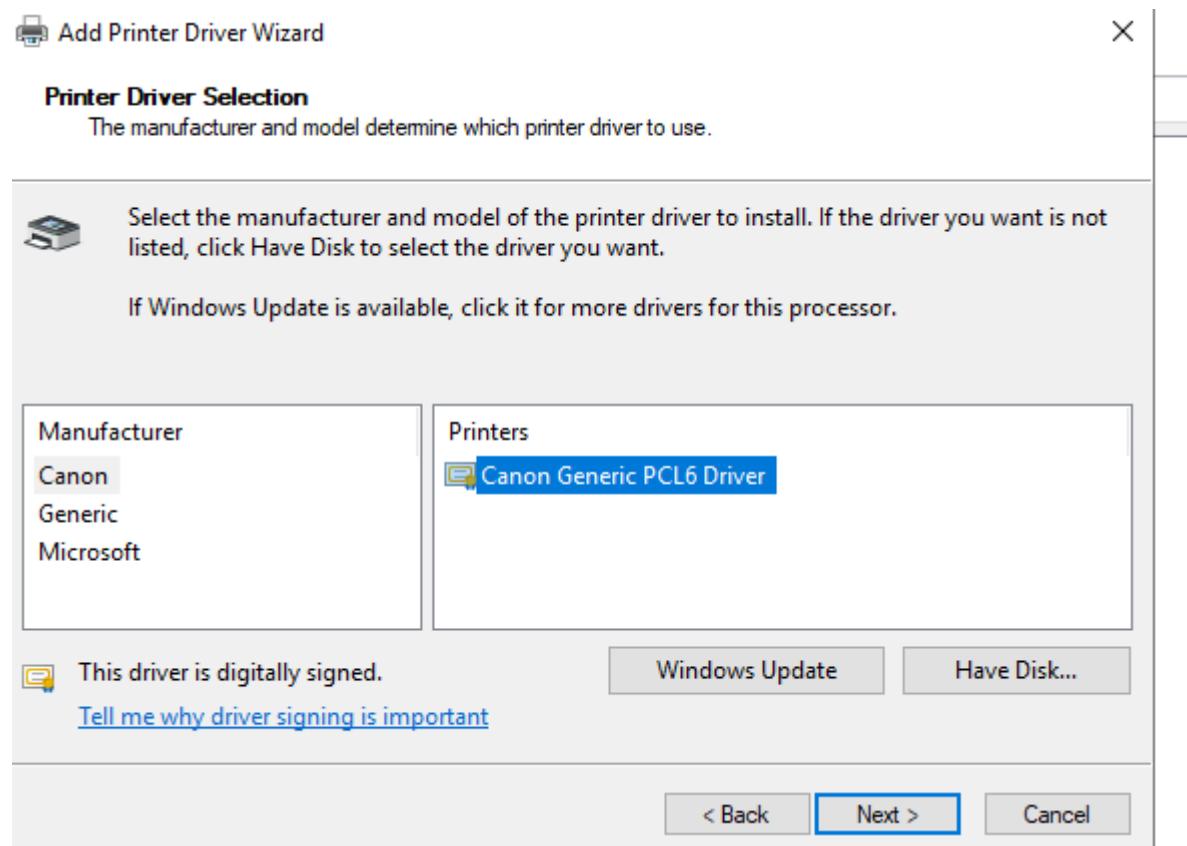
#### Add Standard TCP/IP Printer Port Wizard



Na deze stap is de printerpoort correct geïnstalleerd en kan je deze gebruiken om een printer te configureren. Belangrijk is dat je een driver van de printer hebt (kan je gemakkelijk van het internet downloaden) om de printer te kunnen instellen. De eerste stap is de juiste poort selecteren voor de printer, deze heb je daarnet aangemaakt.



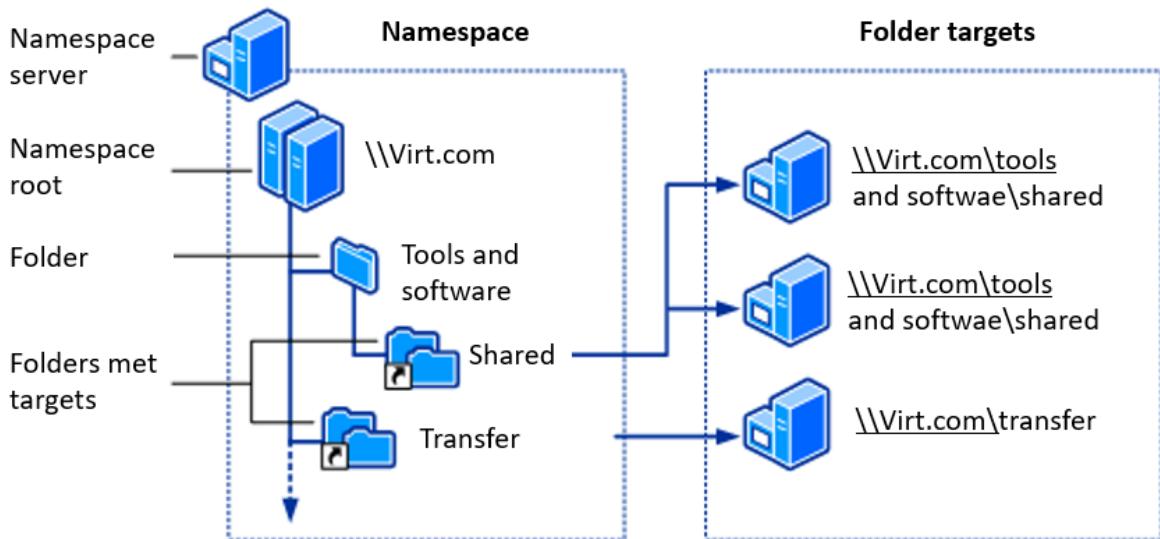
Selecteer de juiste poort en geef de gepaste driver mee. Als de driver niet in de standaardlijst staat, kan je via *Have Disk* naar de locatie browsen.



Nu is de printer zo goed als klaar. Als laatste stap kan je nog wat persoonlijke instellingen zoals de naam en de locatie van de printer ingeven.

### 3.3.6 Fileservers (DFS)

Met een fileserver kan je één of meerdere gedeelde netwerkschijven configureren. Dit is onder andere handig om bestanden te kunnen uitwisselen tussen gebruikers.

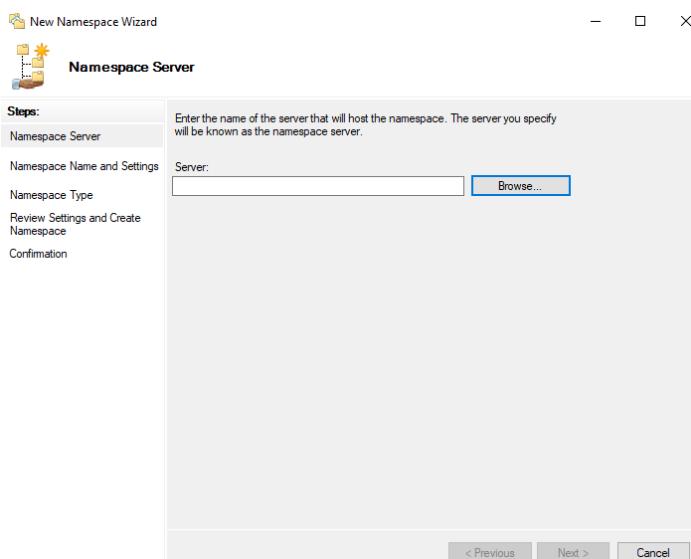


#### 3.3.6.1 Installatie fileservers

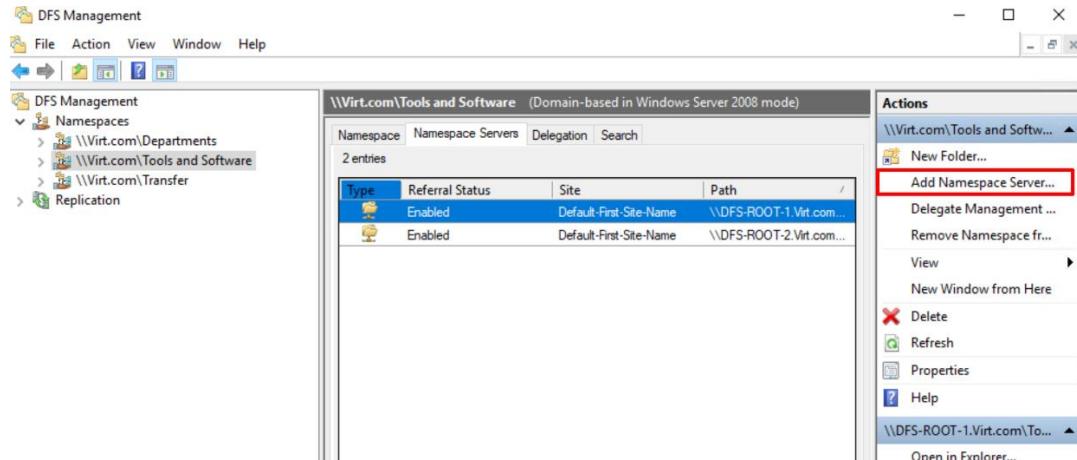
Met de fileservers kan je gemakkelijk bestanden beschikbaar maken voor het hele domein. Best practice wordt er gebruik gemaakt van twee root servers die dan verwijzen naar de effectieve servers waar de bestanden op komen. De servers die hiervoor worden gebruikt in het domein zijn:

- DFSROOT\_1,
- DFSROOT\_2,
- FS\_1,
- FS\_2.

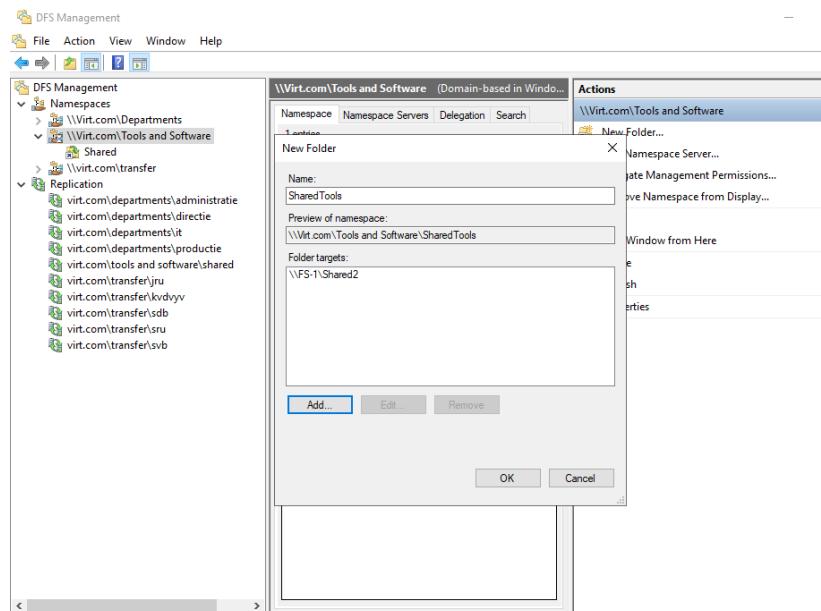
Om de DFS functionaliteit te gebruiken, moet je eerst de rol installeren op de server. Eens dit gebeurd is, kan je via de DFS manager een namespace aanmaken. Als je gebruik maakt van 2 root servers, zijn deze de namespace servers.



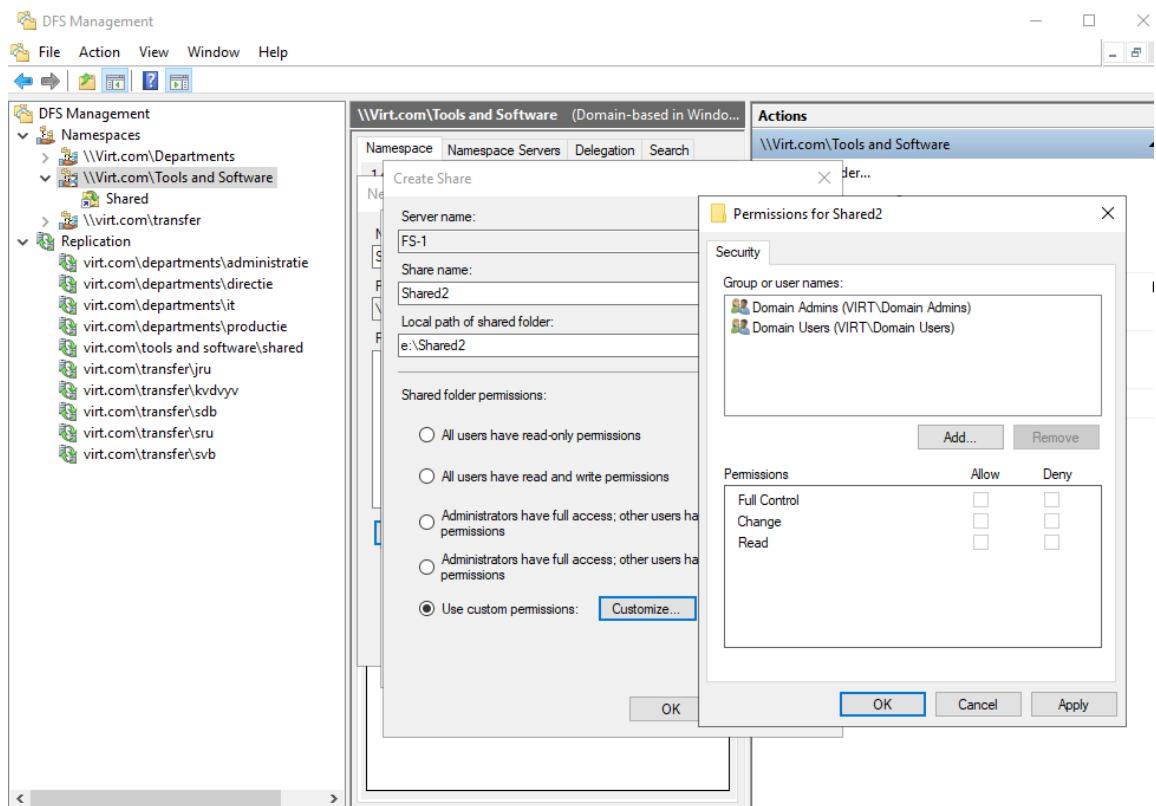
Na deze stap, geef je de namespace een naam en kan je via *edit settings* het pad instellen op de DFS-root en de permissies naar gebruikers toe. Vervolgens kan je de installatie van de namespace voltooien en is er de mogelijkheid om een tweede root server toe te voegen aan deze namespace. Dit maakt het mogelijk om de namespace high available te maken.



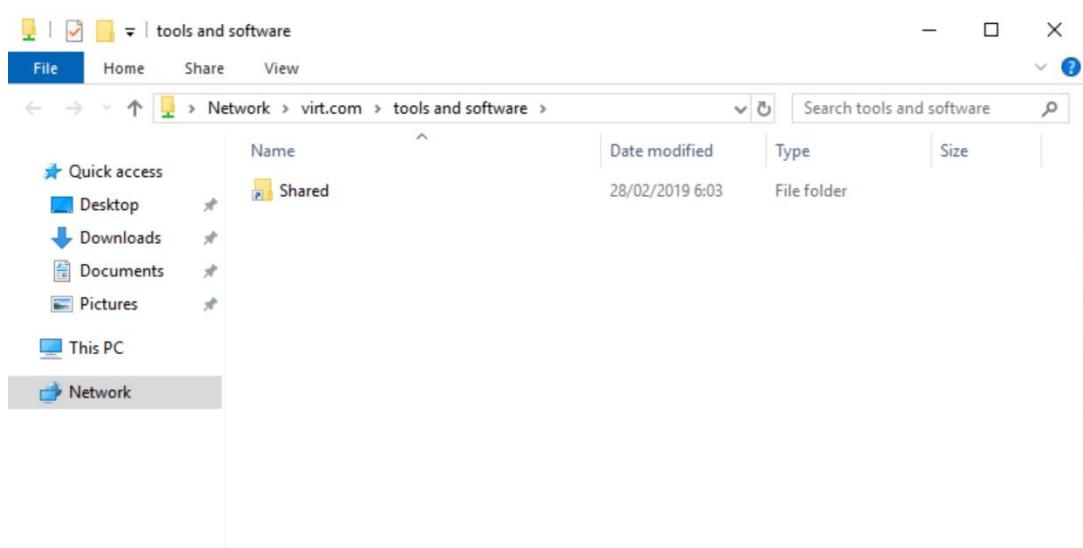
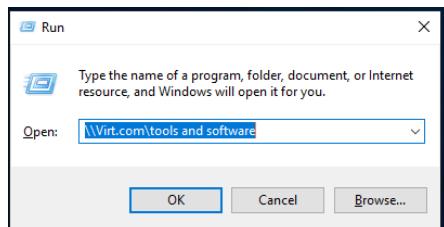
Nu de namespace is aangemaakt en eventueel high available gemaakt is, kan je een folder creëren. Aangeraden is dat je deze folder niet aanmaakt op de root servers. De target pas je dus best aan naar de servers waar de bestanden uiteindelijk moeten terechtkomen (FS\_1 en FS\_2).



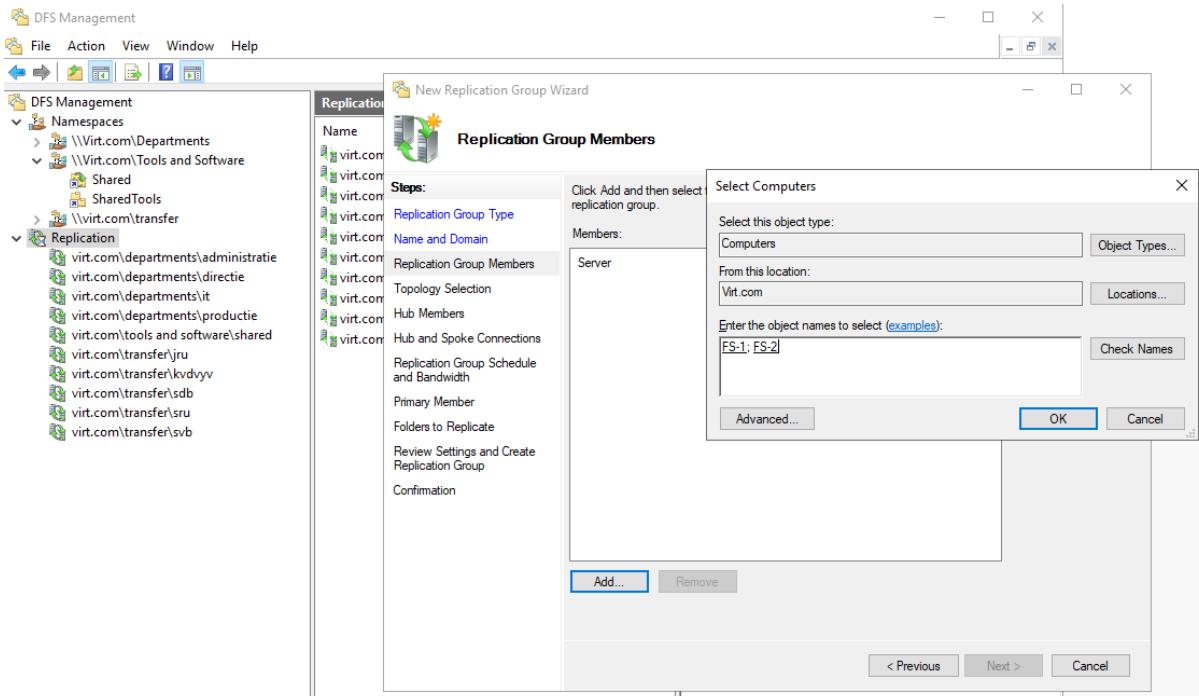
Hierna configureren je de permissies en het pad van de folder op de fileserver. Meestal moet je nog een shared folder aanmaken op de targeted server tenzij deze al is gemaakt. Met de permissies kan je bijvoorbeeld een folder enkel beschikbaar maken voor de admins of voor een bepaalde afdeling van het domein, ...



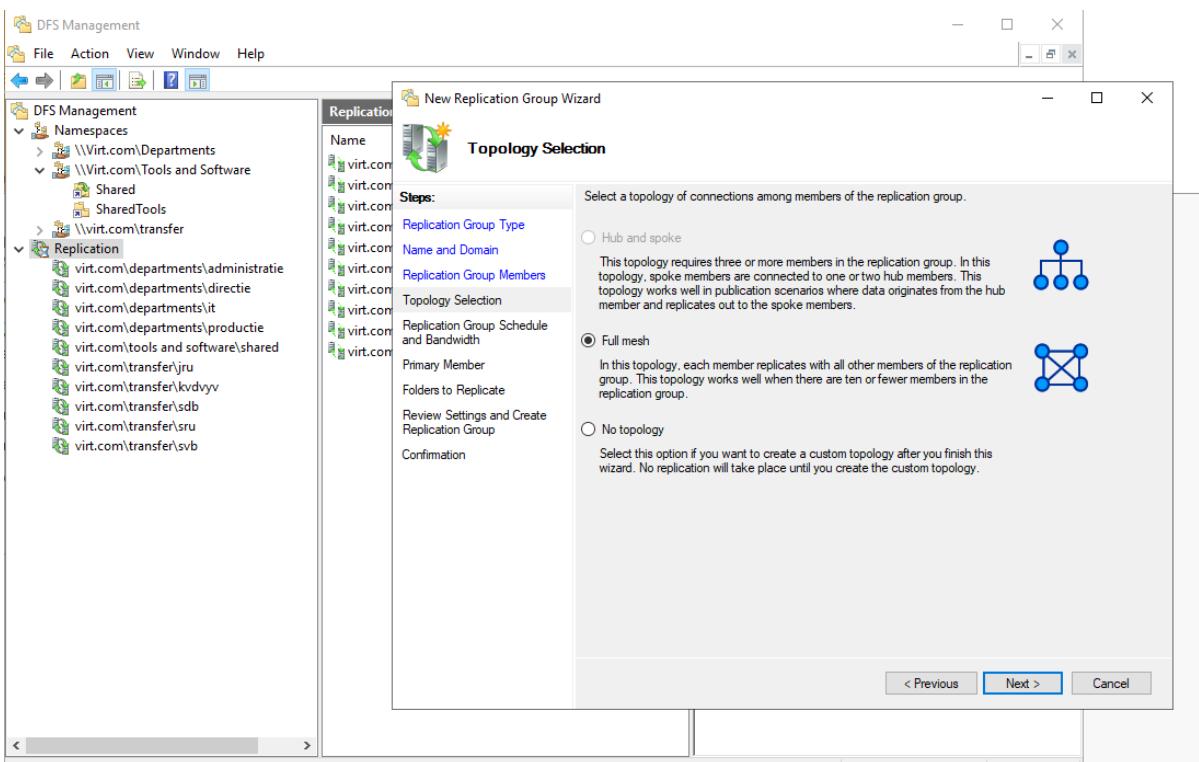
Aan te raden is om de configuratie tussendoor eens te testen. Hiervoor kan je al eens browsen naar de locatie waar de bestanden zich bevinden. Open het RUN programma en voer de namespace in die je wilt testen.



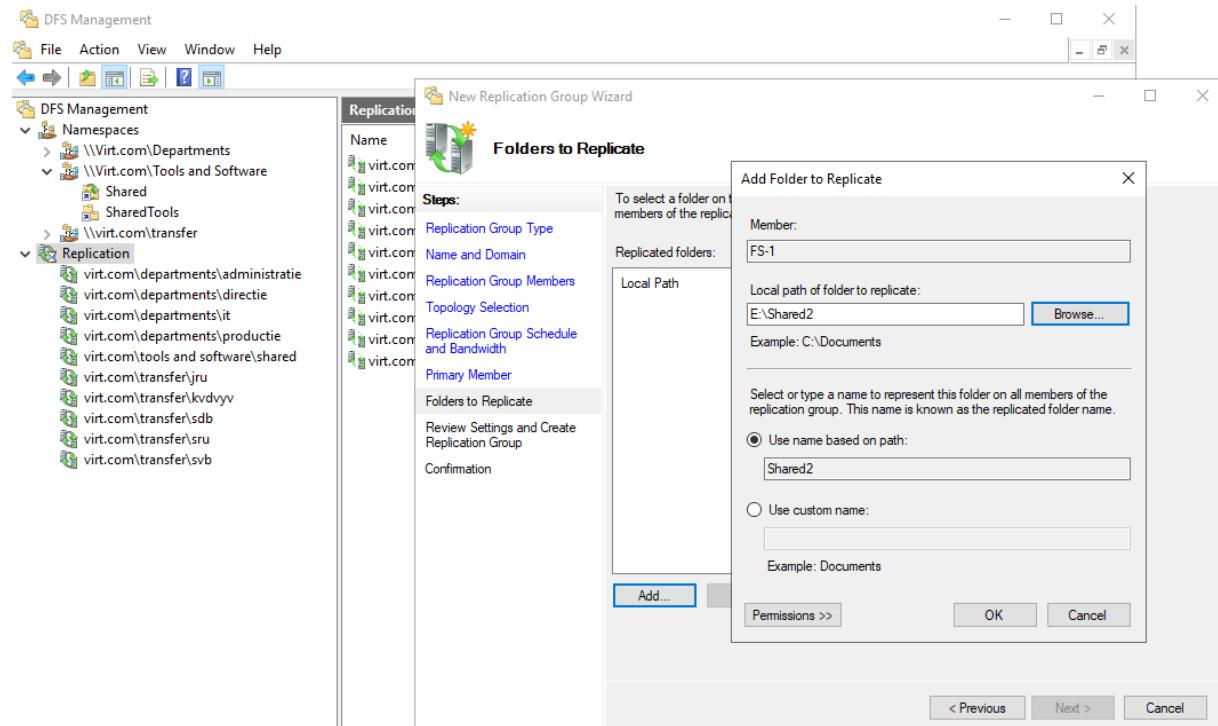
Als je de folder niet ziet staan na deze stappen, is er iets foutgegaan met de configuratie tot nu toe. Als er meerdere targets zijn toegewezen aan een folder, is het aangeraden om deze te synchroniseren. Hiervoor maak je een replicatiegroep aan. Selecteer het type replicatie dat je gaat gebruiken, geef deze een naam en voeg de servers toe waar de bestanden staan (FS\_1 en FS\_2).



Nu de replicatie servers zijn toegevoegd, selecteer de juiste topologie voor het domein. In de demo-omgeving is de Full mesh van toepassing.



Tot slot selecteer je de primary member (van deze server worden de bestanden gerepliceerd naar de andere fileservers) en voeg je de folders toe die gerepliceerd moeten worden.



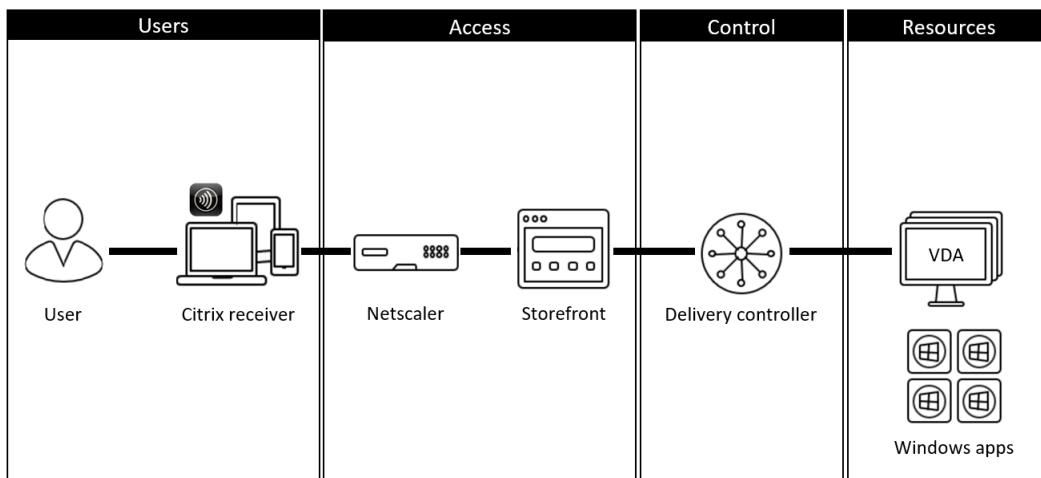
### 3.3.7 Citrix

Citrix is een technologie die je kan gebruiken om desktops en/of applicaties te publiceren. Dit is een handige tool om grote applicaties beschikbaar te stellen voor gebruikers of om toegang tot applicaties te beperken (werknemers in administratie hebben toegang tot andere applicaties dan in productie).

Waarom Citrix en niet RDS (remote desktop services) van Microsoft om applicaties te publishen ?

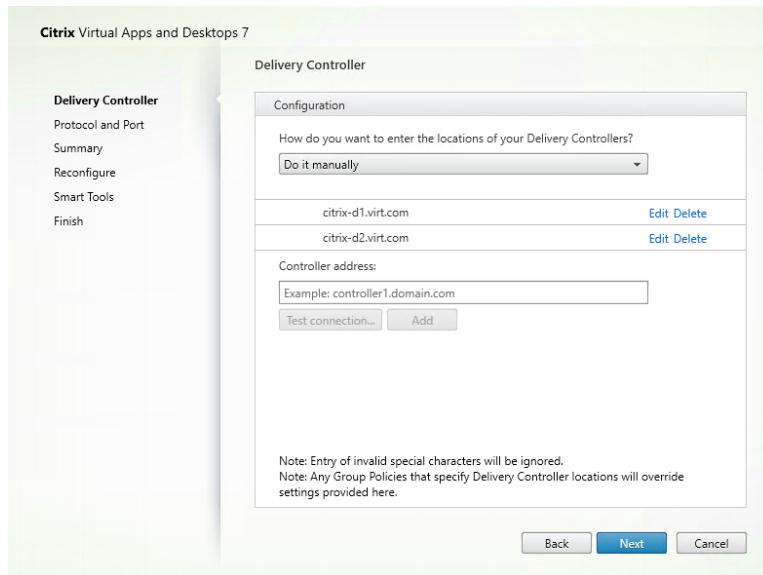
Citrix heeft meer functies en is bedrijfsvriendelijker dan RDS:

- Bredere ondersteuning van systemen (Windows, Linux, HTML5 Chromebooks),
- NetScaler (extern bereikbaar maken van citrix apps, ...),
- Gemakkelijker beheer- en monitoringmogelijkheden,
- Beter beeldbeheer en brede hypervisor / cloud-ondersteuning + Prestatie-optimalisatie.



### 3.3.7.1 Configuratie VDA (Citrix-1, Citrix-2)

De VDA (virtual delivery agent) servers zijn de servers waar de applicaties staan die je wil publiceren. Hier maak je een master image. Daarna leg je de link naar de delivery controllers. Deze delivery controllers moet je in de configuratie definiëren.



Om de VDA high available te maken, configureren je een tweede server met exact dezelfde delivery controllers.

### 3.3.7.2 Configuratie Delivery controllers (Citrix-d1, Citrix-d2)

De delivery controllers publiceren de applicaties van de VDA's naar een StoreFront. Gebruikers zullen deze StoreFront gebruiken om aan de applicaties te geraken en te starten. Als eerste stap maak je een machine catalog aan. Deze catalog bevat de servers waar de applicaties op staan (VDA servers). Om high availability te verkrijgen zijn er 2 VDA servers aangemaakt en deze zijn beide toegevoegd aan de catalog.

The screenshot shows the Citrix Machine Catalog interface. At the top, there is a header with the Citrix logo and navigation links. Below the header, a table displays machine details. The table has columns for Machine Catalog, Machine type, Server OS, User data, No. of machines, Allocated machines, and Provisioning method. There are two entries: one for 'Windows Server 2019' with 'Allocation Type: Random'. The 'Allocated machines' column shows '2' for both rows. The 'Provisioning method' column shows 'Manual' for both rows. Below the table, there is a large, empty white area. At the bottom of the screen, there is a modal dialog titled 'Details - Windows Server 2019'. This dialog has tabs for 'Details', 'Machines', and 'Administrators'. The 'Machines' tab is selected and shows two entries: 'VIRT\CTRIX-VDA1' and 'VIRT\CTRIX-VDA2'. A red rectangular box highlights this section of the interface.

Vervolgens maak je een delivery group aan. Hier komen de apps terecht die je wil publiceren. De delivery group die je aanmaakt kan je limiteren tot bepaalde gebruikers, zo kan je eventueel apps enkel beschikbaar maken voor interne gebruikers terwijl de externe gebruikers deze niet zien staan.

The screenshot shows the Citrix Studio interface. On the left, there is a sidebar with navigation links: 'Introduction' (marked with a checkmark), 'Applications' (which is selected and highlighted in blue), and 'Summary'. In the main area, there is a dialog titled 'Add Applications from Start Menu'. The dialog contains a list of discovered applications, each with a checkbox next to it. The applications listed include: AddSuggestedFoldersToLibraryDialog, AppResolverUX, Calculator, CapturePicker, Character Map, Citrix Health Assistant, Citrix Studio, Citrix Workspace, Command Prompt, CredDialogHost, Defragment and Optimize Drives, and Disk Cleanup. Below the list, it says '0 of 65 applications selected'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. To the right of the dialog, there is a decorative graphic of overlapping green hexagons. The overall interface has a light green background.

Tot slot maak je een StoreFront aan. Hier kan je meerdere servers aan meegeven voor load balancing. Deze load balancing servers zijn de delivery controllers.

Name	Authenticated	Subscription Enabled	Access
BasicApps	Yes	Yes	Internal network only
Store Service	Yes	Yes	Internal network only

Details - Store Service

Delivery Controllers

Name	Type	Servers
BasicApps	XenDesktop	citrix-d1.virt.com, citrix-d2.virt.com

Omdat er in de demo-omgeving 2 servers zijn geconfigureerd voor dezelfde StoreFront, is er een server group gemaakt. Hierdoor kan je de StoreFront URL veranderen naar een algemene naam 'citrix.virt.com' in plaats van de servernaam 'citrix-1.virt.com'. Dit is duidelijker naar de gebruikers toe.

Server Group

Group details

Base URL: <http://citrix.virt.com/>

Number of servers: 2

Configuration: Last propagated from citrix-d1

Nu je de StoreFront hebt aangemaakt, moet je deze linken aan de delivery groep. Zorg er zeker voor dat je de juiste StoreFront server name gebruikt (base URL van de StoreFront).

Console Root

- Citrix Studio (BasicApps)
  - Machine Catalogs
  - AppDisks
  - Delivery Groups
  - Applications
  - Policies
  - Logging
  - Configuration
    - Administrators
    - Controllers
    - Hosting
    - Licensing
    - StoreFront
    - App-V Publishing
    - AppDNA
    - Zones
- Citrix StoreFront
  - Stores
  - Server Group

StoreFront Server

Used by # Delivery Groups

citrix.virt.com

Edit StoreFront Server

Enter the details of an existing StoreFront server that you want to be available from Citrix Workspace app.

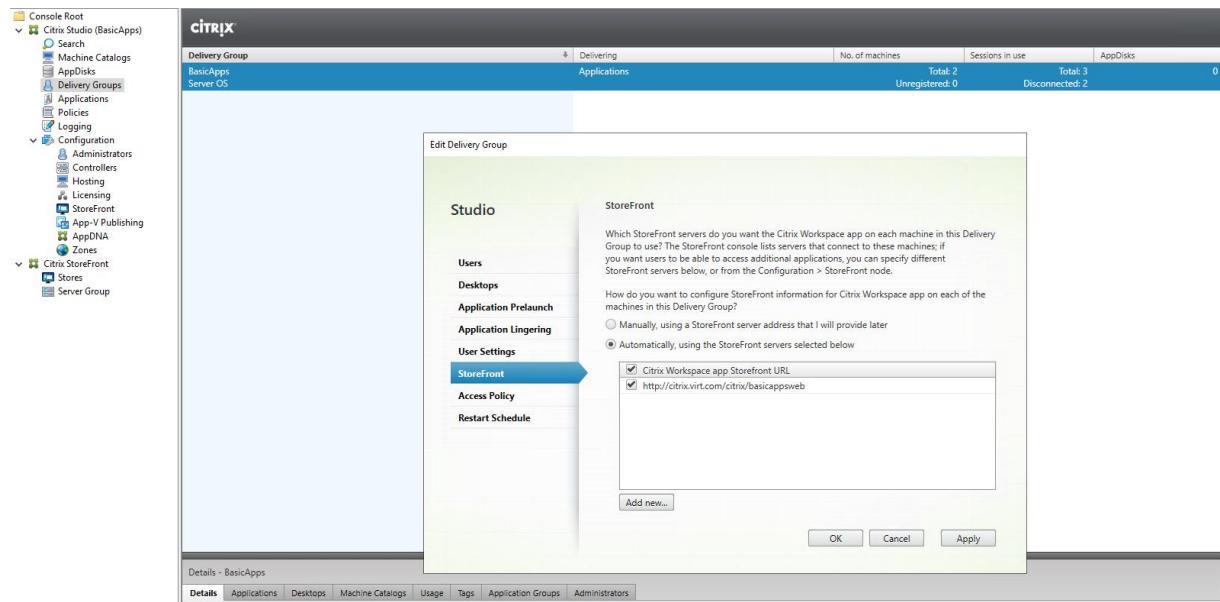
StoreFront server name:

Description:

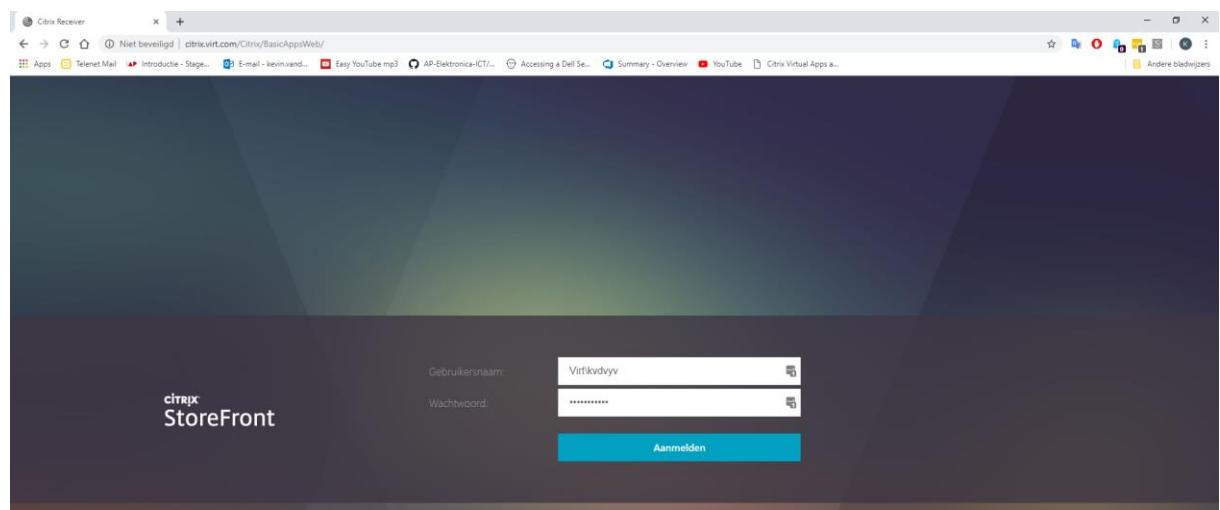
URL:

OK Cancel

Tot slot definieer je deze de StoreFront in de delivery groep.

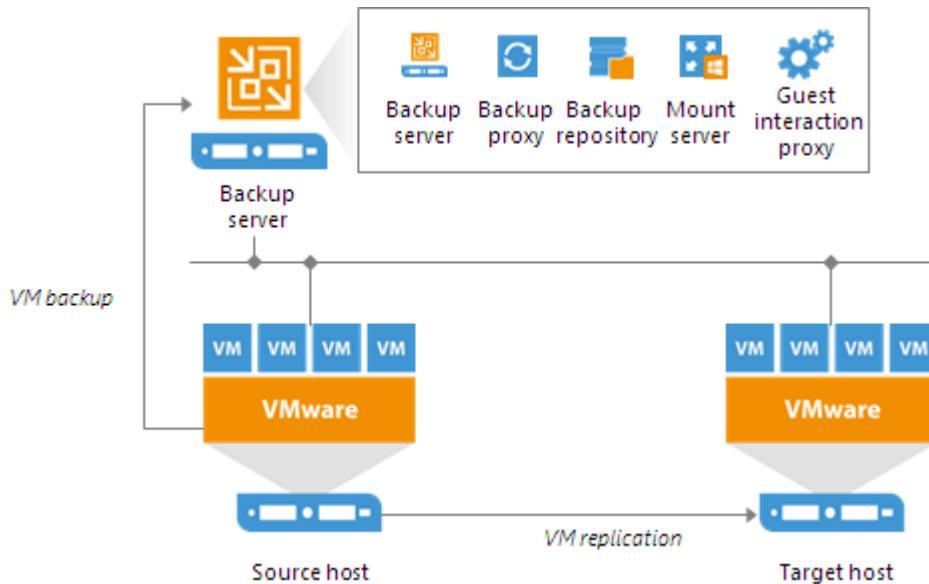


De Citrix configuratie is nu voltooid. De gebruikers kunnen via de Citrix Receiver inloggen en de Apps gebruiken.



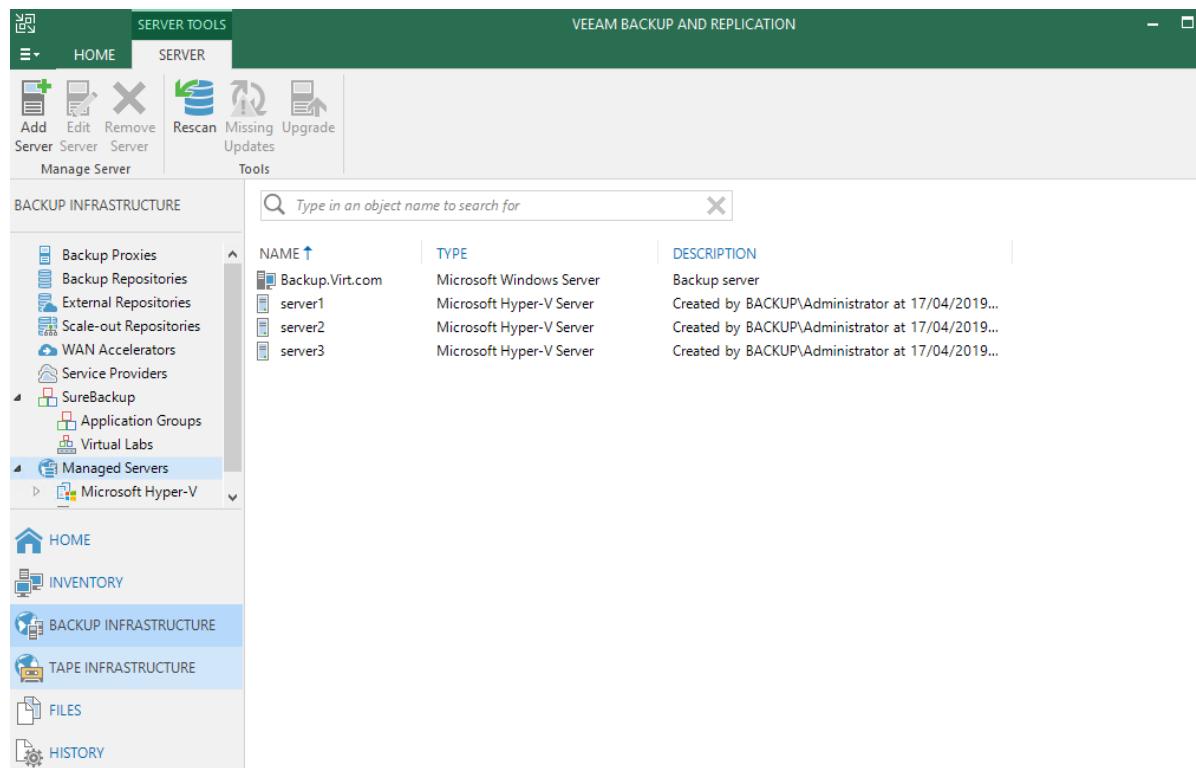
### 3.3.8 Veeam

Veeam is een programma dat je kan gebruiken om back-ups te maken. Deze zijn noodzakelijk om terug te kunnen gaan indien er een server niet meer functioneel is.



#### 3.3.8.1 Configuratie VEEAM (Backup)

In de demo-omgeving gebruiken we VEEAM als backupprogramma. Dit is één van de meest gebruikte en geavanceerde backupprogramma's voor high end gebruik. Om te beginnen moet je een infrastructuur opzetten in de VEEAM configuratie.



Eens deze is opgezet, kan je backup jobs aanmaken. Hierin voeg je de servers toe die je wil backen. Je kan met een extra optie bepaalde VM's uitsluiten als een server geselecteerd is die meerdere virtuele machines bevat.

New Backup Job

**Virtual Machines**  
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.

Name	Virtual machines to backup:		
	Name	Type	Size
Virtual Machines	Citrix_2	VM	25,6 GB
	Citrix_d2	VM	20,7 GB
	DC_1	VM	18,6 GB
	DFSROOT_1	VM	16,1 GB
	FS_1	VM	33,6 GB
	Powershell_AD	VM	19,5 GB
	PS_1	VM	20,4 GB
	Citrix_1	VM	25,4 GB
	Citrix_d1	VM	20,8 GB
	citrix_netscale	VM	16,3 GB
	DC_2	VM	15,2 GB
	DFSROOT_2	VM	15,3 GB
	DMZ_RODC	VM	21,2 GB
	FS_2	VM	38,6 GB
	NetScaler Virtual Appliance	VM	1,49 GB
	Backup	VM	19,0 GB
	Management	VM	14,5 GB

Add...      Remove      Exclusions...      Up      Down      Recalculate

Total size:  
**343 GB**

< Previous      Next >      Finish      Cancel

Belangrijk is om even uit te rekenen hoeveel data je nodig hebt om de back-ups te kunnen opslaan. Een handige tool die deze kan uitrekenen is *The Restore Point Simulator*. De reden waarom er meer restore points gebruikt worden dan ingesteld, is omdat VEEAM zijn cyclus eindigt met een full backup.

## The Restore Point Simulator

Current version : 0.4.1

Feedback via @tdewin or on [GitHub](#)

RPS heavily relies on some open source [javascript frameworks](#)

### Quick Presets

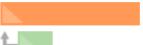
Incremental Weekly Active Full ▾

### Configuration

Style	Incremental
Used Size GB	343
Retention Points	20
Change Rate	10% Conservative
Data left after reduction	50% (100GB > 50GB) 2x Conservative
Interval	Daily
Time Growth Simulation	<input checked="" type="checkbox"/>
ReFS	<input type="checkbox"/>

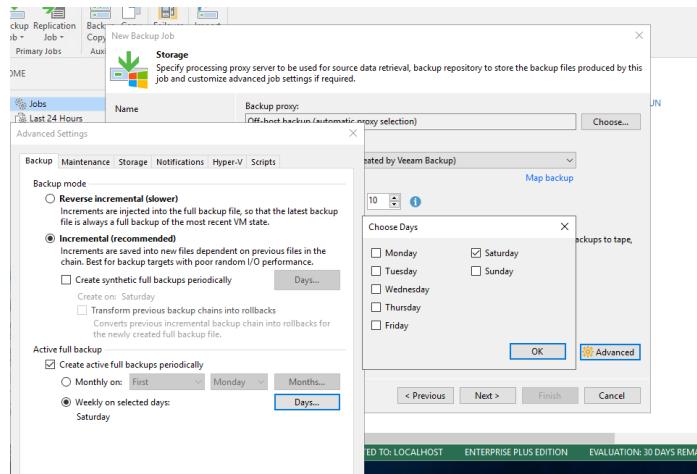
### Incremental Specific

Synthetic	<input type="checkbox"/> MO	<input type="checkbox"/> TU	<input type="checkbox"/> WE	<input type="checkbox"/> TH	<input type="checkbox"/> FR	<input type="checkbox"/> SA	<input type="checkbox"/> SU
Active Full Weekly	<input type="checkbox"/> MO	<input type="checkbox"/> TU	<input type="checkbox"/> WE	<input type="checkbox"/> TH	<input type="checkbox"/> FR	<input checked="" type="checkbox"/> SA	<input type="checkbox"/> SU
Active Full Monthly	<input type="checkbox"/> Jan	<input type="checkbox"/> Feb	<input type="checkbox"/> Mar	<input type="checkbox"/> Apr	<input type="checkbox"/> May	<input type="checkbox"/> Jun	<input type="checkbox"/> Jul
	<input type="checkbox"/> Aug	<input type="checkbox"/> Sep	<input type="checkbox"/> Oct	<input type="checkbox"/> Nov	<input type="checkbox"/> Dec		

26 (20)		full.vbk	202.84 GB
25 (20)		incremental.vib	20.29 GB
24 (20)		incremental.vib	20.3 GB
23 (20)		incremental.vib	20.31 GB
22 (20)		incremental.vib	20.32 GB
21 (20)		incremental.vib	20.33 GB
20		incremental.vib	20.34 GB
19		full.vbk	203.55 GB
18		incremental.vib	20.37 GB
17		incremental.vib	20.38 GB
16		incremental.vib	20.39 GB
15		incremental.vib	20.4 GB
14		incremental.vib	20.41 GB
13		incremental.vib	20.42 GB
12		full.vbk	204.26 GB
11		incremental.vib	20.44 GB
10		incremental.vib	20.45 GB
9		incremental.vib	20.46 GB
8		incremental.vib	20.47 GB
7		incremental.vib	20.48 GB
6		incremental.vib	20.49 GB
5		full.vbk	204.98 GB
4		incremental.vib	20.51 GB
3		incremental.vib	20.52 GB
2		incremental.vib	20.53 GB
1		incremental.vib	20.54 GB
Total			1264.76 GB
Working Space			+ 215.66 GB
Grand Total			1480.42 GB

In de configuratie is er de optie voor incremental back-ups, full back-ups of beide. In de back-up configuratie van de demo-omgeving is er gekozen om beide te gebruiken. Dagelijks loopt een incrementale back-up en elke zaterdag loopt een active full back-up.

Je kan ook kiezen voor een synthetic full back-up, deze verschilt van een active full-backup doordat deze bestanden gebruikt die al op de schijf staan en dus niet veel netwerk bandbreedte nodig heeft. Een nadeel van een synthetic back-up is dat eens er één file corrupt is, deze in elke back-up aanwezig zal zijn.

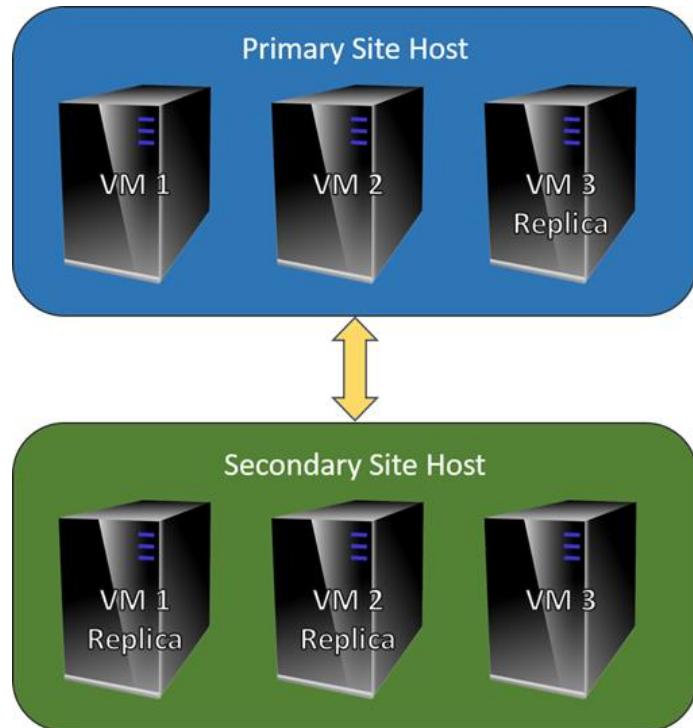


Bij elke job die je hebt uitgevoerd, krijg je een gedetailleerd rapport terug. Dit houdt met andere woorden in dat als er een fout optreedt, deze hier zichtbaar zal zijn. Hieronder vind je een voorbeeld van de job detail waar er een fout opgetreden is tijdens de back-up wegens een connectie die mislukt is.

NAME	STATUS	ACTION
Management	Failed	Task failed. Failed to expand object Management. Error: Cannot find VM Management on host Server3.virt.com
Cntrx_d2	Success	
Cntrx_2	Success	
DFSROOT_1	Success	
FS_1	Success	
DC_1	Success	
Cntrx_1	Success	
DFSROOT_2	Success	
DC_2	Success	
Cntrx_d1	Success	
FS_2	Success	
dc_1	Success	

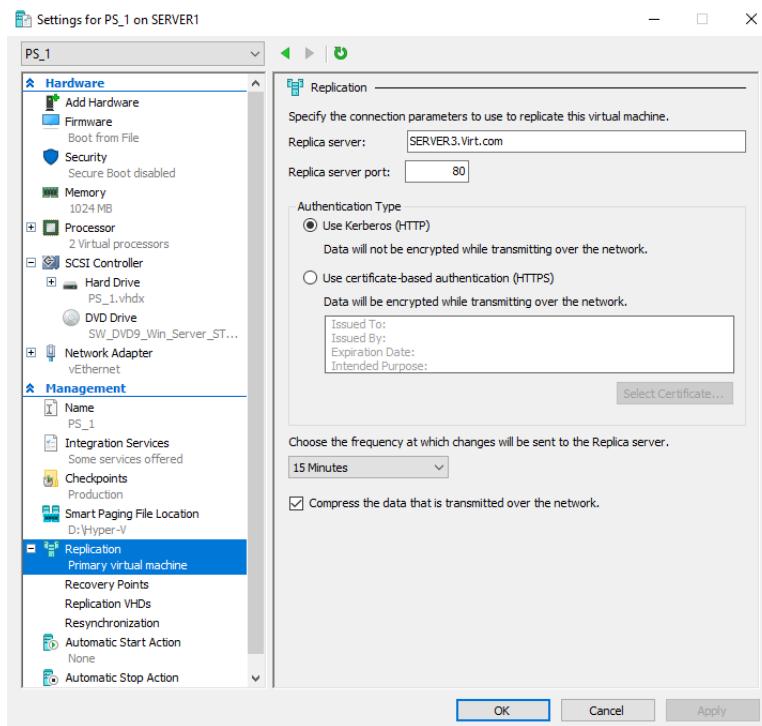
### 3.3.9 Replication

Met replication kan je de VM's (virtuele machines) die niet high available zijn, toch failoveren. Dit betekent dat wanneer er een VM defect geraakt, deze meteen wordt overgenomen door een andere VM. Om replicatie te bekomen, gaat men één fysieke server instellen als een replica server, dit betekent dat je VM's kan "kopiëren" naar deze server. Wanneer de originele VM uitvalt, zal de replica server de gekopieerde VM aanzetten en gebruiken.

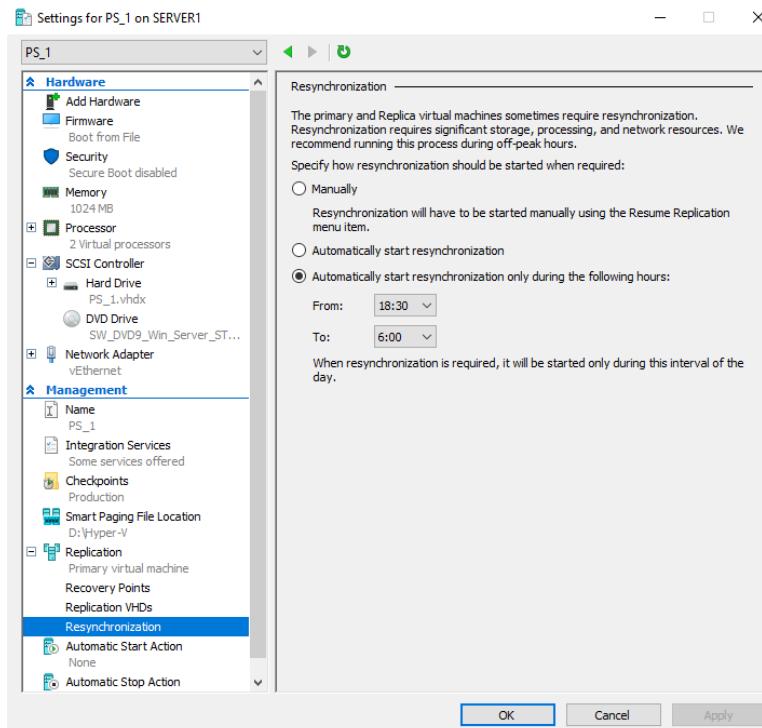


### 3.3.9.1 Configuratie (Server1)

Aangezien de printserver niet high available is in de demo-omgeving, repliceer je deze naar een andere server. Hierdoor kan de VM toch operationeel zijn, voor in het geval de originele defect gaan.

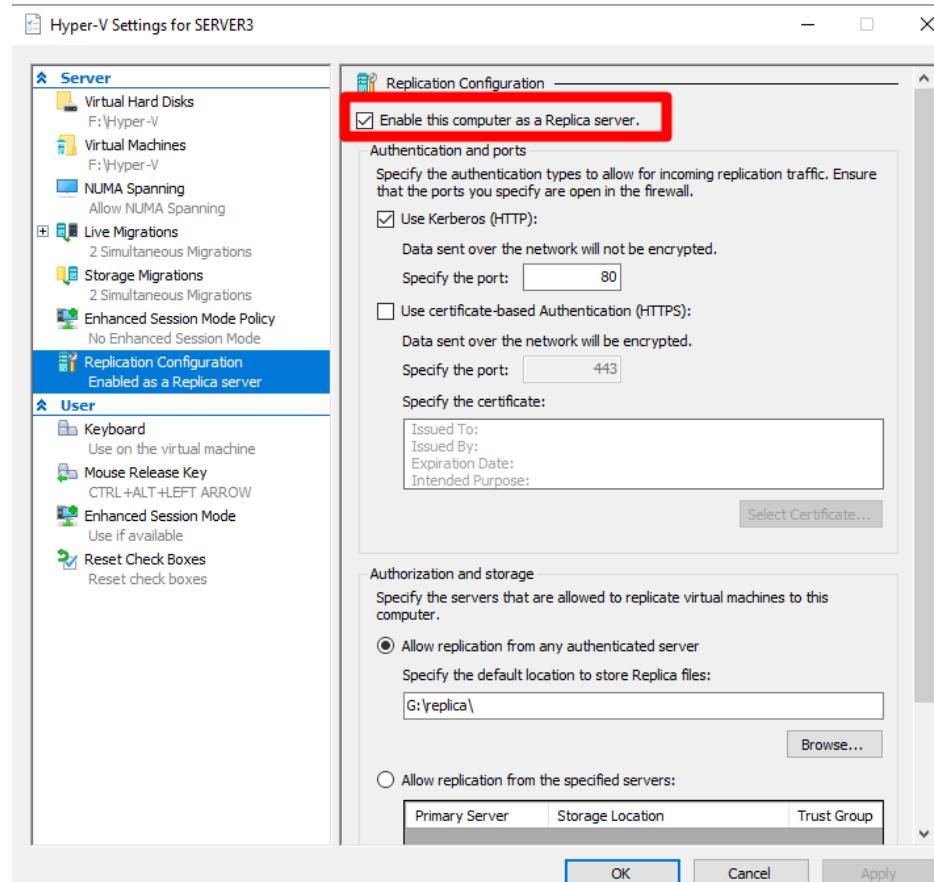


Een belangrijk iets voor de replicatie is dat je de servers moet synchroniseren zodat de gerepliceerde VM up to date is.



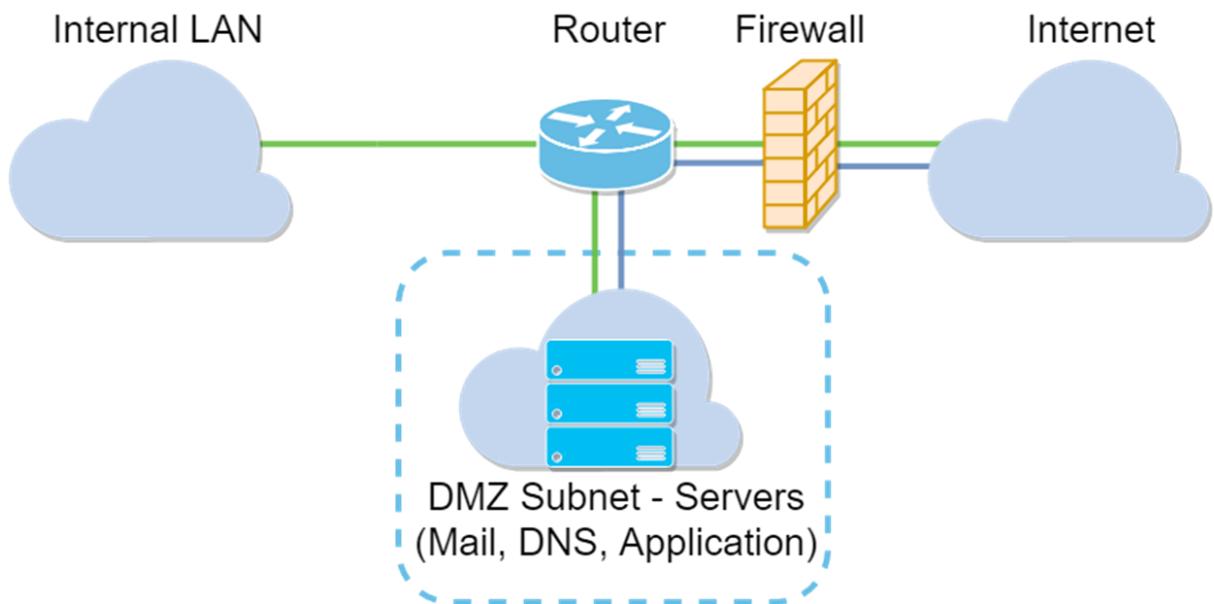
### 3.3.9.2 Installatie (Server3)

Server 3 stel je in als replica server, omdat deze de grootste dataopslag heeft. Hier geef je ook de locatie mee waar de gerepliceerde VM's terecht komen.



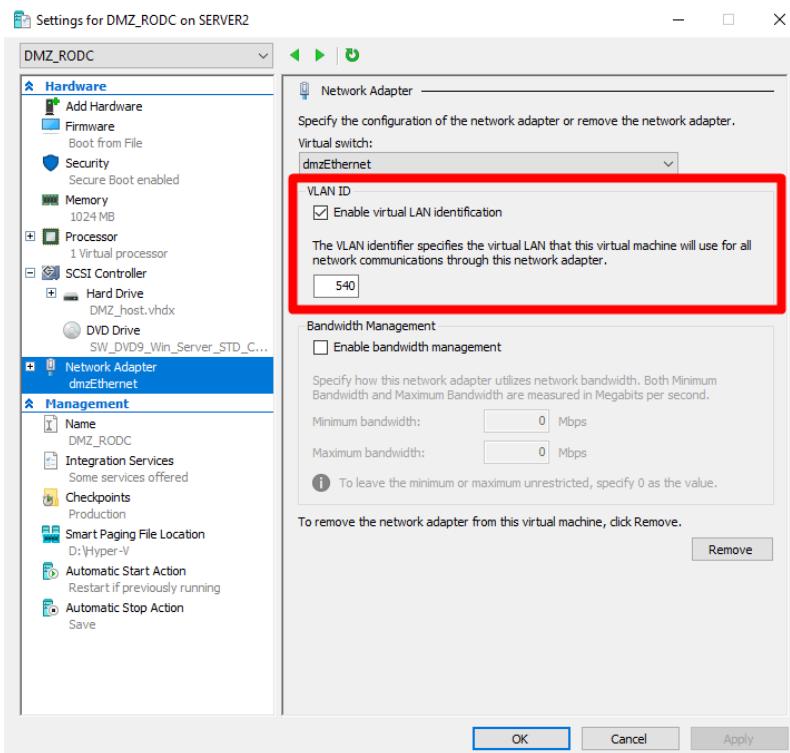
### 3.3.10 DMZ

DMZ staat voor demilitarized zone, dit is een zone die zich bevindt tussen het interne en externe netwerk. Deze zone wordt meestal gebruikt als extra security laag, omdat hierin de publieke toepassingen van het netwerk komen. Hierdoor hebben de externe gebruikers geen toegang tot het interne netwerk.



### 3.3.10.1 Configuratie (Server2)

De DMZ zone is geconfigureerd op server 2, enkel de ethernet channel van server 2 laat de DMZ VLAN door (VLAN 540). Bij het aanmaken van de VM moet je dit id meegeven.



In de DMZ zone staan alle poorten open voor de externe gebruikers. Op zich is dit geen probleem omdat de DMZ losstaat van het interne netwerk.

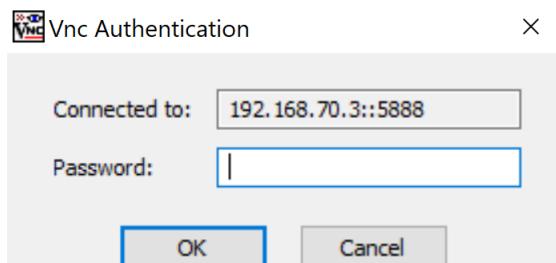
Interconnect - ASA (10 incoming rules)					
1	<input checked="" type="checkbox"/> any	* 192.168.70.0/23	ip	✓ Permit	21
2	<input checked="" type="checkbox"/> Internal_Users	<input checked="" type="checkbox"/> any	ip	✓ Permit	0
3	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	icmp	✓ Permit	14
4	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	snmp	✓ Permit	0
5	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_console	✓ Permit	9
6	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_browser	✓ Permit	68
7	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	Remote/Desktop	✓ Permit	11
8	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	Citrix	✓ Permit	0
9	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	SQL_TCP	✓ Permit	0
...	<input checked="" type="checkbox"/> any	VLAN510_VLAN520_VLAN530_VLAN...	Citrix_udp	✓ Permit	0
<input checked="" type="checkbox"/> management (0 implicit incoming rules)					
<input checked="" type="checkbox"/> Global (1 implicit rule)					
1	<input checked="" type="checkbox"/> any	* any	ip	✗ Deny	Implicit rule

Deze configuratie kan je simpel testen door een applicatie te gebruiken waar je van op afstand moet inloggen. Voor de test is TightVNC gebruikt. TightVNC heeft standaard poort 5902 nodig om te kunnen communiceren, maar deze poort was in demo-omgeving al in gebruik. Hierdoor is de poort aangepast naar 5888.

De connectie naar de fysieke server is onmogelijk, omdat deze niet in de DMZ staat en poort 5888 dus niet open staat.

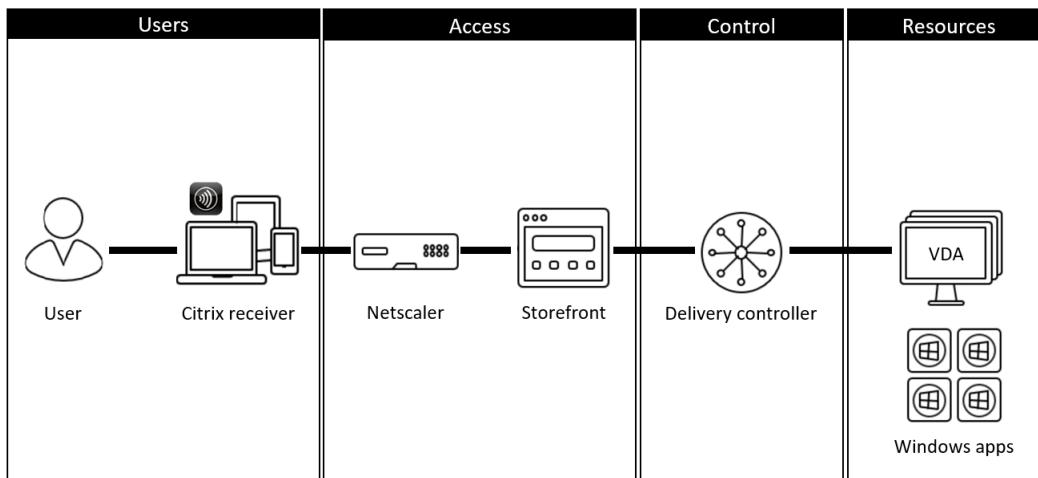


De connectie naar de VM in de DMZ zone is wel mogelijk, hier staan namelijk alle poorten open (deze kan je wel limiteren tot de publieke toepassingen).



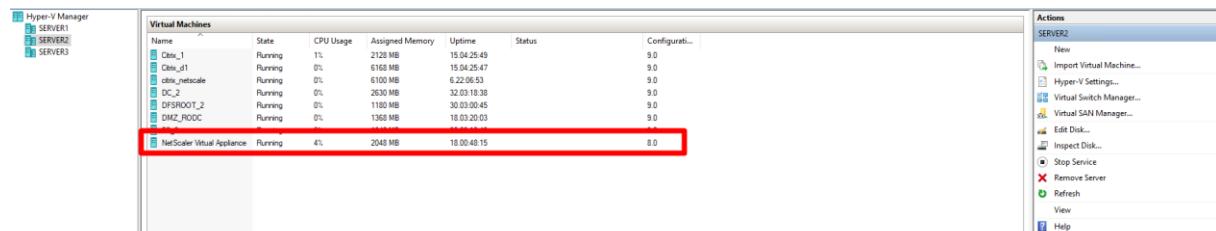
### 3.3.11 NetScaler

De netscaler is een toepassing die je kan gebruiken om applicaties beschikbaar te stellen voor zowel interne als externe gebruikers. De netscaler heeft een grote impact op de performantie, beveiliging en schaalbaarheid van de application delivery.



#### 3.3.11.1 Configuratie (NetScaler Virtual Appliance)

Om extern een remote connection naar de Citrix server te kunnen leggen, moet je een NetScaler configureren. Deze NetScaler plaats je best in de DMZ zone zodat de externe gebruikers hier aan kunnen. De eerste stap is de NetScaler virtual appliance downloaden van de Citrix site. Eens deze gedownload is, kan je de VM importeren op een hypervisor waar de DMZ zone staat.



Start de VM en stel het IP-adres van de NetScaler in. Dit is een management IP-adres, niet het IP waar de externe gebruikers naartoe geleid worden.

```
The key's randomart image is:
+--[ DSA 1024]---+
| .=o *o...
| ++o+o.E
| ++=...
| ..o.o
| oSo
| . . +
| o o
|
+-----+
.
kern.sched.idlespinthresh: 4 -> 32
Start daemons: syslogd Apr 19 13:10:15 <kern.info> ns syslogd: kernel boot file
is /flash/ns-12.0-53.13
inetd cron httpd monit sshd .

!There is no ns.conf in the /nsconfig!

start Netscaler software
put: no terminal type specified and no TERM environmental variable.
Inter NetScaler's IPv4 address []:
Inter Netmask []:
Inter Gateway IPv4 address []

Status: Running
```

Vanaf nu kan je de configuratie uitvoeren via de browser. Aangezien er enorm veel functionaliteiten zijn voor de NetScaler, is het zeker aangeraden om de browser te gebruiken en niet de CLI.

In de browser stel je de standaard instellingen in (subnet IP-adres, netmask, tijdzone, ...). Eens dit ingesteld is, kan je de Citrix XenApp and XenDesktop configureren. Het is aangeraden om alle informatie van de Citrix servers te noteren voor je hieraan begint, namelijk de StoreFront URL, de STA servers (Citrix delivery controllers) en de Authenticatie.

Het certificaat onderdeel kan je later aanvullen, maar de NetScaler zal niet werken zonder dit certificaat. De andere onderdelen kan je alvast invullen.

NetScaler Gateway		Basic Settings	
Gateway IP Address	192.168.70.150	1	NetScaler Gateway
Gateway FQDN	testnetscaler.com	2	Server Certificate
Port	443	3	StoreFront
Redirect requests from port 80 to secure port	Yes	4	Authentication
Server Certificate			
Certificate File	RSA_SERVERKeyPair	Common Name	testnetscaler.com
		Days to Expire	362
StoreFront			
StoreFront URL	http://netscale-citrix.virt.com	Secure Ticket Authority URL	http://netscale-citrix.virt.com
Receiver for Web Path	/Citrix/TestAppsWeb	Default Active Directory Domain	Virt.com
Authentication			
Type	Domain		
192.168.70.3	Domain	Primary	

De wizard heeft nu een virtuele server aangemaakt op de NetScaler (192.168.70.150). Deze server is down, omdat er geen certificaat gekoppeld is. Om dit in orde te brengen kan je een self-signed certificaat aanmaken, dit leg ik hieronder uit.

Om te beginnen maak je eerst de Root Key aan. Deze zal je nodig hebben om de Root Request te kunnen aanmaken. Navigeer naar *Traffic Management > SSL > SSL Files*. Hier creëer je een RSA Key.

>Create RSA Key

Key Filename\*  
Choose File RSA\_ROOT.key

Key Size(bits)\*  
1024

Public Exponent Value\*  
3

Key Format\*  
PEM

PEM Encoding Algorithm

PEM Passphrase

Confirm PEM Passphrase

Create Close

Met deze Key kan je een Root Request aanmaken. Die zal op zijn beurt nodig zijn voor het Root certificaat. Geef de request een naam, organisatie naam, provincie en land.

#### ← Create Certificate Signing Request (CSR)

Request File Name\*

Choose File ▾ RSA\_ROOT.req

Key Filename\*

Choose File ▾ RSA\_ROOT.key

Key Format

PEM  DER

PEM Passphrase (For Encrypted Key)

Digest Method\*

SHA1

Distinguished Name Fields

Common Name\*

NS-ROOT-CA

Organization Name\*

TestNetscaler

Organization Unit

Email Address

City

State or Province\*

Antwerp

Country\*

BELGIUM

Attribute Fields

Met de aangemaakte Key en het Request, kan je het Root certificaat aanmaken. Selecteer voor het certificaat type *Root-CA* en geef de Key en Request mee.

#### ← Certificate

Certificate File Name\*

Choose File ▾ RSA\_ROOT.cert

Certificate Format

PEM  DER

Certificate Type\*

Root-CA

Certificate Request File Name\*

Choose File ▾ /nsconfig/ssl/RSA\_ROOT.req

Key Filename\*

Choose File ▾ /nsconfig/ssl/RSA\_ROOT.key

Key Format

PEM  DER

PEM Passphrase (For Encrypted Key)

Validity Period (Number of Days)

365

**Create** **Close**

Maak nu terug een Key en een Request aan voor het server certificaat. Daarna maak je het server certificaat aan. Verander wel het type van het certificaat naar *Server*. Je zal merken dat dit certificaat de Root files nodig heeft.

#### Certificate

Certificate File Name\*

Certificate Format  
 PEM  DER

Certificate Type\*

Certificate Request File Name\*

Certificate Format  
 PEM  DER

Validity Period (Number of Days)

CA Certificate File Name\*

CA Certificate File format  
 PEM  DER

CA Key File Name\*

CA Key File Format  
 PEM  DER

PEM Passphrase (For Encrypted CA Key)

CA Serial File Number\*

**Create** **Close**

Link nu dit certificaat aan de virtuele server en de status zal veranderen.

NetScaler Gateway Virtual Servers

Add	Edit	Delete	Statistics	Visualizer	Microsoft EMS/Intune Integration	Action	Search ▾
<input type="checkbox"/>	Name	State	IP Address	Port	Protocol	Maximum Users	Current Users Total Connected Users
<input type="checkbox"/>	_XD_192.168.70.100_80	<span style="color:red;">● DOWN</span>	192.168.70.100	80	SSL	0	0 0
<input type="checkbox"/>	_XD_192.168.70.150_443	<span style="color:green;">● UP</span>	192.168.70.150	443	SSL	500	0 0

Bij deze is de NetScaler configuratie klaar. Vergeet niet de config te downloaden zodat je deze kan importeren in de Citrix StoreFront.

Dashboard

**Universal Licenses**  
  
 Current Universal Licenses: 0

**HDX Sessions**  
  
 Current HDX Sessions: 0

**CPU Usage**  
  
 Current CPU Usage: 0.70%

**Memory Usage**  
  
 Current Memory Usage: 16.32%

**Active User Sessions**  

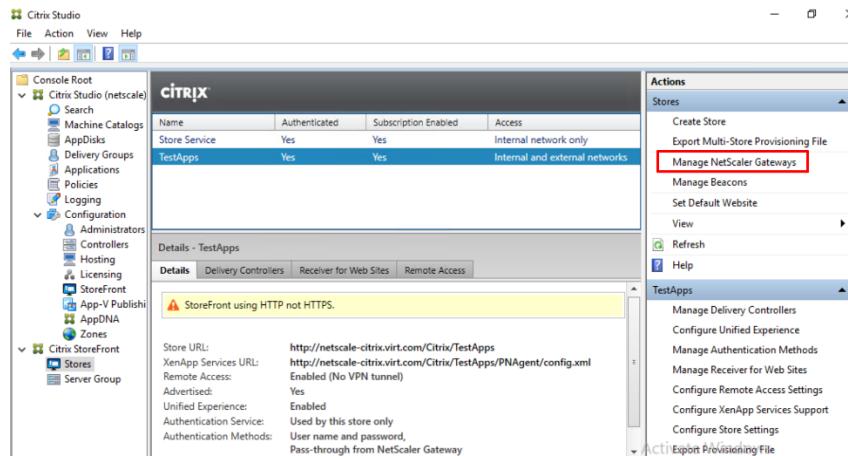
Username	Group Name	Client IP
		No items

**Create New Gateway** **Download file**

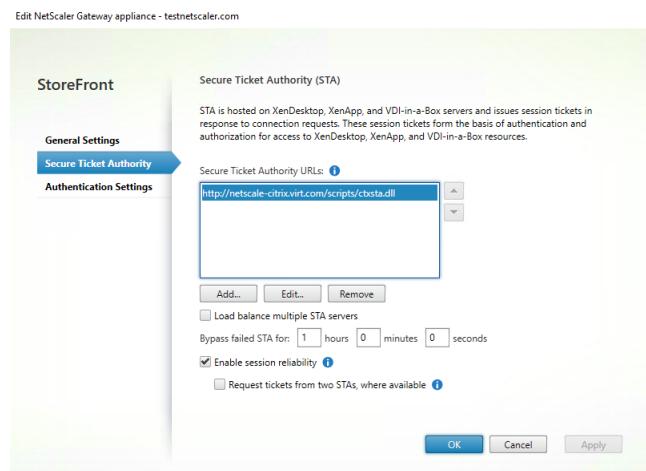
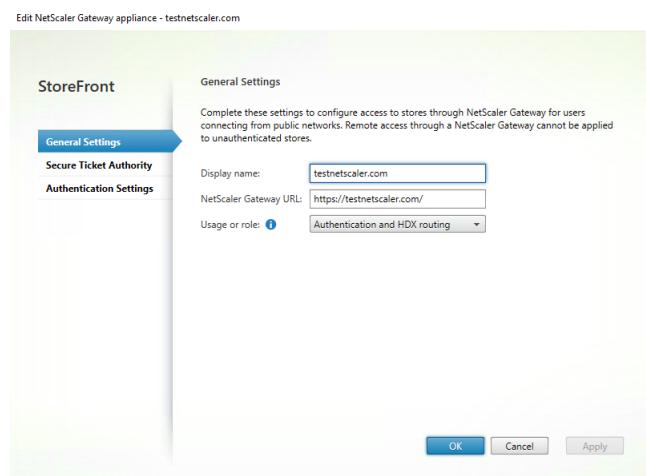
Configured Virtual Servers for XenApp/XenDesktop

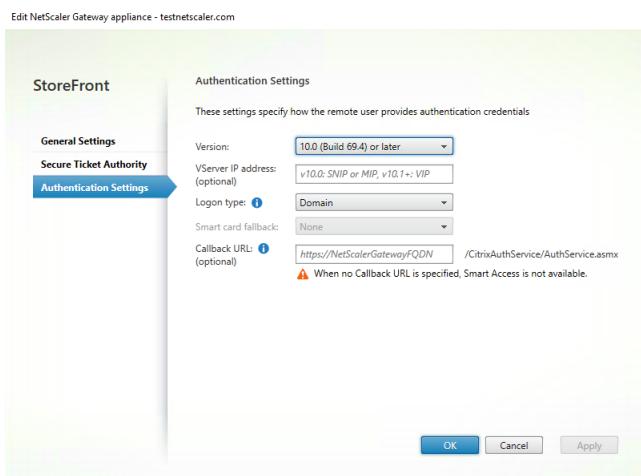
- NetScaler.com
- testnetscaler.com

Log in op de Citrix StoreFront server en navigeer naar de store. Selecteer *Manage NetScaler Gateways*. Hier kan je de config importeren en is de configuratie klaar. Om iets meer controle te hebben, kan je deze ook zelf instellen.



In deze configuratie stel je de naam in, de NetScaler URL, de STA servers (Citrix delivery controllers) en de authenticatie die je gebruikt.





Tot slot stel je de remote access nog in op de StoreFront. Deze staat standaard uit en moet je dus aanzetten.

#### Configure Remote Access Settings - TestApps

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a NetScaler Gateway appliance.

##### Enable Remote Access

Select the permitted level of access to internal resources

Allow users to access only resources delivered through StoreFront (No VPN tunnel) [i](#)

Allow users to access all resources on the internal network (Full VPN tunnel) [i](#)

Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.

NetScaler Gateway appliances:  testnetscaler.com



Add...

Default appliance:

testnetscaler.com

OK

Cancel

Als het goed is, zou er nu bij de StoreFront Store access zowel internal als external moeten staan.

Name	Authenticated	Subscription Enabled	Access
Store Service	Yes	Yes	Internal network only
TestApps	Yes	Yes	Internal and external networks

Details - TestApps

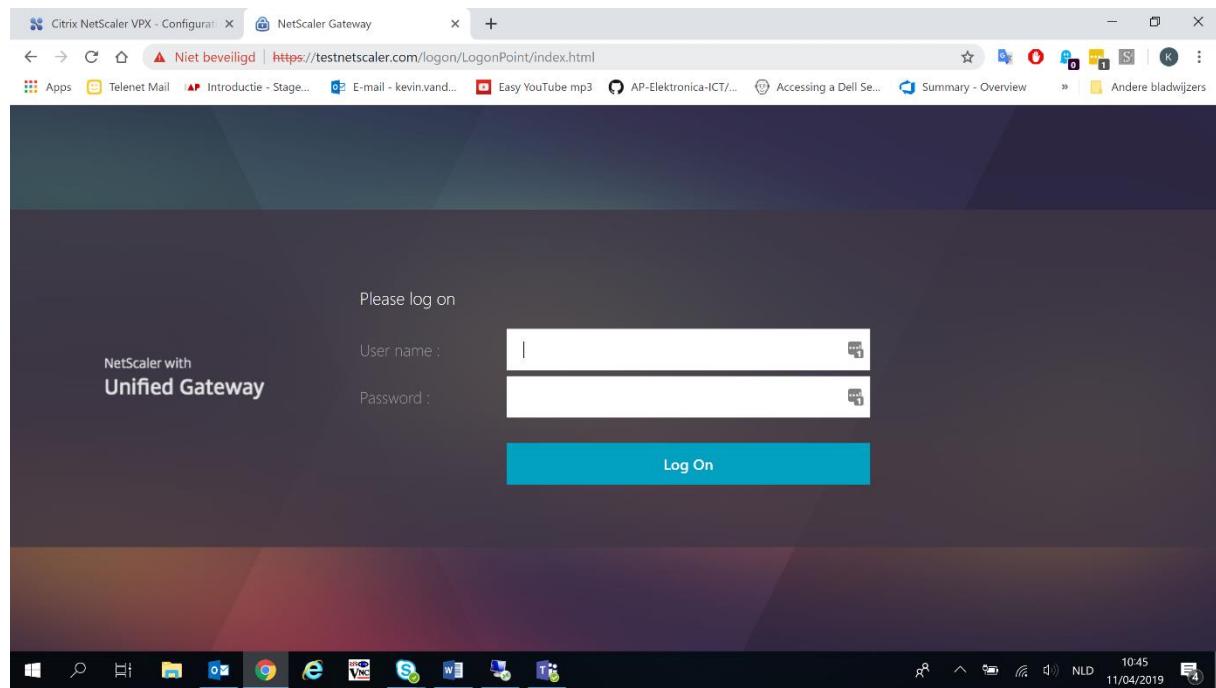
Store URL: http://netscale-citrix.virt.com/Citrix/TestApps  
 XenApp Services URL: http://netscale-citrix.virt.com/Citrix/TestApps/PNAgent/config.xml  
 Remote Access: Enabled (No VPN tunnel)

De configuratie is nu voltooid voor zowel de NetScaler als de Citrix StoreFront. Je kan nu browsen naar het NetScaler adres (testnetscaler.com in de demo-omgeving). Hou er wel rekening mee dat je een DNS adres hiervoor moet kopen als deze in gebruik genomen wordt. Voor een testomgeving is dit niet nodig zolang je het IP-adres en DNS naam in de host file van je computer zet.

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10     x.acme.com            # x client host
#      192.168.68.35   Citrix.virt.com       # citrix webhost
#      192.168.68.44   Citrix.virt.com       # citrix webhost
#      192.168.68.21   netscaler.virt.com    # citrix webhost netscale
#      192.168.68.50   netscale-citrix.virt.com # citrix webhost netscale
#      192.168.70.150  testnetscaler.com    # citrix webhost netscale

# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
```

Nu deze in de hosts file staat, kan je surfen naar de NetScaler ook al heb je geen DNS naam gekocht. Deze NetScaler zal de gebruikers doorsturen naar de Citrix Receiver waar de applicaties staan die gepubliceerd zijn.



### 3.3.12 Azure AD Connect

Met Azure AD Connect kan je de active directory van het domein synchroniseren naar de cloud. Hierdoor is het mogelijk om met één identiteit zowel de cloud als interne toepassingen te gebruiken. Ook kan je met Azure AD Connect single sign-on instellen.

#### 3.3.12.1 Installatie (AD\_connect)

Op de Azure site download je de Azure AD Connect. Best practice installeer je deze op een aparte VM om de domaincontroller te syncen naar de Azure cloud.

The screenshot shows the Azure portal interface for managing Azure AD Connect. On the left, there's a sidebar with various options like Overview, Getting started, Manage (Users, Groups, Roles and administrators, Enterprise applications, Devices, App registrations, Application proxy, Licenses), and Azure AD Connect (which is selected). The main content area has the following sections:

- SYNC STATUS:** Shows 'Not Installed' for Active Directory UPN Suffix and Last Sync, and 'Disabled' for Password Hash Sync.
- USER SIGN-IN:** Shows 'Disabled' for Federation, Seamless single sign-on, and Pass-through authentication, with '0 domains' for each.
- ON-PREMISES APPLICATIONS:** A section for configuring remote access for on-premises applications, with a link to Head to Application Proxy.

In de setup is er de keuze tussen een custom install of een express install. Voor extra controle en toepassingen neem je best de custom install. Vervolledig nu de volgende stappen tot je aan de *Connect your directies* stap bent. Hier geef je de forest van je domein in. Zoals je hieronder kan zien, moet je de UPN (userPrincipalName) suffix verifiëren in Azure.

The screenshot shows the Microsoft Azure Active Directory Connect setup wizard. The left sidebar lists steps: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, **Azure AD sign-in** (which is selected), Domain/OU Filtering, Identifying users, Filtering, Optional Features, and Configure. The main content area is titled "Azure AD sign-in configuration". It says: "To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain." A table shows the "Active Directory UPN Suffix" (virt.com) and "Azure AD Domain" (Not Verified). A red box highlights this row. Below the table, it says: "Select the on-premises attribute to use as the Azure AD username" and "USER PRINCIPAL NAME" (set to userPrincipalName). At the bottom, there's a checkbox: "Continue without matching all UPN suffixes to verified domains" and a warning message in a red box: "Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. Learn more".

In de demo-omgeving is er gebruik gemaakt van het domein *Virt.com*, maar deze DNS is niet aangekocht. Hierdoor is het onmogelijk om de virt.com UPN suffix te verifiëren.

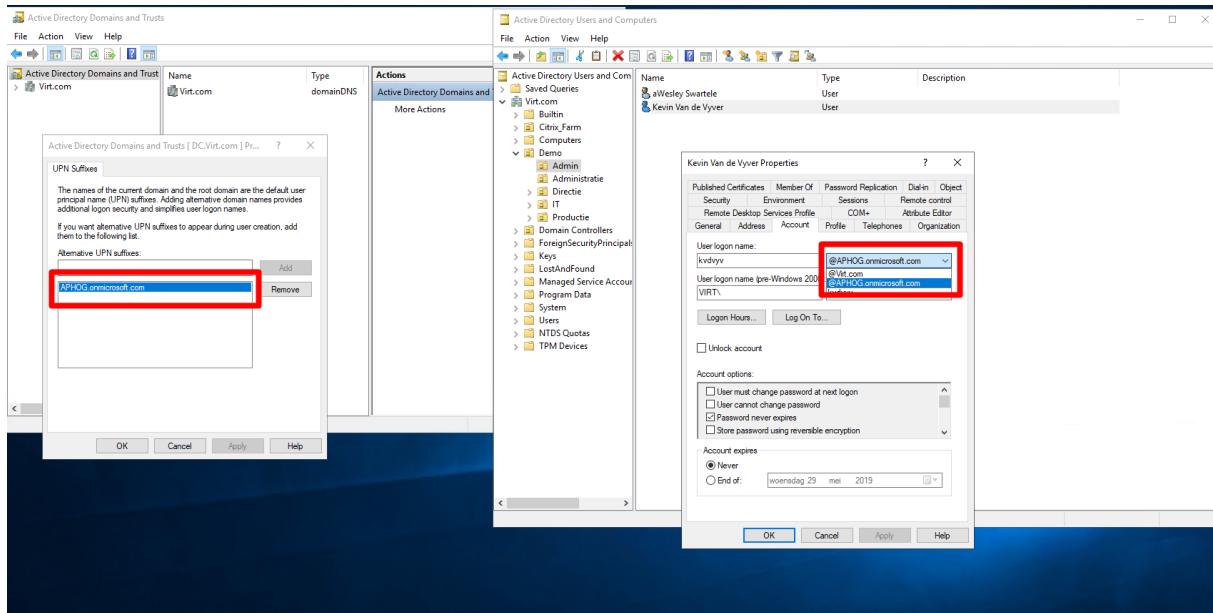
The screenshot shows the Azure portal interface for managing custom domains. On the left, there's a sidebar with various service icons. The main area is titled 'AP - Custom domain names > virt.com'. It displays fields for 'RECORD TYPE' (set to 'TXT'), 'ALIAS OR HOST NAME' (@), 'DESTINATION OR POINTS TO ADDRESS' (MS=ms85647616), and 'TTL' (3600). Below these fields is a link to 'Share these settings via email'. A prominent red box highlights a warning message: 'Verify domain' followed by 'Verification will not succeed until you have configured your domain with your registrar as described above.' At the bottom of this box is another message: 'Could not find the DNS record for this domain. DNS changes may take up to 72 hours to propagate. Please try again later.'

Om dit probleem te omzeilen kan je een andere suffix aanmaken in het domein. Wanneer je inlogt op Azure met een Microsoft account, heeft deze standaard een geverifieerd onmicrosoft domein. Deze UPN voeg je toe in het het domein van je omgeving.

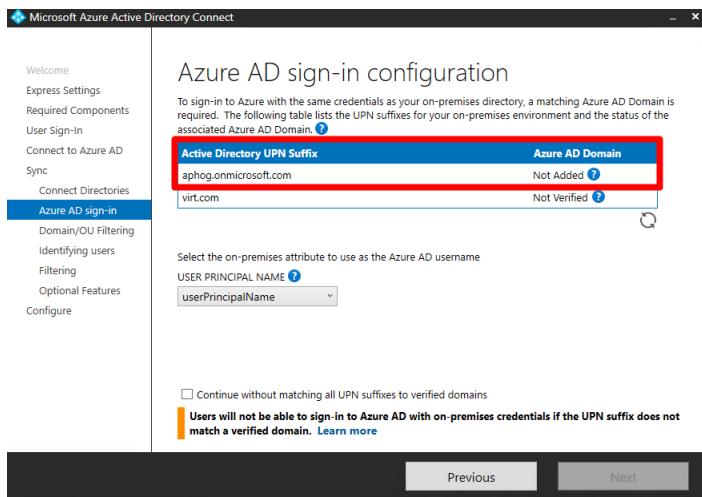
The screenshot shows the Azure Active Directory portal with the 'Custom domain names' section selected in the sidebar. The main area has a search bar and buttons for 'Add custom domain', 'Refresh', 'Troubleshoot', and 'Columns'. A large red box highlights a message: 'Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?'. Below this are filters for 'Status' (Any, Federated, Primary) and buttons for 'Apply' and 'Reset'. A search bar is also present. The table lists two domains: 'APHOG.onmicrosoft.com' with a green checkmark and 'STATUS' column value 'Available', and 'virt.com' with an orange triangle and 'STATUS' column value 'Unverified'.

NAME	STATUS	FEDERATED	PRIMARY
APHOG.onmicrosoft.com	Available		
virt.com	Unverified		

Op de domaincontroller open je de *Active Directory Domains and Trust* tool en voeg je ook de suffix `onmicrosoft.com` toe. Nu kan je in *Active Directory Users and Computers* de suffix van de gebruikers aanpassen.



Nu de suffix is toegevoegd aan het domein, kan de installatie van de Azure connect verder verlopen. Bij de *Azure AD sign-in* stap verschijnt een extra UPN suffix met de state *Not Added*. Dit is voldoende om verder te kunnen gaan.



Voor het domein `virt.com` of `onmicrosoft.com` zijn geen specifieke vereisten, de volgende opties laat je op de default waarden staan. Je kan er voor kiezen om het volledige domein te synchroniseren of slechts bepaalde onderdelen of gebruikers.

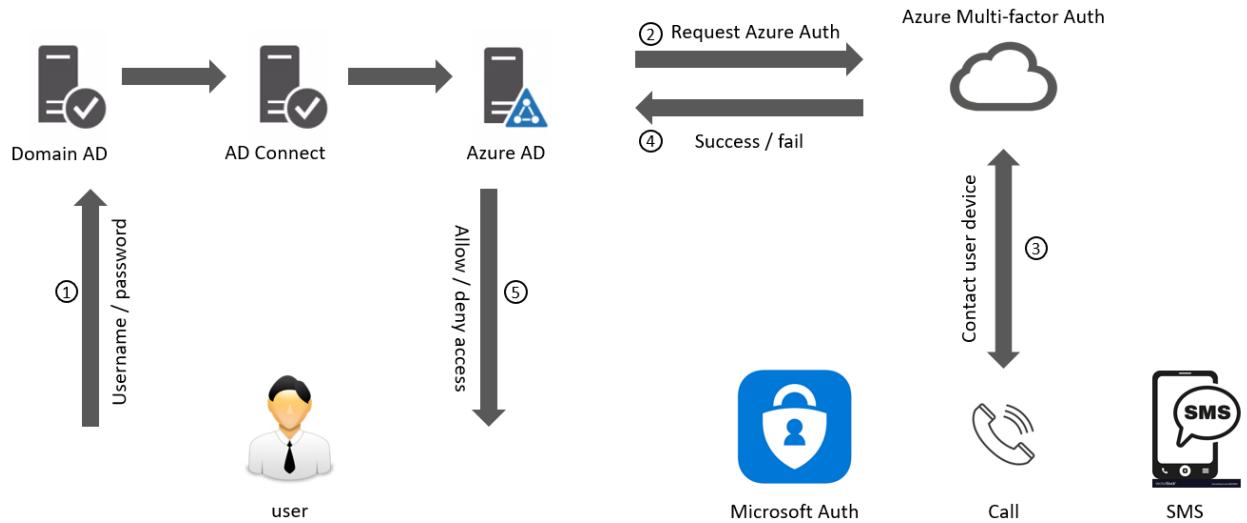
Na de setup is de active directory van het domein gesynchroniseerd met de Azure Active Directory. Om na te kijken of de synchronisatie al gebeurd is, kan je op de Azure site de gebruikers zien. Alle users die hierin staan, kunnen vanaf nu met hun domeinlogin ook aan de Azure applicaties. Een website die je kan gebruiken om te testen is [myapps.microsoft.com](http://myapps.microsoft.com).

NAME	USER NAME	USER TYPE	SOURCE
AS	aWesley Swartele	Member	Windows Server AD
U	ik jij	Member	Azure Active Directory
JU	Julie jru. Rutten	Member	Windows Server AD
KV	Kevin Van de Vyver	Member	Windows Server AD
KR	krbtgt_920	Member	Windows Server AD
OD	On-Premises Direct Sync	Member	Windows Server AD
SS	Sam svab. Van Bog	Member	Windows Server AD
SS	Seppe sdb. De Beu	Member	Windows Server AD
SS	Sophie sru. Rutten	Member	Windows Server AD
WW	Wesley wswart. Sw	Member	Windows Server AD

Een extra optie die je kan instellen met Azure AD Connect is *Single sign-on*. Dit verhoogt de productiviteit van de gebruikers, omdat ze weer een paswoord minder moeten onthouden. Eens ingelogd op de computer met het domein account, kan je zonder opnieuw je paswoord in te geven inloggen op de cloud.

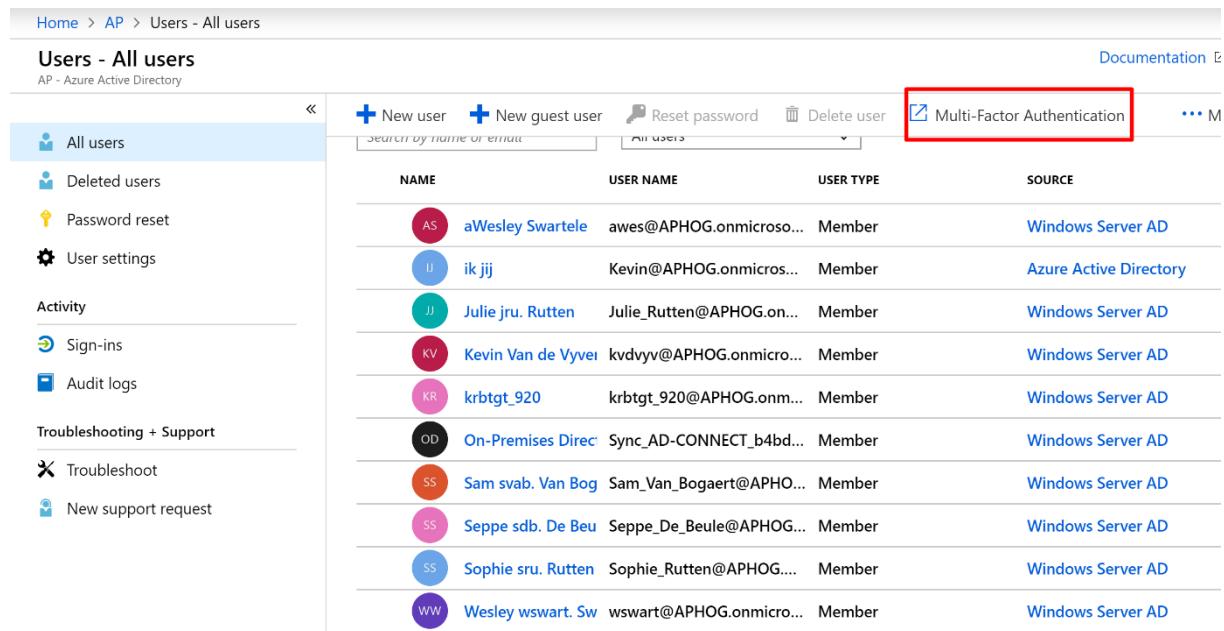
### 3.3.13 Multi-factor Authenticatie

In vorig hoofdstuk is Active Directory gesynchroniseerd met de Azure cloud. Ook is er Single sign-on ingesteld voor de gebruikers. Om de beveiliging van de accounts te verbeteren, is er multi-factor authenticatie geconfigureerd op de Azure active directory.



### 3.3.13.1 Configuratie MFA

In de Azure Active Directory is er een optie voor MFA in de gebruikers sectie. Hier kan men de MFA instellen voor de gebruikers.



The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. On the left, there's a sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Activity', 'Sign-ins', 'Audit logs', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area displays a table of users with columns: NAME, USER NAME, USER TYPE, and SOURCE. A red box highlights the 'Multi-Factor Authentication' button at the top right of the table header. The table contains 11 user entries, each with a small circular profile picture and their respective details.

NAME	USER NAME	USER TYPE	SOURCE
AS aWesley Swartele	aWesley.Swartele@APHOG.onmicrosoft.com	Member	Windows Server AD
IJ ik jij	Kevin@APHOG.onmicrosoft.com	Member	Azure Active Directory
JJ Julie jru. Rutten	Julie.Rutten@APHOG.onmicrosoft.com	Member	Windows Server AD
KV Kevin Van de Vyvei	kvdyv@APHOG.onmicrosoft.com	Member	Windows Server AD
KR krbtgt_920	krbtgt_920@APHOG.onmicrosoft.com	Member	Windows Server AD
OD On-Premises Direct	Sync_AD-CONNECT_b4bd...	Member	Windows Server AD
SS Sam svab. Van Bog	Sam_Van_Bogaert@APHOG.onmicrosoft.com	Member	Windows Server AD
SS Seppe sdb. De Beu	Seppe_De_Beu@APHOG.onmicrosoft.com	Member	Windows Server AD
SS Sophie sru. Rutten	Sophie_Rutten@APHOG.onmicrosoft.com	Member	Windows Server AD
WW Wesley wswart. Sw	wswart@APHOG.onmicrosoft.com	Member	Windows Server AD

Wanneer er een gebruiker voor de eerste keer inlogt op een cloud toepassing zal deze een type MFA moeten selecteren voordat hij verder kan gaan. Deze MFA zal dan voor alle volgende logins gebruikt worden, je hoeft dit dus maar één keer op te geven.

### Aanvullende beveiligingsverificatie

Beveilig uw account door telefonische verificatie toe te voegen aan uw wachtwoord. [Bekijk de video voor meer informatie over hoe u uw account kunt beveiligen](#)

#### Stap 1: Hoe kunnen we contact met u opnemen?

Mobiele app

Hoe wilt u de mobiele app gebruiken?

- Meldingen ontvangen voor verificatie
- Verificatiecode gebruiken

Als u deze verificatiemethoden wilt gebruiken, moet u de Microsoft Authenticator-app instellen.

[Instellen](#)



[Activeringsstatus controleren.](#)

[Volgende](#)

Volg de stappen om een authenticator applicatie op je smartphone te installeren en te configureren.

Andere mogelijkheden zijn authenticatie via SMS of opgebeld worden.

### **3.3.14 Secure wireless**

## 3.4 Powershell

Powershell is een ingebouwde command line van windows en is een populaire tool voor IT departementen om taken te automatiseren. Powershell kan je gebruiken om heel wat windows-opties te configureren via scripts. Dat gaat sneller en gemakkelijker dan via de GUI.

### 3.4.1 Domaincontroller (PS\_AD)

In puntje 3.3.1 is de DC via de GUI geconfigureerd, maar dit kan ook snel en eenvoudig met powershell. Prerequisite is uiteraard steeds dat de domaincontroller een statisch IP-adres heeft. Ook dit kan je met powershell instellen.

Om het IP van een interface aan te passen, moet je eerst de naam (alias) hiervan opzoeken. Dit kan met het commando *Get-NetIPAddress*.

Geef IP, subnet en gateway op met het commando *New-NetIPAddress*.

Voor hulp met de correcte syntax hiervan typ je *get-help New-NetIPAddress*.

```
PS C:\Users\Administrator> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "192.168.68.60" -PrefixLength 23 -DefaultGateway 192.168.68.1

IPAddress      : 192.168.68.60
InterfaceIndex  : 4
InterfaceAlias   : Ethernet
AddressFamily    : IPv4
Type            : Unicast
PrefixLength    : 23
PrefixOrigin     : Manual
SuffixOrigin     : Manual
AddressState     : Tentative
ValidLifetime   : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::.MaxValue)
SkipAsSource    : False
PolicyStore      : ActiveStore

IPAddress      : 192.168.68.60
InterfaceIndex  : 4
InterfaceAlias   : Ethernet
AddressFamily    : IPv4
Type            : Unicast
PrefixLength    : 23
PrefixOrigin     : Manual
SuffixOrigin     : Manual
AddressState     : Invalid
ValidLifetime   : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::.MaxValue)
SkipAsSource    : False
PolicyStore      : PersistentStore

PS C:\Users\Administrator>
```

De server heeft nu een vast IP-adres, nu kan je de domaincontroller configureren. Om deze te installeren heb je eerst de naam van de service nodig. Het volgende commando lijst alle windows features op; *get-windowsfeature*. Zoek de service die je nodig hebt uit de lijst. Installeer de feature AD-Domain-Services.



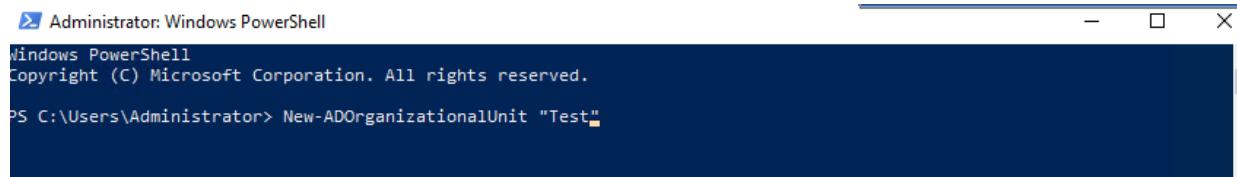
De server promoten tot domaincontroller kan je met *Install-ADDSForest*. Dit commando bevat een hele reeks parameters om het de domein te configureren. Om het overzichtelijk te houden worden de parameters onder elkaar weergegeven, maar voor de effectieve installatie plaats je deze achter elkaar.

```
Install-ADDSForest
- CreateDnsDelegation:$false
- DatabasePath "C:\Windows\NTDS"
- DomainName "powershell.com"
- DomainNetbiosName "POWERSHELL"
- InstallDns:$true
- LogPath "C:\Windows\NTDS"
- NoRebootOnCompletion:$false
- SysvolPath "C:\Windows\SYSVOL"
- Force:$true
```

Na het vorige commando zal de server automatisch herstarten.

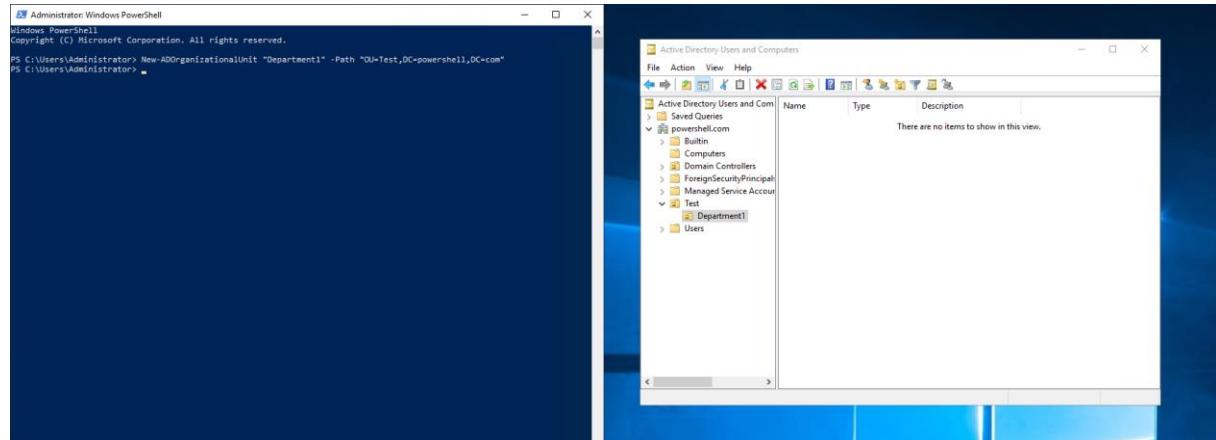
Vervolgens kan je de structuur van het domein opzetten.

Om een organizational unit (OU) toe te voegen, kan je volgend commando gebruiken; *New-ADOrganizationalUnit*. Zonder de -path parameter zal deze in de root OU gezet worden.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-ADOrganizationalUnit "Test"
```



Nu de structuur is opgezet, kan je security groups aanmaken. Dit kan met het commando *New-ADGroup*. Ook dit commando bevat een aantal parameters. De voornaamste parameters zijn:

- Name
- GroupCategory (distribution / security)
- GroupScope (local / global / universal)

Om gebruikers toe te voegen tot een security group wordt *Add-ADGroupMember* gebruikt. Dit commando heeft volgende parameters nodig:

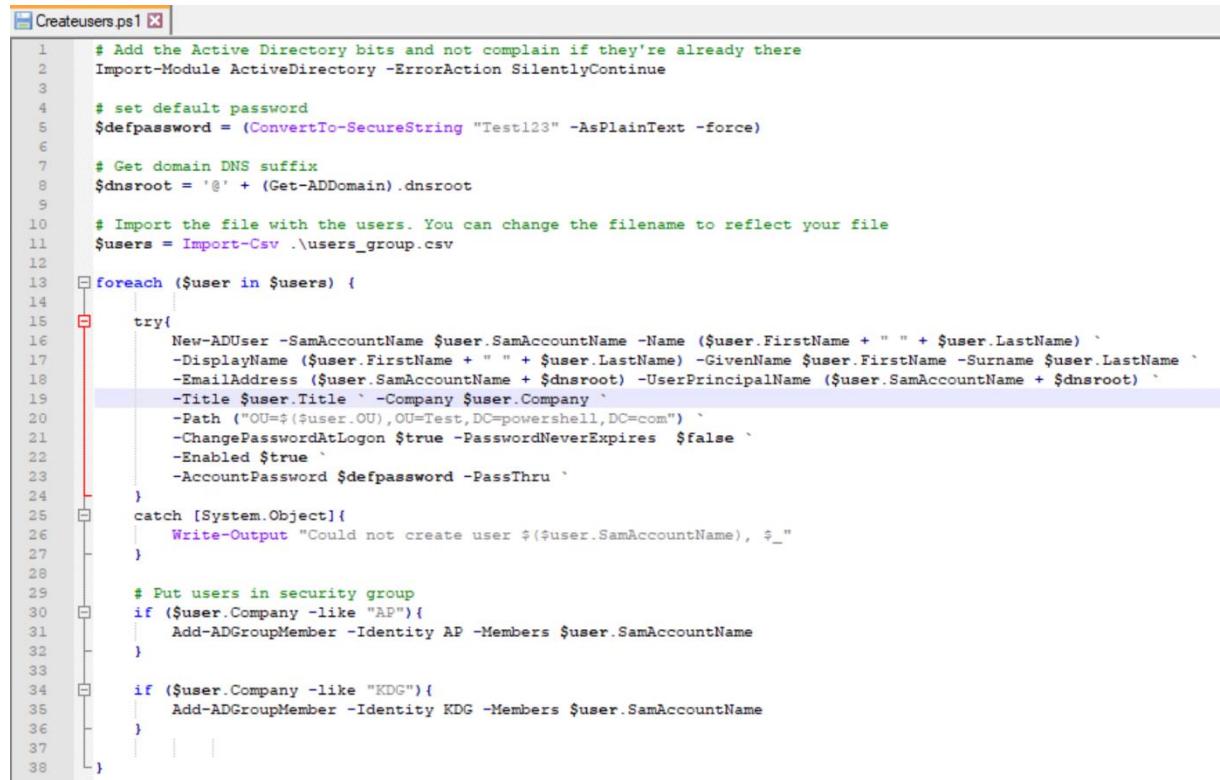
- Identity (naam van security group)
- Members (gebruiker om toe te voegen)

Tot slot kan je de gebruikers aanmaken, in een security group plaatsen en in de correcte organizational unit zetten. Hiervoor gebruik je het commando *New-ADUser*. Dit commando bevat te veel parameters om hier uit te leggen, op de volgende pagina staat een script als voorbeeld. Het script zal meerdere users aanmaken en automatisch in de bijhorende security group en organizational unit plaatsen.

Ter voorbereiding van het script is er een comma separated value bestand (.csv) nodig met alle users en hun informatie.

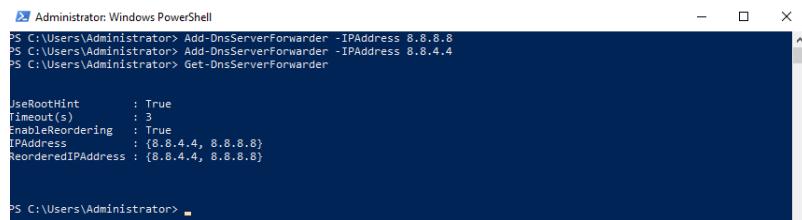
 users\_group.csv - Notepad  
File Edit Format View Help  
FirstName,LastName,SamAccountName,Company,Title,OU  
Jackie,Chan, Jackie Chan,AP,Leerkracht,Department2  
Karate,Kid,Karate Kid,AP,Student,Department2  
Kristof,Gaga, Kristof Gaga,KDG,Student,Department1

Hieronder worden alle voorgaande commando's gebruikt in één script om gebruikers aan te maken en aan de juiste groepen en OU's toe te voegen.



```
1 # Add the Active Directory bits and not complain if they're already there
2 Import-Module ActiveDirectory -ErrorAction SilentlyContinue
3
4 # set default password
5 $defpassword = (ConvertTo-SecureString "Test123" -AsPlainText -force)
6
7 # Get domain DNS suffix
8 $dnsroot = '@' + (Get-ADDomain).dnsroot
9
10 # Import the file with the users. You can change the filename to reflect your file
11 $users = Import-Csv .\users_group.csv
12
13 foreach ($user in $users) {
14
15     try{
16         New-ADUser -SamAccountName $user.SamAccountName -Name ($user.FirstName + " " + $user.LastName) ` 
17             -DisplayName ($user.FirstName + " " + $user.LastName) -GivenName $user.FirstName -Surname $user.LastName ` 
18             -EmailAddress ($user.SamAccountName + $dnsroot) -UserPrincipalName ($user.SamAccountName + $dnsroot) ` 
19             -Title $user.Title ` -Company $user.Company ` 
20             -Path ("OU=$($user.OU),OU=Test,DC=powershell,DC=com") ` 
21             -ChangePasswordAtLogon $true -PasswordNeverExpires $false ` 
22             -Enabled $true ` 
23             -AccountPassword $defpassword -PassThru ` 
24     }
25     catch [System.Object]{
26         Write-Output "Could not create user $($user.SamAccountName), $_"
27     }
28
29     # Put users in security group
30     if ($user.Company -like "AP"){
31         Add-ADGroupMember -Identity AP -Members $user.SamAccountName
32     }
33
34     if ($user.Company -like "KDG"){
35         Add-ADGroupMember -Identity KDG -Members $user.SamAccountName
36     }
37 }
38 }
```

De structuur is nu opgezet, users zijn aangemaakt en de domain services zijn correct geïnstalleerd. Rest enkel de DNS installatie nog. Als eerste stap kijk je na of er al forwarders aanwezig zijn op de server met *Get-DnsServerForwarder*. Indien er adressen aanwezig zijn die je niet gebruikt, kan je die nu verwijderen. Voeg vervolgens de forwarders toe met *Add-DnsServerForwarder -IPAddress x.x.x.x*.

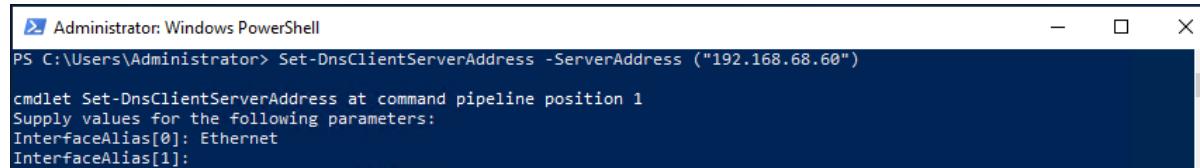


```
PS C:\Users\Administrator> Add-DnsServerForwarder -IPAddress 8.8.8.8
PS C:\Users\Administrator> Add-DnsServerForwarder -IPAddress 8.8.4.4
PS C:\Users\Administrator> Get-DnsServerForwarder

UseRootHint      : True
Timeout(s)       : 3
EnableReordering : True
IPAddress        : {8.8.4.4, 8.8.8.8}
ReorderedIPAddress : {8.8.4.4, 8.8.8.8}

PS C:\Users\Administrator>
```

Tot slot moet je de server vertellen dat hij gebruik moet maken van deze DNS client server.



```
PS C:\Users\Administrator> Set-DnsClientServerAddress -ServerAddress ("192.168.68.60")

cmdlet Set-DnsClientServerAddress at command pipeline position 1
Supply values for the following parameters:
InterfaceAlias[0]: Ethernet
InterfaceAlias[1]:
```

### **3.5 Besluit**