

De opbouw van een bedrijfsomgeving

Scriptie ingediend tot het behalen van de graad van
PROFESSIONELE BACHELOR IN DE ELEKTRONICA-ICT

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 wekte **Ferranti** mijn nieuwsgierigheid op omdat zij een intrigerende opdracht aanboden. De uitdaging bestond uit het opstarten van een fysiek en virtueel bedrijf 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 aangeboden 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 kreeg ik de mogelijkheid om alle ICT facetten van het bedrijf te verkennen. Hiervoor zette ik een fictief bedrijf op 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, ...).

Een permanente monitoring (OMS) en back-ups (VEEAM) vangen alle noodsituaties op.

Inhoudsopgave

Table of Contents

De opbouw van een bedrijfsomgeving.....	Error! Bookmark not defined.
Ferranti Computer Systems nv ~ Silta	Error! Bookmark not defined.
Woord vooraf	1
Samenvatting	2
Inhoudsopgave.....	4
De opbouw van een netwerk infrastructuur	6
1 Inleiding	6
2 Onderzoek	7
2.1 Infrastructuur design.....	7
2.2 Netwerk design.....	8
3 Configuraties	9
3.1 Hardware (RAID, OS installatie, iDRAC)	9
3.1.1 Server 1 + Server 2.....	9
3.1.2 Server 3	12
3.2 Netwerk.....	13
3.2.1 Firewall.....	13
3.2.2 Switch.....	14
3.2.3 Servers	16
3.3 Toepassingen.....	17
3.3.1 Domaincontroller.....	18
3.3.1.1 Installatie primary domaincontroller	18
3.3.1.2 Installatie back-up domaincontroller	21
3.3.2 Group policies	24
3.3.2.1 Configuratie default browser	24
3.3.2.2 Configuratie browser startpagina	25
3.3.2.3 Configuratie drive mapping.....	29
3.3.3 DNS.....	32
3.3.3.1 Installatie DNS.....	32
3.3.4 DHCP	34
3.3.4.1 Installatie DHCP	34
3.3.5 Printserver	36
3.3.5.1 Installatie printserver.....	36
3.3.6 Fileservers (DFS).....	40

3.3.6.1 Installatie fileservers	40
3.3.7 Citrix	45
3.3.7.1 Configuratie VDA	46
3.3.7.2 Configuratie Delivery controllers	47
3.3.8 Veeam.....	50
3.3.8.1 Configuratie VEEAM.....	50
3.3.9 Replication.....	55
3.3.9.1 Configuratie.....	56
3.3.9.2 Installatie.....	57
3.3.10 DMZ.....	58
3.3.10.1 Configuratie.....	59
3.3.11 NetScaler.....	61
3.3.11.1 Configuratie.....	61
3.3.12 Azure AD Connect.....	70
3.3.12.1 Installatie.....	70
3.3.13 Multi-factor Authenticatie.....	74
3.3.13.1 Configuratie MFA	75
3.3.14 Windows Server Update Services (WSUS).....	76
3.3.14.1 Configuratie WSUS.....	77
3.3.15 SMTP Server.....	84
3.3.15.1 Configuratie mail server.....	84
3.3.15.2 iDRAC monitoring.....	87
3.4 Powershell	89
3.4.1 Domaincontroller (PS_AD)	89
4 Besluit	93
5 Bibliografie	94
5.1 Gevolgde tutorials	94
5.2 Geraadpleegde bronnen.....	94
6 Verklarende woordenlijst	95
7 Lijst van figuren	98

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 1 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,
- fileserver,
- citrix,
- replication,
- dmz,
- netscaler,
- veeam,
- azure ad connect,
- multi-factor authentication,
- wsus,
- smtp.

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

2 Onderzoek

In dit hoofdstuk zal ik de benadering van het project verder uitleggen. Om een project tot een goed einde 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 geback-up en gemonitord wordt, is er hiervoor een fysieke server aan toegewezen. Deze server heeft de 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).

DELL PowerEdge R620



2 CPU's 12 cores total
2x 67,2 GB (OS – RAID 1)
4x 136 GB (VM – RAID 10)

DELL PowerEdge R720



2 CPU's 12 cores total
2x 67,2 GB (OS – RAID 1)
4x 136 GB (VM – RAID 10)

DELL PowerEdge R420



2 CPU's 8 cores total
3x 3TB (RAID 5)

Figuur 2-1 Infrastructuurdesign

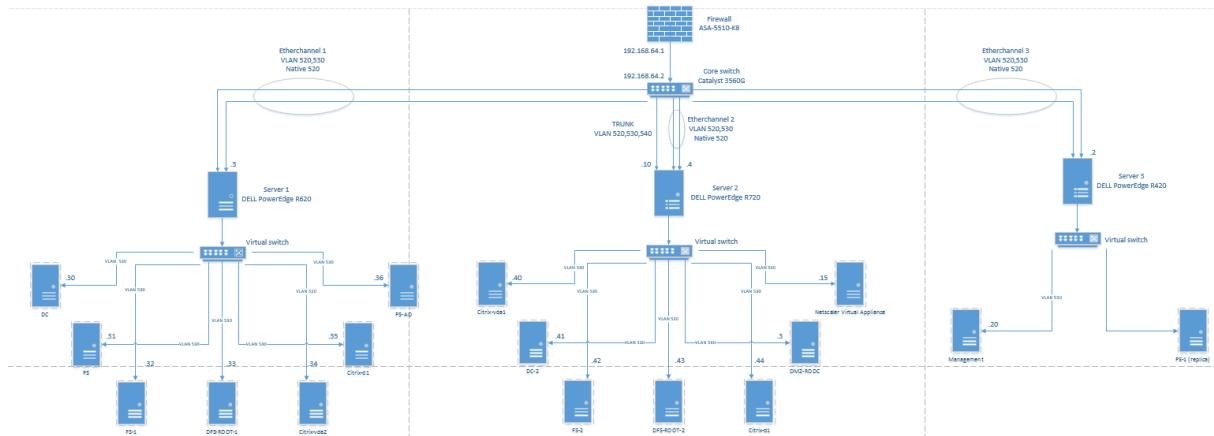
2.2 Netwerk design

Na het vastleggen van het infrastructuurontwerp, kon ik beginnen 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, maak je gebruik van etherchannels (2 fysieke links als één logische link). Als er één van de twee links defect raakt, verplaatst het verkeer zich 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, ...).



Figuur 2-2 Netwerkdesign

3 Configuraties

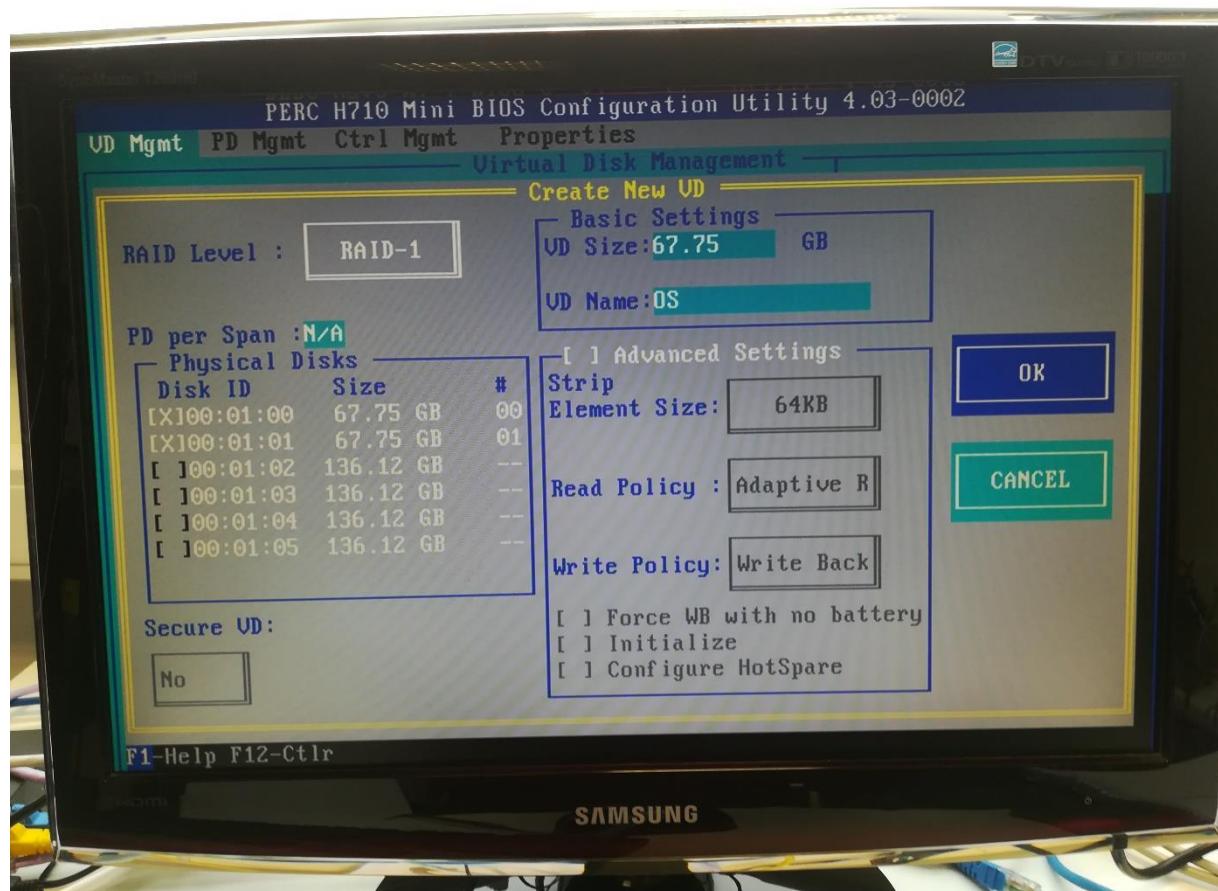
In dit hoofdstuk leg ik uit welke configuraties er zijn gebeurd en hoe ik deze precies heb geconfigureerd.

3.1 Hardware (RAID, OS installatie, iDRAC)

3.1.1 Server 1 + Server 2

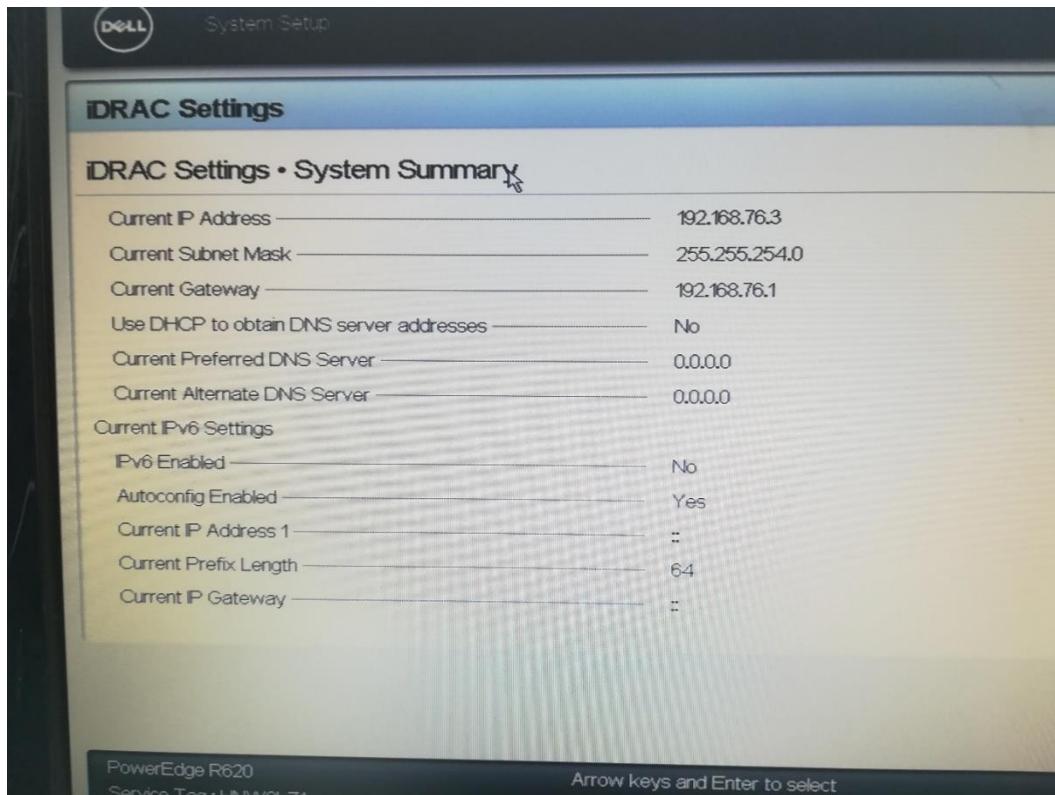
Aangezien servers 1 en 2 exact dezelfde configuratie hebben, zijn deze samengenomen in dit onderdeel. Beide maken gebruik van een RAID 1 (mirror) level waar het operating systeem opstaat, hierdoor blijft het OS intact al is er een schijf defect. Ook hebben de servers een RAID 10 (striping + mirror) level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

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



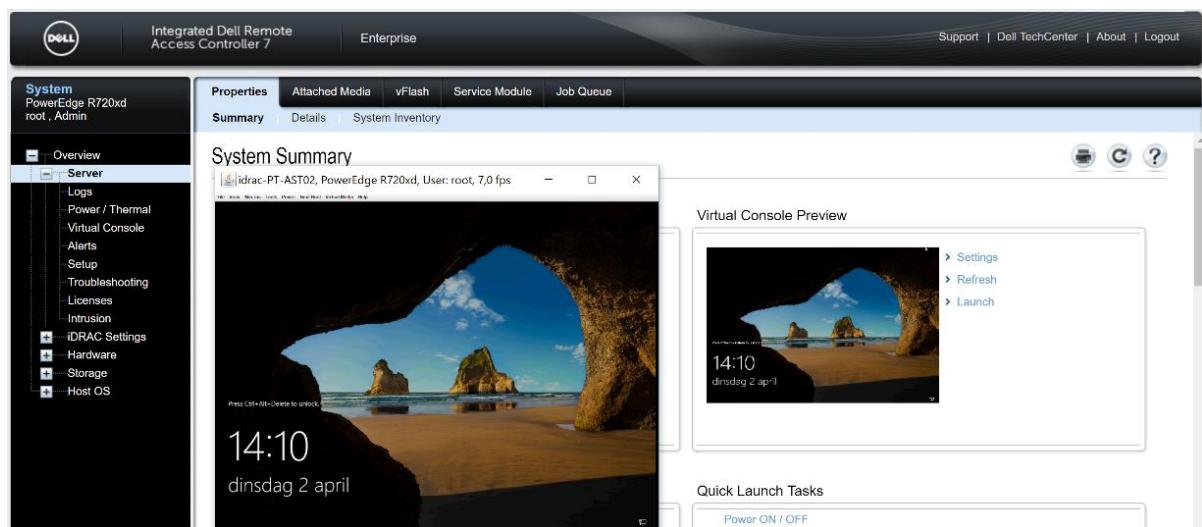
Figuur 3-1 RAID Config

In de system setup van de servers maak je iDRAC instellingen zodat je vanop afstand toegang krijgt tot de servers, zelfs wanneer de server uitgeschakeld is of nog geen besturingssysteem heeft.



Figuur 3-2 iDRAC Config

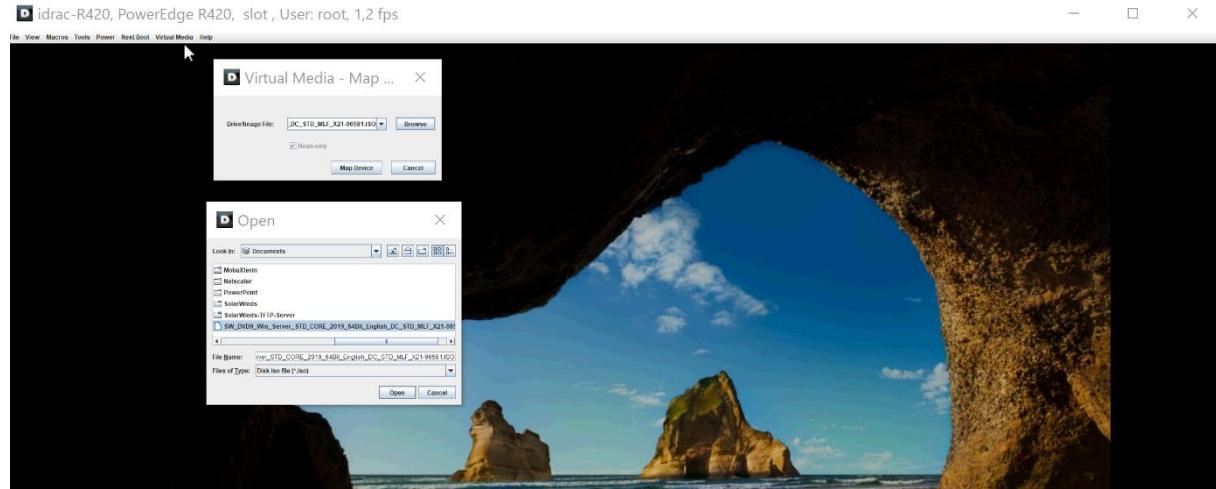
Dit vergemakkelijkt de installatie van de servers. Servers staan steeds ergens in een datacenter, en dit is niet noodzakelijk in de buurt van je werkplek. Het is niet de bedoeling om een USB-stick of DVD in de server te steken om het besturingssysteem of software te installeren. Alles moet vanop afstand 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.



Figuur 3-3 iDRAC Browser

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 installeert.

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 naveer 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 net alsof er een DVD in een DVD-lezer zit waarvan er opgestart kan worden.



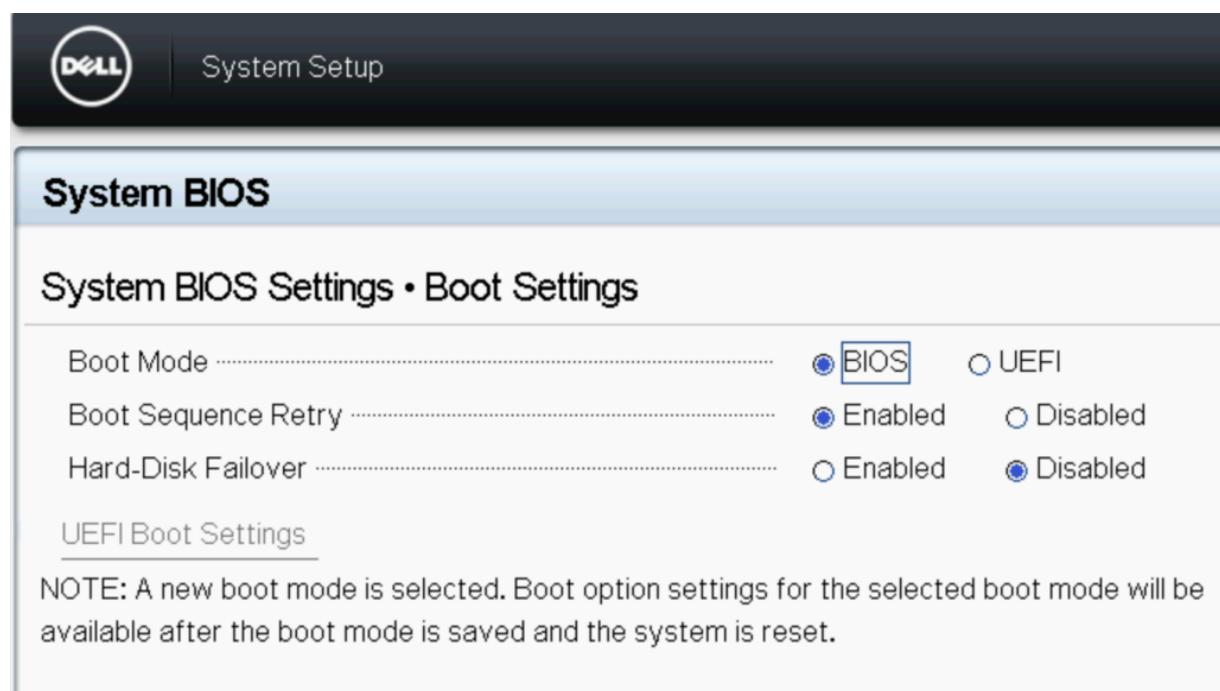
Figuur 3-4 iDRAC Media

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 3 TB in deze server met een RAID 5 level om geheugenverlies tegen te gaan. Door deze RAID configuratie blijft er een totaal van 5.5 TB 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 reden hiertoe is dat MBR enkel schijven tot 2 TB ondersteunt. Als je dus schijven gebruikt die groter zijn dan 2 TB, zal er dataopslag verloren gaan.

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



Figuur 3-5 Boot Mode

3.2 Netwerk

3.2.1 Firewall

De firewall zorgt voor de beveiliging van het netwerk door middel van access lists. Standaard zijn alle 65535 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.

Interconnect_ASA (10 incoming rules)						
1	<input checked="" type="checkbox"/> any	192.168.70.0/23	ip	✓ Permit	28	
2	<input checked="" type="checkbox"/> #Internal_Users	any	ip	✓ Permit	0	
3	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	#icmp	✓ Permit	0	
4	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	snmp	✓ Permit	0	
5	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_console	✓ Permit	3	
6	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	iDRAC_browser	✓ Permit	133	
7	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	Remote_Desktop	✓ Permit	1	
8	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	Citrix	✓ Permit	0	
9	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	SQL_TCP	✓ Permit	0	
10	<input checked="" type="checkbox"/> #VPN_Users	VLAN510_VLAN520_VLAN530_VLAN...	Citrix_udp	✓ Permit	0	
management (0 implicit incoming rules)						
Global (1 implicit rule)						
1	any	any	ip	✗ Deny		Implicit rule

Figuur 3-6 Access-Lists

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 tot 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.

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

Figuur 3-7 Static Routes

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

3.2.2 Switch

De switch in de demo omgeving, 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, pas je enkel de switchconfiguratie aan en hoeft je geen kabels meer 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.

```
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
```

Figuur 3-8 VLAN's

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 routering mogelijk te maken tussen de VLAN's op een layer 3 switch, zet je de routing aan.

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

Figuur 3-9 Routing

Om ervoor te zorgen dat de netwerkverbindingen een hoge beschikbaarheid hebben maak je gebruik 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.

```
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
```

Figuur 3-10 Port-Channels

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

```
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
```

Figuur 3-11 DMZ VLAN

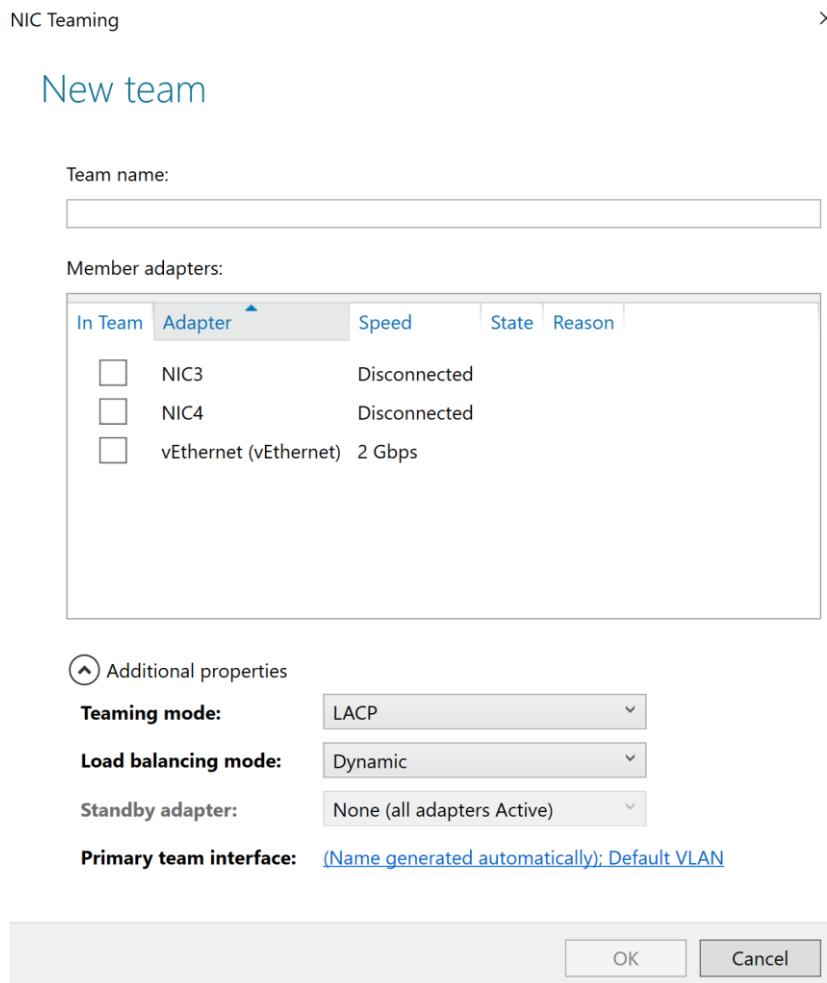
3.2.3 Servers

De netwerkconfiguratie van de servers is vrij eenvoudig. 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. Doe je dit niet, dan maakt de switch de port-channel niet aan en krijg je “errors”.

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)	192.168.66.2, 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

Figuur 3-12 NIC-Teaming

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.



Figuur 3-13 NIC-Teaming Config

3.3 Toepassingen

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

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		

Figuur 3-14 VM's Server1

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		

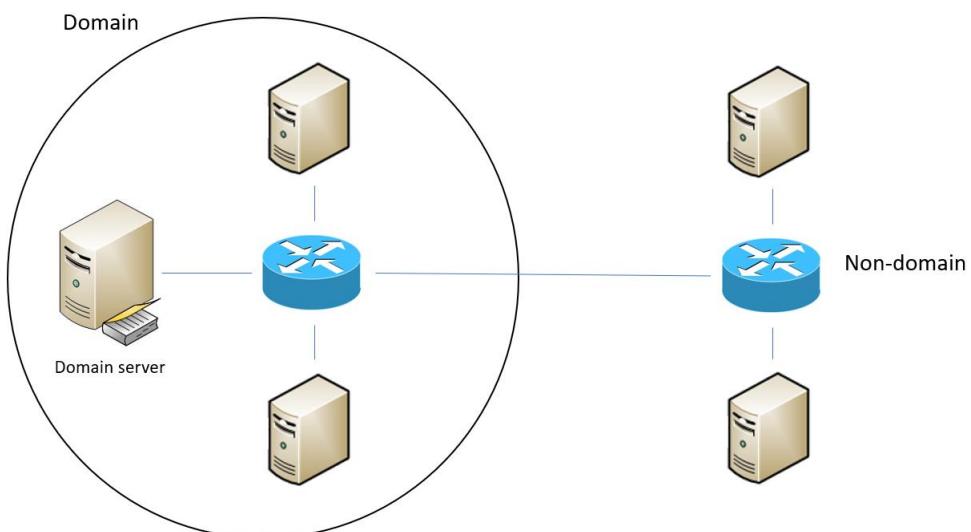
Figuur 3-15 VM's Server2

Virtual Machines						
Name	State	CPU Usage	Assigned Memory	Uptime	Status	
Azure_connect	Running	0%	1972 MB	4.18:52:36		
Backup	Running	0%	2284 MB	4.19:05:49		
Management	Running	0%	714 MB	4.19:28:17		
MFA_server	Off					
NPS	Off					
PS_1	Off					
SMTP	Running	0%	1732 MB	6.02:30:38		
WSUS	Running	0%	1886 MB	4.19:23:35		

Figuur 3-16 VM's Server3

3.3.1 Domaincontroller

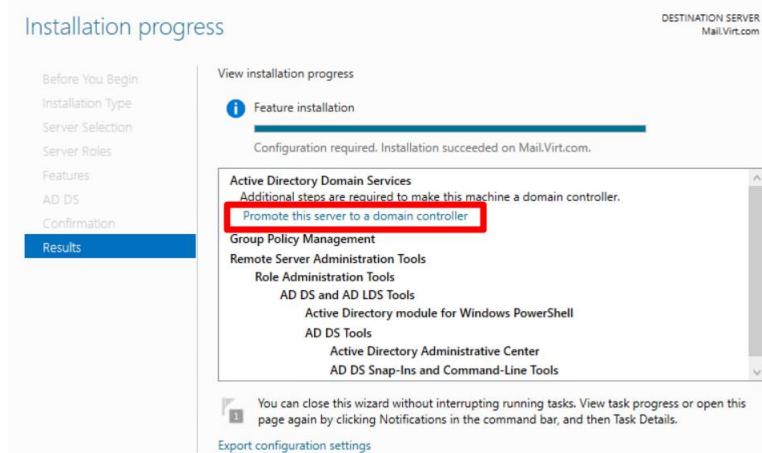
De domaincontroller beheert de rechten van alle users op het domein, wat handig is voor grote netwerken. Als je geen domaincontroller zou gebruiken, moet de administrator op iedere PC de rechten aanpassen.



Figuur 3-17 Domaincontroller

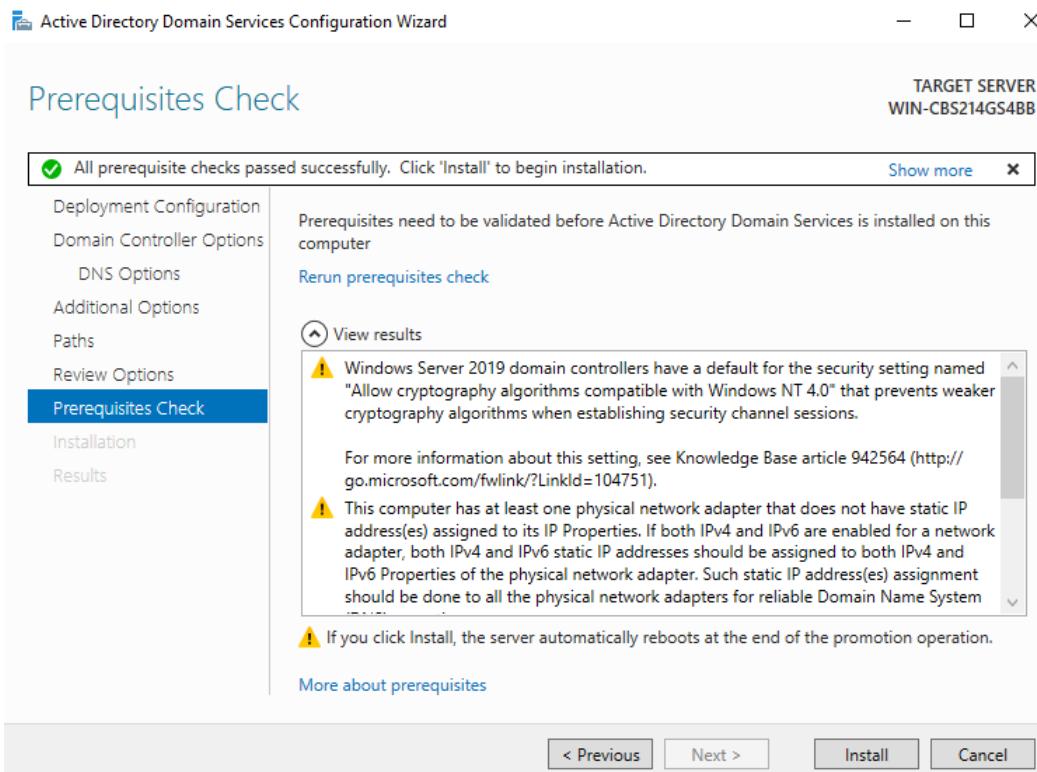
3.3.1.1 Installatie primary domaincontroller

DC_1 is de primaire domaincontroller en zal een nieuw domein moeten aanmaken. Dit installeer je via de server manager. De volgende stap na het installeren van de rol is de server promoten tot een domaincontroller.



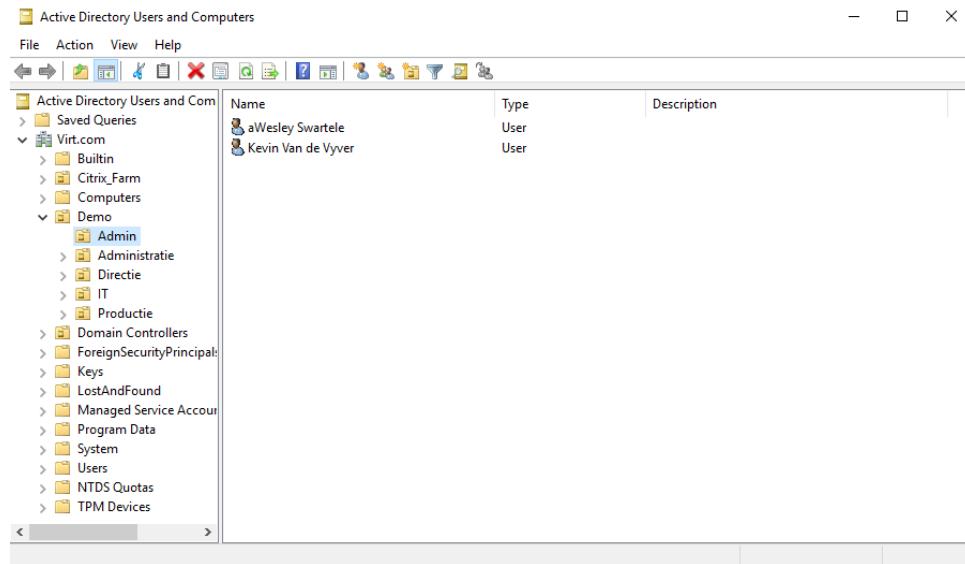
Figuur 3-18 Promote DC Role

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



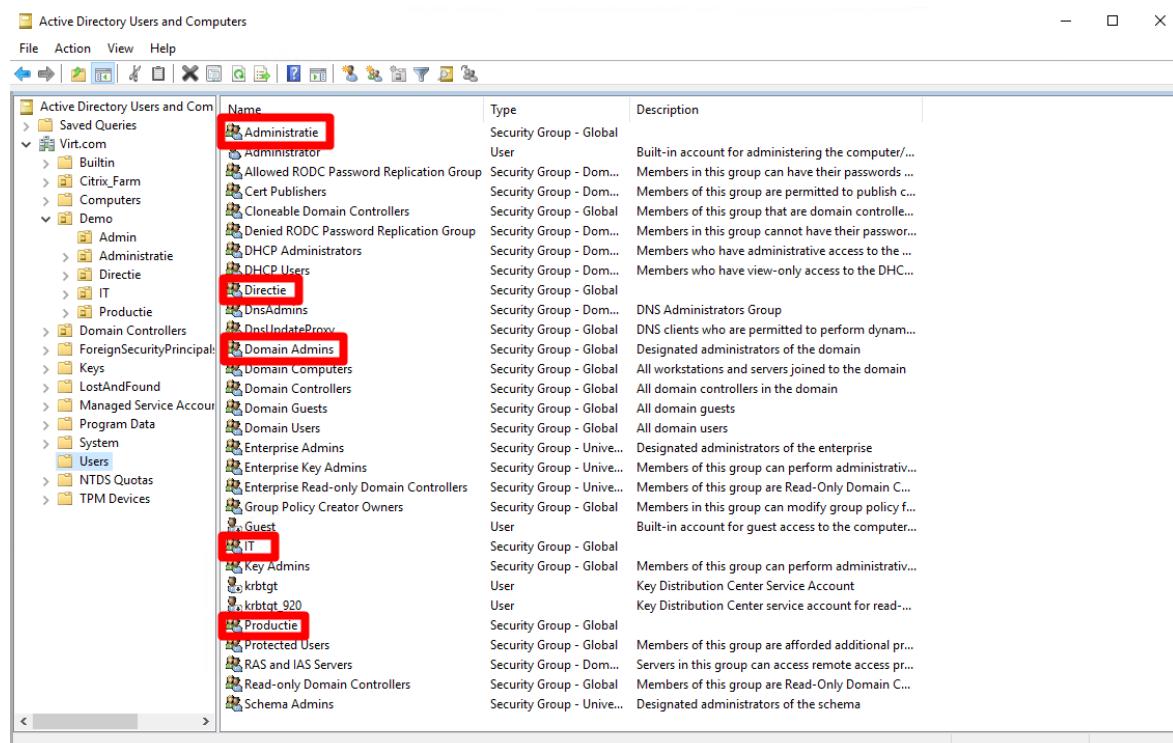
Figuur 3-19 DC Prerequisites Check

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



Figuur 3-20 AD-Structuur

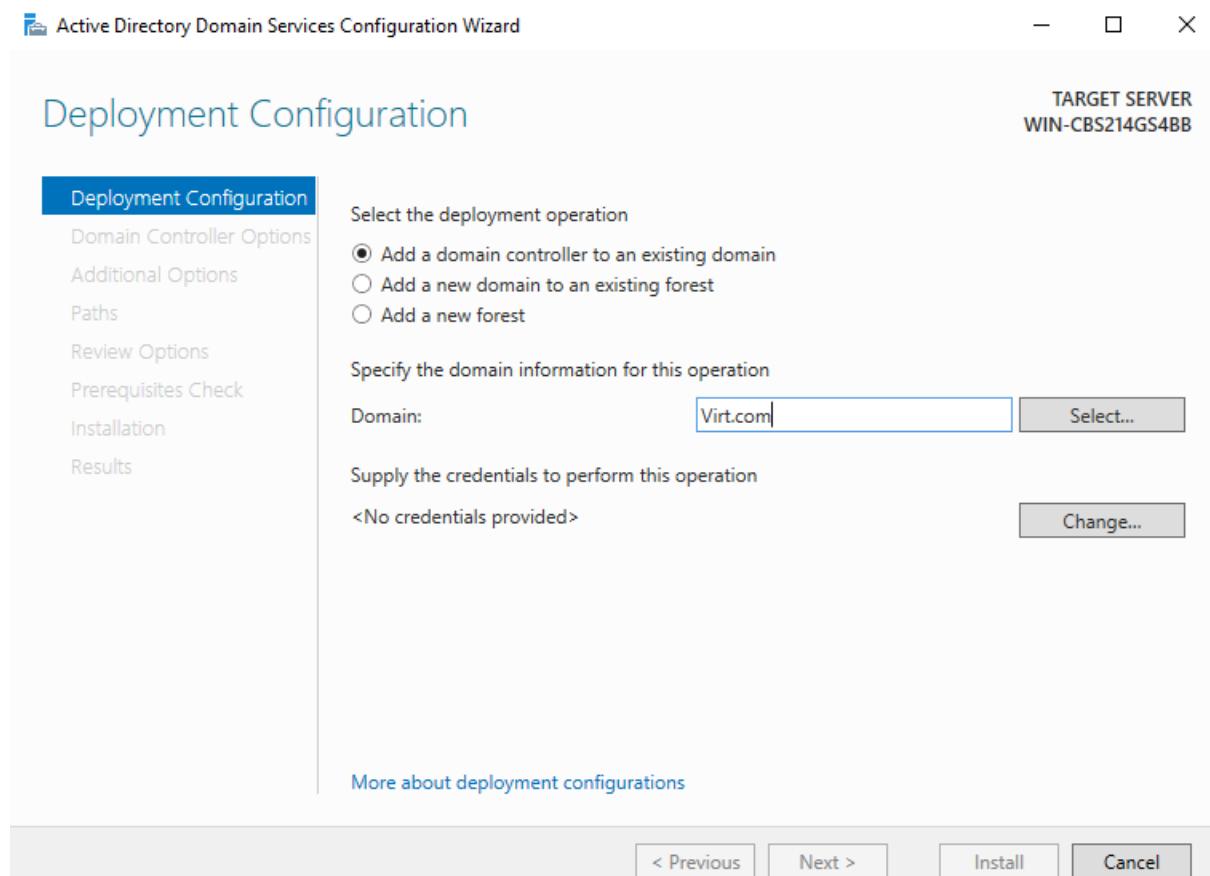
Voor elk departement is er een security groep aangemaakt. Alle gebruikers die tot die groep behoren voeg je hieraan toe. Deze groepen maken het mogelijk om de rechten van de gebruikers in te stellen op heel het domein. Dit is een veel efficiëntere en snellere manier dan dat je op elke computer individueel de rechten moet aanpassen.



Figuur 3-21 AD Security-Groups

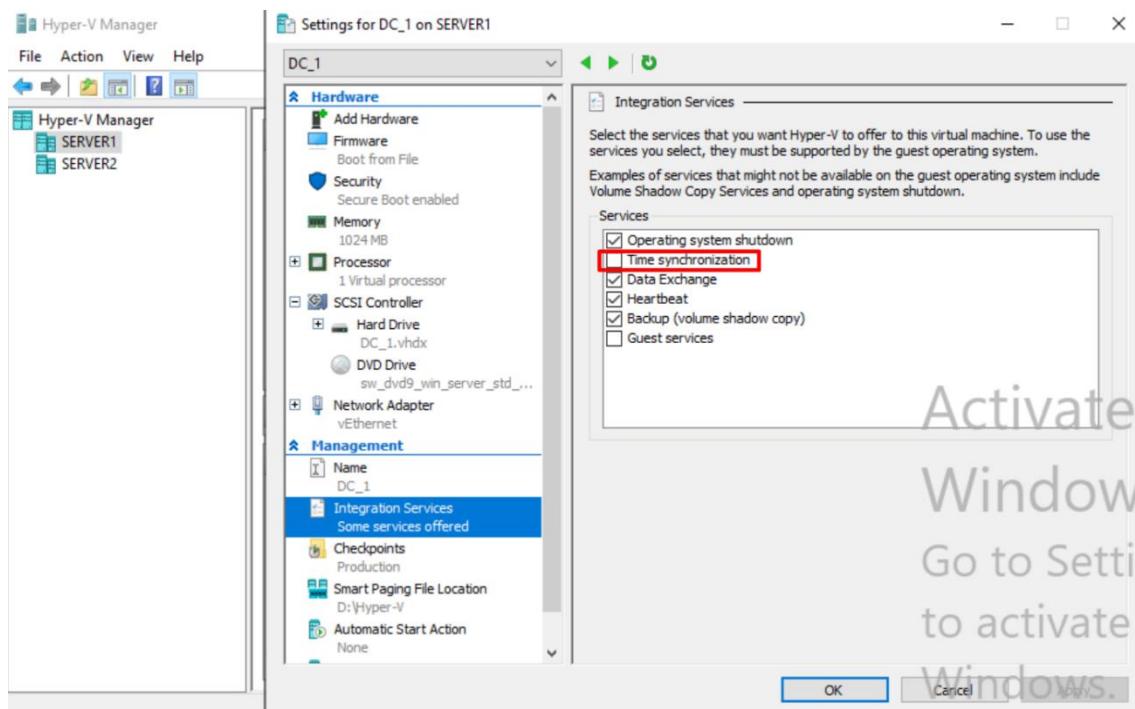
3.3.1.2 Installatie back-up domaincontroller

DC_2 is de back-up 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.



Figuur 3-22 Back-up DC

In een domein is het belangrijk dat je de tijd synchroniseert tussen alle VM's. Als dit niet het geval is, kunnen er problemen optreden. De synchronisatie stel je in met de w32tm service. Deze staat standaard geactiveerd in een windows server omgeving. Een belangrijke opmerking is dat als je de tijd synchroniseert 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.



Figuur 3-23 Time Integration Service

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

The command completed successfully.

C:\Users\kvdvyv>
```

Figuur 3-24 Tijdserver

Log nu in op de tijdserver en selecteer een externe tijdserver waarmee je wenst te 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\kvdvyv>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\kvdvyv>
```

Figuur 3-25 Delay

Om de externe tijdserver te gebruiken, moet je deze instellen in de w32tm config. Via volgend commando is dit mogelijk.

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

De laatste stap is de w32tm config updaten en synchroniseren.

```
w32tm /config /update
```

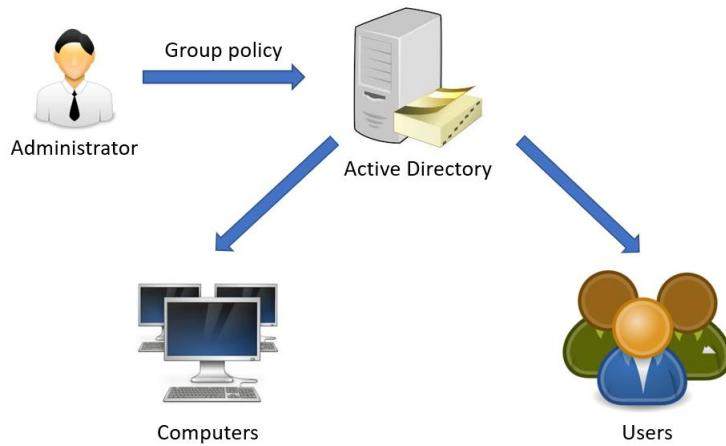
```
w32tm /resync
```

Tot slot moeten de clients nu de primary domaincontroller gebruiken als tijdserver. Soms gebeurt 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 beheert de administrator instellingen en configuraties van gebruikers en computers. 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.



Figuur 3-26 Group policies

3.3.2.1 Configuratie default browser

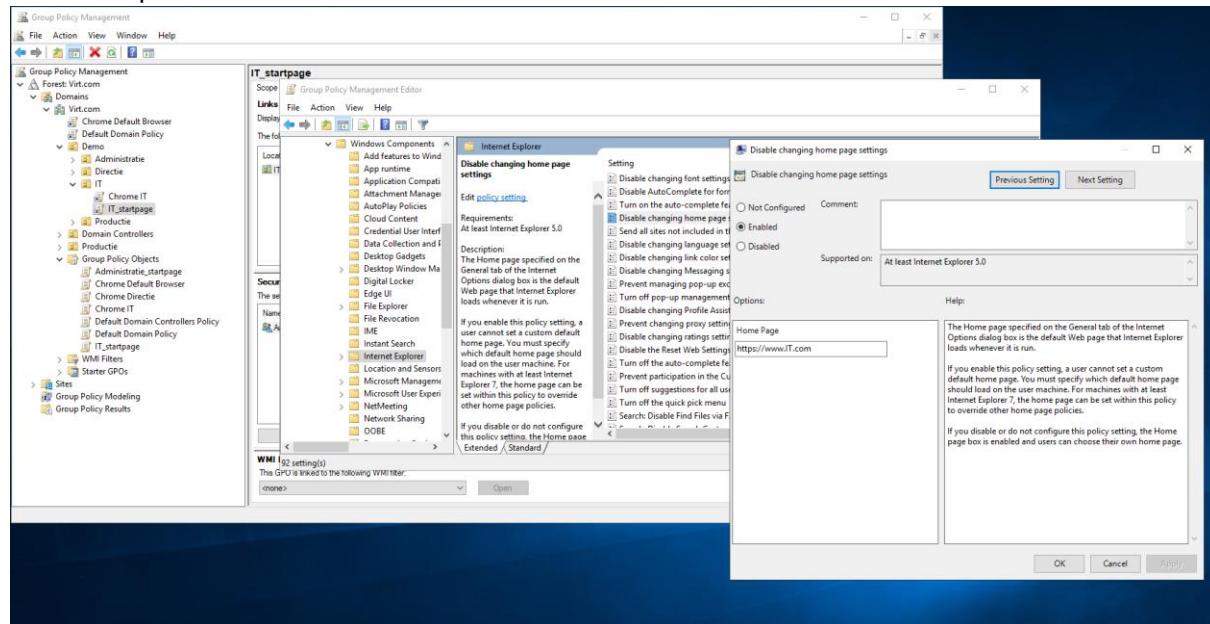
Om bijvoorbeeld chrome als default browser in te stellen voor bepaalde functies, download je een bestand van het internet of je kiest ervoor om er zelf één aan te maken. Enkele voorbeelden van deze functies zijn links of bestanden.

```
<?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

Met group policies pas je de startpagina van de browser aan. 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, omdat je daar een template voor moet downloaden.

Internet explorer:

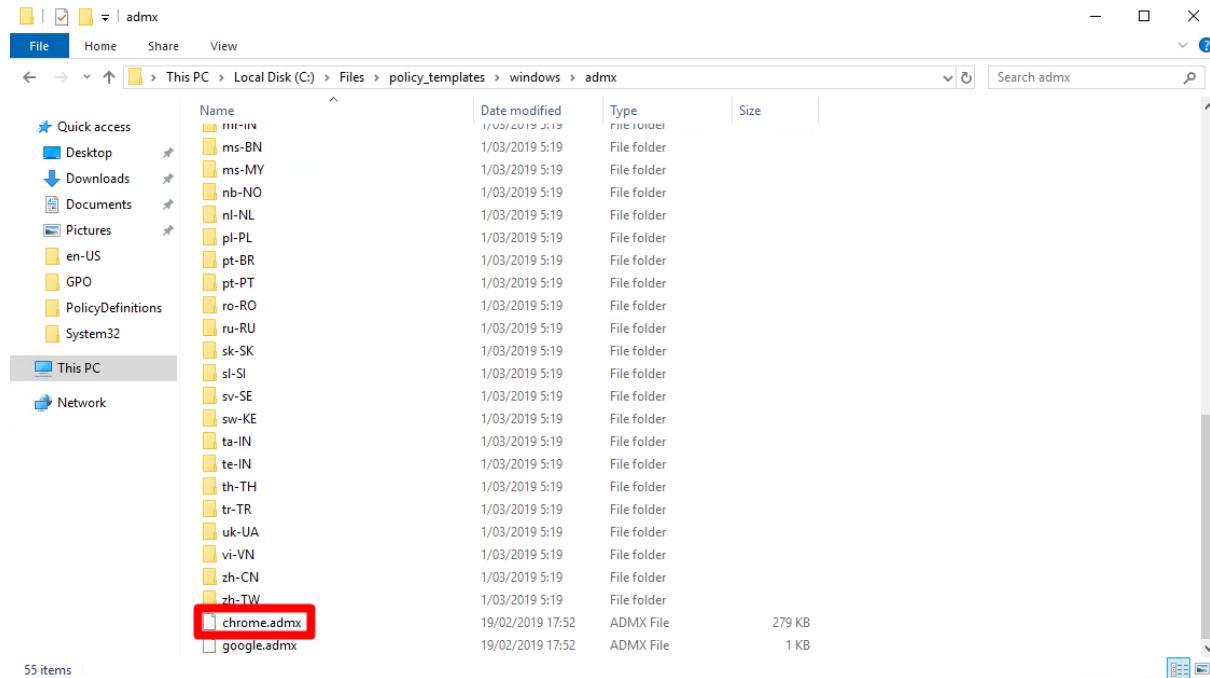


Figuur 3-27 Disable changing home page settings

De template die je nodig hebt voor chrome haal je op met deze URL:
http://dl.google.com/dl/edged/chrome/policy/policy_templates.zip

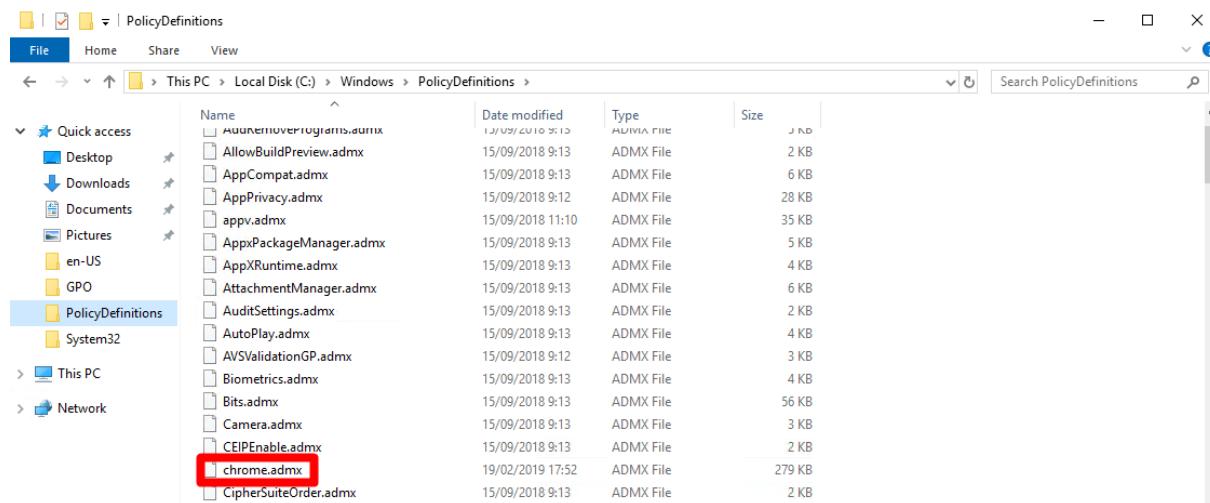
Na het downloaden, unzip je het bestand op de server en navigeer je naar de windows folder. Hier zie je 2 belangrijke folders, namelijk *adm* en *admx*

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



Figuur 3-28 chrome.admx

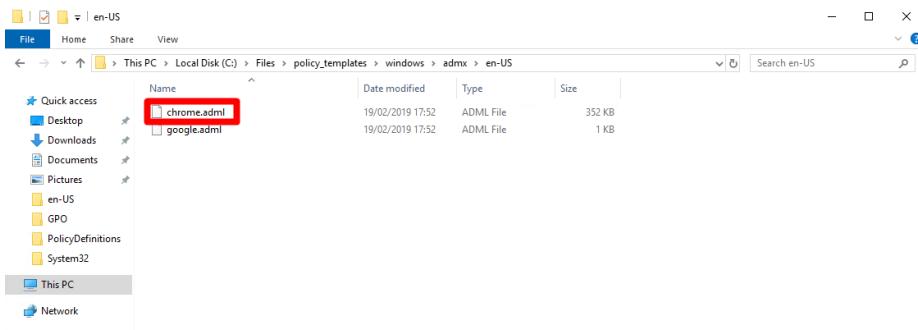
Open een nieuwe verkenner, navigeer naar C:\Windows\PolicyDefinitions en plak het bestand daar.



Figuur 3-29 PolicyDefinitions

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

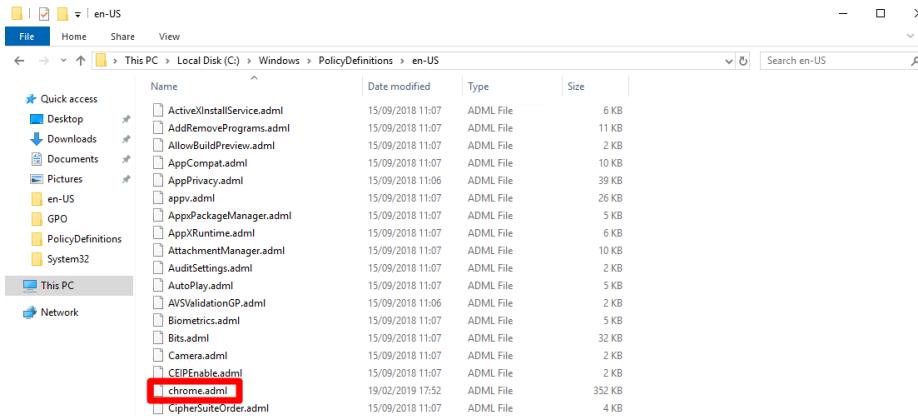
C:/Files/policy_templates/windows/admx/en-US



Figuur 3-30 chrome.adml

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

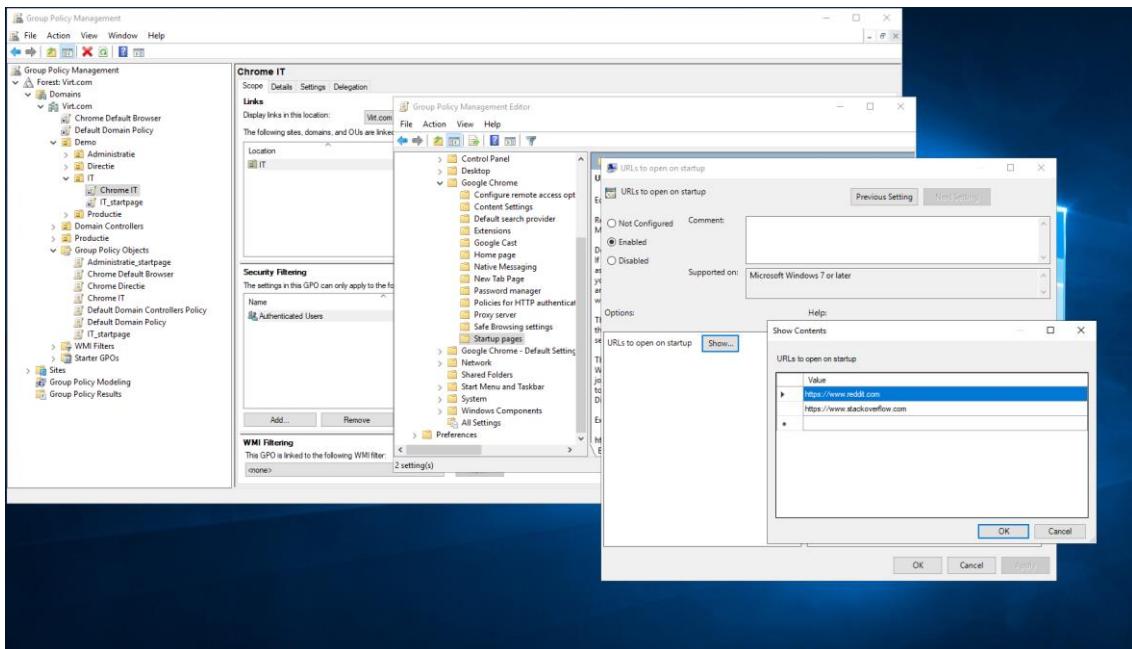
C:/Windows/PolicyDefinitions/en-US



Figuur 3-31 PolicyDefinitions taal folder

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:

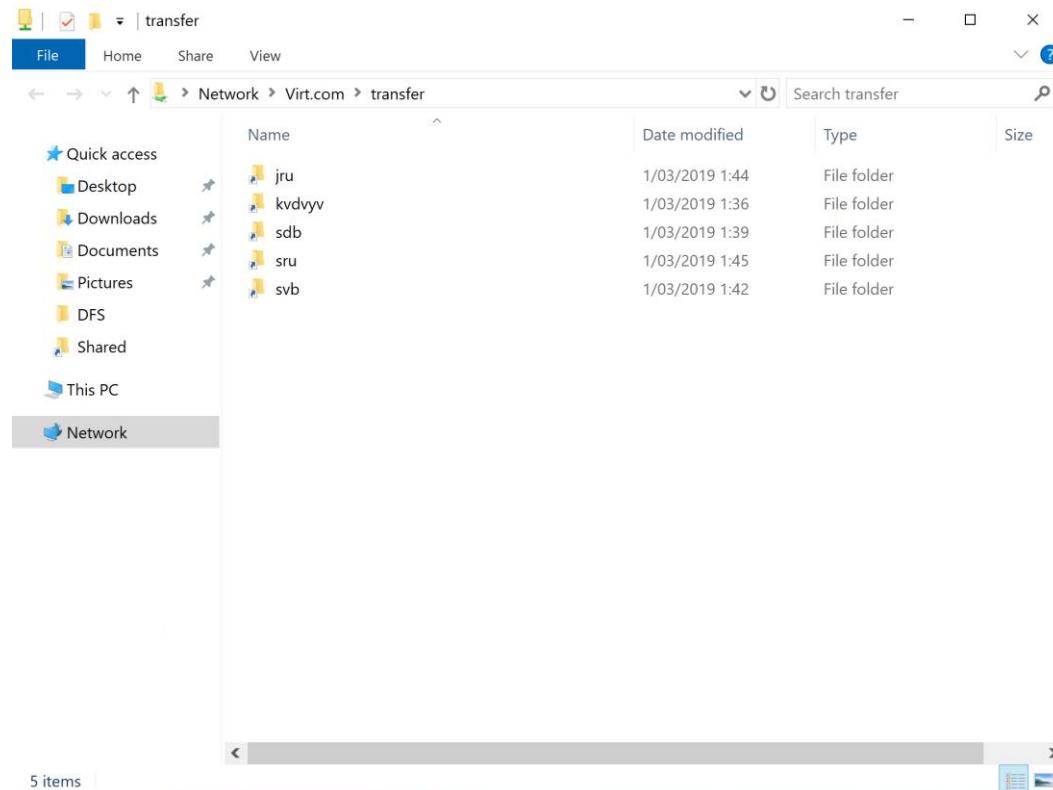


Figuur 3-32 URLs to open on startup

3.3.2.3 Configuratie drive mapping

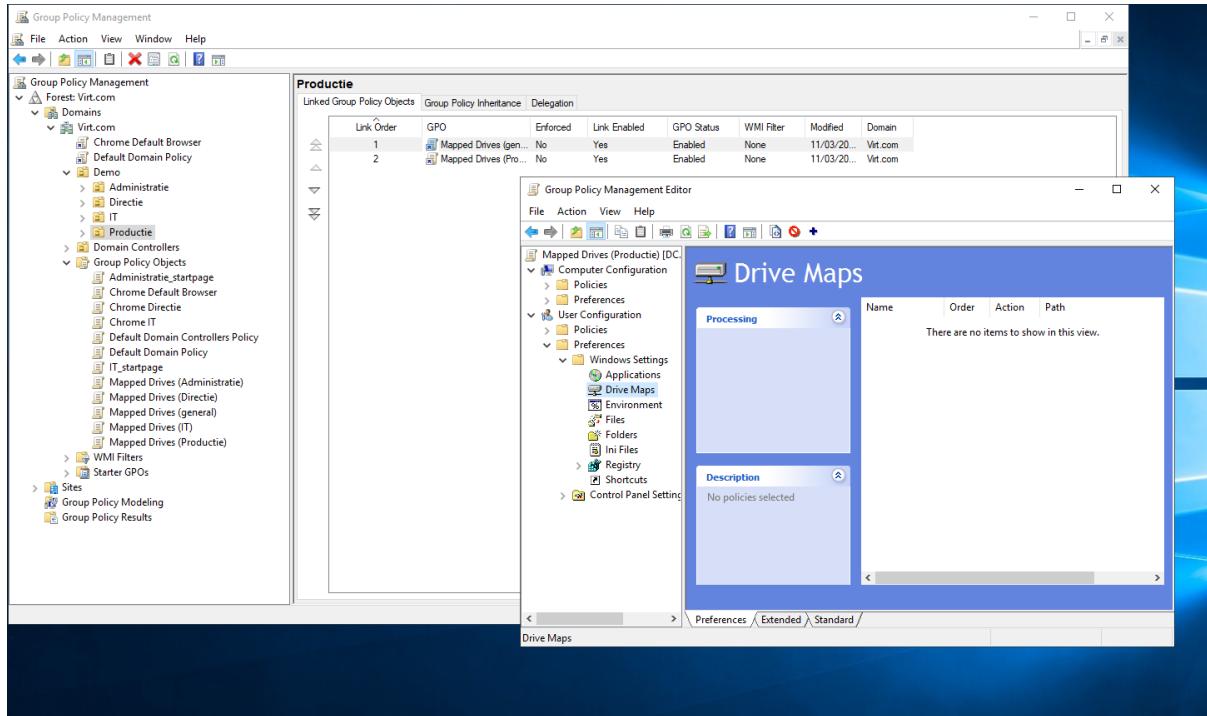
Een ander voordeel van group policies is drive mapping. Hiermee kan je bepaalde netwerkschijven zichtbaar maken voor gebruikers in een domein. Een opmerking hierbij is dat de mappen al beschikbaar waren voor de gebruikers als je het pad meegeeft, maar dit is niet echt evident.

\\\virt.com\transfer



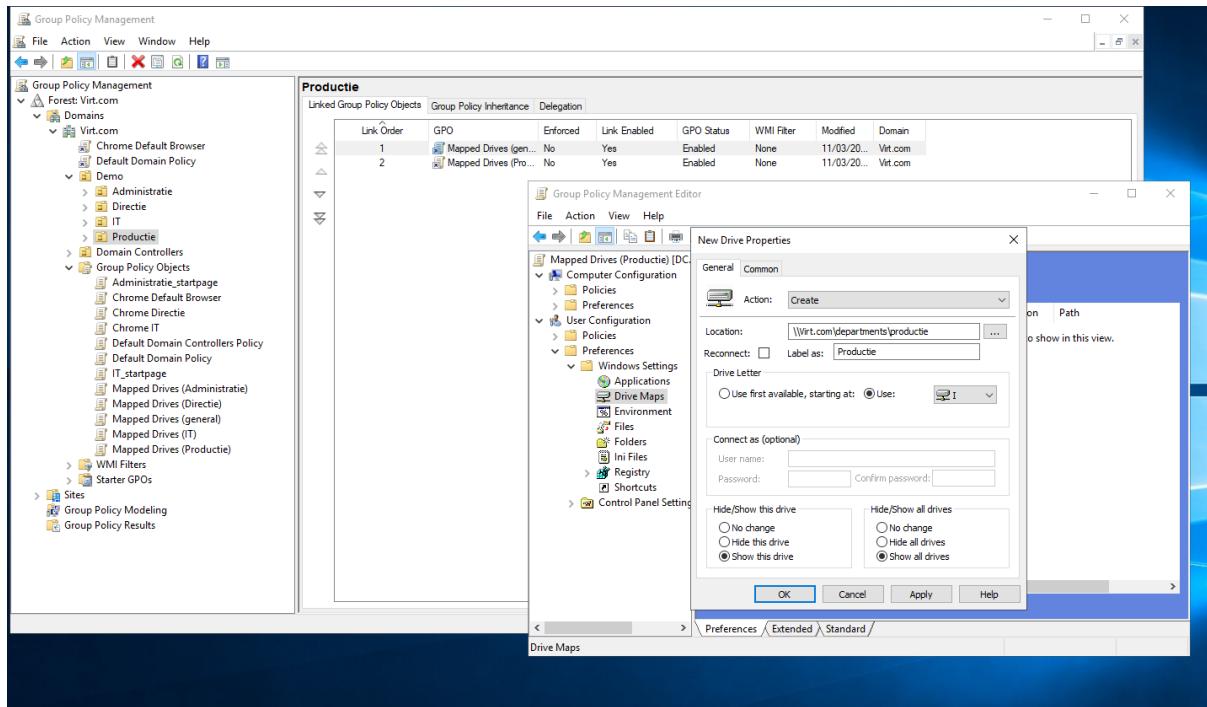
Figuur 3-33 Transferfolder

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.



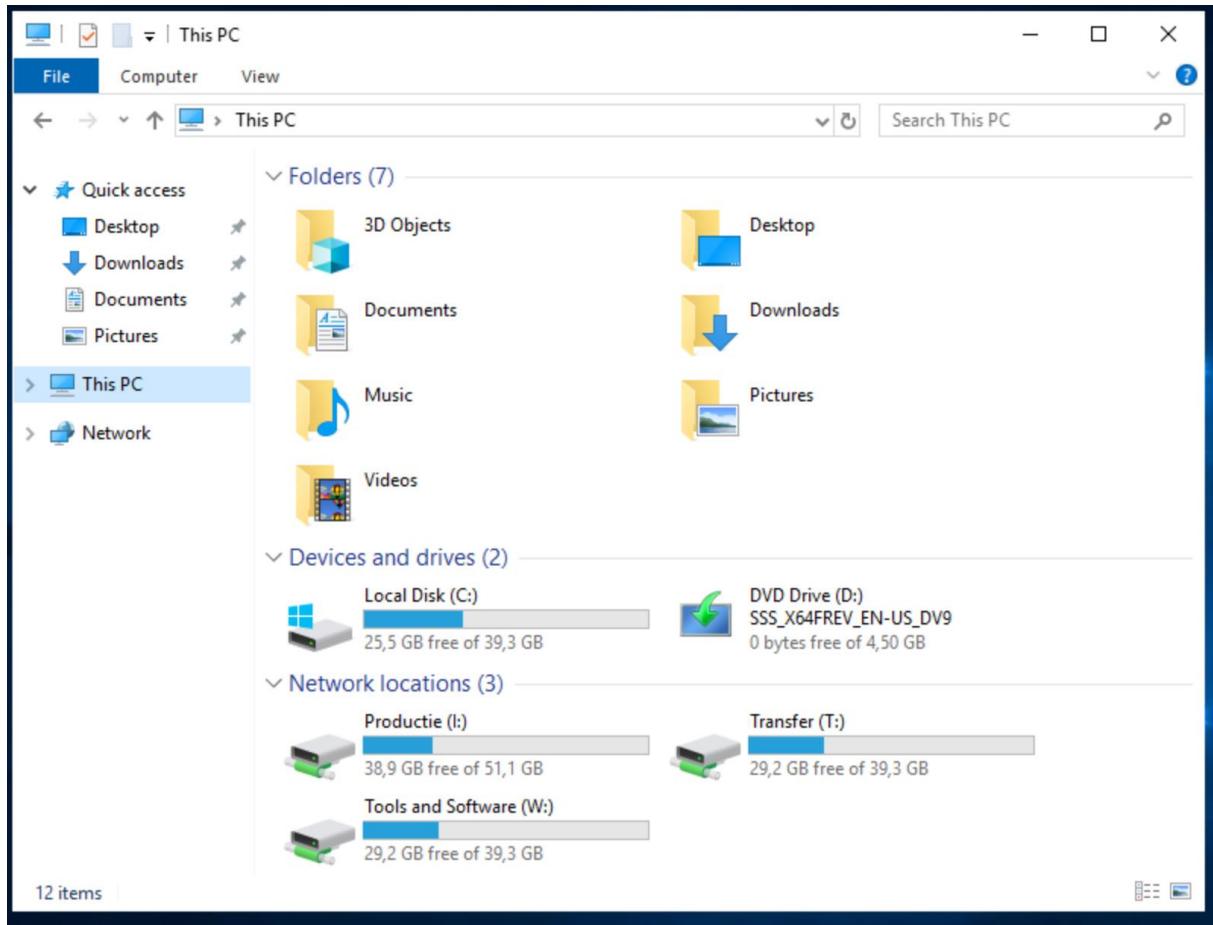
Figuur 3-34 Drive Maps GPO

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



Figuur 3-35 Drive Maps Config

Na het aanmaken van deze group policy kan het departement *Productie* gemakkelijk toegang krijgen tot deze schijf. Hieronder vind je een resultaat van het departement.



Figuur 3-36 Drive Maps Result

3.3.3 DNS

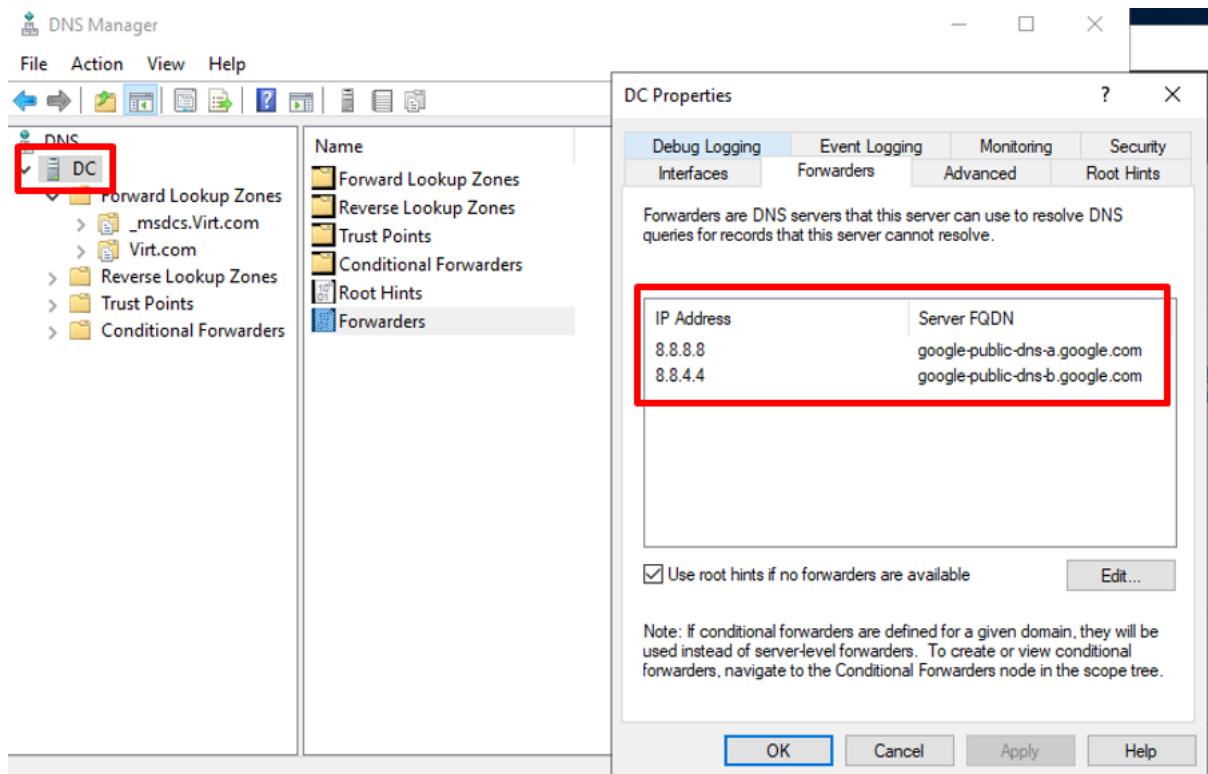
Domain Name System, afgekort DNS maakt het mogelijk om op het internet te zoeken naar adresnamen in plaats van enkel IP-adressen. In de demo omgeving is de DNS toepassing samengenomen met de domaincontroller.

3.3.3.1 Installatie DNS

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

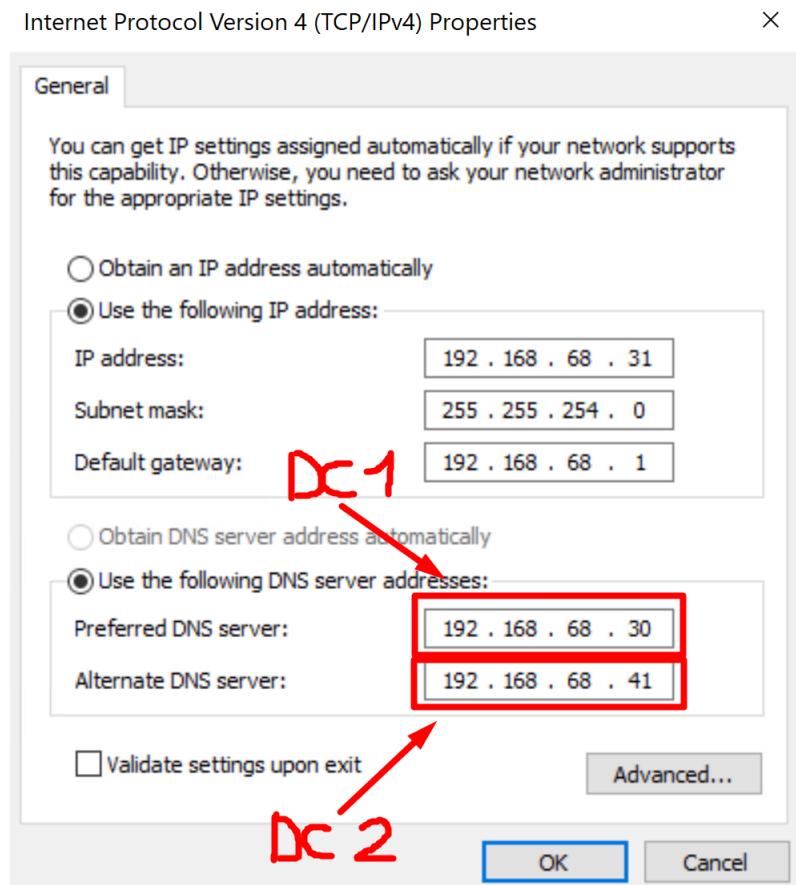
- OpenDNS,
- Cloudflare,
- Google Public DNS,
- Norton ConnectSafe,
- Comodo Secure DNS,
- Quad9,
- Verisign DNS.

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



Figuur 3-37 DNS Forwarders

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



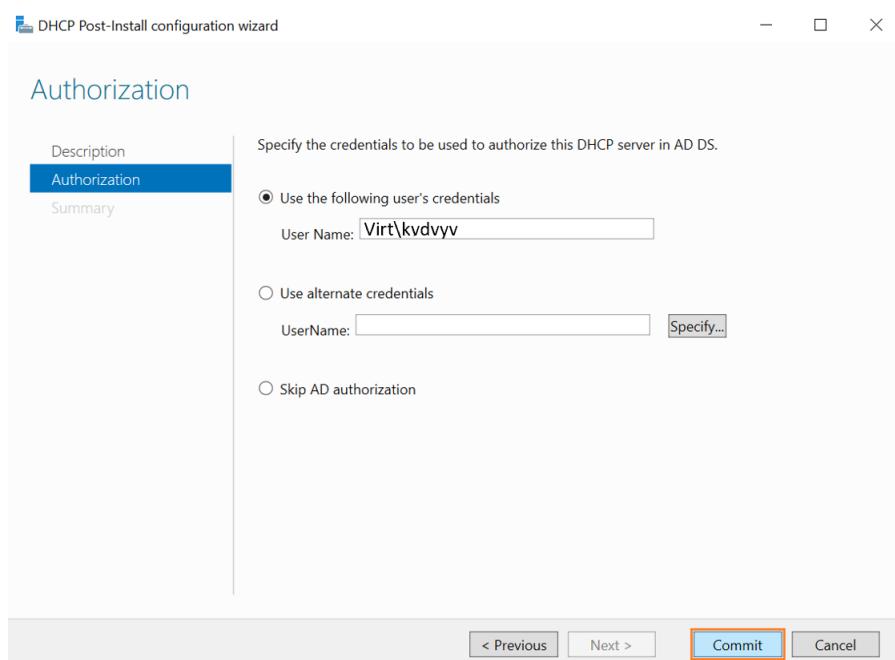
Figuur 3-38 DNS Servers

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.

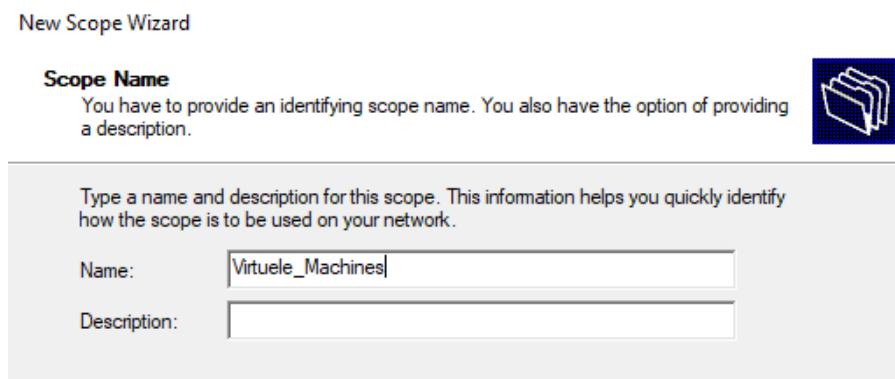
3.3.4.1 Installatie DHCP

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



Figuur 3-39 Autorisatie

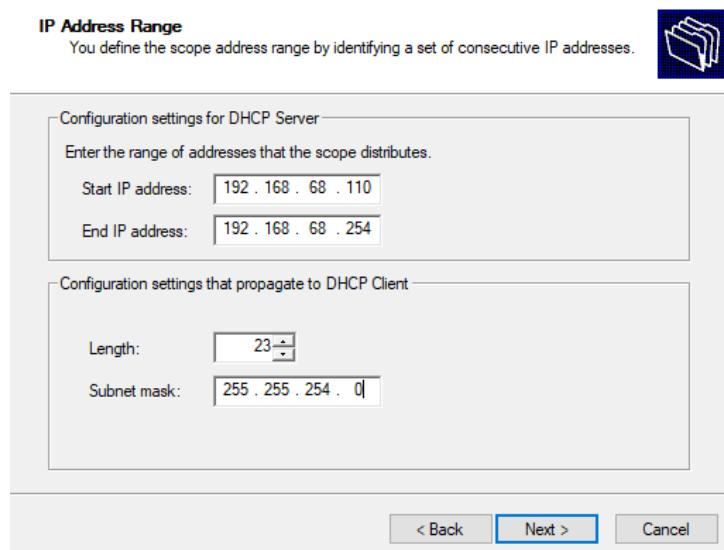
Open nu de DHCP applicatie op de server en maak een nieuwe scope aan, geef deze een naam en eventueel een beschrijving.



Figuur 3-40 Scope Name

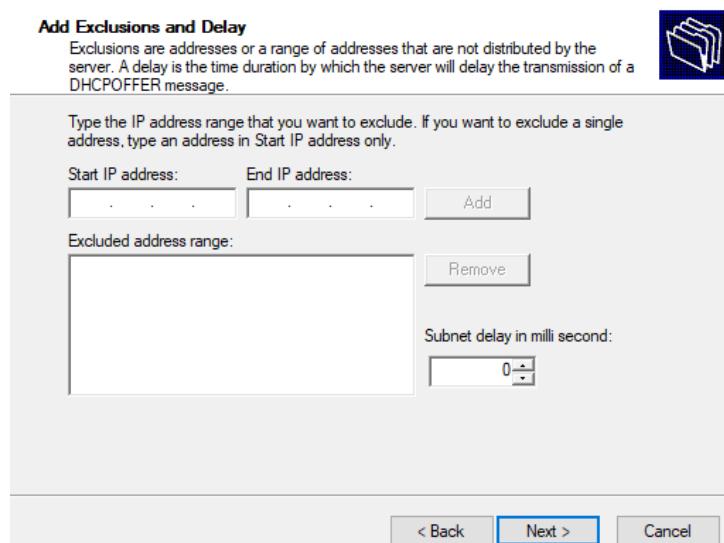
De volgende stap is de range instellen van de beschikbare IP-adressen, uitgesloten adressen kan je hierna nog instellen.

New Scope Wizard



Figuur 3-41 IP-range

New Scope Wizard



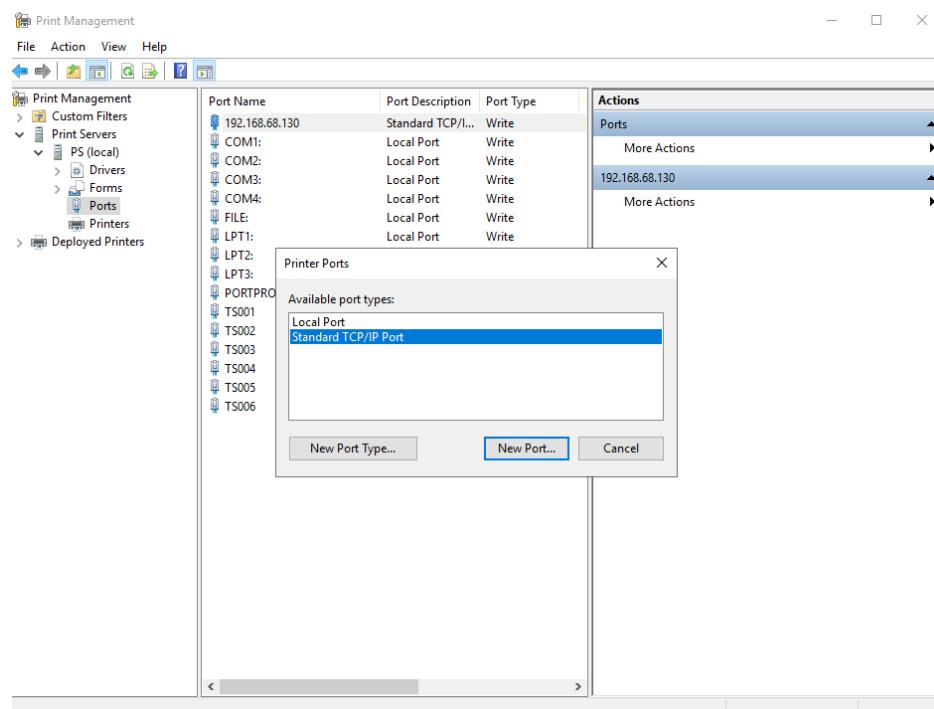
Figuur 3-42 IP-Exclusions

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

Een printer is één van de meest gebruikte apparaten in een bedrijf en 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.



Figuur 3-43 Add Port

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

Add Standard TCP/IP Printer Port Wizard

Add port

For which device do you want to add a port?



Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address:

Port Name:

< Back

Next >

Cancel

Figuur 3-44 printer IP

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

Additional port information required

The device could not be identified.



The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

Standard

Generic Network Card

Custom

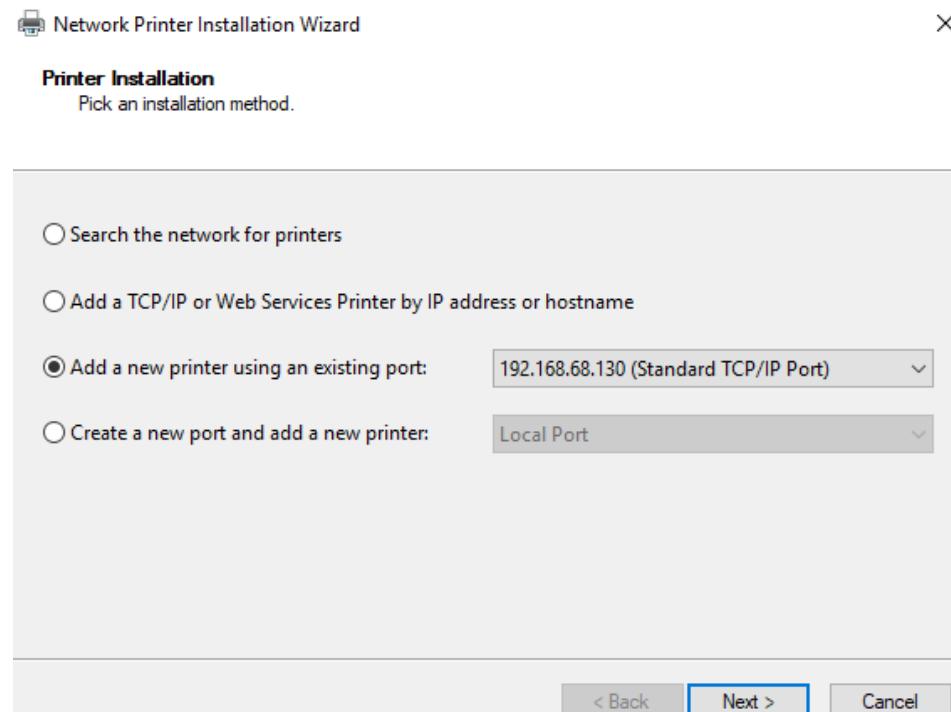
< Back

Next >

Cancel

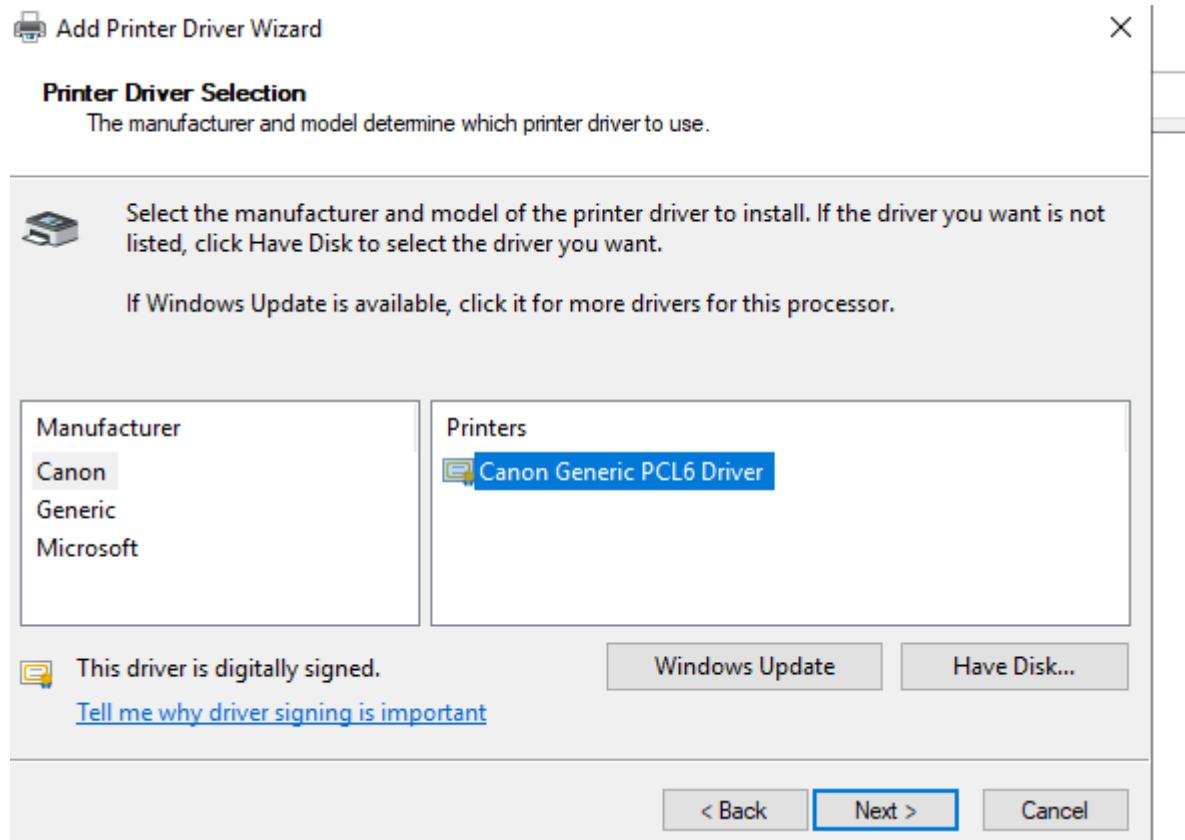
Figuur 3-45 Device Type

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.



Figuur 3-46 Add Printer

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.

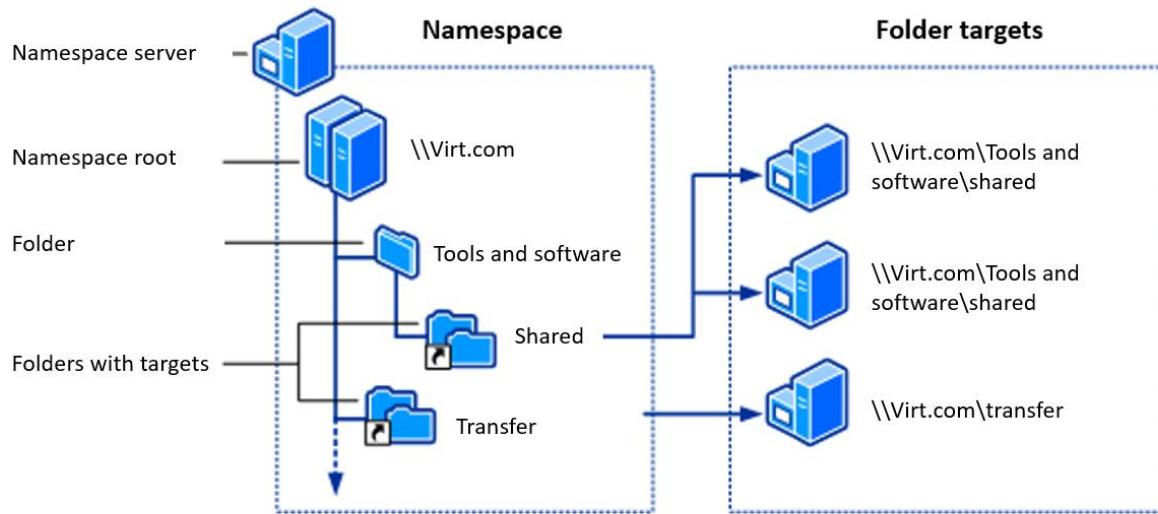


Figuur 3-47 Select Driver

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 uit te wisselen tussen gebruikers.



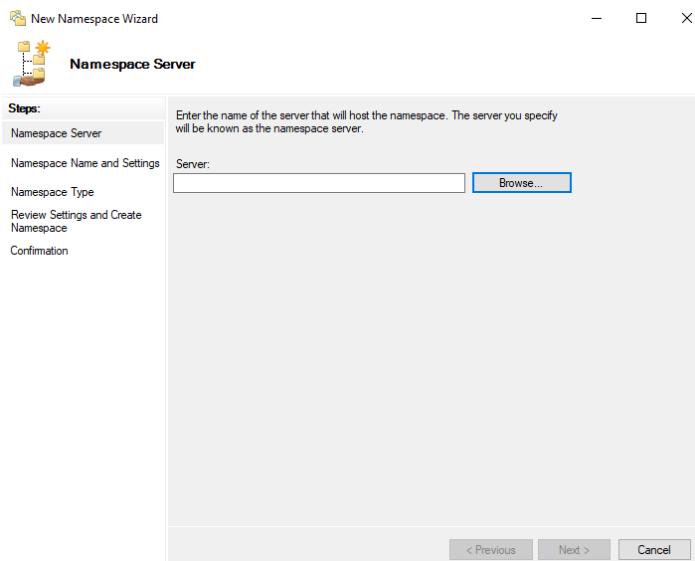
Figuur 3-48 Fileserver

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 worden weggezet. De servers die hiervoor worden gebruikt in het domein zijn:

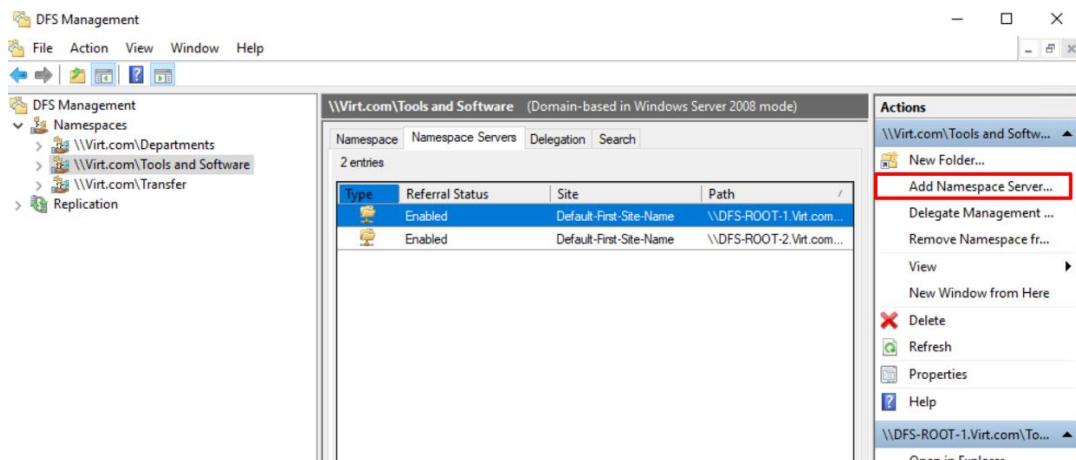
- DFSROOT_1,
- DFSROOT_2,
- FS_1,
- FS_2.

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.



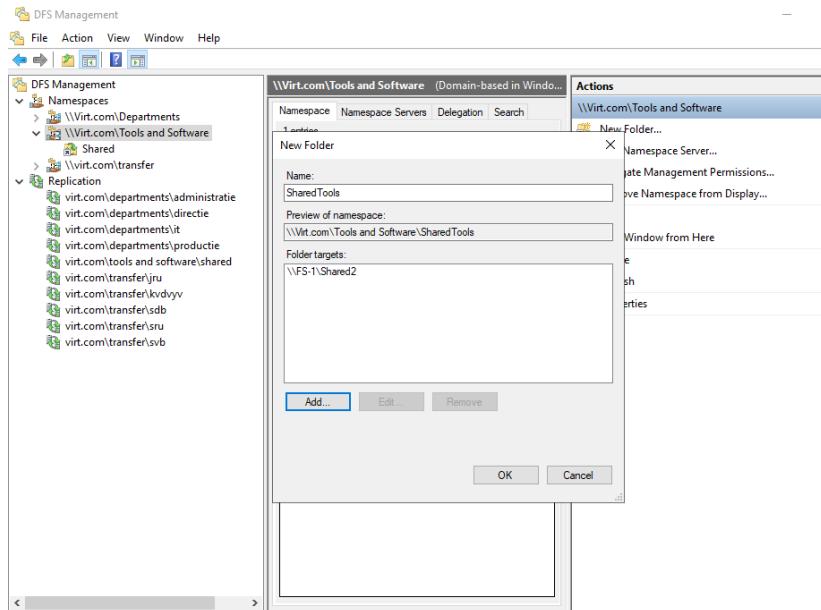
Figuur 3-49 New Namespace

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.



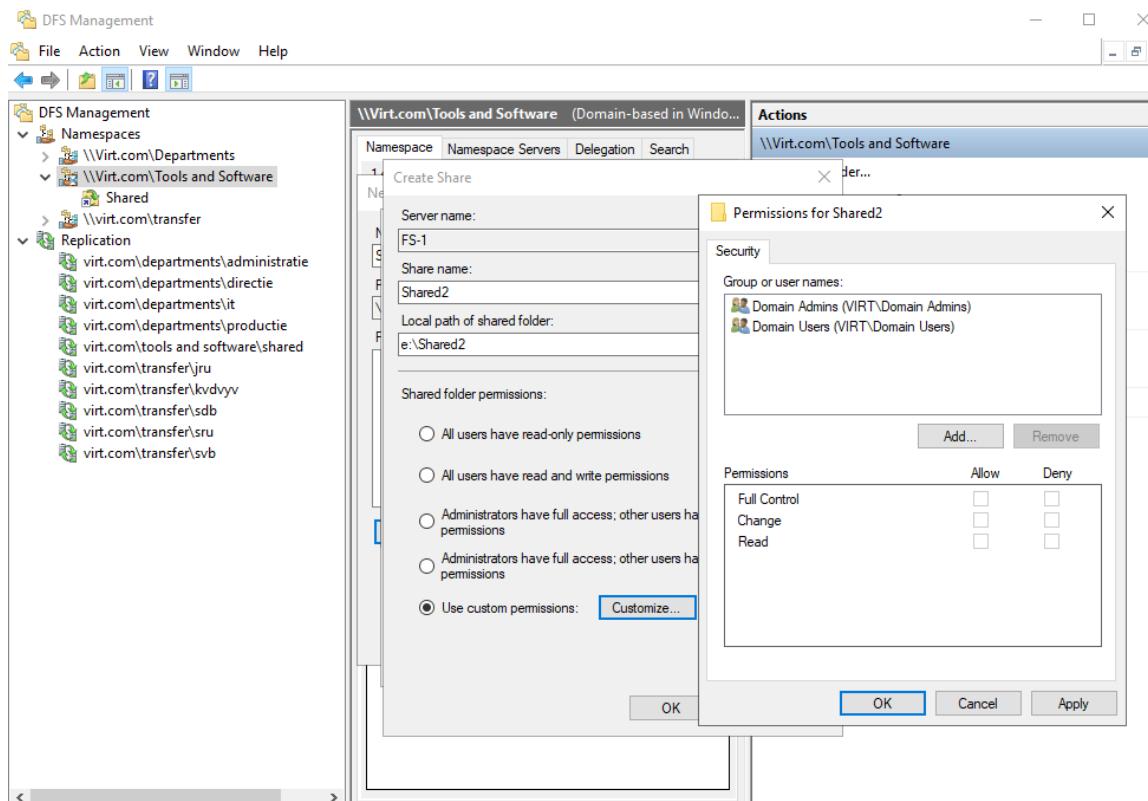
Figuur 3-50 Add Namespace Server

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).



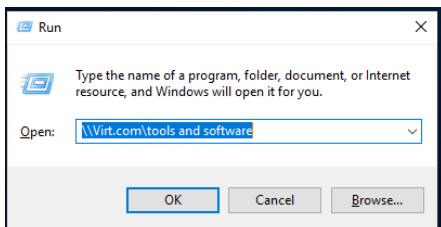
Figuur 3-51 New Shared Folder

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, ...

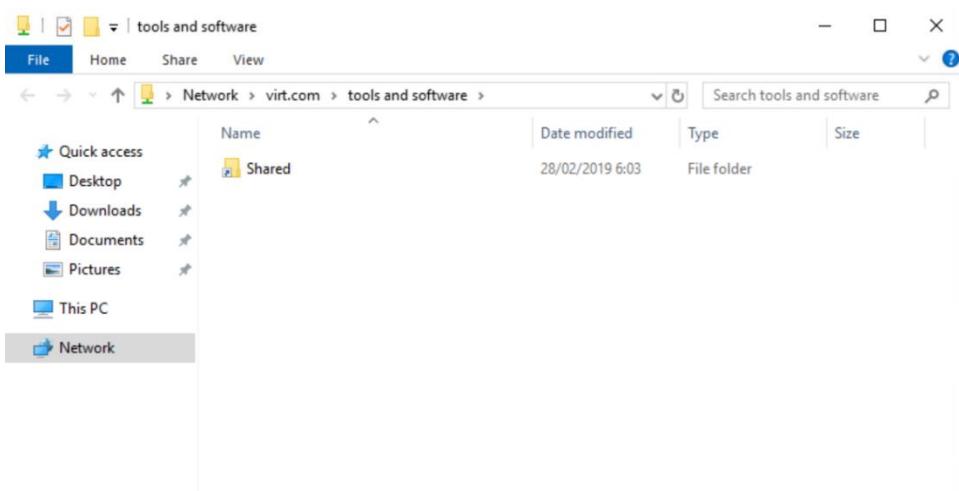


Figuur 3-52 Folder Permissions

Het is aan te raden 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.

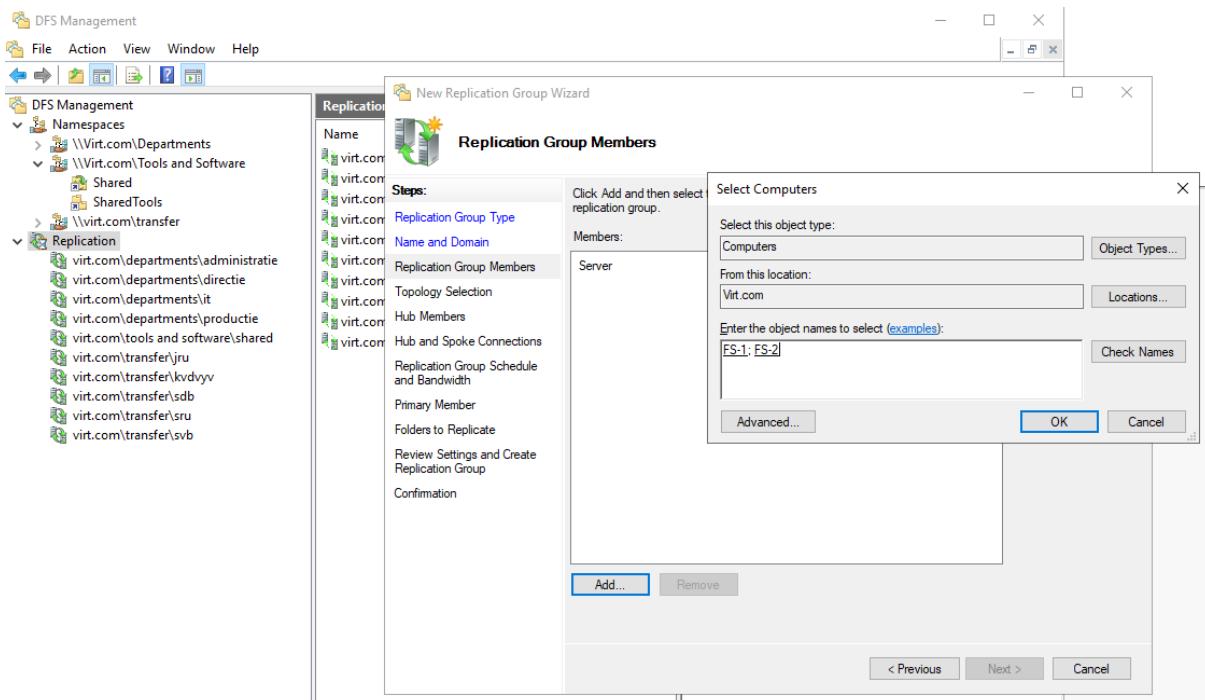


Figuur 3-53 Fileserver Path



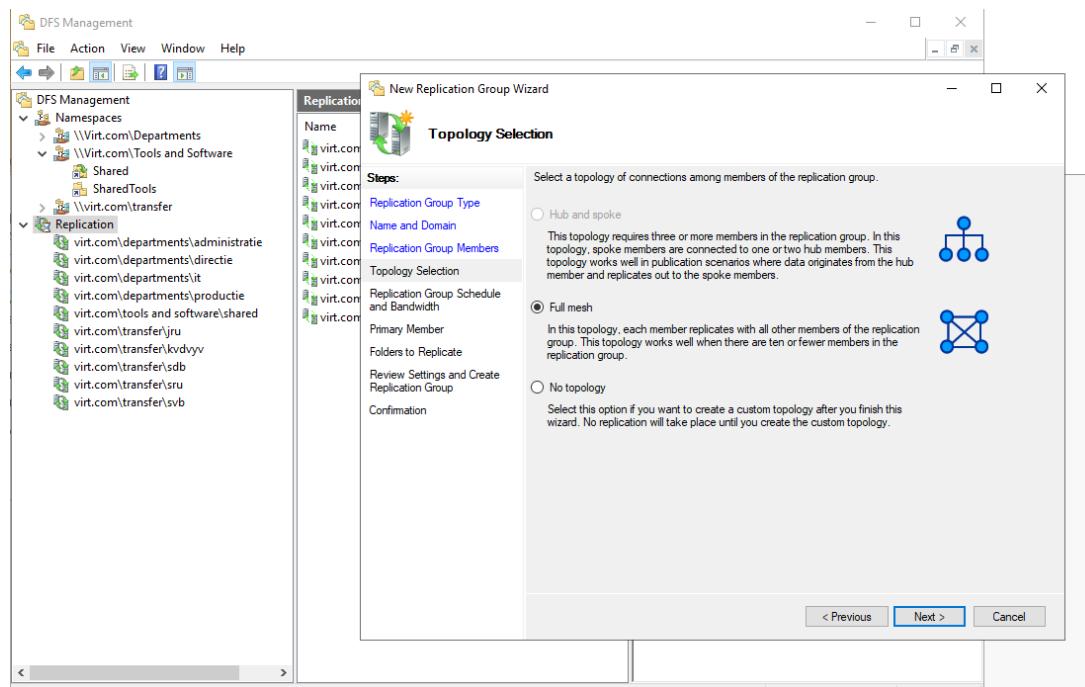
Figuur 3-54 Fileserver Folder

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).



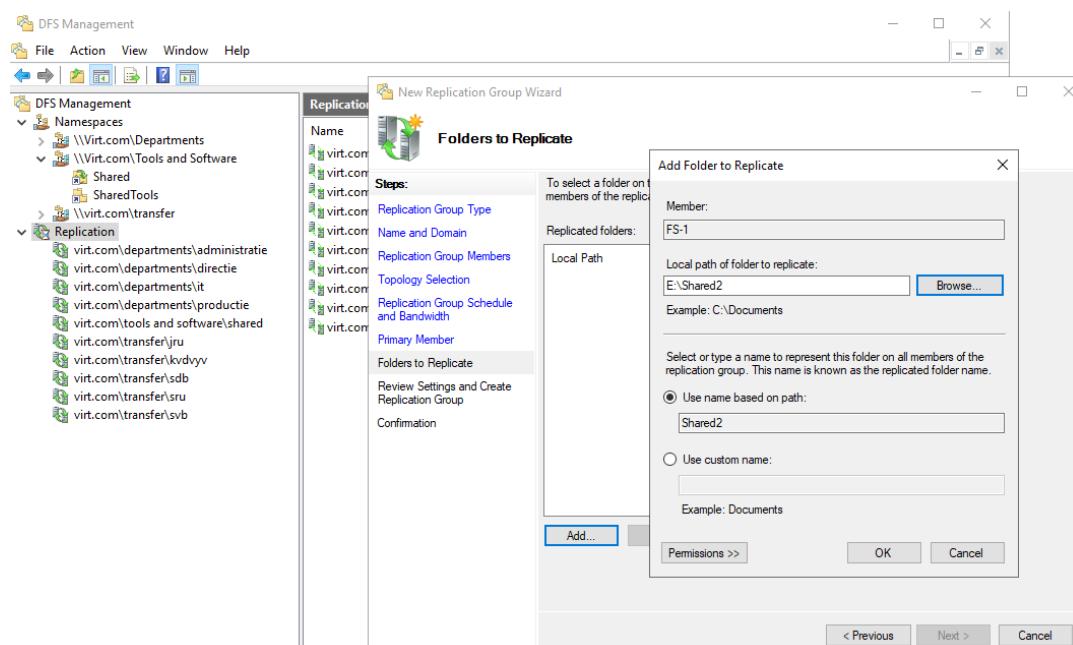
Figuur 3-55 New Replication Group

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



Figuur 3-56 Replication Topology

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.



Figuur 3-57 Folders To Replicate

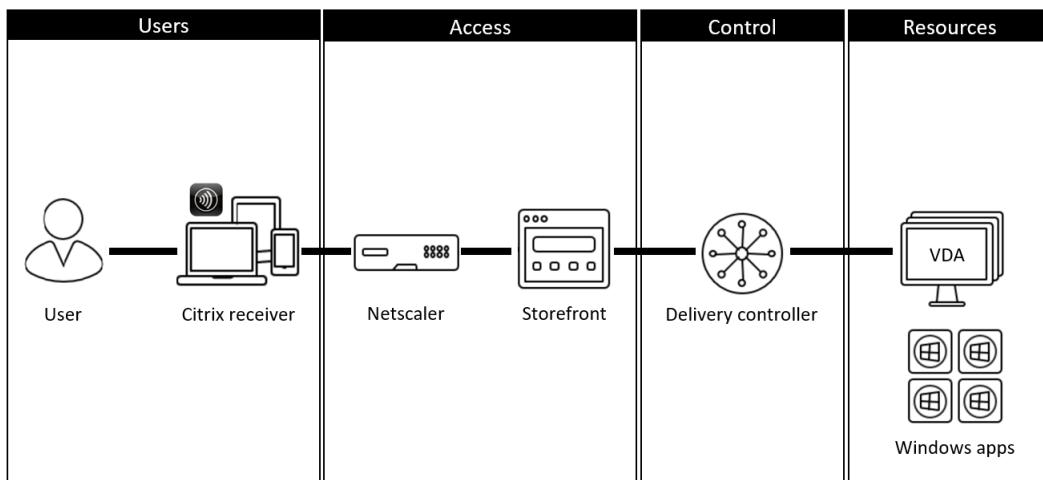
3.3.7 Citrix

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 (werknelmers 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:

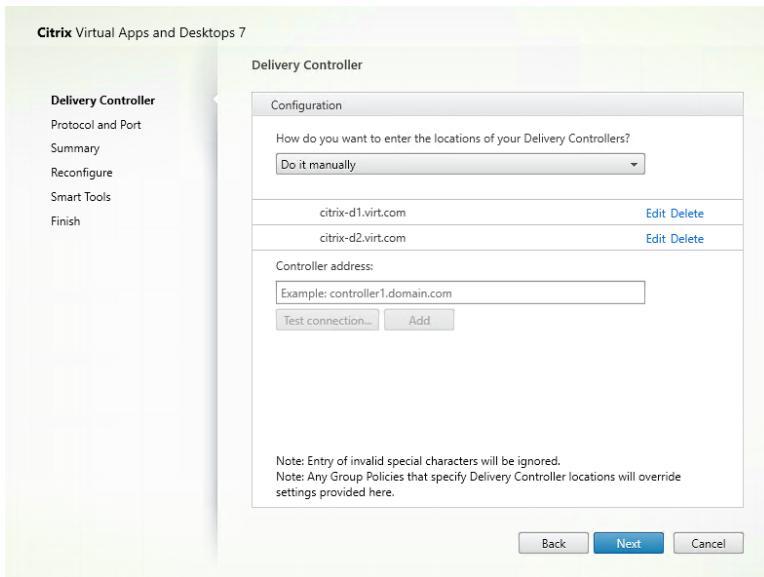
- Bredere ondersteuning van systemen (Windows, Linux, HTML5 Chromebooks),
- NetScaler (extern bereikbaar maken van citrix apps, ...),
- Eenvoudiger beheer- en monitoringmogelijkheden,
- Beter beeldbeheer en brede hypervisor / cloud-ondersteuning + Prestatie-optimalisatie.



Figuur 3-58 Citrix

3.3.7.1 Configuratie VDA

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.



Figuur 3-59 Specifieer Delivery Controller

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

3.3.7.2 Configuratie Delivery controllers

De *delivery controllers* publiceren de applicaties van de VDA's naar een StoreFront. Gebruikers zullen deze StoreFront gebruiken om toegang te krijgen tot de applicaties en deze op te starten. Als eerste stap maak je een machine catalog aan. Deze catalog bevat de servers waar de applicaties opstaan (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 bar with the Citrix logo and some status information. Below this is a table with columns: Machine Catalog, Machine type, No. of machines, and Allocated machines. The table shows one entry for 'Windows Server 2019' with 'Server OS' as the type, 2 machines listed, and 2 allocated machines. Below the table is a large, empty white area representing the catalog view. A second screenshot below it shows a 'Details - Windows Server 2019' page with tabs for Details, Machines, and Administrators. The Machines tab is selected, showing two entries: 'VIRT\CTRIX-VDA1' and 'VIRT\CTRIX-VDA2'. This second window is highlighted with a red border.

Figuur 3-60 Machine Catalog

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. Op deze manier kan je eventueel apps enkel beschikbaar maken voor interne gebruikers terwijl de externe gebruikers deze niet zien staan.

The screenshot shows the 'Add Applications' dialog from Citrix Studio. On the left, there is a navigation pane with 'Studio' selected, and sections for 'Introduction', 'Applications', and 'Summary'. The main area is titled 'Add Applications from Start Menu' and contains a list of discovered applications. A scrollable list box shows items like '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 are 'OK', 'Cancel', 'Back', 'Next', and 'Cancel' buttons. To the right of the dialog, there is a decorative graphic of three overlapping circles.

Figuur 3-61 Applications

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 Receiver for Web Sites

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

Figuur 3-62 *StoreFront* Servers

Omdat er in de demo-omgeving 2 servers geconfigureerd zijn 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

Figuur 3-63 *StoreFront* URL

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

citrix.virt.com

Used by # Delivery Groups
1

Edit StoreFront Server

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

StoreFront server name:
citrix.virt.com

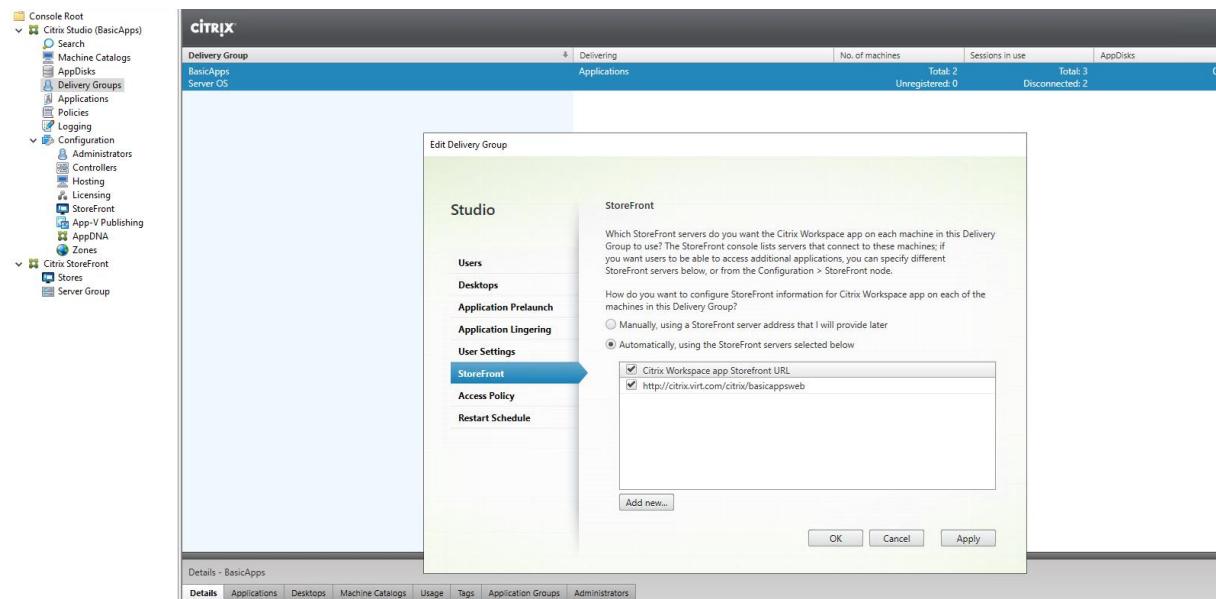
Description:
StoreFront BasicApps

URL:
http://citrix.virt.com/citrix/basicappsweb

OK Cancel

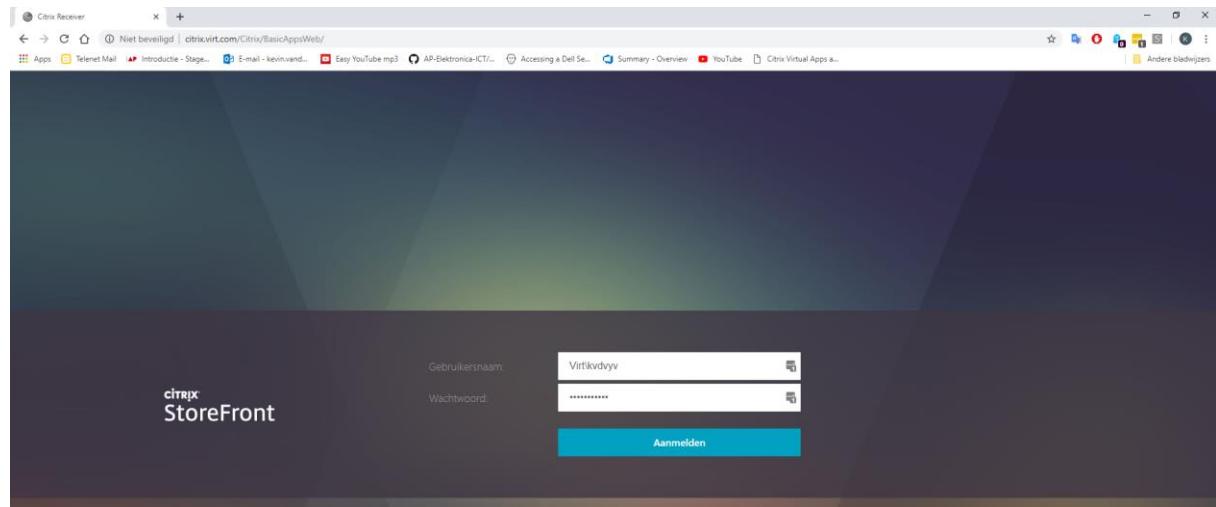
Figuur 3-64 *StoreFront* Link

Tot slot definieer je deze StoreFront in de delivery groep.



Figuur 3-65 StoreFront Delivery Controller

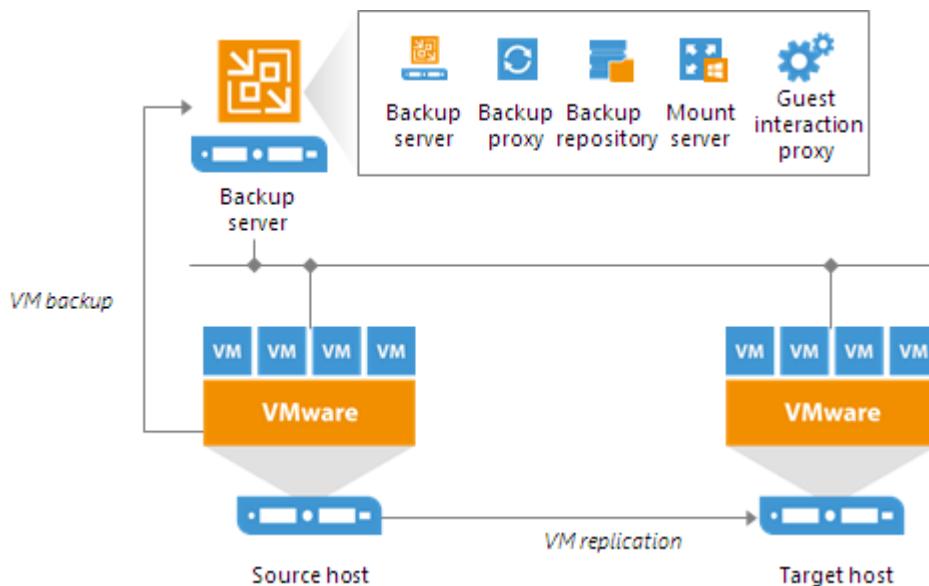
De Citrix configuratie is nu voltooid. De gebruikers kunnen via de Citrix Receiver inloggen en de Apps gebruiken.



Figuur 3-66 StoreFront Login Pagina

3.3.8 Veeam

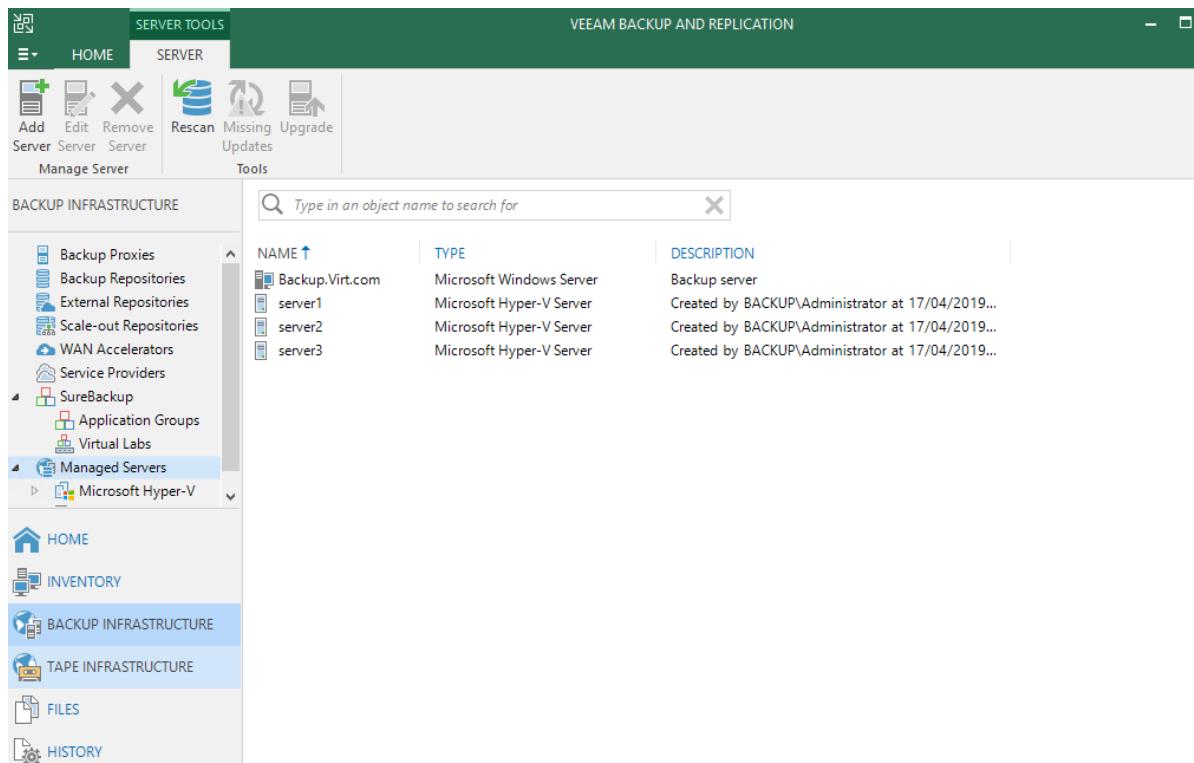
Veeam is een programma dat back-ups maakt. Back-ups zijn noodzakelijk om terug te kunnen gaan indien er een server niet meer functioneel is.



Figuur 3-67 VEEAM

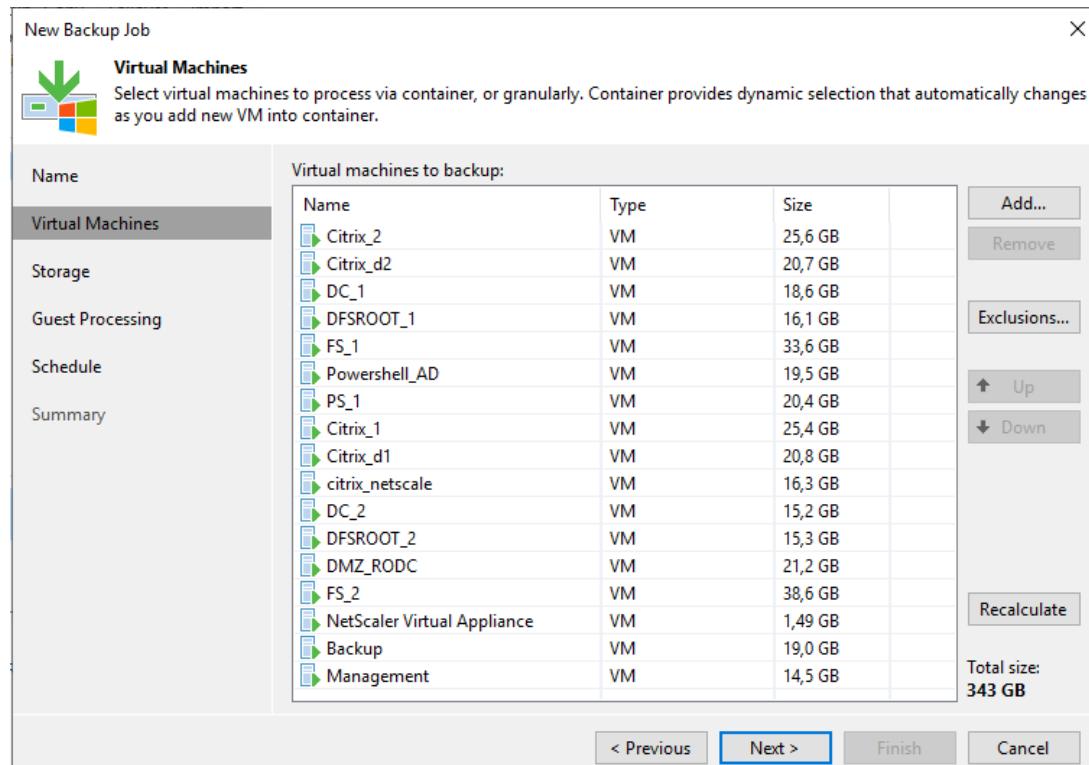
3.3.8.1 Configuratie VEEAM

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



Figuur 3-68 Backup Infrastructure

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



Figuur 3-69 Add VM's To Backup

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 dat er zijn ingesteld, is omdat VEEAM zijn cyclus eindigt met een full back-up.

The Restore Point Simulator

Current version : 0.4.1

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

RPS heavily relies on some opensource [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	1 Year ▾ 20%
ReFS	<input type="checkbox"/>

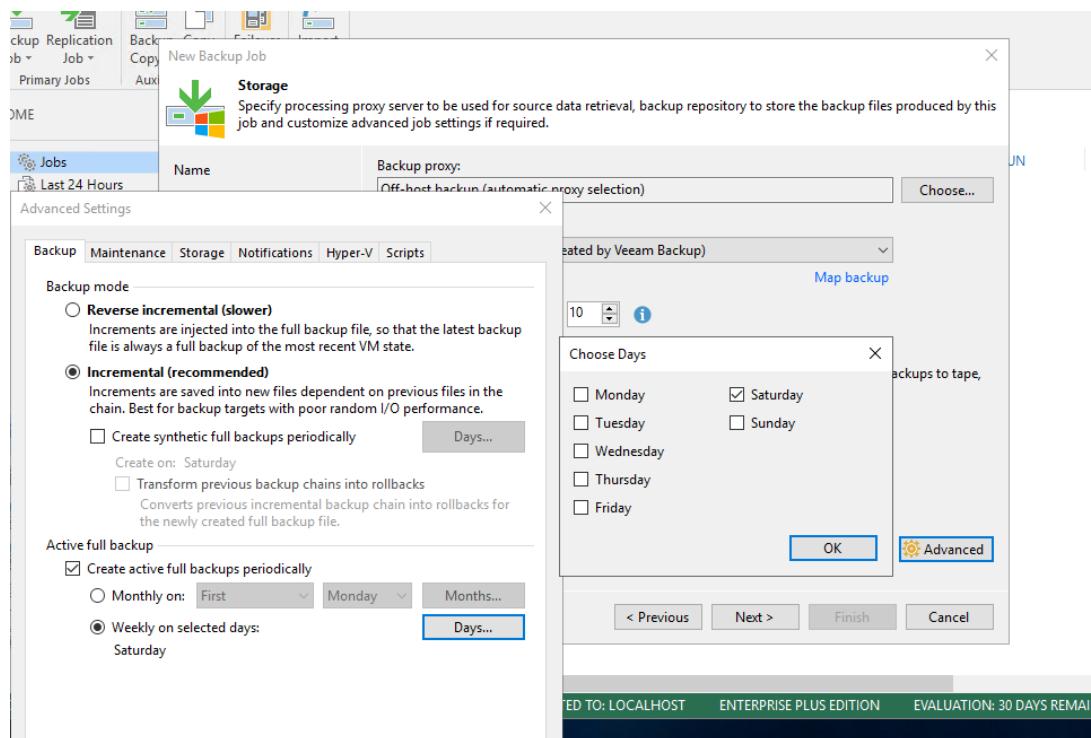
Incremental Specific

Synthetic MO TU WE TH FR SA SU
 Active Full Weekly MO TU WE TH FR SA SU
 Active Full Monthly Jan Feb Mar Apr May Jun
 Jul Aug Sep Oct Nov 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

Figuur 3-70 Backup Simulation

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-back-up 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.



Figuur 3-71 Backup Type and Schedule

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.

The screenshot shows the Veeam Backup & Replication interface. The main window displays a table of backup jobs, one of which has failed. Below the table, there is a summary of the backup process, including duration, processing rate, and bottleneck information. At the bottom, a detailed list of objects processed during the backup is shown, with some entries marked as failed.

JOB NAME	SESSION TYPE	STATUS	START TIME	END TIME
Daily + Full Weekly (Incremental)	Backup	Success	29/03/2019 20:00	29/03/2019 20:09
Daily + Full Weekly (Incremental)	Backup	Success	28/03/2019 20:00	28/03/2019 20:09
Daily + Full Weekly (Active File)	Backup	Success	28/03/2019 09:02	28/03/2019 10:24
Daily + Full Weekly (Incremental)	Backup	Failed	27/03/2019 20:39	27/03/2019 20:40
Daily + Full Weekly (Incremental)	Backup	Failed	27/03/2019 20:29	27/03/2019 20:29
Daily + Full Weekly (Incremental)	Backup	Failed	27/03/2019 20:18	27/03/2019 20:19
Daily + Full Weekly (Incremental)	Backup	Failed	27/03/2019 20:00	27/03/2019 20:08
Daily + Full Weekly (Incremental)	Backup	Failed	26/03/2019 20:40	26/03/2019 20:41
Daily + Full Weekly (Incremental)	Backup	Failed	26/03/2019 20:30	26/03/2019 20:30
Daily + Full Monthly (Incremental)	Backup	Failed	26/03/2019 20:18	26/03/2019 20:18

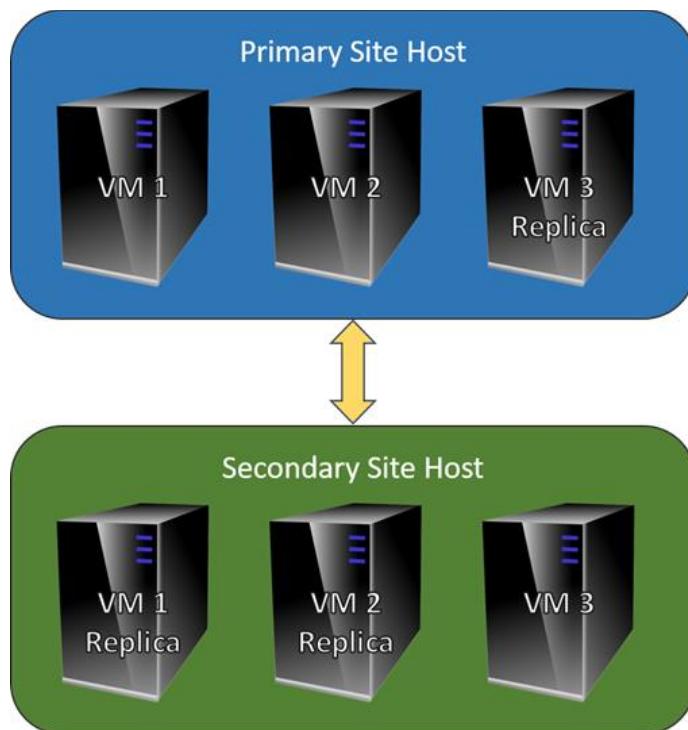
SUMMARY	DATA	STATUS	THROUGHPUT (ALL TIME)
Duration: 08:17	Processed: 248,0 GB (100%)	Success: 12 (green circle)	
Processing rate: 63 MB/s	Read: 13,1 GB	Warnings: 0	
Bottleneck: Source	Transferred: 4,8 GB (2,7x)	Errors: 1 (red circle)	

NAME	STATUS	ACTION	DURATI...
Management	Failed	Task failed. Failed to expand object Management. Error: Cannot find VM Management on host Server3.vim.com	
Cnrv_d2	Success	Network traffic verification detected no corrupted blocks	
Cnrv_2	Success		
DSRROOT_1	Success		
FS_1	Success		
DC_1	Success		
Cnrv_1	Success		
DSRROOT_2	Success		
DC_2	Success		
Cnrv_d1	Success		
FS_2	Success		
dc_1	Success		

Figuur 3-72 Backup Report

3.3.9 Replication

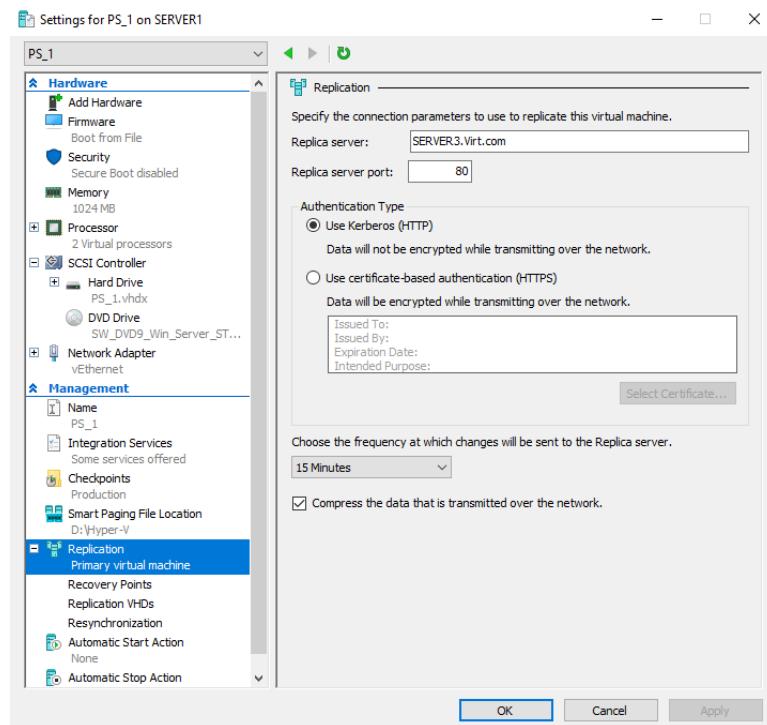
Met replication kan je de VM's (Virtual Machines) die niet high available zijn, toch failoveren. Dit betekent dat wanneer er een VM defect geraakt, deze meteen wordt overgenomen door een andere VM. Om replicatie te bekomen, gaat men 1 fysieke server instellen als een replica server. Op deze manier kan je VM's "kopiëren" naar deze server. Wanneer de originele VM uitvalt, zal de replica server de gekopieerde VM aanzetten en gebruiken.



Figuur 3-73 Repliaction

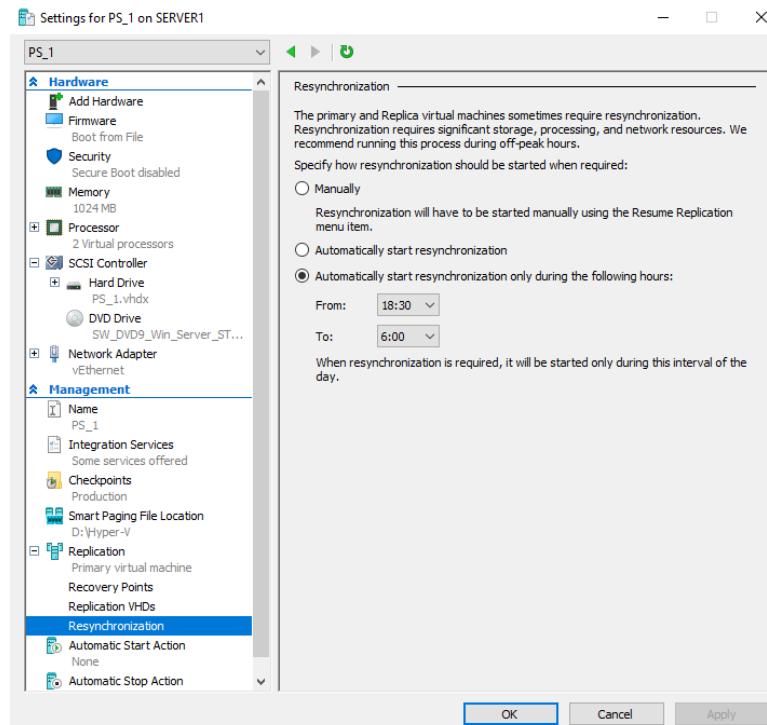
3.3.9.1 Configuratie

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



Figuur 3-74 Definieer Replica Server

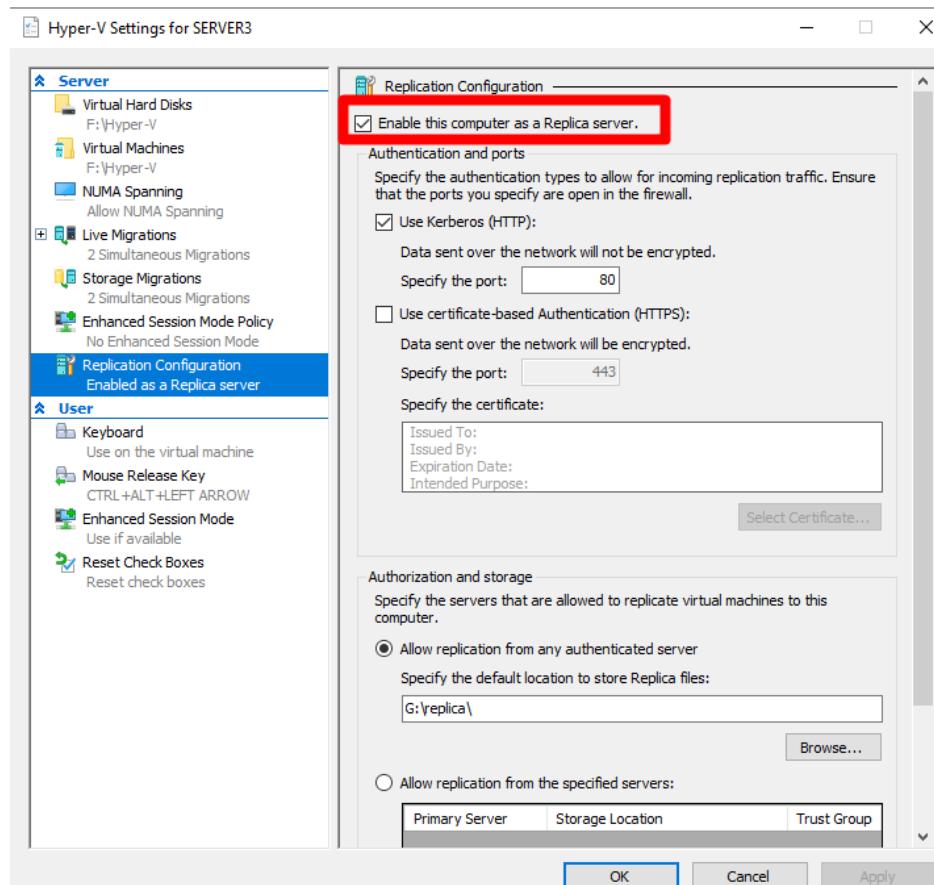
Voor de replicatie is het belangrijk dat je de servers synchroniseert zodat de gerepliceerde VM up to date is.



Figuur 3-75 Replication Synchronisatie

3.3.9.2 Installatie

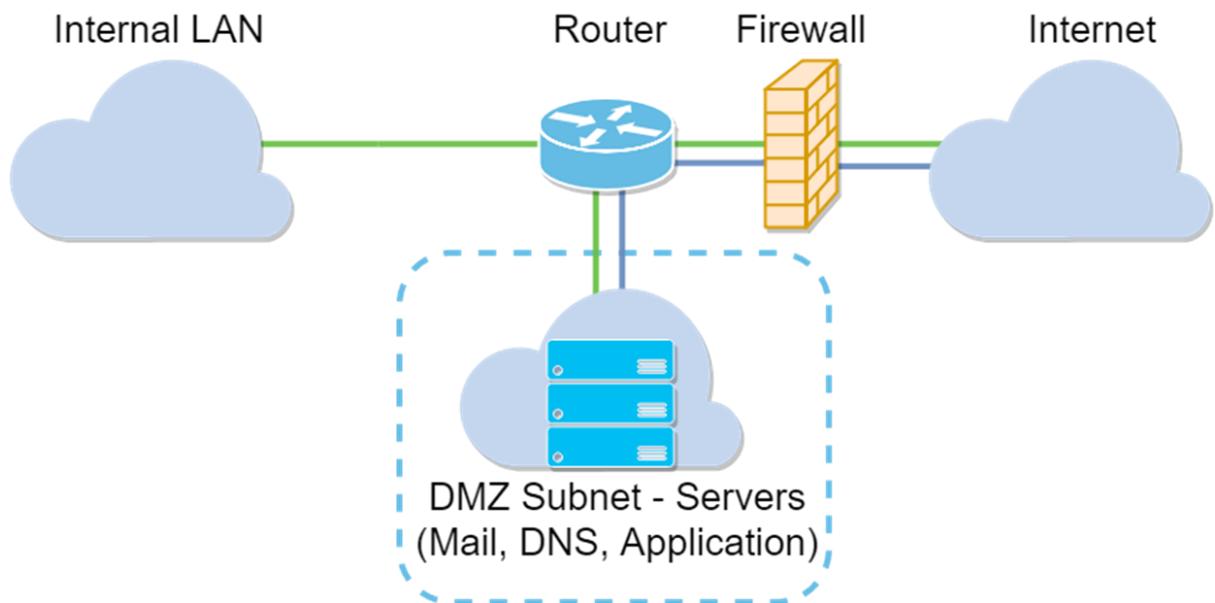
Server 3 stel je in als replica server, omdat deze de grootste dataopslag heeft. Hier geef je ook de locatie mee waar de gerepliceerde VM's terechtkomen.



Figuur 3-76 Enable Replica Server

3.3.10 DMZ

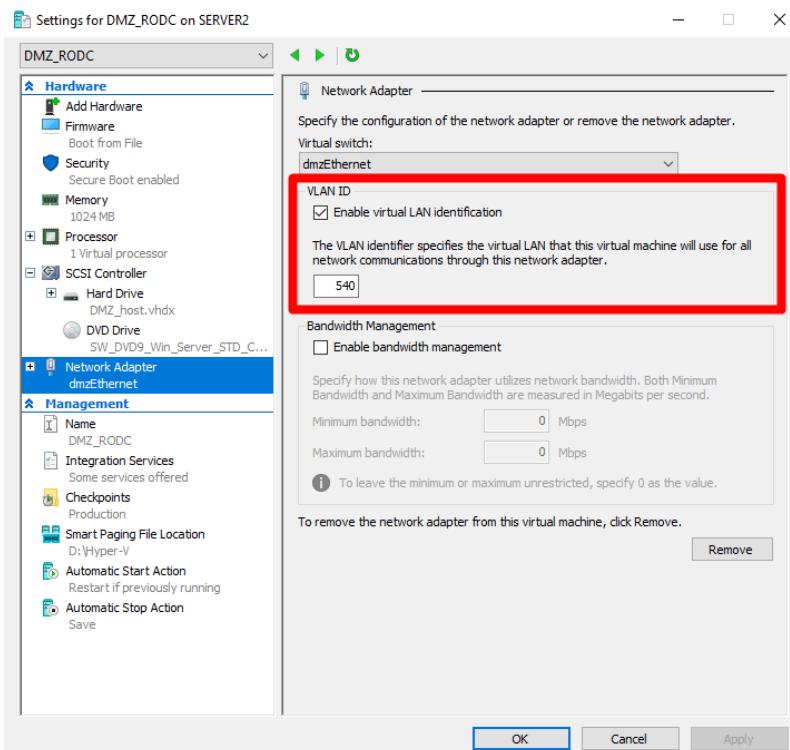
DMZ staat voor *demilitarized zone*. Dit is een zone die zich bevindt tussen het interne en externe netwerk. Deze zone wordt meestal gebruikt als extra security laag, omdat hierin de publieke toepassingen van het netwerk komen. Hierdoor hebben de externe gebruikers geen toegang tot het interne netwerk.



Figuur 3-77 DMZ

3.3.10.1 Configuratie

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.



Figuur 3-78 VLAN identificatie

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

Figuur 3-79 DMZ Access-list

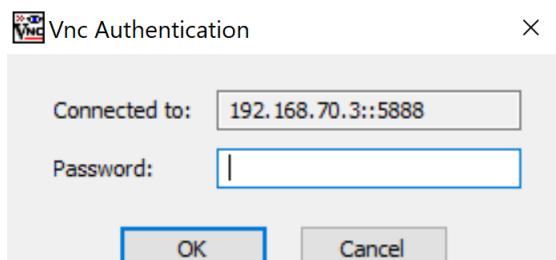
Deze configuratie kan je simpel testen door een applicatie te gebruiken waar je van op afstand moet inloggen. Voor de test is TightVNC gebruikt. TightVNC heeft standaard poort 5902 nodig om te kunnen communiceren, maar deze poort was in demo-omgeving al in gebruik. Hierdoor is de poort aangepast naar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

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



Figuur 3-80 LAN Test

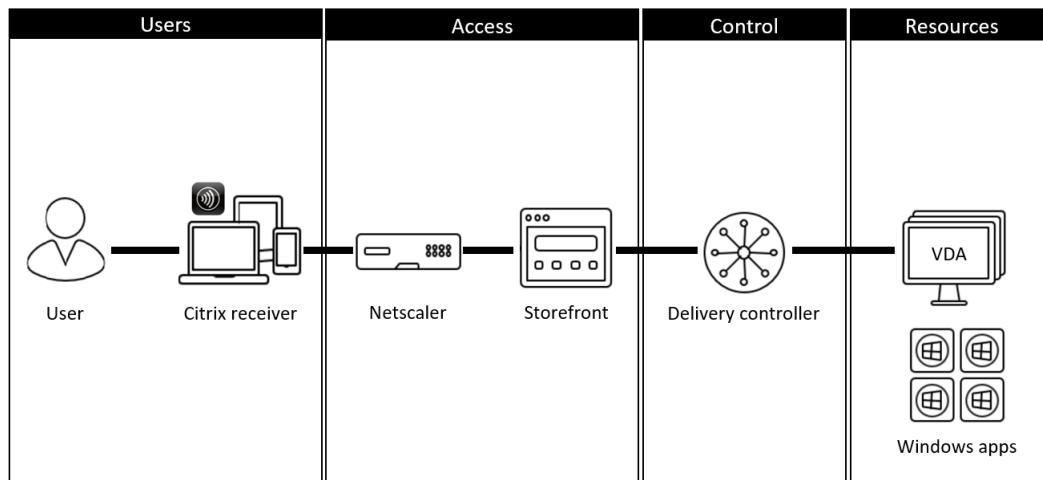
De connectie naar de VM in de DMZ zone is wel mogelijk. Hier staan namelijk alle poorten open (deze kan je wel limiteren tot de publieke toepassingen).



Figuur 3-81 DMZ Test

3.3.11 NetScaler

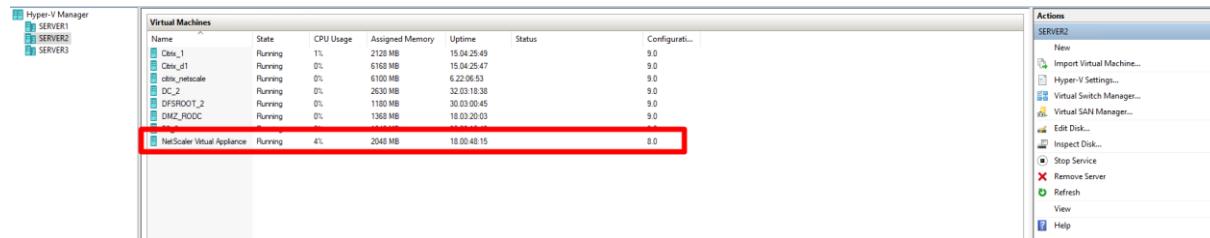
De *netscaler* is een toepassing die je gebruikt om applicaties beschikbaar te stellen voor zowel interne als externe gebruikers. De netscaler heeft een grote impact op de performantie, beveiliging en schaalbaarheid van de application delivery.



Figuur 3-82 NetScaler

3.3.11.1 Configuratie

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



Figuur 3-83 NetScaler Virtual Appliance

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.

```

NetScaler Virtual Appliance on SERVER3 - Virtual Machine Connection
File Action Media Clipboard View Help
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.
!Enter NetScaler's IPv4 address []:
!Enter Netmask []:
!Enter Gateway IPv4 address []:
Status: Running

```

Figuur 3-84 NetScaler Netwerk Configuratie

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, configureer je de Citrix XenApp and XenDesktop. 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 vul je alvast in.

Basic Settings	
1	NetScaler Gateway
2	Server Certificate
3	StoreFront
4	Authentication

Figuur 3-85 NetScaler Config

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 maak je een self-signed certificaat aan, dit leg ik hieronder uit.

Om te beginnen maak je eerst de Root Key aan. Deze heb je nodig 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

Figuur 3-86 Root RSA Key

Met deze Key maak je een Root Request aan. 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)
[empty]

Digest Method*
SHA1

Distinguished Name Fields

Common Name*
NS-ROOT-CA

Organization Name*
TestNetscaler

Organization Unit
[empty]

Email Address
[empty]

City
[empty]

State or Province*
Antwerp

Country*
BELGIUM

Attribute Fields

Figuur 3-87 Root CSR

Met de aangemaakte Key en het Request, maak je het Root certificaat aan. 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)
[empty]

Validity Period (Number of Days)
365

Create Close

Figuur 3-88 Root Certificaat

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.

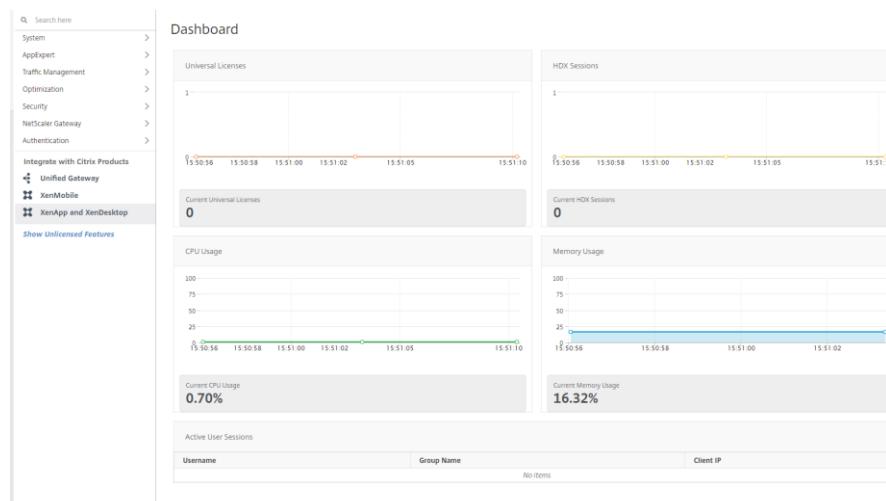
Figuur 3-89 Server Certificaat

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

NetScaler Gateway Virtual Servers								
	Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
	_XO_192.168.70.100_80	DOWN	192.168.70.100	80	SSL	0	0	0
	_XO_192.168.70.150_443	UP	192.168.70.150	443	SSL	500	0	0

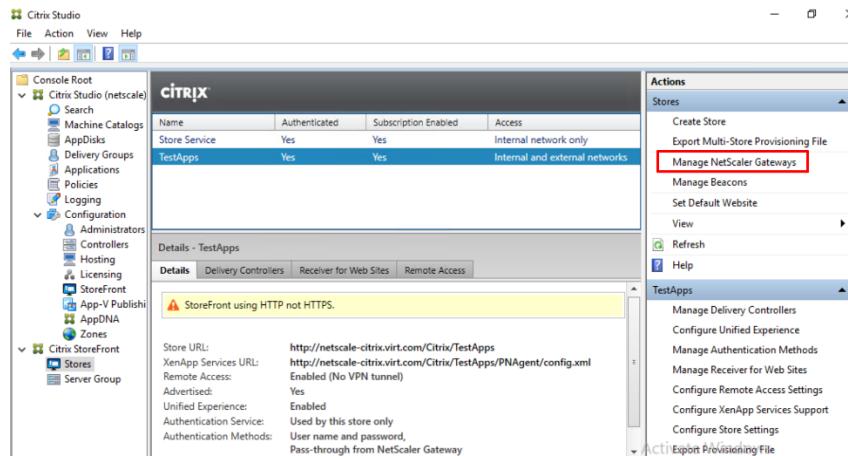
Figuur 3-90 Link Server Certificaat

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



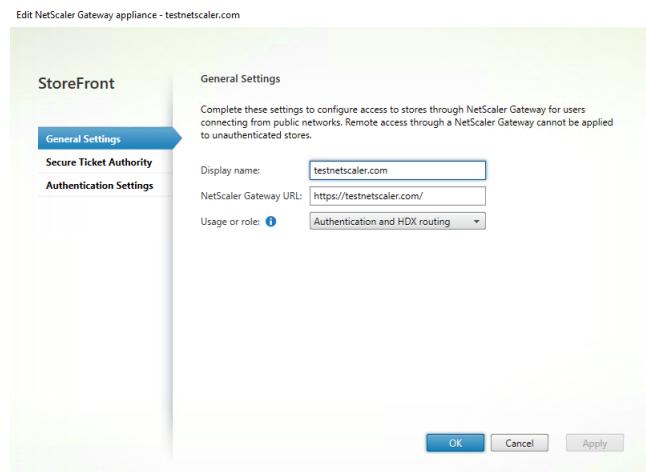
Figuur 3-91 NetScaler Download config

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

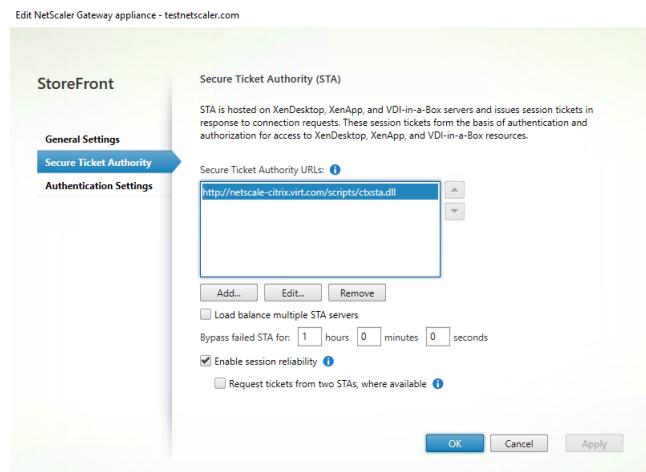


Figuur 3-92 Citrix NetScaler Gateway

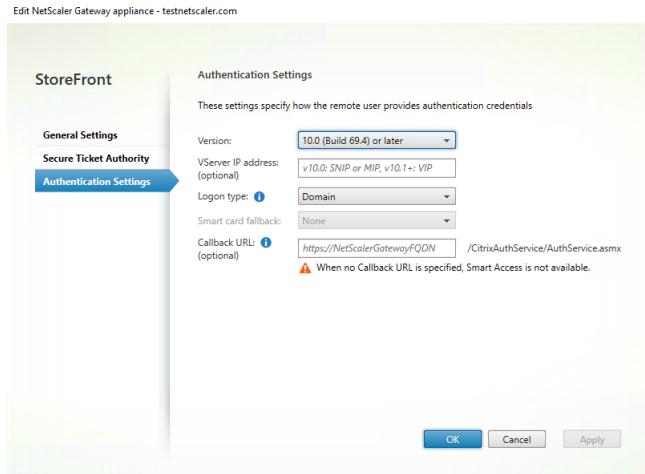
In deze configuratie stel je de naam in, de NetScaler URL, de STA servers (Citrix delivery controllers) en de authenticatie die je gebruikt.



Figuur 3-93 Citrix NetScaler URL

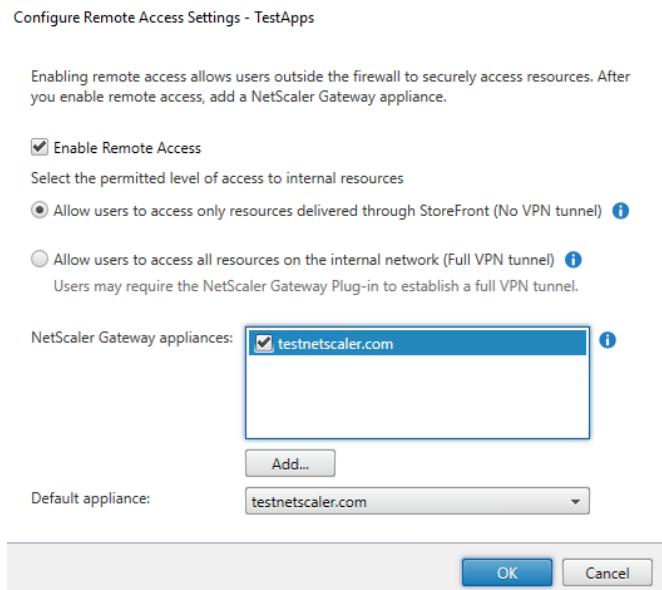


Figuur 3-94 Citrix STA Server



Figuur 3-95 Citrix NetScaler Authenticatie

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



Figuur 3-96 Citrix NetScaler Remote Access

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

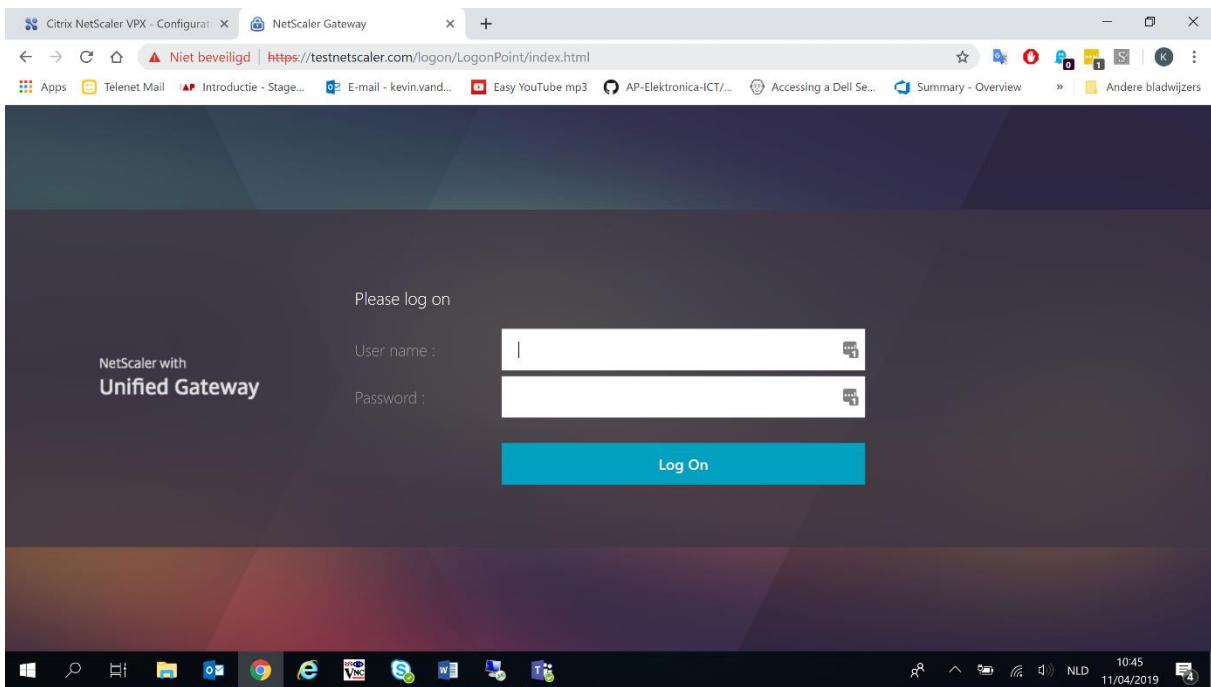
Figuur 3-97 Citrix StoreFront Access

De configuratie is nu voltooid voor zowel de NetScaler als de Citrix StoreFront. Je kan nu navigeren 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
```

Figuur 3-98 Hosts bestand

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



Figuur 3-99 NetScaler Login Pagina

3.3.12 Azure AD Connect

Met Azure AD Connect synchroniseer je de active directory van het domein 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

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 with the 'Azure AD Connect' section selected in the sidebar. The main content area displays the following information:

- SYNC STATUS:** Not Installed. Includes 'Last Sync' (Sync has never run) and 'Password Hash Sync' (Disabled).
- USER SIGN-IN:** Federation (Disabled, 0 domains), Seamless single sign-on (Disabled, 0 domains), and Pass-through authentication (Disabled, 0 agents).
- ON-PREMISES APPLICATIONS:** A link to configure remote access for on-premises applications.

Figuur 3-100 Azure AD Connect

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' wizard with the 'Azure AD sign-in' step selected. The main content area displays the following configuration:

- Active Directory UPN Suffix:** virt.com
- Azure AD Domain:** Not Verified
- User Principal Name:** userPrincipalName
- Note:** A message states: "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".

Figuur 3-101 Azure AD Domain

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 Microsoft Azure portal with the URL [https://portal.azure.com/#blade/HubsBlade](#). The left sidebar shows 'AP - Custom domain names' under 'Custom domain names'. The main pane displays the 'virt.com' custom domain configuration. It includes 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 red box highlights a warning message: 'Verify domain Verification will not succeed until you have configured your domain with your registrar as described above.' At the bottom, another red box highlights an error message: 'Could not find the DNS record for this domain. DNS changes may take up to 72 hours to propagate. Please try again later.'

Figuur 3-102 Verify Domain

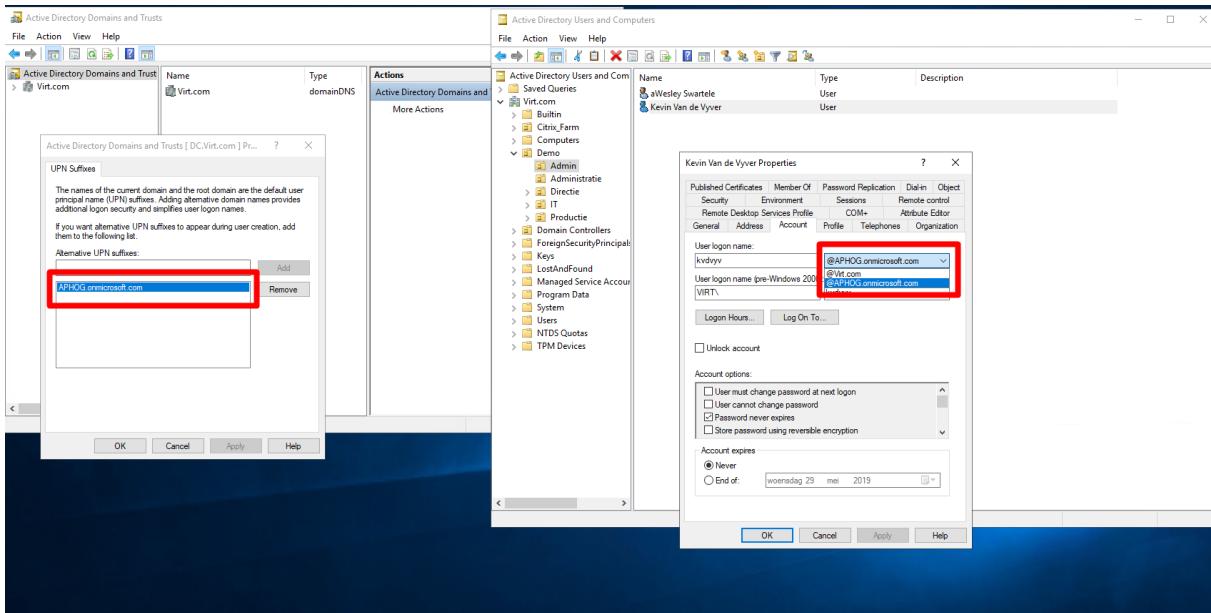
Om dit probleem te omzeilen maak je een andere suffix aan in het domein. Wanneer je inlogt op Azure met een Microsoft account, heeft deze standaard een geverifieerd onmicrosoft domein. Deze UPN voeg je toe in het domein van je omgeving.

The screenshot shows the 'AP - Custom domain names' page within the 'Azure Active Directory' section. The left sidebar lists various Azure services, with 'Custom domain names' selected. The main pane displays a table of custom domains. The table has columns: NAME, STATUS, FEDERATED, and PRIMARY. It shows two entries: 'APHOG.onmicrosoft.com' with a green checkmark in the FEDERATED column and 'virt.com' with an orange triangle icon in the STATUS column.

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

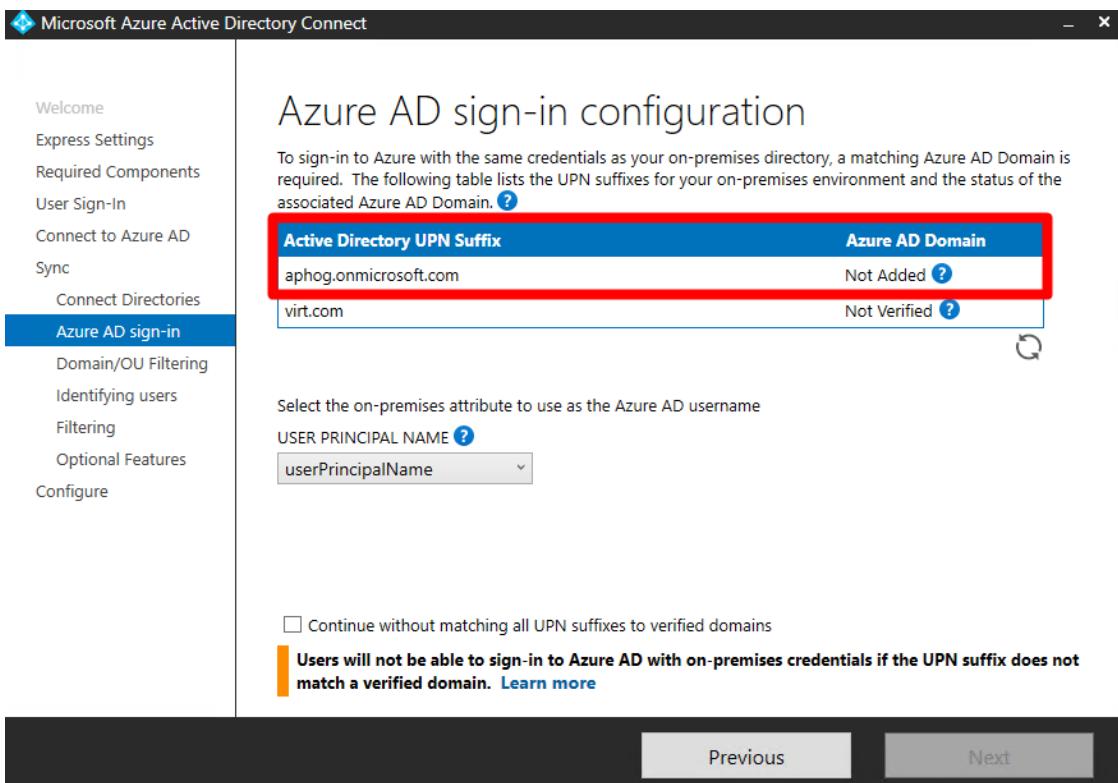
Figuur 3-103 CustomDomain

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.



Figuur 3-104 Add UPN Suffix

Eens de suffix is toegevoegd aan het domein, loopt de installatie van de Azure connect verder. 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.



Figuur 3-105 Azure AD Verified Domain

Voor het domein virt.com of onmicrosoft.com zijn geen specifieke vereisten, de volgende opties laat je op de default waarden staan. Je kiest ervoor om ofwel 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 voltooid is, kan je op de Azure site de gebruikers zien. Alle users die hierin staan, hebben vanaf nu met hun domeinlogin ook toegang tot Azure applicaties. Een website die je kan gebruiken om te testen is *myapps.microsoft.com*.

The screenshot shows the 'Users - All users' page in the Azure Active Directory portal. On the left, there's a sidebar with navigation 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. The data includes:

NAME	USER NAME	USER TYPE	SOURCE
AS	aWesley Swartele	awes@APHOG.onmicro... Member	Windows Server AD
IJ	ik jij	Kevin@APHOG.onmicro... Member	Azure Active Directory
JR	Julie jru. Rutten	Julie_Rutten@APHOG.on... Member	Windows Server AD
KV	Kevin Van de Vyver	kvdvyy@APHOG.onmicro... Member	Windows Server AD
KR	krbtgt_920	krbtgt_920@APHOG.on... Member	Windows Server AD
OD	On-Premises Direct...	Sync_AD-CONNECT_b4bd... Member	Windows Server AD
SS	Sam svab. Van Bog	Sam_Van_Bogaert@APHO... Member	Windows Server AD
SS	Seppe sdb. De Beu	Seppe_De_Beule@APHOG... Member	Windows Server AD
SS	Sophie sru. Rutten	Sophie_Rutten@APHOG.... Member	Windows Server AD
WW	Wesley wswart. Sw	wswart@APHOG.onmicro... Member	Windows Server AD

Figuur 3-106 Azure AD Users

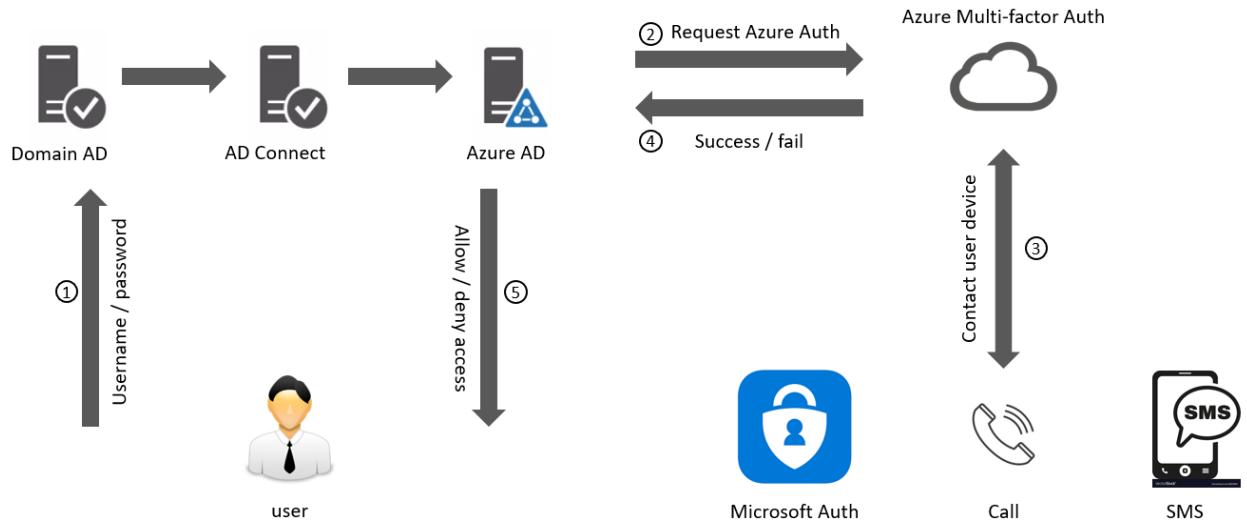
Een extra optie die je kan instellen met Azure AD Connect is *Single sign-on*. Dit verhoogt de productiviteit van de gebruikers, omdat ze weer een paswoord minder moeten onthouden. Eens ingelogd op de computer met het domein account, log je in op de cloud zonder dat je opnieuw je paswoord moet ingeven.

The screenshot shows the 'User sign-in' configuration page in the Microsoft Azure Active Directory Connect interface. The left sidebar has links for 'Welcome', 'Tasks', 'Connect to Azure AD', 'User Sign-In' (which is selected), 'Single sign-on', and 'Configure'. The main area is titled 'User sign-in' and asks 'Select the Sign On method.' There are five radio button options: 'Password Hash Synchronization', 'Pass-through authentication' (which is selected), 'Federation with AD FS', 'Federation with PingFederate', and 'Do not configure'. Below this, it says 'Select this option to enable single sign-on for your corporate desktop users:' followed by a checked checkbox labeled 'Enable single sign-on'. A note at the bottom states: 'We recommend kevin@APHOG.onmicrosoft.com to be a cloud only Company Administrator account so that kevin@APHOG.onmicrosoft.com is able to manage pass-through authentication in the event of an on-premises failure. Learn more'. At the bottom are 'Previous' and 'Next' buttons.

Figuur 3-107 Single Sign-on

3.3.13 Multi-factor Authenticatie

In het 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.



Figuur 3-108 Azure Multi-factor Authenticatie

3.3.13.1 Configuratie MFA

In de *Azure Active Directory* is er een optie voor MFA in de gebruikers sectie. Hier kan je 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 for '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 for 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	awes@APHOG.onmicro...	Member Windows Server AD
IJ	ik jij	Kevin@APHOG.onmicro...	Member Azure Active Directory
JJ	Julie jru. Rutten	Julie_Rutten@APHOG.on...	Member Windows Server AD
KV	Kevin Van de Vyvei	kvdyv@APHOG.onmicro...	Member Windows Server AD
KR	krbtgt_920	krbtgt_920@APHOG.onm...	Member Windows Server AD
OD	On-Premises Direct...	Sync_AD-CONNECT_b4bd...	Member Windows Server AD
SS	Sam svab. Van Bog...	Sam_Van_Bogaert@APHO...	Member Windows Server AD
SS	Seppe sdb. De Beu	Seppe_De_Beule@APHOG...	Member Windows Server AD
SS	Sophie sru. Rutten	Sophie_Rutten@APHOG....	Member Windows Server AD
WW	Wesley wswart. Sw...	wswart@APHOG.onmicro...	Member Windows Server AD

Figuur 3-109 Multi-Factor Setting

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

Figuur 3-110 Multi-Factor Type

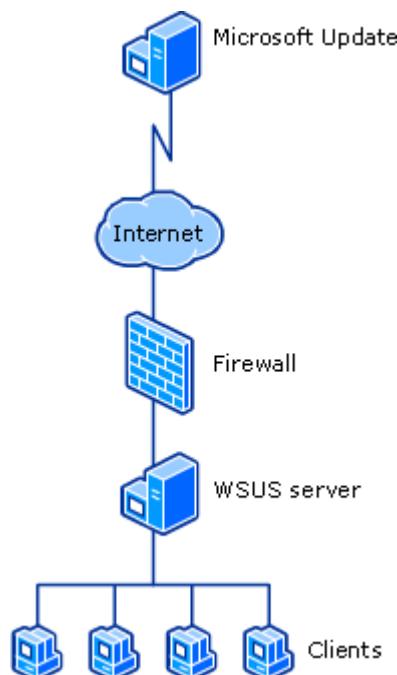
Volg de stappen om een authenticator applicatie op je smartphone te installeren en te configureren.

Andere mogelijkheden zijn authenticatie via SMS of opgebeld worden.

3.3.14 Windows Server Update Services (WSUS)

Windows Server Update Services, afgekort WSUS is een programma dat administrators vaak gebruiken om windows machines up to date te houden in een netwerk. Het is niet de bedoeling dat alle windows clients de updates rechtstreeks bij Microsoft halen. Sommige clients hebben mogelijk zelfs geen internettoegang. WSUS kan je installeren op een server die dan zal dienen als een update verdeler. De server haalt automatisch updates van de Microsoft update website om die in het netwerk uit te delen aan computers, servers, ...

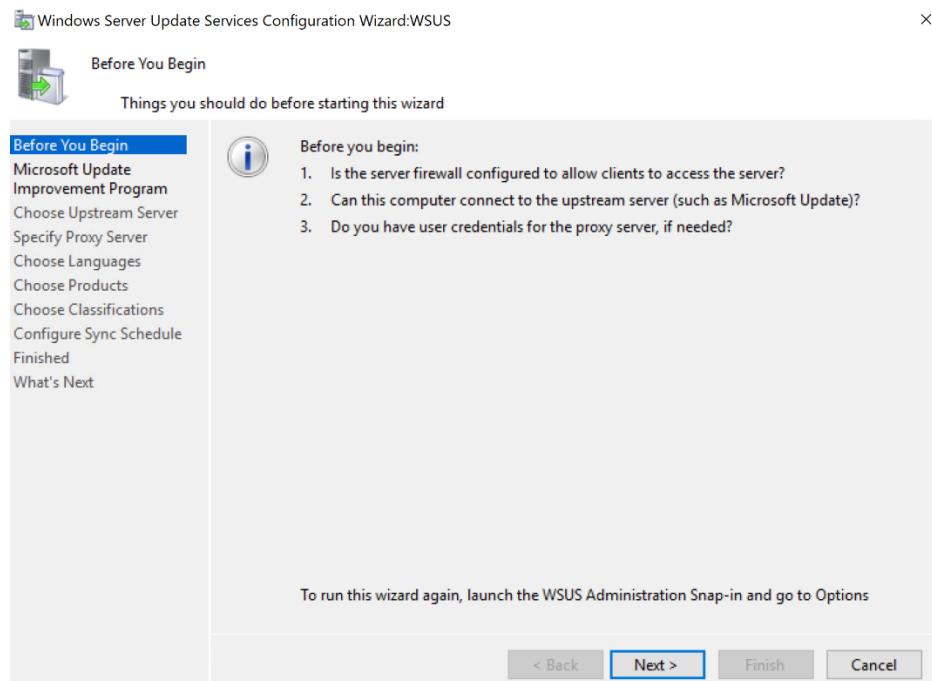
Via WSUS en GPO heb je echter controle over welke updates wanneer geïnstalleerd zullen worden. Zo kan je bepaalde updates blokkeren, en andere kan je over een periode verdelen zodat niet alle clients op hetzelfde moment dezelfde update installeren.



Figuur 3-111 WSUS

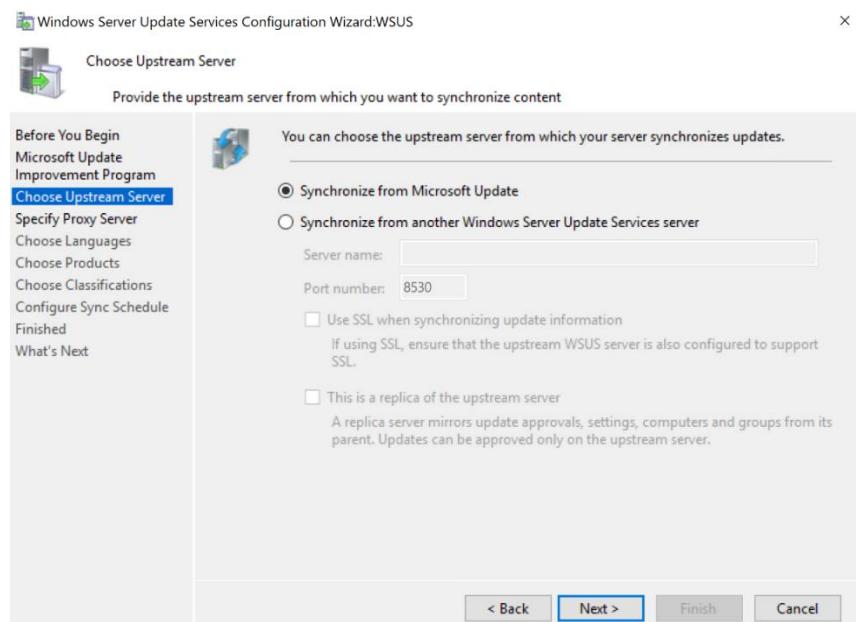
3.3.14.1 Configuratie WSUS

Via de server manager installeer je de Windows Server Update Services rol. Dit is een redelijk grote rol en het zal enige tijd in beslag nemen voor deze geïnstalleerd is. Vervolgens kan je de Windows Server Update Services applicatie starten. Deze zal een setup starten voor de toepassing.



Figuur 3-112 WSUS Setup

Als dit de eerste Windows Server Update Services server is, selecteer je in de volgende stappen om te synchroniseren met Microsoft Update. Als dit een tweede server is, kan je deze laten synchroniseren van een bestaande server.



Figuur 3-113ynchronisatie

De setup begint na deze stap met synchroniseren. Dit duurt wel even dus kan je alvast de GPO's maken die nodig zijn. De belangrijkste GPO's om in te stellen zijn:

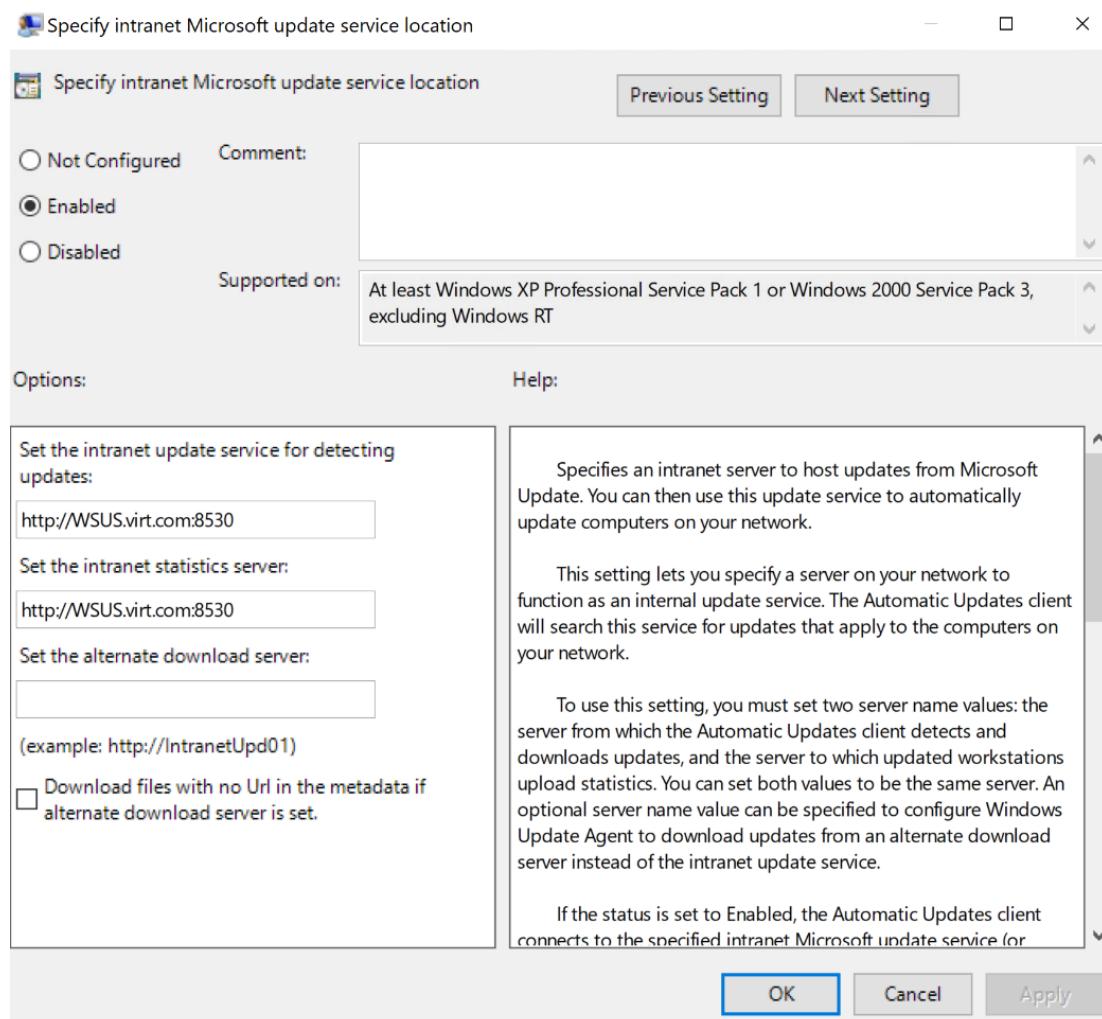
- Specify intranet Microsoft update service location
- Turn off auto-restart for updates during active hours
- Automatic Updates detection frequency
- Configure Automatic updates

Setting	State	Comment
Windows Update for Business		
Automatic Updates detection frequency	Enabled	No
Configure Automatic Updates	Enabled	No
Specify intranet Microsoft update service location	Enabled	No
Turn off auto-restart for updates during active hours	Enabled	No
Allow Automatic Updates immediate installation	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Allow signed updates from an intranet Microsoft update service	Not configured	No
Allow updates to be downloaded automatically over metered connections	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure auto-restart warning notifications schedule for updates	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Display options for update notifications	Not configured	No
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down	Not configured	No
Do not allow update deferral policies to cause scans against Windows Update	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Do not display 'Install Updates and Shut Down' option in Shutdown	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Enable client-side targeting	Not configured	No
Enabling Windows Update Power Management to automatically turn off the computer	Not configured	No
No auto-restart with logged on users for scheduled automatic updates	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No

Figuur 3-114 WSUS GPO's

Specify intranet Microsoft update service location

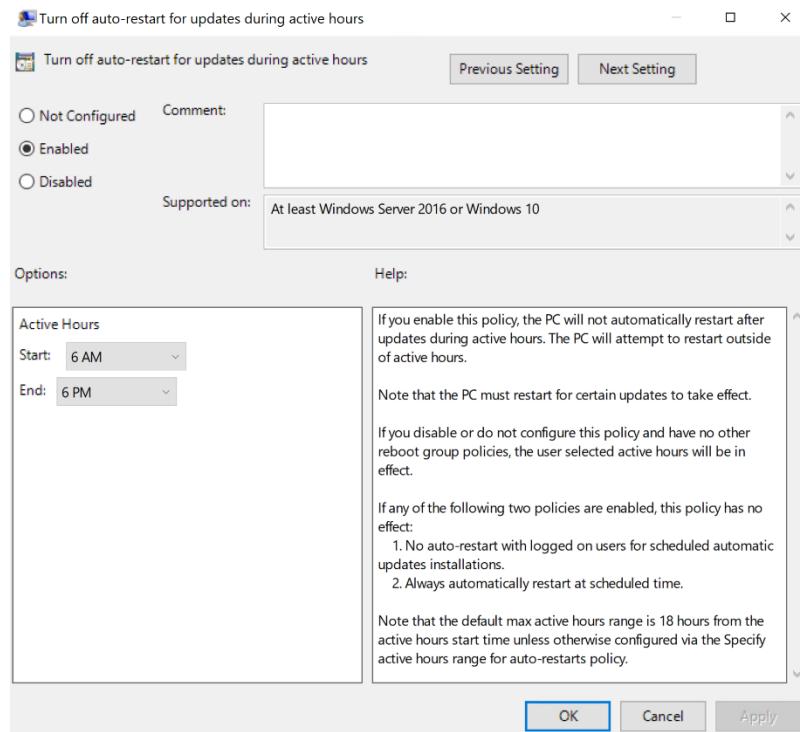
Met deze GPO stel je de server in waarvan de updates geïnstalleerd moeten worden.



Figuur 3-115 Specify Intranet Microsoft update service location

Turn off auto-restart for updates during active hours

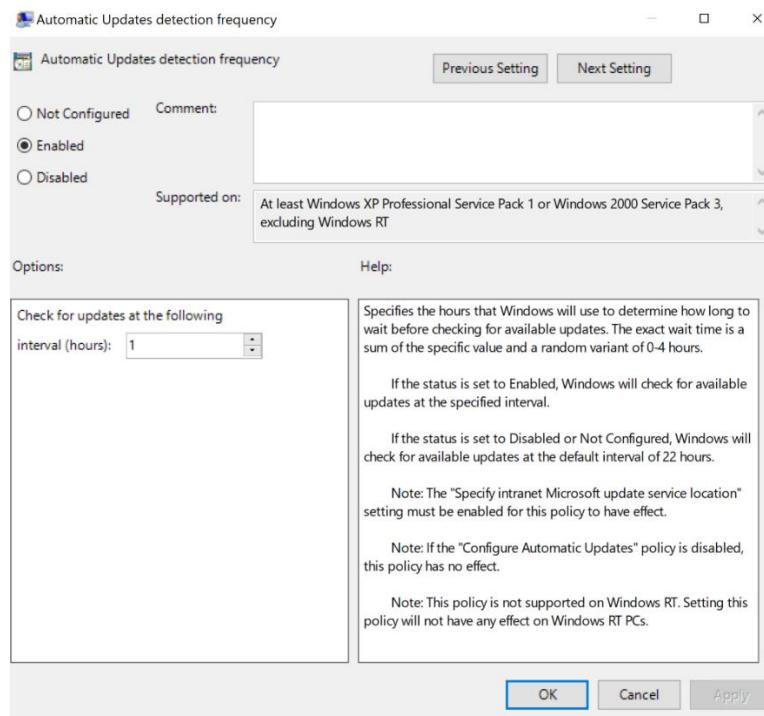
Deze GPO gaat er voor zorgen dat de computers, servers, ... niet herstarten tijdens specifieke tijden. Zo vermijd je dat gebruikers geen toegang meer hebben tot bepaalde applicaties (als je servers high available zijn kan je deze op aparte tijden updaten en heb je dit probleem niet).



Figuur 3-116 Turn off auto-restart for updates during active hours

Automatic Updates detection frequency

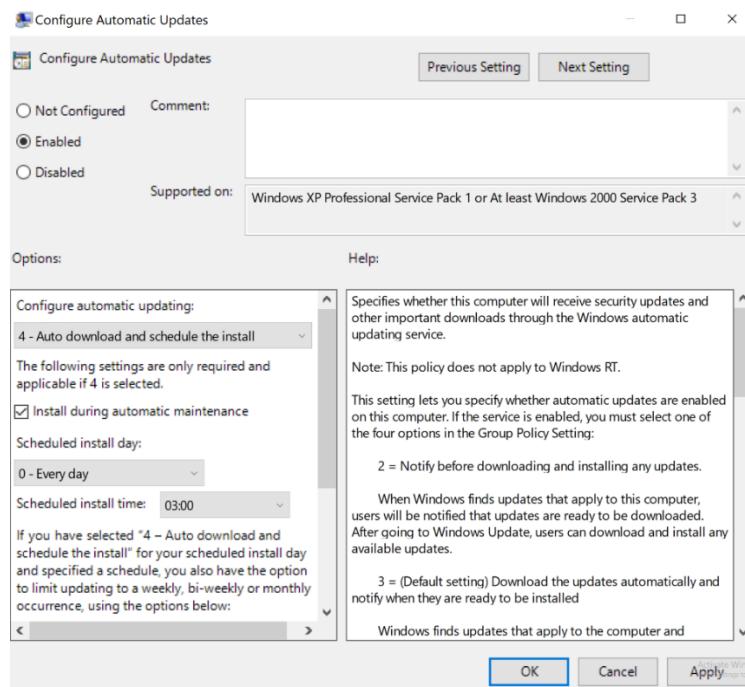
Deze GPO stelt het interval in om te checken of er al dan niet updates zijn.



Figuur 3-117 Automatic Updates detection frequency

Configure Automatic updates

Deze GPO geeft je meer opties wanneer de updates gebeuren. Zo zorg je ervoor dat niet elk apparaat tegelijk gaat updaten. In de demo-omgeving zijn de servers opgedeeld in verschillende OU's waardoor de meeste applicaties ten alle tijden beschikbaar blijven.



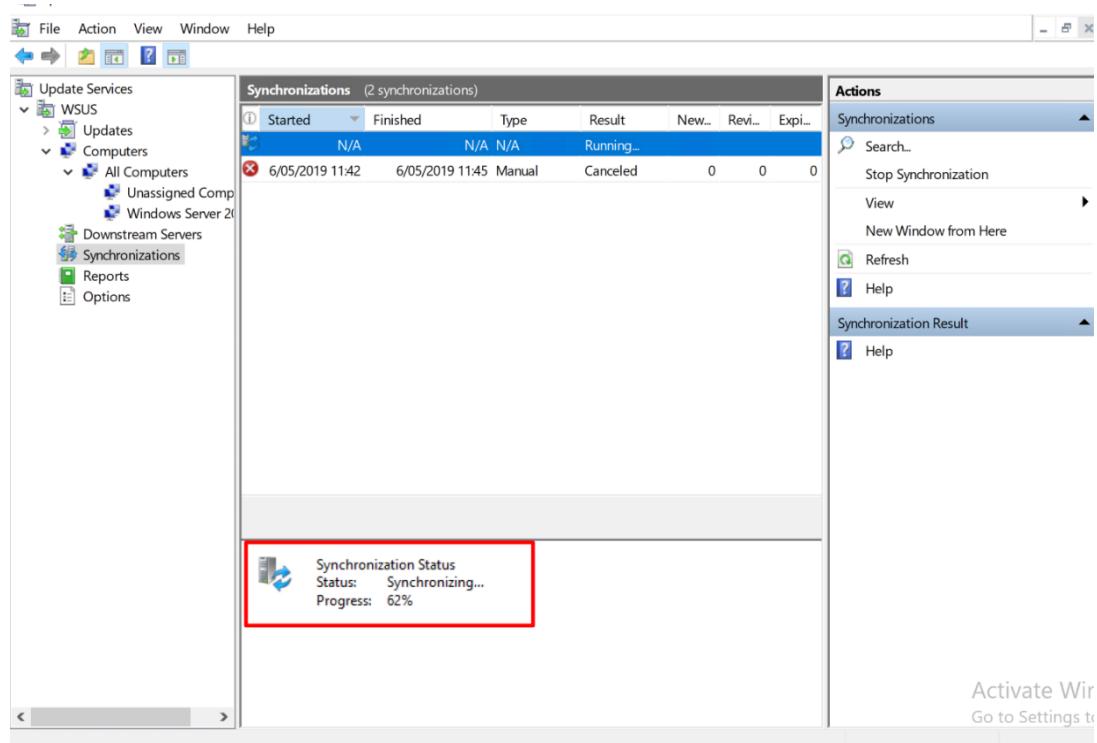
Figuur 3-118 Configure Automatic updates

Zoals je hieronder ziet, zijn er verschillende GPO's aangemaakt voor elke servergroep.

The screenshot shows the Group Policy Management console. On the left, a tree view displays various GPOs under 'Forest: Virt.com'. A red box highlights a group of three GPOs under the 'Demo' folder: 'UpdateRotation1', 'UpdateRotation2', and 'UpdateRotation3', each containing a 'WSUS-X' sub-GPO. On the right, the details for the 'WSUS-Citrix' GPO are shown. The 'Scope' tab is selected, showing the link to 'Virt.com'. The 'Links' section lists 'Citrix_Farm' with 'Enforced' set to 'No' and 'Link Enabled' to 'Yes'. The 'Security Filtering' section shows 'Authenticated Users' assigned to the GPO. The 'WMI Filtering' section indicates no filter is applied.

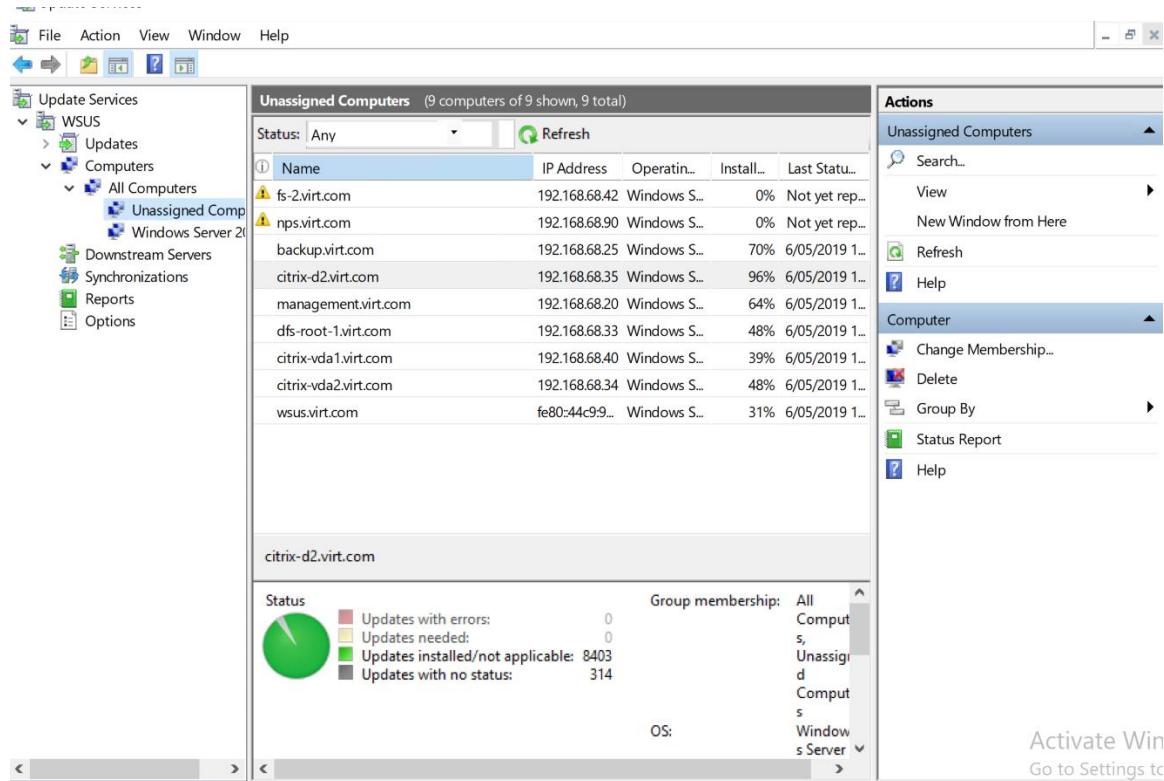
Figuur 3-119 GPO Groepen

Nadat de GPO's ingesteld zijn, moet eerst de synchronisatie voltooien. Je kan de status van de synchronisatie bijhouden in de Synchronizations tab.



Figuur 3-120 Running Synchronization

Naarmate de synchronisatie vordert, zullen de PC's verschijnen in de computer tab. Hier zie je welke computers er al gesynchroniseerd zijn en welke bezig zijn.



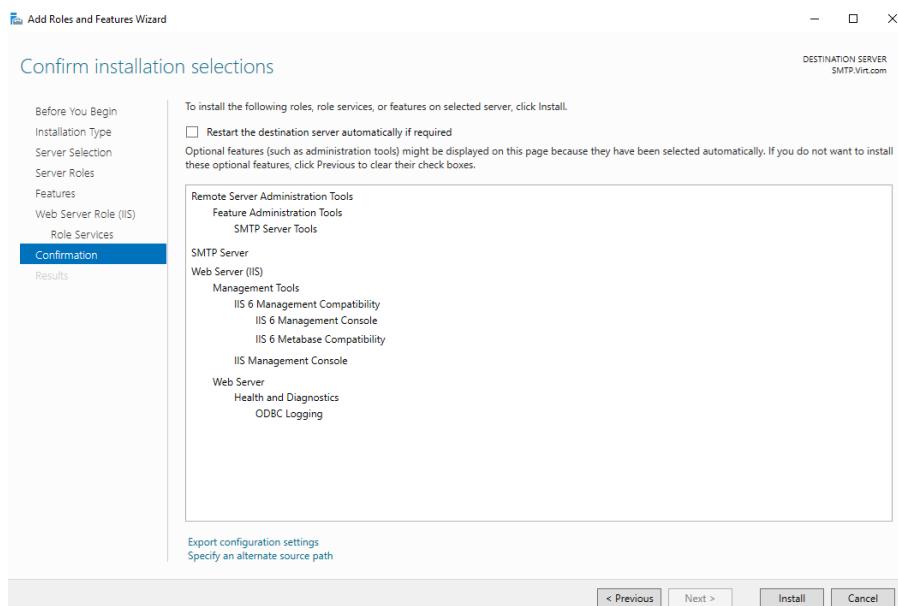
Figuur 3-121 Synchronization Status

3.3.15 SMTP Server

Simple Mail Transfer Protocol, afgekort SMTP is een standaard om e-mails te versturen over het internet. SMTP gebruikt TCP-poort 25 voor de communicatie tussen de SMTP-servers.

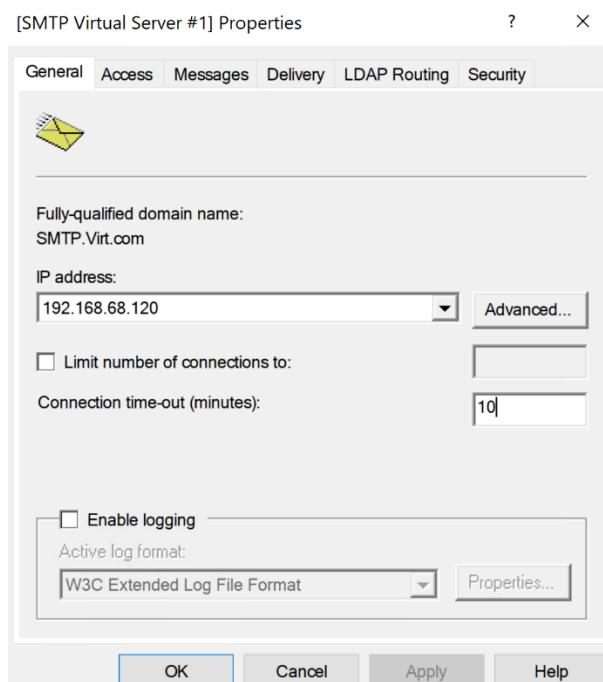
3.3.15.1 Configuratie mail server

Eerst installeer je de SMTP server rol, hierbij installeert de server ook de IIS functionaliteit. Deze heb je nodig om de SMTP server te configureren.



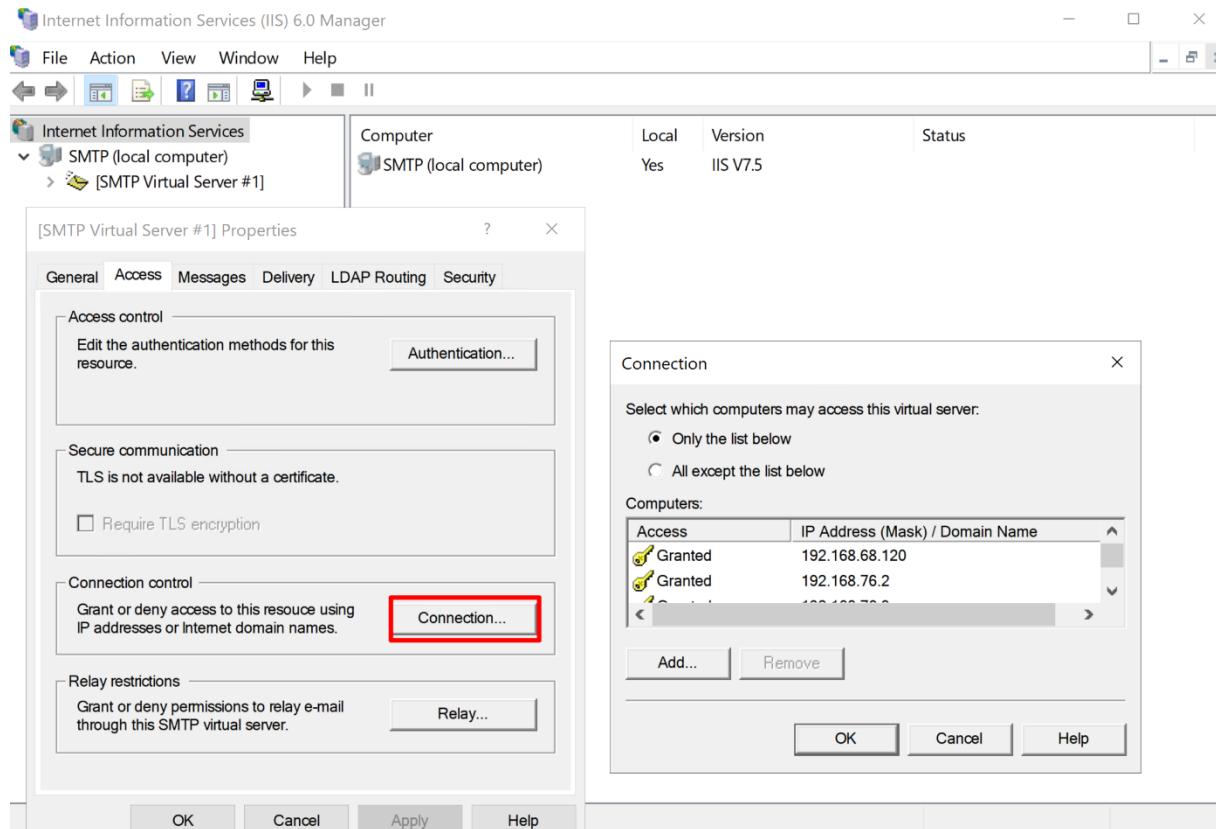
Figuur 3-122 SMTP Role

Eens geïnstalleerd, start je de IIS manager en configureer je SMTP. De eerste stap is het IP adres meegeven dat je gebruikt voor de SMTP server.



Figuur 3-123 SMTP IP Address

Vervolgens limiteer je de servers die toegang hebben tot de mailserver. In de demo-omgeving hebben de iDRAC-adressen toegang tot de mailserver.



Figuur 3-124 SMTP Connection Config

Voor de relay limitering zijn dezelfde servers toegevoegd. Nu deze properties ingesteld zijn, zal de service geactiveerd worden moet dit nog niet gebeurd zijn. Je kan de service best ook automatisch laten starten wanneer de server opstart/herstart.

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

PS C:\Users\Administrator> set-service smtspsvc -StartupType Automatic
PS C:\Users\Administrator> get-service smtspsvc

Status    Name            DisplayName
-----  ----            -----------
Running  smtspsvc       Simple Mail Transfer Protocol (SMTP)

PS C:\Users\Administrator>
```

Figuur 3-125 Authomatic Service Startup

Om te testen of de mailserver werkt, maak je een testmail in powershell met volgend commando.

```
Send-MailMessage -SMTPServer 192.168.68.120 -To <your mail address> -From SMTP@virt.com -  
Subject "test" -Body "Test mail via PowerShell"
```

Als de SMTP server correct geconfigureerd is, zou je een mail moeten ontvangen.



Figuur 3-126 Test Mail

3.3.15.2 iDRAC monitoring

In de iDRAC browser heb je de optie om alerts te versturen via email. Zo ben je altijd op de hoogte van de status van de servers. Om mails te kunnen versturen moet je in de iDRAC netwerk settings een static DNS Domain Name instellen, anders zal de iDRAC geen mails kunnen verzenden.

The screenshot shows three main sections of the iDRAC network configuration:

- Common Settings:**

Attribute	Value
Register DRAC on DNS	<input type="checkbox"/>
DNS DRAC Name	Server3
Auto Config Domain Name	<input type="checkbox"/>
Static DNS Domain Name	virt.com
- Auto Config:**

Attribute	Value
Enable DHCP Provisioning	Disable
- IPv4 Settings:**

Attribute	Value
Enable IPv4	<input checked="" type="checkbox"/>
DHCP Enable	<input type="checkbox"/>
Static IP Address	192.168.76.2
Static Gateway	192.168.76.1
Static Subnet Mask	255.255.254.0
Use DHCP to obtain DNS server addresses	<input type="checkbox"/>
Static Preferred DNS Server	192.168.68.30
Static Alternate DNS Server	192.168.68.41

Figuur 3-127 iDRAC Netwerk settings

Vervolgens navigeer je naar Alerts > SNMP and Email Settings. Hier geef je je email adres mee en de naam/IP van de SMTP server. Om te testen of de iDRAC server succesvol mails kan sturen, heb je een test optie.

The screenshot shows the "Destination Email Addresses" section of the iDRAC configuration. It displays a table with four rows, each representing an email alert:

Email Alert Number	State	Destination Email Address	Test Email
Email Alert 1	<input checked="" type="checkbox"/>	<email adres>	<input type="button" value="Send"/>
Email Alert 2	<input type="checkbox"/>		<input type="button" value="Send"/>
Email Alert 3	<input type="checkbox"/>		<input type="button" value="Send"/>
Email Alert 4	<input type="checkbox"/>		<input type="button" value="Send"/>

SMTP (Email) Server Address Settings

The screenshot shows the "SMTP (Email) Server Address Settings" section of the iDRAC configuration. It displays a table with five fields:

Attribute	Value
SMTP (Email) Server IP Address or FQDN / DNS Name	192.168.68.120
Enable Authentication	<input type="checkbox"/>
Username	
Password	
SMTP Port Number	25

Figuur 3-128 iDRAC SMTP Settings

Als dit lukt, is de laatste stap de alerts instellen die je wil ontvangen. In de demo-omgeving zijn de alerts gefilterd tot system health, storage, warning en critical. In de alerts lijst vink je de Email box aan. Dit doe je voor alle pagina's.

Category	Alert	Severity	Email	SNMP Trap	IPMI Alert	Remote System Log	WS Eventing	OS Log	Action
System Health	Amperage	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Amperage	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Auto Sys Reset	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Battery Event	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Battery Event	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Processor	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Processor	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action
System Health	Proc Absent	!	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Action

Figuur 3-129 iDRAC Alerts

Ook hier verstuur je een testmail om te zien of je deze aankrijgt. Onderaan heb je het veld *Test Event*. Hier geef je de event ID mee, deze Id's vind je op de dell.com website. Hieronder zie je de link:

https://www.dell.com/support/manuals/be/nl/bedhs1/dell-opnmang-sw-v8.1/eemi_13g_v1.2-v1/pdr-event-messages?guid=guid-53260e23-fd91-4ccf-8846-5d68f7eb36c4&lang=en-us

Figuur 3-130 iDRAC Alert Mail

3.4 Powershell

Powershell is een ingebouwde command line van windows en is een populaire tool voor IT departementen om taken te automatiseren. Powershell gebruik je om de verschillende 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 doe je 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

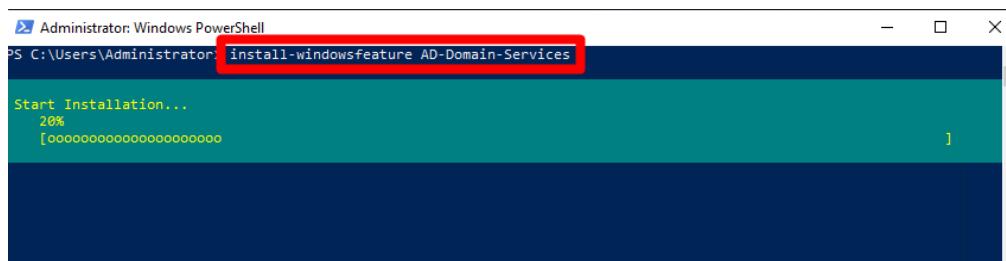
IPAddress      : 192.168.68.60
InterfaceIndex : 4
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type           : Unicast
PrefixLength   : 23
PrefixOrigin    : Manual
SuffixOrigin    : Manual
AddressState   : Tentative
ValidLifetime  : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite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

Figuur 3-131 New IP Address

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.



Figuur 3-132 Install Role

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

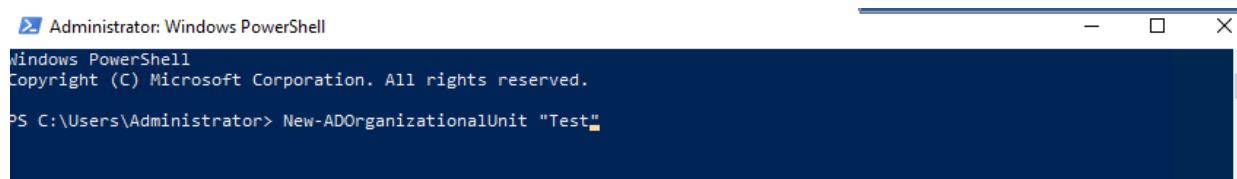
```
Install-ADDSForest
- CreateDnsDelegation:$false
- DatabasePath "C:\Windows\NTDS"
- DomainName "powershell.com"
- DomainNetbiosName "POWERSHELL"
- InstallDns:$true
- LogPath "C:\Windows\NTDS"
- NoRebootOnCompletion:$false
- SysvolPath "C:\Windows\SYSVOL"
- Force:$true
```

Figuur 3-133 *Install Forest (promote server)*

Na het vorige commando zal de server automatisch herstarten.

Vervolgens kan je de structuur van het domein opzetten.

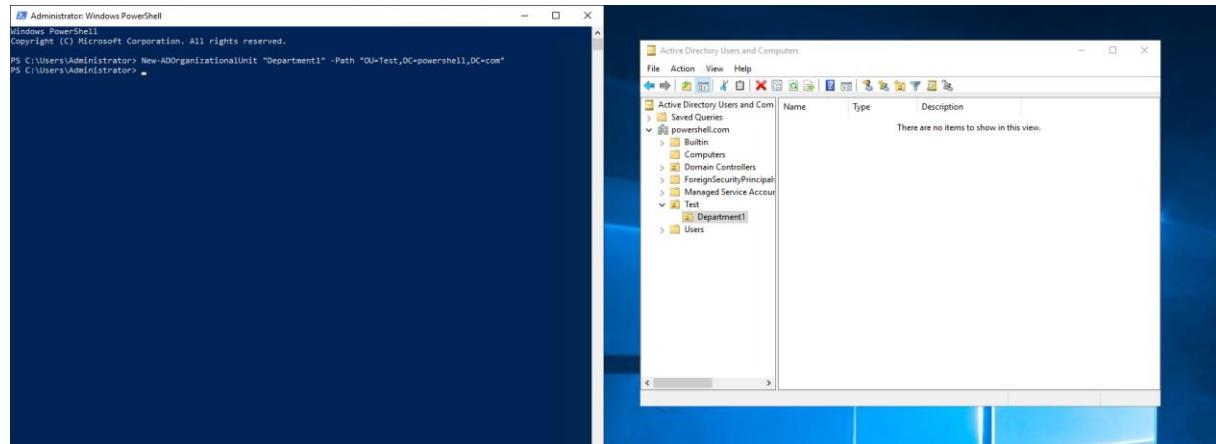
Om een organizational unit (OU) toe te voegen, gebruik je volgend commando; *New-ADOrganizationalUnit*. Zonder de -path parameter zal deze in de root OU gezet worden.



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

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

Figuur 3-134 *New Organizational Unit*



Figuur 3-135 *Setup AD Structure*

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

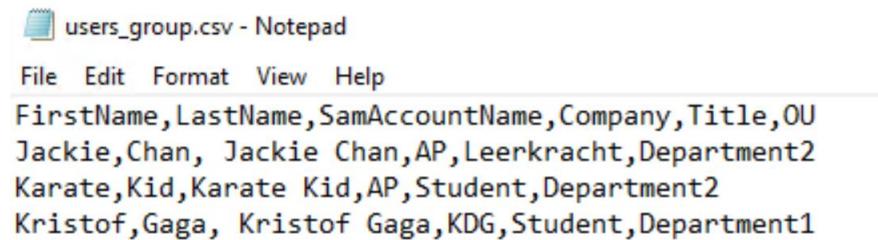
- Name
- GroupCategory (distribution / security)
- GroupScope (local / global / universal)

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 maak je de gebruikers aan. Deze plaats je in een security group en in de correcte organizational unit. 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.



The screenshot shows a Notepad window with the title "users_group.csv - Notepad". The menu bar includes File, Edit, Format, View, and Help. The content of the file is a CSV (comma-separated values) file with the following data:

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

Figuur 3-136 Comma Separated Value File

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 "AB"){
31         Add-ADGroupMember -Identity AB -Members $user.SamAccountName
32     }
33
34     if ($user.Company -like "KDG"){
35         Add-ADGroupMember -Identity KDG -Members $user.SamAccountName
36     }
37     ...
38 }
```

Figuur 3-137 AD User Script

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, verwijder je die nu. 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>
```

Figuur 3-138 DNS Forwarders

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]:
```

Figuur 3-139 Set DNS Server

4 Besluit

Het begin van de stage verliep wat moeizaam, omdat ik geen voorkennis had van serverbeheer. Met het nodige opzoekwerk, kwam het project stilaan op gang. Sommige toepassingen waren wat moeilijker op te zetten dan anderen, maar uiteindelijk was de serveromgeving helemaal uitgerold. De omgeving telt 15 toepassingen die op de dag van vandaag gevraagd worden door klanten.

De stage zelf heb ik als zeer positief ervaren. Er was een aangename werksfeer en het personeel was bereid om me te helpen in nood. Na een paar weken kwam ik tot de conclusie dat ik verder wil gaan met deze technologieën wanneer ik ben afgestudeerd.

5 Bibliografie

5.1 Gevolgde tutorials

- Technet Microsoft – Active Directory (<https://blogs.technet.microsoft.com/uktechnet/2016/06/08/setting-up-active-directory-via-powershell/>)
- Toddklindt – Scripting (<https://www.toddklindt.com/blog/Lists/Posts/Post.aspx?ID=747>)
- Jasoncoltrin – Timeserver (<https://jasoncoltrin.com/2018/08/02/how-to-set-clock-time-on-ad-domain-controller-and-sync-windows-clients/>)

5.2 Geraadpleegde bronnen

- Cisco (<https://community.cisco.com/t5/technology-and-support/ct-p/technology-support>)
- Spiceworks (<https://community.spiceworks.com/>)
- Wikipedia (<https://www.wikipedia.com>)
- Citrix (<https://www.citrix.com/support/>)
- Microsoft (<https://docs.microsoft.com>)
- Youtube (<https://www.youtube.com>)

6 Verklarende woordenlijst

Citrix

Citrix is een technologie die je gebruikt 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 (werknelmers 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.

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. Deze adressen blijven herbruikbaar als een computer wordt uitgeschakeld.

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.

DNS

DNS regelt de netwerkconfiguratie. Deze zet IP-adressen om naar namen en omgekeerd. Zo hoef je geen IP-adressen van de servers te onthouden, maar maak je gebruik van de servernamen.

Domaincontroller

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

Fileserver

Een fileserver biedt de mogelijkheid om 1 of meerdere gedeelde netwerkfolders te configureren. Dit is handig om bestanden uit te wisselen tussen gebruikers en het vergemakkelijkt het back-uppen van de data.

Group policies

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

iDRAC

De iDRAC (*Dell Remote Access Controller*) is een management tool om servers vanop 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.

Netscaler

De *netscaler* is een toepassing die je gebruikt 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.

Printserver

De printserver stelt de beschikbare printers in het domein op het netwerk aan de gebruikers beschikbaar. Dit biedt de mogelijkheid aan iedereen die op het domein zit om van alle printers gebruik te maken. De printserver zorgt ook voor de installatie van de noodzakelijke printerdrivers.

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.

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, stel je 1 fysieke server in als een replica server. Dit betekent dat je VM's "kopiert" 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.

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.

SMTP

Simple Mail Transfer Protocol, afgekort SMTP gebruik je om e-mails te versturen over het internet. SMTP gebruikt TCP-poort 25 voor de communicatie tussen de SMTP-servers.

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.

VPN

VPN of *Virtual Private Network* is een privé netwerk binnen een groter netwerk. Hiermee maak je onder andere een connectie naar de netwerkomgeving van de demo-omgeving.

WSUS

Windows Server Update Services, afgekort WSUS is een programma dat administrators vaak gebruiken om apparaten up to date te houden in een netwerk. Dit programma is te installeren op een server die dan zal dienen als een update uitdeler. De server haalt automatisch updates van de Microsoft update website om die in het netwerk uit te delen aan computers, servers, ...

7 Lijst van figuren

Figuur 2-1 Infrastructuurdesign.....	7
Figuur 2-2 Netwerkdesign.....	8
Figuur 3-1 RAID Config.....	9
Figuur 3-2 iDRAC Config.....	10
Figuur 3-3 iDRAC Browser.....	10
Figuur 3-4 iDRAC Media	11
Figuur 3-5 Boot Mode.....	12
Figuur 3-6 Access-Lists.....	13
Figuur 3-7 Static Routes.....	13
Figuur 3-8 VLAN's.....	14
Figuur 3-9 Routing	15
Figuur 3-10 Port-Channels.....	15
Figuur 3-11 DMZ VLAN.....	15
Figuur 3-12 NIC-Teaming.....	16
Figuur 3-13 NIC-Teaming Config.....	16
Figuur 3-14 VM's Server1	17
Figuur 3-15 VM's Server2.....	17
Figuur 3-16 VM's Server3.....	17
Figuur 3-17 Domaincontroller.....	18
Figuur 3-18 Promote DC Role.....	18
Figuur 3-19 DC Prerequisites Check	19
Figuur 3-20 AD-Structuur	20
Figuur 3-21 AD Security-Groups.....	20
Figuur 3-22 Back-up DC.....	21
Figuur 3-23 Time Integration Service.....	22
Figuur 3-24 Tijdserver.....	22
Figuur 3-25 Delay.....	22
Figuur 3-26 Group policies.....	24
Figuur 3-27 Disable changing home page settings	25
Figuur 3-28 chrome.admx.....	26
Figuur 3-29 PolicyDefinitions.....	26
Figuur 3-30 chrome.adml	27
Figuur 3-31 PolicyDefinitions taal folder.....	27
Figuur 3-32 URLs to open on startup.....	28
Figuur 3-33 Transfer folder	29
Figuur 3-34 Drive Maps GPO.....	30
Figuur 3-35 Drive Maps Config	30
Figuur 3-36 Drive Maps Result.....	31
Figuur 3-37 DNS Forwarders	32
Figuur 3-38 DNS Servers	33
Figuur 3-39 Autorisatie.....	34
Figuur 3-40 Scope Name	34
Figuur 3-41 IP-range.....	35
Figuur 3-42 IP-Exclusions.....	35
Figuur 3-43 Add Port	36
Figuur 3-44 printer IP.....	37
Figuur 3-45 Device Type.....	37
Figuur 3-46 Add Printer.....	38

Figuur 3-47 Select Driver.....	39
Figuur 3-48 Fileserver.....	40
Figuur 3-49 New Namespace.....	41
Figuur 3-50 Add Namespace Server	41
Figuur 3-51 New Shared Folder.....	42
Figuur 3-52 Folder Permissions.....	42
Figuur 3-53 Fileserver Path.....	43
Figuur 3-54 Fileserver Folder.....	43
Figuur 3-55 New Replication Group	43
Figuur 3-56 Replication Topology	44
Figuur 3-57 Folders To Replicate.....	44
Figuur 3-58 Citrix	45
Figuur 3-59 Specifieer Delivery Controller.....	46
Figuur 3-60 Machine Catalog.....	47
Figuur 3-61 Applications.....	47
Figuur 3-62 StoreFront Servers	48
Figuur 3-63 StoreFront URL.....	48
Figuur 3-64 StoreFront Link	48
Figuur 3-65 StoreFront Delivery Controller.....	49
Figuur 3-66 StoreFront Login Pagina.....	49
Figuur 3-67 VEEAM.....	50
Figuur 3-68 Backup Infrastructure.....	50
Figuur 3-69 Add VM's To Backup	51
Figuur 3-70 Backup Simulation.....	52
Figuur 3-71 Backup Type and Schedule	53
Figuur 3-72 Backup Report.....	54
Figuur 3-73 Repliaction.....	55
Figuur 3-74 Definieer Replica Server.....	56
Figuur 3-75 Replication Synchronisatie.....	56
Figuur 3-76 Enable Replica Server	57
Figuur 3-77 DMZ	58
Figuur 3-78 VLAN identificatie.....	59
Figuur 3-79 DMZ Access-list.....	59
Figuur 3-80 LAN Test.....	60
Figuur 3-81 DMZ Test.....	60
Figuur 3-82 NetScaler.....	61
Figuur 3-83 NetScaler Virtual Appliance	61
Figuur 3-84 NetScaler Netwerk Configuratie.....	62
Figuur 3-85 NetScaler Config.....	62
Figuur 3-86 Root RSA Key	63
Figuur 3-87 Root CSR	64
Figuur 3-88 Root Certificaat.....	64
Figuur 3-89 Server Certificaat	65
Figuur 3-90 Link Server Certificaat.....	65
Figuur 3-91 NetScaler Download config.....	65
Figuur 3-92 Citrix NetScaler Gateway.....	66
Figuur 3-93 Citrix NetScaler URL.....	66
Figuur 3-94 Citrix STA Server	66
Figuur 3-95 Citrix NetScaler Authenticatie.....	67
Figuur 3-96 Citrix NetScaler Remote Access	67

Figuur 3-97 Citrix StoreFront Access.....	68
Figuur 3-98 Hosts bestand.....	68
Figuur 3-99 NetScaler Login Pagina.....	69
Figuur 3-100 Azure AD Connect.....	70
Figuur 3-101 Azure AD Domain.....	70
Figuur 3-102 Verify Domain.....	71
Figuur 3-103 Custom Domain.....	71
Figuur 3-104 Add UPN Suffix.....	72
Figuur 3-105 Azure AD Verified Domain.....	72
Figuur 3-106 Azure AD Users.....	73
Figuur 3-107 Single Sign-on	73
Figuur 3-108 Azure Multi-factor Authenticatie	74
Figuur 3-109 Multi-Factor Setting.....	75
Figuur 3-110 Multi-Factor Type	75
Figuur 3-111 WSUS	76
Figuur 3-112 WSUS Setup	77
Figuur 3-113 yunchronisatie.....	77
Figuur 3-114 WSUS GPO's	78
Figuur 3-115 Specify Intranet Microsoft update service location.....	79
Figuur 3-116 Turn off auto-restart for updates during active hours	80
Figuur 3-117 Automatic Updates detection frequency	81
Figuur 3-118 Configure Automatic updates	81
Figuur 3-119 GPO Groepen.....	82
Figuur 3-120 Running Synchronization.....	83
Figuur 3-121 Synchronization Status.....	83
Figuur 3-122 SMTP Role.....	84
Figuur 3-123 SMTP IP Address.....	84
Figuur 3-124 SMTP Connection Config.....	85
Figuur 3-125 Authomatic Service Startup.....	85
Figuur 3-126 Test Mail.....	86
Figuur 3-127 iDRAC Netwerk settings	87
Figuur 3-128 iDRAC SMTP Settings.....	87
Figuur 3-129 iDRAC Alerts	88
Figuur 3-130 iDRAC Alert Mail	88
Figuur 3-131 New IP Address	89
Figuur 3-132 Install Role	89
Figuur 3-133 Install Forest (promote server)	90
Figuur 3-134 New Organizational Unit	90
Figuur 3-135 Setup AD Structure.....	90
Figuur 3-136 Comma Separated Value File.....	91
Figuur 3-137 AD User Script	92
Figuur 3-138 DNS Forwarders.....	92
Figuur 3-139 Set DNS Server.....	92