

EINDPROJECT: NV-POC



erasmus
HOGESCHOOL BRUSSEL

NV POC

1. Analyse van NV-POC	5
1.1 Inleiding.....	5
1.2 Analyse benodigdheden klant.....	5
1.2.1 Behoeften NV-POC.....	5
1.3 Netwerk Topologie.....	6
1.3.1 Addressing Table.....	6
1.4 Hardware.....	7
1.4.1 Firewall.....	7
1.4.2 Switches	8
1.4.3 Acces Points	10
1.4.4 NAS.....	11
1.4.5 UPS	12
1.4.6 ISP.....	14
1.5 Servers.....	15
1.5.1 On Premise vs Cloud	15
1.5.2 Lenovo ThinkSystem SR650	16
1.6 Licenties.....	17
1.6.1 VMware VShpere Essential Kit.....	17
1.6.2 Microsoft 365	17
1.6.3 Windows Server	18
1.6.4 Azure Servers.....	19
1.7 Kosten	20
2. On premise.....	22
2.1 Firewall Fortigate 100 ^E	22
2.1.2 interfaces	23
2.1.3 Static Routes	27
2.1.4 Policies	28
2.1.5 Virtual IP.....	32
2.1.6 VPN.....	32
2.1.7 security profiles.....	34
2.2 Switch.....	35
2.3 Virtuele machines	36
2.4 Domain Controller 1.....	37
2.4.1 Active Directory.....	37
2.4.2 GPO's.....	41
2.4.3 DNS.....	42
2.5 Printer server	43

2.6 Webserver.....	44
2.6.1 Ubuntu Linux.....	44
2.6.2 Portainer.io	44
2.6.3 Domain name	45
2.6.4 CloudFlare DNS records	45
2.6.5 Nginx Proxy manager	46
2.6.6 WordPress.....	49
2.6.7 Website	50
2.7 RD gateway server	51
2.8 TrueNAS	57
2.9 Windows Client	61
2.10 Radius Server	62
3. Cloud	63
3.1 Azure	63
3.1.1 Terraform	63
3.1.2 Virtual Network.....	67
3.1.3 Virtual Network Gateway.....	67
3.1.4 Local Network Gateway	67
3.1.5 Connection	68
3.1.6 Tunnel in Firewall (on premise)	68
3.1.7 Adresses in Firewall (on Premise)	68
3.1.8 Policies in Firewall (on Premise)	69
3.1.9 Static route in Firewall (on Premise).....	70
3.1.10 Domain Controller 2.....	71
3.1.11 Microsoft Defender for cloud	74
3.2 Microsoft.....	75
3.2.1 Intune	75
3.2.2 Domeinnaam toevoegen.....	76
3.2.3 AD Connect	77
3.2.4 Licenties	82
3.3.5 Microsoft Teams	84
3.3.6 Microsoft Defender.....	85
3.3.7 Microsoft Exchange.....	86
3.3.8 Defender voor Virtuele Machine	87
4. Back-ups	89
4.1 Local Backup.....	89
4.2 Cloud backup.....	90

5. Zelfreflecties.....	95
5.1 Zelfreflectie Zacharias Osselaer	95
5.2 Zelfreflectie Soufyan Naimi.....	96
5.3 Zelfreflectie Yusuf Coban	97

1. Analyse van NV-POC

1.1 Inleiding

We werden gevraagd om een volledige vervanging te doen van de IT-infrastructuur van NV-POC, die een aankomende online webshop willen launchen. Hierbij geven ze aan dat ze zich meer en meer willen inzetten in de digitale wereld. We hebben ons voorstel ontwikkeld gezien de verwachte groei- en expansiemogelijkheden.

1.2 Analyse benodigdheden klant

Om een effectieve oplossing te bieden, hebben we grondig de behoeften van NV-POC geanalyseerd. Dit omvatte een diepgaand begrip van hun huidige IT-infrastructuur, operationele processen en specifieke vereisten met betrekking tot de webshop. Onze aanpak is erop gericht om niet alleen aan de huidige behoeften te voldoen, maar ook om flexibiliteit te bieden voor toekomstige groei.

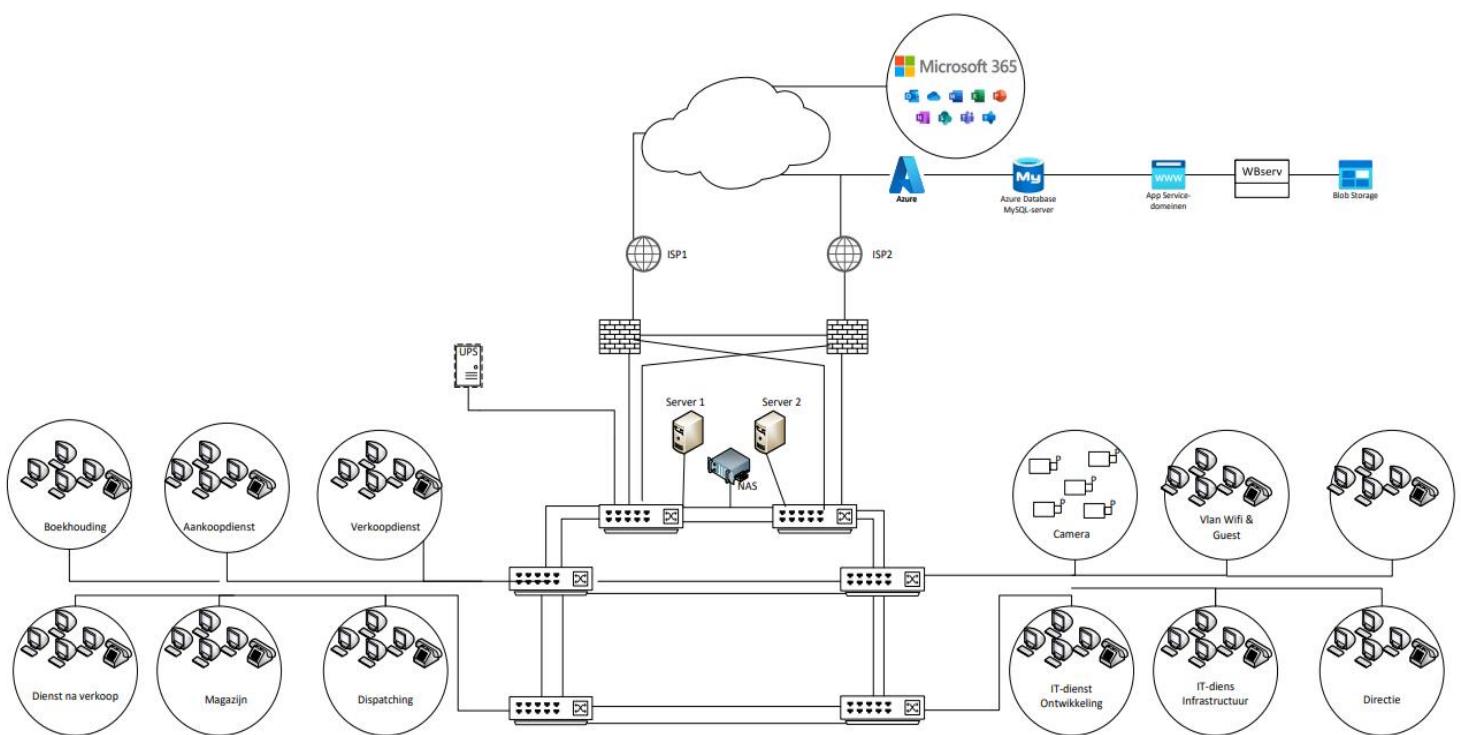
1.2.1 Behoeften NV-POC

Dit zijn de behoeften van onze klant:

- 32 eindgebruikers
- 100Mbps aan de eindgebruikers kunnen leveren
- 2 wifi SSID's (personeel/gast)
- Gasten hebben internet-toegang → niet aan eigenlijke bedrijfsnetwerk
- Sociale media zijn uitgeschakeld voor het personeel, behalve voor verkoop
- Voldoende redundantie
- Proxy/Firewall
- LAN
- DMZ

1.3 Netwerk Topologie

Onze voorgestelde netwerk topologie is ontworpen om een veilige, snelle en betrouwbare communicatie te waarborgen tussen alle systemen en gebruikers. We hebben aandacht besteed aan beveiligingslagen en redundantie om de integriteit van het netwerk te waarborgen.



1.3.1 Addressing Table

afdeling	VLAN Naam	VLAN	Network address	Mask	First IP range	Last IP range
Boekhouding	VLAN_Boekhouding	10	172.16.10.X	/24	172.16.10.1	172.16.10.254
Aankoopdienst	VLAN_Aankoopdienst	20	172.16.20.X	/24	172.16.20.1	172.16.20.254
Verkoopdienst	VLAN_Verkoopdienst	30	172.16.30.X	/24	172.16.30.1	172.16.30.254
Dienst Na verkoop	VLAN_DienstNaVerkoop	40	172.16.40.X	/24	172.16.40.1	172.16.40.254
Magazijn	VLAN_Magazijn	50	172.16.50.X	/24	172.16.50.1	172.16.50.254
Dispatching	VLAN_Dispatching	60	172.16.60.X	/24	172.16.60.1	172.16.60.254
IT-dienst Infrastructuur	VLAN_Infrastructuur	70	172.16.70.X	/24	172.16.70.1	172.16.70.254
IT-dienst Ontwikkeling	VLAN_Ontwikkeling	80	172.16.80.X	/24	172.16.80.1	172.16.80.254
Directie	VLAN_Directie	90	172.16.90.X	/24	172.16.90.1	172.16.90.254
Raad Van bestuur	VLAN_Bestuur	100	172.16.100.X	/24	172.16.100.1	172.16.100.254
personeel WIFI	VLAN_Personeel	110	10.10.0.X	/21	10.10.0.1	10.10.7.254
personeel Guest	VLAN_Guest	120	10.10.8.X	/21	10.10.8.1	10.10.15.254
Server	VLAN_server	130	10.10.16.X	/24	10.10.16.1	10.10.16.254
Camera	VLAN_Camera	140	10.10.17.X	/24	10.10.17.1	10.10.17.254
DMZ	Geen		10.10.10.X	/24	10.10.10.1	10.10.10.254

1.4 Hardware

Het aanschaffen van hardware is een belangrijke stap voor bedrijven en individuen die op zoek zijn naar een effectieve IT-infrastructuur. Dit is een essentiële rol in de stap naar een succesvol bedrijf. Dit is wat wij zouden aankopen om dit waar te maken.

1.4.1 Firewall

Wij hebben gekozen om 2 firewalls aan te kopen en deze ook te gebruiken als Router. Dit omdat je dan verkeer kunt filteren op basis van poortnummers, IP-adressen en protocollen. Dit voorkomt ongeautoriseerde toegang tot het intern netwerk en beschermt tegen cyberaanvallen.

1.4.1.1 Fortinet FortiGate 80F Firewall



<https://licensewise.nl/products/fortigate-80f>

specificaties:

- 8x Gigabit switch poorten
- 2x Gigabit RJ45/SFP Shared Media poorten
- Firewall performance: 10 Gbps
- IPS throughput: 1.4 Gbps (HTTP / enterprise mix)
- NGFW throughput: 1 Gbps
- New sessions per second (TCP): 45.000
- Concurrent sessions (TCP): 1.500.000

Prijs:

Prijs exclusief BTW: € 1356,25 x 2 = €2712,50

1.4.1.2 Fortigate UTP bundel

Unified Threat Protection

De meest gekozen FortiGuard bundel voor FortiGate firewalls (voorheen UTM). Geschikt voor alle organisaties die, naast de beveiliging van de ATP bundel, ook Web filtering voor het beveiligen en beperken van het webverkeer en/of een FortiGuard Antispam willen gebruiken. Deze gaan we jaarlijks moeten betalen voor elke Firewall.

Prijs exclusief BTW: €923,03 x 2 = €1846,06

1.4.2 Switches

Een switch is een apparaat in computernetwerken dat gegevenspakketten efficiënt doorstuurt tussen apparaten binnen een lokaal netwerk. In tegenstelling tot hubs gebruikt een switch MAC-adressen om gegevens gerichter te verzenden, wat de netwerkprestaties verbetert. Switches zijn essentieel voor het opzetten van stabiele en snelle netwerken in zowel thuis- als zakelijke omgevingen. Ze worden gebruikt om het verkeer te beheren en communicatie tussen apparaten te optimaliseren. We kiezen hier voor 4 Cisco WS-C2960X-48FPS-L switches en 2 Cisco CBS220-24P-4X switches.

1.4.2.1 Cisco WS-C2960X-48FPS-L



Specificaties:

24 x 10/100/1000 Mb/s Gigabit Ethernet (RJ45) PoE+

24 x 10/100/1000 Mb/s Gigabit Ethernet (RJ45) PoE

4 x 10/100/1000 Mb/s Gigabit SFP (Uplink)

1 x USB-B (Console)

1 x USB-A

1 x Ethernet (RJ45) (Console)

Electrical:

PoE Power budget: 740

Performance:

Forwarding Rate: 107.1 Mpps

Switching Bandwidth: 216 Gb/s

Prijs:

Prijs exclusief BTW: €1860,74 x 4 = €7442,96

License van Switch: 4 x €523,65 = €2094,60

<https://maxict.nl/cisco-catalyst-ws-c2960x-48fps-l-netwerk-switch-managed-l2l3-gigabit-ethernet-101001000-power-over-etherne...>

https://www.bhphotovideo.com/c/product/1513477-REG/cisco_wsc2960x48fpsl_catalyst_2960x_48fps_l_etherne...

https://www.bhphotovideo.com/c/product/1513477-REG/cisco_wsc2960x48fpsl_catalyst_2960x_48fps_l_etherne...

<https://maxict.nl/cisco-c2960x-dna-e-48-5y-softwarelicentie-uitbreiding-licentie-5-jaar-p28813358.html>

1.4.2.2 Cisco CBS220-24P-4X Switch



- Switch-laag: Layer 2 (L2)
- Type basis-switching RJ-45 Ethernet-poorten: Gigabit Ethernet (10/100/1000)
- Aantal basis-switching RJ-45 Ethernet-poorten: 24
- MAC-adrestabel: 8192 entries
- Switchingcapaciteit: 128 Gbit/s
- Netwerkstandaard: Ondersteunt verschillende IEEE-standaarden, waaronder IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3u, IEEE 802.3x, IEEE 802.3at, IEEE 802.3z, enz.
- Power over Ethernet (PoE): Ondersteunt PoE, wat betekent dat de switch in staat is om stroom te leveren aan aangesloten apparaten zoals IP-telefoons, camera's, en andere PoE-compatibele apparaten.
- Rack-montage: Het apparaat kan in een rack worden gemonteerd.

Prijs:

Prijs exclusief BTW: € 482,00 x 2 = € 964

https://www.dustin.be/nl/netwerk-switches/cisco/bus-220-smtswitch-24p-ge-poe-4x10g-sfp-plus-art-cbs220-24p-4x-eu-num-12267798?gad_source=1&gclid=CjwKCAiAmZGrBhAnEiwAo9qHififwORG9jYCfaSRuXt4iKfft0VII-9XSp9c4gzQCMRLG8S0FX1uCRoCAu0QAvD_BwE

1.4.3 Acces Points

1.4.3.1 Aruba AP-505 Wifi 6

De Aruba AP-505 is een draadloos accespoint dat we gekozen hebben voor ons project. Het accespoint is ontworpen voor grote bedrijven, met zijn Dual-Band Wifi 6 kan je zowel op 2,4 GHz als 5GHz aan u de keuze. Zeer eenvoudig te installeren en beheren, je kan bovendien via een mobiele app monitoren van op afstand. We hebben dan ook een Aruba Central AP Foundation licentie aangeschaft voor een centraal beheer van 3 jaar.



Specificaties:

- Dual-band WiFi 6 indoor access point
- Doorvoersnelheid tot 574Mbps (2.4GHz) en 1200 Mbps (5 GHz)
- Unified AP: beheer met of zonder controller
- 1x Gigabit LAN-poort met PoE+ (802.3at)
- 1x Gigabit Ethernetpoort
- Zendvermogen: 21dBm en 21dBm (2.4GHz en 5GHz)
- Versterking: 4,9 dBi (2.4 GHz) en 5,7 dBi (5 GHz)
- Beheer via Aruba Central

Prijs:

Prijs AP's exclusief BTW: € 387,00 x 4 = € 1 548,00

Prijs licentie exclusief BTW voor 3 jaar: € 250,00

AP: <https://www.wifishop.nl/aruba-ap-505-rw-indoor-11-ax-wifi-6-access-point/pid=64389>

Licentie: <https://www.routershop.nl/aruba-central-ap-fnd-3yr-sub-e-stu/pid=74453>

1.4.4 NAS

1.4.4.1 Synology DiskStation DS1821+

Voor de opslag hebben we gekozen voor de Synology DiskStation DS1821+. Deze is perfect geschikt voor kleine of middelgrote bedrijven zoals die van ons. Heeft 8 plaatsen voor harde schijven u kan dus naargelang uw bedrijf groeit uw opslag aanpassen aan uw eigen wensen. We hebben tijdelijk 5 HDD van 2TB maar deze kan altijd aangepast worden. We gebruiken deze NAS als storage. We gaan ook gebruik maken van Cloud sync. Dit wil zeggen dat als we onze on-prem NAS gaan connecteren met Azure Blob storage. Dit via het IP-adres van de NAS. En voor de Back-up dit gaan we doen op onze domain controller.

Wij kiezen voor een RAID 6. Het maakt gebruik van dubbele pariteit. Dit betekent dat als er twee harde schijven falen, het zorgt voor een bescherming. De keuze om RAID 6 te gebruiken in plaats van RAID 5 is omdat RAID 6, het zich meer focust op fouttolerantie. Wij vinden daarom dat deze RAID geschikt is.



Specificaties:

- Processor Model: AMD Ryzen V1500B.
- Processor Snelheid: 2.20 GHz.
- Geheugencapaciteit: 4096 MB.
- Harddisk Bays: 8x 3.5 / 2.5.
- Uitbreidbaar naar 18 schijven met uitbreidingseenheden.
- RAID modi: 0, 1, 10, 5, 6, Basic, JBOD, Synology Hybrid RAID.
- Energieverbruik: 26.18, 59.8 (Access) Watt.

Prijs:

Prijs exclusief BTW: € 891,74

Harde schijven van 2TB : € 21,99 x 5 = € 109,95

Totaal : € 891,74 + € 109,95 = € 1 001,69

1.4.5 UPS

Voor u een UPS aanschaft, is het belangrijk om de power consumptie te weten. Het is een apparaat dat wordt beschermd tegen stroomuitval. Wij gaan enkel de belangrijkste hardware op de UPS aansluiten. Zodat gevoelige hardware veilig blijft. Voor dat je een UPS aankoopt moet je wel eerst weten wat er op verbonden wordt en hoeveel deze ook verbruiken.

Power consumption:

- Fortigate 80F: 16 Watt
- Lenovo Thinksystem SR650: 340 Watt
- Cisco Catalyst WS-C2960X-48FPS-L: 149 Watt x 4 = 594 Watt
- Cisco CBS220-24P--4X: 195 Watt x 2 = 390 Watt
- Synology Diskstation DS1821+ = 60 Watt
- Totaal = 1400 Watt + 30%(marge) = 1820 Watt

De UPS die we gaan kopen moet 1820 Watt kunnen leveren.

1.2.5.1 APC Smart-UPS 2200VA LCD RM 2U 230V



Capaciteit:

- 2200 VA / 1980 Watt
- Nominale uitgangsspanning: 230V

Uitgangsaansluitingen:

- (8) IEC 320 C13
- IEC 320 C19

We gaan een adapter gebruiken omdat onze uitgangsaansluiting niet voldoet aan de Europese normen.

Input:

- Nominale invoerspanning: 230V

Batterijen:

- Typische oplaadtijd: 3 uur

Kenmerken:

- Automatische zelftest
- Koude start mogelijk
- Aanpasbare gevoeligheid voor spanning
- Hoorbare alarmen
- Beheerbaar via het netwerk
- Voorspellende foutmelding

Prijs: €1598,27

Garantie:

3 jaar reparatie of vervanging (exclusief batterij) en 2 jaar voor de batterij

<https://www.redshell.nl/apc-smart-ups-smt2200rmi2uc-noodstroomvoeding-8x-c13-1x-c19-usb-rack-mountable-smartconnect-2200va/>

1.4.6 ISP

Wij hebben besloten om gebruik te maken van twee verschillende Internet Service Providers (ISP): Telenet en Proximus. Het doel van deze aanpak is om de betrouwbaarheid en stabiliteit van uw internetverbinding te verbeteren. Door twee vertrouwde providers te gebruiken, creëert u redundantie zodat de connectiviteit behouden blijft, zelfs als één provider uitvalt of tijdelijk niet beschikbaar is.

1.4.6.1 Proximus

Internet Pro+

Meer mogelijkheden met een vast IP-adres

- Tot 100 Mbps download en tot 40 Mbps upload
- 1 vast IP-adres en router inbegrepen
- Onbeperkt maandelijks datavolume
- Geïntegreerde firewall
- Herstelling binnen 5 werkdagen

€ 99/maand

Contacteer mij 

[Opties](#)

1.4.6.2 Telenet

Business Fibernet

- 10 @telenet.be mailboxen
- Gratis installatie t.w.v. € 70,25
- Supersnelle internetverbinding*
- Onbeperkt datavolume
- Variabel IP adres (vast mogelijk)

500 Mbps max. downloadsn snelheid
30 Mbps max. uploadsn snelheid

vanaf **€58,88** per maand

[Bestellen](#)

 **Vast IP-adres**

€ 28,00 /maand

Voordelen van een Vast IP-adres:

- Een mailserver of eigen website voor je bedrijf
- Videobewaking vanop afstand

Van zodra je abonnement is geïnstalleerd kan u het **Vast IP-adres activeren** via Mijn Telenet.

1.5 Servers

1.5.1 On Premise vs Cloud

Het kiezen tussen on-premises en Cloud infrastructuur is een belangrijke beslissing voor bedrijven. Deze keuze heeft veel impact op de schaalbaarheid, kosten en de flexibiliteit. Hier gaan we volgens de noden van het bedrijf analyseren wat de beste verdeling is.

Domain Controller I (DC1)	On premise
Domain Controller II (DC2)	On premise
Webserver	Cloud
DNS	On premise
Email	Cloud
Web	Cloud
DHCP	On premise
NAS	On premise
File server	On premise

- 1ste Domain Controllers en DNS zetten we op On premise, deze biedt directe controle over de beveiliging van deze kritieke infrastructuurcomponenten en zorg voor een lage latency.
- 2de Domain Controller gaan we op de Cloud doen. Dit helpt voor de schaalbaarheid, veiligheid en redundantie.
- Email is op de Cloud omdat Microsoft Cloudbaseerde oplossing geeft, deze gaan we ook implementeren.
- Web gaan we via Azure doen, omdat we bij het aanmaken van een webserver een database bij krijgen.
- DHCP On premise omdat het sneller en veiliger is.
- NAS On premise voor veiligheid en efficiëntie.
- File server on premise gebruiken we voor veiligheid en biedt makkelijke controle over data.

1.5.2 Lenovo ThinkSystem SR650

Als server voor ons bedrijf hebben we gekozen voor de Lenovo ThinkSystem. De keuze tussen on-Premises en Cloud gebaseerde servers hangt af van de specifieke behoeften van de organisatie. Wij kiezen hier voor een fysieke server omdat dit ons voordeliger lijkt voor het bedrijf. We gaan 2 servers aan kopen en gebruik maken van Load Balancing. Dit zorgt ervoor dat prestatie omhooggaat, omdat taken worden verdeeld over onze 2 servers.



Specificaties:

- *Processoren:* Max. 2 tweede generatie Intel® Xeon® Platinum-processoren, maximaal 205W
- *Geheugen:* Max. 7.5 TB in 24x DIMM-slots met 128GB DIMM's en Intel® Optane™ DC Persistent Memory; 2666MHz/2933MHz TruDDR4
- Ondersteuning van HBA/RAID:HW RAID (max. 24-poorts) met flash-cache; max. 16-poorts HBA's
- *Netwerkinterface:* 2/4-poorts 1GbE LOM; 2/4-poorts 10GbE LOM (Base-T of SFP+); 1x dedicated 1GbE-beheerpoort
- *Voeding:* 2X hot-swap/redundant: 550W/750W/1100W/1600W 80 PLUS Platinum; of 750W 80 PLUS Titanium; of -48V DC 80 PLUS Platinum
- *Ondersteunde besturingssystemen:* Microsoft, Red Hat, SUSE, VMware.

Ga naar lenovopress.com/osig voor meer informatie.

Prijs:

Prijs exclusief BTW: € 2.129,72 x 2 = €4.259,44

Harde schijven van 2TB : 2x (€ 21,99 x 3) = € 131,94

https://www.senetic.be/product/7X06AOPSEA?srsltid=AfmBOoqQW58BgMtGJy3EXLnYzjp8LHnpy8-AOg9_v2N0PFvd6NcOLJCRimg

1.6 Licenties

1.6.1 VMware VShpere Essential Kit

Voor onze VM hebben we VMware VShpere Essential Kit gekozen, met deze kit hebben we recht tot 6 CPU licenties. Aangezien onze servers twee CPU hebben (2CPU x 2 servers) gaan we enkel 1 licentie nodig hebben.

Prijs: **€ 535,35/jaar**

<https://store-us.vmware.com/vmware-vsphere-essentials-kit-5653279100.html>

1.6.2 Microsoft 365

We moeten voor elke persoon in het bedrijf een Microsoft 365 licentie aankopen. Hierbij kiezen wij voor Microsoft 365 E3. Deze licentie bevat alles wat de werkgever/werknemer nodig heeft.

Prijs:

€ 35,70 x 32 users = € 1142,40

Microsoft 365 E3 EEA (no Teams)

35,70 € gebruiker/maand
(jaarabonnement)

De prijs is exclusief btw.

[Neem contact op met de verkoopafdeling](#)

Probeer het één maand gratis uit >

Bekijk de voorwaarden van de proefversie >

Meer informatie >

✓ Microsoft 365 apps voor desktops en mobiele apparaten

✓ Windows voor ondernemingen

✓ 1TB cloudopslag

✓ Belangrijke mogelijkheden voor beveiliging en identiteitsbeheer

Inbegrepen apps en services

The screenshot shows a grid of Microsoft 365 app icons, including Word, Excel, PowerPoint, Windows, Outlook, Exchange, SharePoint, OneNote, OneDrive, Microsoft Stream, Microsoft Bookings, Microsoft Publisher, Microsoft Access, Microsoft Engage, Microsoft Insights, Microsoft Lists, Microsoft Forms, Microsoft Sway, Microsoft Visio, Microsoft Power Apps, Microsoft Power Automate, Microsoft Planner, Microsoft To Do, and Microsoft Loop. Below the grid is a small watermark that says 'Clipchamp'.

1.6.3 Windows Server

Windows Server 2022-editie	Ideaal voor	Licentiemodel	CAL-vereisten ^[1]	Geadviseerde verkoopprijs (MSRP) ^[4]
Datacenter ^[2]	Hooggevirtualiseerde datacenters en cloudomgevingen	Core-basis	Windows Server CAL	\$ 6.155
Standard ^[2]	Fysieke of minimaal gevirtualiseerde omgevingen	Core-basis	Windows Server CAL	\$ 1069
Essentials	Kleine bedrijven met maximaal 25 gebruikers en 50 apparaten	Speciale servers (serverlicentie) ^[3]	Geen CAL vereist	\$ 501

Via de site van Microsoft hebben wij besproken welke server het beste gaat zijn voor het bedrijf. We kiezen hier om de standard Edition te kopen.

Kenmerken:

- **Gebruikersinterface:** Windows Server 2022 heeft doorgaans een grafische gebruikersinterface (GUI) vergelijkbaar met de Windows-desktopomgeving.
- **Serverrollen en -functies:** Standaard edities ondersteunen meestal verschillende serverrollen en -functies, waaronder Active Directory, DNS, DHCP, bestandsservices, webserver (IIS), Hyper-V, en meer.
- **Beveiliging:** Verbeterde beveiligingsfuncties, waaronder Windows Defender Antivirus, BitLocker-drive-encryptie en Windows Defender Firewall.
- **PowerShell:** Krachtige PowerShell-scripts en automatiseringsmogelijkheden voor systeembeheerders.

Prijs exclusief btw: € 722,11 x 2 = € 1444,22

https://www.reichelt.com/nl/nl/software-windows-server-2022-standaard-16-kernen-en--ms-p73-08328-p311982.html?utm_source=psuma&utm_medium=tweakers.nl&PROVID=2845

1.6.4 Azure Servers

1.6.4.1 Webserver

We hebben gezegd dat we onze Webserver on Cloud gingen doen. Een webserver opzetten in Microsoft Azure biedt de mogelijkheid om webapplicaties te hosten op een schaalbare, veilige en betrouwbare Cloud infrastructuur.

Wij kiezen voor Linux VM, zodat we Docker containers er op kunnen laten draaien.

Specificaties:

- Oracle Linux 8.8 (LVM) - Gen2
- 4 CPU Cores
- 16GB RAM
- 128GB SSD

Prijs: **146.39 euro/maand**

1.6.4.2 Active Directory server

Aangezien we 1 Domain Controller on Cloud gaan gebruiken, hebben we een Windows server 2022 VM aangekocht.

Specificaties:

- Windows Server 2022 Datacenter: Azure Edition Hotpatch - Gen2
- 4 CPU Cores
- 16GB RAM
- 128GB SSD

Prijs: **123.13 euro/maand**

1.6.4.3 MySQL Database

De website van NVPOC heeft een database nodig voor zijn bestellingen. Hierbij gaan we via Azure een database kopen.

Specificaties:

- 16GB
- ZRS

Prijs: 0.2496 euro/GB * 16GB /maand = **3.99 euro/maand**

1.6.4.4 Blob Storage

We gaan Blob storage gebruiken als back-up voor onze NAS. Blob storage is perfect bruikbaar als back-up, omdat het veel data kan oplagen. Zoals eerder vermeld maken we hier gebruik van Cloud Sync.

Prijs: 0,00911 euro/GB * 10000GB = **91,10 euro/maand**

Prijzen hebben we berekend via <https://portal.azure.com/>.

1.7 Kosten

EENMALIGE KOSTEN

	stuks	prijs/stuk	prijs/totaal
Fortigate 80F	2	1.356,25 €	2.712,50 €
Cisco CBS220-24P-4X	2	482,00 €	964,00 €
Cisco Catalyst WS-C2960X-48FPS-L	4	1.860,74 €	7.442,96 €
Aruba AP-505 Wifi 6	4	387,00 €	1.548,00 €
Synology DiskStation DS1821+	1	891,74 €	891,74 €
Western Digital WD Red Pro 3.5" NAS 2TB	11	21,99 €	241,89 €
Lenovo Thinksystem SR650	2	2.129,72 €	4.259,44 €
APC Smart-UPS 2200VA LCD RM 2U 230V	1	1.598,27 €	1.598,27 €
Windows Server 2022 Standard	2	722,11 €	1.444,22 €

totaal excl. BTW
BTW 21%

Totaal incl. BTW **25.534,65 €**

JAARLIJKSE KOSTEN

	Stuks	Prijs/stuk	Prijs/jaar
Fortigate UTP bundel	2	923,03 €	1.846,06 €
Access Point Licentie	4	83,33 €	333,32 €
VMware VShpere Essential Kit	1	535,35 €	535,35 €
Cisco C2960X-DNA-E-48-5Y	4	523,65 €	2.094,60 €
	Totaal ind. BTW		4.809,33 €

MAANDELIJKSE KOSTEN

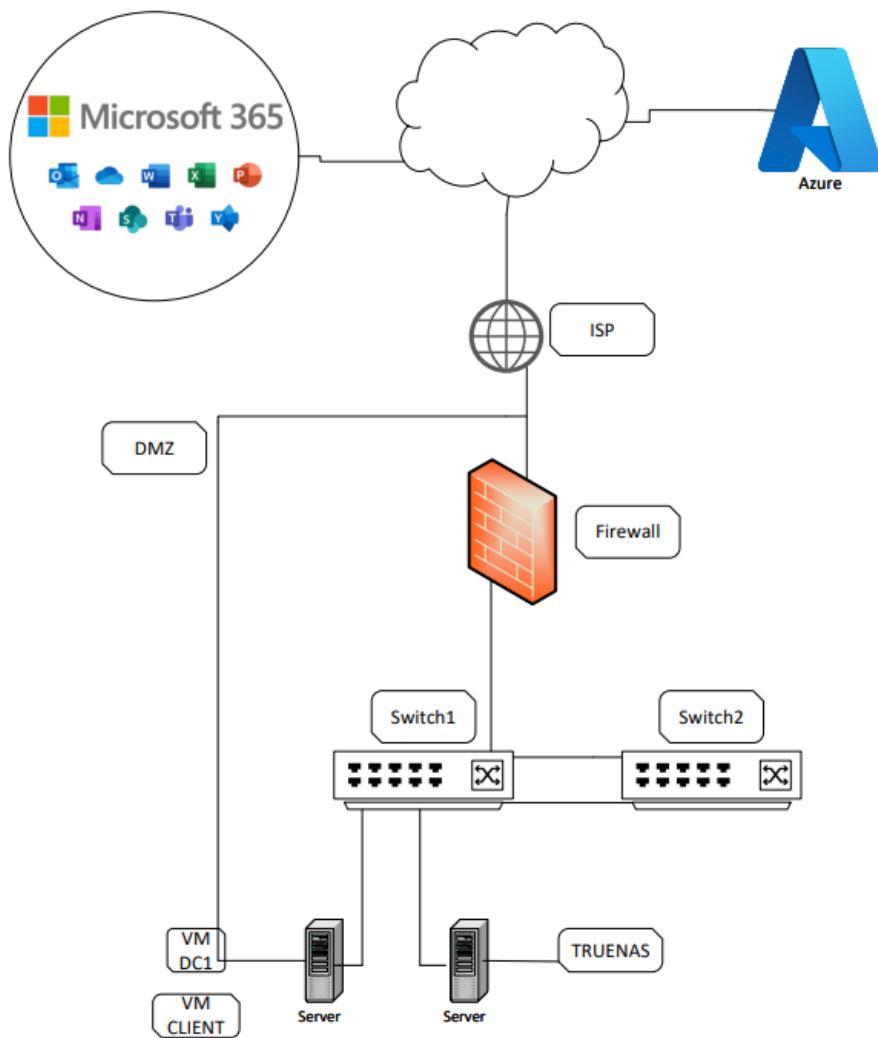
	Stuks	Prijs/stuks	Prijs/maand
Internet Pro+ Proximus	1	99,00 €	99,00 €
Business Fibernet Telenet	1	58,88 €	58,88 €
Linux VM	1	146,39 €	146,39 €
Azure Windows server VM	1	123,13 €	123,13 €
Azure Blob Storage	1	91,10 €	91,10 €
Azure SQL Database	1	3,99 €	3,99 €
Vaste IP telenet	1	28,00 €	28,00 €
M365 E3	32	35,70 €	1.142,40 €
	Totaal ind. BTW		1.142,40 €

Implementatie van onze project

Voor ons project hebben we moeten kiezen met wat voor apparatuur we gaan werken. Ook hebben we grondig nagedacht over hoe dat we alles gaan aanpakken om dit project goed te kunnen uitvoeren.

We hebben besloten om te werken met volgende apparatuur:

- 2 servers van DELL
- 2 switches van CISCO
- 1 firewall Fortigate 100E
- AZURE
- Hyper-V server 1: DC1, 2 Windows clients, Ubuntu server (webserver), RD Gateway server
- Hyper-V server 2: TrueNAS



2. On premise

2.1 Firewall Fortigate 100E

Voor onze firewall twijfelen we tussen pfSense, een opensource firewall die geen licentie nodig heeft, en Fortigate. Omdat we al genoeg fysieke firewalls op de campus hebben, hebben we besloten om deze te gebruiken.

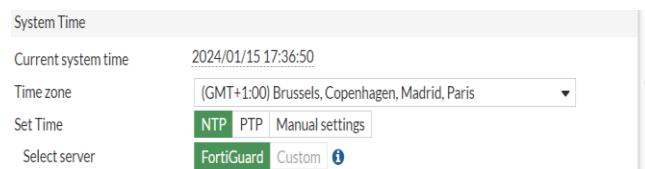
Om verbinding te maken met de firewall hebben we eerst alles via ethernet kabel gedaan om een directe link te hebben met onze pc. We surfen daarna naar 192.168.100.99 met als login admin.

Voor dat we beginnen met werken aan de firewall moeten we eerst zien om een factory reset te uitvoeren, zodat we zeker zijn dat onze firewall helemaal leeg is om eraan te beginnen.

Daarna doen we de volgende:

- Onze tijdzone aanpassen naar Brussel voor juiste logs.
- Een static route naar de Wan1 met de juiste default gateway adres.
- Wan IP toepassen naar de IP dat we gekregen hebben van onze docent.

Voor de tijdzone is dit belangrijk zo dat we de correcte uur krijgen en datum op onze logs.



Static Routes			
Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.2.171.1	wan1	Enabled
wan1	Physical Interface	10.2.171.253/255.255.255.0	PING HTTPS SSH HTTP FMG-Access

```
CLI Console (1) ✎
FortiGate-100E # execute factoryreset
```

2.1.2 interfaces

WAN1

Op onze WAN1 interface gaan we een vaste IP-adres geven. Zodat we vanuit thuis kunnen verbinden met onze firewall. We geven als services http, https, ping, ... mee. Maar in een echte omgeving zouden we alles uitzetten. Het IP-adres 10.2.172.253/24 is onze private IP die we hebben gekregen voor dit project.

The screenshot shows the configuration interface for the WAN1 interface. The interface is a Physical Interface named 'wan1'. It has an Alias field, a VRF ID of 0, and is assigned to the WAN role. The estimated bandwidth is set at 0 kbps for both upstream and downstream. The addressing mode is set to Manual, and the IP/Netmask is 10.2.171.253/255.255.255.0. Under Administrative Access, several services are enabled: HTTPS, FMG-Access, HTTP, SSH, and RADIUS Accounting. PING, SNMP, and Security Fabric Connection are also listed but are disabled. LLDP settings are configured to use VDOM settings for both receive and transmit. At the bottom right, there are 'OK' and 'Cancel' buttons.

Name	wan1
Alias	
Type	Physical Interface
VRF ID	0
Role	WAN
Estimated bandwidth	0 kbps Upstream 0 kbps Downstream
Address	
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP/Netmask	10.2.171.253/255.255.255.0
Secondary IP address	<input type="checkbox"/>
Administrative Access	
IPv4	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> PING <input checked="" type="checkbox"/> FMG-Access <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FTM <input type="checkbox"/> RADIUS Accounting <input type="checkbox"/> Security Fabric Connection <input type="checkbox"/> Speed Test
Receive LLDP	<input checked="" type="checkbox"/> Use VDOM Setting <input type="checkbox"/> Enable <input type="checkbox"/> Disable
Transmit LLDP	<input checked="" type="checkbox"/> Use VDOM Setting <input type="checkbox"/> Enable <input type="checkbox"/> Disable

DMZ

Voor onze DMZ-interface hebben we de default IP gelaten, later hebben we deze range gebruikt voor de configuratie van onze webserver. Verder hebben we de Create address object matching subnet aangelaten om later firewall policy's aan te maken. Voor onze security is DMZ een must voor onze webserver die voor heel de wereld toegankelijk is. Zo kunnen we onze interne configuratie veilig houden.

Name: dmz

Alias:

Type: Physical Interface

VRF ID: 0

Role: DMZ

Address

Addressing mode: Manual

IP/Netmask: 10.10.10.1/255.255.255.0

Create address object matching subnet: dmz

Name: dmz

Destination: 10.10.10.1/255.255.255.0

Secondary IP address: (disabled)

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
	<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input checked="" type="checkbox"/> Security Fabric Connection
	<input type="checkbox"/> Speed Test		

Receive LLDP: Use VDOM Setting | Enable | Disable

Transmit LLDP: Use VDOM Setting | Enable | Disable

OK | Cancel

VLAN-interface

We hebben al onze VLANS meegegeven op poort 2 die verbonden is met onze switch door een Trunk. Elke VLAN krijgt zijn eigen IP-range, we maken dan ook direct een object van de VLAN en geven de juiste services mee. Hier is een voorbeeld van boekhouding maar dit geldt voor alle ander VLANS.

	port2	Physical Interface	0.0.0.0/0.0.0.0					14
•	Aankoopdienst	VLAN	172.16.20.1/255.255.255.0	PING			172.16.20.1-172.16.20.254	3
•	Boekhouding	VLAN	172.16.10.1/255.255.255.0	PING	1		172.16.10.2-172.16.10.254	5
•	Camera	VLAN	10.10.17.1/255.255.255.0	PING			10.10.17.2-10.10.17.254	2
•	Dienstnavorkoop	VLAN	172.16.40.1/255.255.255.0	PING	1		172.16.40.2-172.16.40.254	3
•	Directie	VLAN	172.16.90.1/255.255.255.0	PING			172.16.90.2-172.16.90.254	3
•	Dispatching	VLAN	172.16.60.1/255.255.255.0	PING			172.16.60.2-172.16.60.254	3
•	GuestWifi	VLAN	10.10.8.1/255.255.254.0	PING			10.10.8.2-10.10.9.254	2
•	ITdienstInfa	VLAN	172.16.70.1/255.255.255.0	PING			172.16.70.2-172.16.70.254	2
•	ITdienstOntwik	VLAN	172.16.80.1/255.255.255.0	PING SSH			172.16.80.2-172.16.80.254	4
•	Magazijn	VLAN	172.16.50.1/255.255.255.0	PING			172.16.50.2-172.16.50.254	3
•	PersonnelWifi	VLAN	10.10.0.1/255.255.248.0	PING			10.10.0.2-10.10.7.254	2
•	RaadVanBestuur	VLAN	172.16.100.1/255.255.255.0	PING			172.16.100.2-172.16.100.254	3
•	Server	VLAN	10.10.1.1/255.255.255.0	PING HTTPS HTTP RADIUS Accounting				9
•	Verkooppdienst	VLAN	172.16.30.1/255.255.255.0	PING			172.16.30.1-172.16.30.254	3

Edit Interface

Name

Alias

Type

VLAN protocol

Interface

VLAN ID [Edit](#)

VRF ID [i](#)

Role [i](#)

Address

Addressing mode [Manual](#) [DHCP](#) [Auto-managed by IPAM](#) [PPPoE](#)

IP/Netmask

Create address object matching subnet

Name

Destination

Secondary IP address

Administrative Access

IPv4	<input type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP i	<input checked="" type="checkbox"/> PING
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection i

NV POC

We duiden hieraan voor een DHCP-server zodat bijvoorbeeld users uit boekhouding hun IP krijgen via hetzelfde range van het departement. Maar bij de VLANS server en camera zetten we dit uit, zij krijgen hun IP statisch. Bij server is dit heel belangrijk Zodat de IP van onze domain controller, nooit random veranderd.

DHCP Server

DHCP status	<input checked="" type="button"/> Enabled <input type="button"/> Disabled
Address range	172.16.10.2-172.16.10.254 +
Netmask	255.255.255.0
Default gateway	<input checked="" type="button"/> Same as Interface IP <input type="button"/> Specify
DNS server	<input checked="" type="button"/> Same as System DNS <input type="button"/> Same as Interface IP <input checked="" type="button"/> Specify
DNS server 1	10.10.16.20 <input type="button"/>
DNS server 2	8.8.8.8 <input type="button"/>
Lease time <i>i</i>	<input checked="" type="button"/> 604800 second(s)

Advanced

Network

Device detection <i>i</i>	<input checked="" type="button"/>
Security mode	<input type="button"/>

Hier nog een overzicht van onze VLAN IP's.

afdeling	VLAN Naam	VLAN	Network address	Mask	First IP range	Last IP range
Boekhouding	VLAN_Bokhouding	10	172.16.10.X	/24	172.16.10.1	172.16.10.254
Aankoopdienst	VLAN_Aankoopdienst	20	172.16.20.X	/24	172.16.20.1	172.16.20.254
Verkoopdienst	VLAN_Verkoopdienst	30	172.16.30.X	/24	172.16.30.1	172.16.30.254
Dienst Na verkoop	VLAN_DienstNaVerkoop	40	172.16.40.X	/24	172.16.40.1	172.16.40.254
Magazijn	VLAN_Magazijn	50	172.16.50.X	/24	172.16.50.1	172.16.50.254
Dispatching	VLAN_Dispatching	60	172.16.60.X	/24	172.16.60.1	172.16.60.254
IT-dienst Infrastructuur	VLAN_Infrastructuur	70	172.16.70.X	/24	172.16.70.1	172.16.70.254
IT-dienst Ontwikkeling	VLAN_Ontwikkeling	80	172.16.80.X	/24	172.16.80.1	172.16.80.254
Directie	VLAN_Directie	90	172.16.90.X	/24	172.16.90.1	172.16.90.254
Raad Van bestuur	VLAN_Bestuur	100	172.16.100.X	/24	172.16.100.1	172.16.100.254
personeel WIFI	VLAN_Personeel	110	10.10.0.X	/21	10.10.0.1	10.10.7.254
personeel Guest	VLAN_Guest	120	10.10.8.X	/21	10.10.8.1	10.10.15.254
Server	VLAN_server	130	10.10.16.X	/24	10.10.16.1	10.10.16.254
Camera	VLAN_Camera	140	10.10.17.X	/24	10.10.17.1	10.10.17.254
DMZ	Geen		10.10.10.X	/24	10.10.10.1	10.10.10.254

2.1.3 Static Routes

We voorzien een statische route naar het internet via onze WAN1 met default-gateway dat we gekregen hebben. Deze statische route leggen we verder uit in deel 3: Cloud.

The screenshot shows the 'Edit Static Route' dialog box. The 'Destination' section is set to 'Subnet' and 'Internet Service' with the value '0.0.0.0/0.0.0.0'. The 'Gateway Address' is '10.2.171.1'. The 'Interface' is 'wan1'. The 'Administrative Distance' is '10'. There is a comment field 'Write a comment...' with '0/255' characters available. The 'Status' is 'Enabled'. An 'Advanced Options' button is visible at the bottom.

Hier maken we een statische route naar onze Azure virtueel netwerk, die gaat verbinden via de VPN-tunnel

The screenshot shows the 'Edit Static Route' dialog box. The 'Destination' section is set to 'Subnet' and 'Internet Service' with the value '10.0.0.0/255.255.0.0'. The 'Interface' is 'ToAzureVPN'. The 'Administrative Distance' is '2'. There is a comment field 'Write a comment...' with '0/255' characters available. The 'Status' is 'Enabled'. An 'Advanced Options' button is visible at the bottom. At the bottom right are 'OK' and 'Cancel' buttons.

The screenshot shows a table of static routes. The columns are 'Destination', 'Gateway IP', 'Interface', and 'Status'. There are two entries:

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.2.171.1	wan1	Enabled
10.0.0.0/16	172.172.179.7	ToAzureVPN	Enabled

interface.

2.1.4 Policies

VLAN naar WAN

We geven al onze VLANS toegang tot het internet maar met een web filtering, zodat sommige departementen niet op bepaalde sociale media kunnen.

The screenshot shows a detailed configuration for a network policy:

- Name:** AankoopdienstToWan
- Incoming Interface:** Aankoopdienst
- Outgoing Interface:** wan1
- Source:** Aankoopdienst address
- Destination:** all
- Schedule:** always
- Service:** DNS, HTTP, HTTPS, PING
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based (selected)
- Firewall / Network Options:**
 - NAT: Enabled
 - IP Pool Configuration: Use Outgoing Interface Address (selected)
 - Preserve Source Port: Enabled
 - Protocol Options: PROT default
- Security Profiles:**
 - AntiVirus: Enabled
 - Web Filter: Enabled, WEB, blocked socials
 - DNS Filter: Enabled
 - Application Control: Enabled

DMZ naar WAN | Wan naar DMZ

Om netwerkverkeer door te laten tussen DMZ en WAN maken hier een policy met de nodige services. Van DMZ naar WAN is het belangrijk om NAT aan te zetten, dit kan helpen bij het maskeren van interne IP-adressen en het verbeteren van beveiliging.

The screenshot shows two side-by-side policy configuration windows. Both policies have the following settings:

- Name:** DMZ-WAN and WAN-DMZ
- Incoming Interface:** dmz
- Outgoing Interface:** wan1
- Source:** dmz
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ✓ ACCEPT, ✘ DENY, IPsec
- Inspection Mode:** Flow-based
- Firewall / Network Options:**
 - NAT: Enabled
 - IP Pool Configuration: Use Outgoing Interface Address
 - Preserve Source Port: Enabled
 - Protocol Options: PROT default
- Security Profiles:** None

Server naar VLAN

Voor elke VLAN gaan we een policy aanmaken, waardoor deze ook internet access krijgen. Een voorbeeld hiervan is onze client boekhouding VM die wordt toegevoegd.

The screenshot shows a single policy configuration window for "ServerToBoekhouding". The settings are as follows:

- Name:** ServerToBoekhouding
- Incoming Interface:** Server
- Outgoing Interface:** Boekhouding
- Source:** Server address
- Destination:** Boekhouding address
- Schedule:** always
- Service:** ALL
- Action:** ✓ ACCEPT, ✘ DENY, IPsec
- Inspection Mode:** Flow-based
- Firewall / Network Options:**
 - NAT: Enabled
 - Protocol Options: PROT default
- Security Profiles:**
 - AntiVirus: Enabled
 - Web Filter: Enabled
 - DNS Filter: Enabled
 - Application Control: Enabled
 - File Filter: Enabled
- SSL Inspection:** SSL no-inspection
- Logging Options:**
 - Log Allowed Traffic: Enabled
 - Log Type: Security Events
 - Log Destination: All Sessions
- Comments:** Write a comment... 0/1023
- Enable this policy:** Enabled

NV POC

Server naar server

Om connectie te hebben tussen interne apparaten in de VLAN server maken we hier een policy aan.

Edit Policy

Name	<input type="text" value="server-fw"/>
Incoming Interface	<input type="button" value="Server"/>
Outgoing Interface	<input type="button" value="Server"/>
Source	<input type="button" value="all"/> <input type="button" value="+"/>
IP/MAC Based Access Control	<input type="button" value="+"/>
Destination	<input type="button" value="all"/> <input type="button" value="+"/>
Schedule	<input type="button" value="always"/>
Service	<input type="button" value="ALL"/> <input type="button" value="+"/>
Action	<input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/> <input type="button" value="IPsec"/>
Inspection Mode	<input checked="" type="radio" value="Flow-based"/> Flow-based <input type="radio" value="Proxy-based"/> Proxy-based

Firewall / Network Options

NAT	<input type="checkbox"/>
Protocol Options	<input type="button" value="PROT default"/> <input type="button" value="▼"/>

Security Profiles

AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>

Server naar Azure VPN | Azure VPN naar server

Deze policy is belangrijk voor onze connectie tussen on-premise en cloud. Voor meer informatie kan je doorgaan naar hoofdstuk "Cloud".

Edit Policy

Name	<input type="text" value="ToAzureVPN"/>
Incoming Interface	<input type="button" value="Server"/>
Outgoing Interface	<input type="button" value="ToAzureVPN"/>
Source	<input type="button" value="all"/> +
IP/MAC Based Access Control	<input type="button" value="+"/>
Destination	<input type="button" value="AzureVirtualNetwork01"/> +
Schedule	<input type="button" value="always"/>
Service	<input type="button" value="ALL"/> +
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY <input type="radio"/> IPsec
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based

Edit Policy

Name	<input type="text" value="FromAzureVPN"/>
Incoming Interface	<input type="text" value="ToAzureVPN"/>
Outgoing Interface	<input type="text" value="Server"/>
Source	<input type="text" value="AzureVirtualNetwork01"/> ✖
	+
IP/MAC Based Access Control	i
Destination	<input type="text" value="all"/> ✖
	+
Schedule	<input type="text" value="always"/> ✖
Service	<input type="text" value="ALL"/> ✖
	+
Action	✓ ACCEPT ✗ DENY IPsec

Inspection Mode Flow-based Proxy-based

SSL-VPN tunnel interface → VLAN

Deze policy laat ons aan onze gekozen VLAN's connecteren. We kunnen dit voor elke VLAN doen maar wij doen dit enkel met onze server VLAN en onze IT dienst ontwikkeling. Dit kunnen we ten alle tijden veranderen naar onze wens.

SSL-VPN tunnel interface (ssl.root) → ITdienstOntw 1									
SSh-Switch	admin Guest-group SSO_Guest_Users admin guest student yusuf SSLVPN_TUNNEL_ADDR1	ITdienstOntw address	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	All	51.70 kB
ROOTSSL2SER	admin SSLVPN_TUNNEL_ADDR1	Server address	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	UTM	955.33 MB

SSL-VPN tunnel interface (ssl.root) → Server 1									
ROOTSSL2SER	admin SSLVPN_TUNNEL_ADDR1	Server address	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	UTM	955.33 MB

SSL-VPN tunnel interface → DMZ

Deze policy zorgt ervoor dat we via onze SSL VPN naar onze webserver kunnen gaan die in onze DMZ zit.

SSL-VPN tunnel interface (ssl.root) → dmz 1									
SSH-Ubuntu	admin Guest-group SSO_Guest_Users admin guest student yusuf SSLVPN_TUNNEL_ADDR1	dmz	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	UTM	33.30 MB
ROOTSSL2SER	admin SSLVPN_TUNNEL_ADDR1	Server address	always	ALL	✓ ACCEPT	✗ Disabled	ssl no-inspection	UTM	33.30 MB

Server naar Wan

Voor internet toegang op onze servers maken we hier een policy aan met de nodige services.

Edit Policy

Name i	SERVER2WAN
Incoming Interface	Server
Outgoing Interface	wan1
Source	Server address
IP/MAC Based Access Control i	
Destination	all
Schedule	always
Service	HTTP HTTPS PING
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec
Inspection Mode	Flow-based Proxy-based

2.1.5 Virtual IP

DMZ http(s)

Door het gebruik van virtuele IP's voor HTTP en HTTPS in de DMZ, kunnen organisaties externe gebruikers veilige toegang bieden tot web-diensten zonder directe toegang tot het interne netwerk. En het risico verminderen dat aanvallers directe toegang krijgen tot gevoelige interne bronnen door gebruik te maken van de gescheiden DMZ. Het maakt niet uit wat het bron-IP-adres is. Alle verzoeken zullen worden geforward naar het IP adres 10.10.10.3.

DMZ_HTTP	0.0.0 → 10.10.10.3 (TCP: 80 → 80)	wan1	1	9,767	3 seconds ago
DMZ_HTTPS	0.0.0 → 10.10.10.3 (TCP: 443 → 443)	wan1	1	5,503	8 seconds ago

2.1.6 VPN

SSL VPN

Om vanuit thuis te werken aan onze server van ons fictief bedrijf, gebruiken wij een Secure Socket Layer Virtual Private Network. Een veilige manier om via het internet contact te kunnen leggen naar onze server VLAN.

The screenshot shows the SSL-VPN configuration interface. At the top, there is a table with three rows:

full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

Below this is the "SSL-VPN Settings" section, which includes the following fields:

- Connection Settings** (radio button selected):
 - Enable SSL-VPN:
 - Listen on Interface(s): wan1
 - Listen on Port: 10443
 - Info message: "Web mode access will be listening at <https://10.2.171.253:10443>"
 - Server Certificate: Fortinet_Factory
 - Info message: "You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one." with a "Create Certificate" button.
- Redirect HTTP to SSL-VPN** ():
 - Restrict Access: Allow access from any host
- Idle Logout** ():
 - Inactive For: 300 Seconds
- Require Client Certificate** ()

At the bottom is the "Authentication/Portal Mapping" section:

Create New		Edit	Delete	Send SSL-VPN Configuration
Users/Groups		Portal		
admin		full-access		

IPsec Tunnel

Dit is een VPN tunnel die geconnecteerd is aan onze cloud. Voor een uitgebreidere uitleg kan u doorgaan naar “3.1.6 Tunnel in firewall”

Edit VPN Tunnel

Name	ToAzureVPN		
Comments	Comments 0/255		
Network			
Remote Gateway : Static IP Address (172.172.179.7), Interface : wan1			
Authentication			
Authentication Method : Pre-shared Key			
IKE Version : 2			
Phase 1 Proposal			
Algorithms : AES256-SHA1, 3DES-SHA1, AES256-SHA256			
Diffie-Hellman Group : 2			
Phase 2 Selectors			
Name	Local Address	Remote Address	Add
ToAzureVPN	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Edit
		OK Cancel	

2.1.7 security profiles

Web filters

Via hier maken we beveiligings profielen aan die bijvoorbeeld al het verkeer naar sociale media afbreken of enkel facebook en twitter doorlaten. Het filteren van slechte pagina's en malware.

allow facebook and twitter		0
blocked socials		1
default	Default web filtering.	0
monitor-all	Monitor and log all visited URLs, flow-based.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

Name

Comments

Feature set Flow-based Proxy-based

FortiGuard Category Based Filter

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

Edit Delete Search			
URL	Type	Action	Status
https://twitter.com/	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> Enable
https://www.facebook.com/	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> Enable

Name

Comments

Feature set Flow-based Proxy-based

FortiGuard Category Based Filter

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

Edit Delete Search			
URL	Type	Action	Status
https://www.instagram.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable
https://www.snapchat.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable
https://www.tiktok.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable
https://web.whatsapp.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable
https://www.facebook.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable
https://twitter.com/	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enable

2.2 Switch

Op onze switch hebben we elke VLAN toegevoegd tot een poort. Dit doen we omdat in een bedrijf je verschillende VLANS gaat meegeven met aantal poorten. Tussen de 2 switchen hebben we een EtherChannel aangemaakt deze doen we voor redundantie en verbeterd de bandbreedte. We trunken ook van onze switch naar de firewall en van switch naar server hier laten we al onze VLANS door op deze trunk.

```

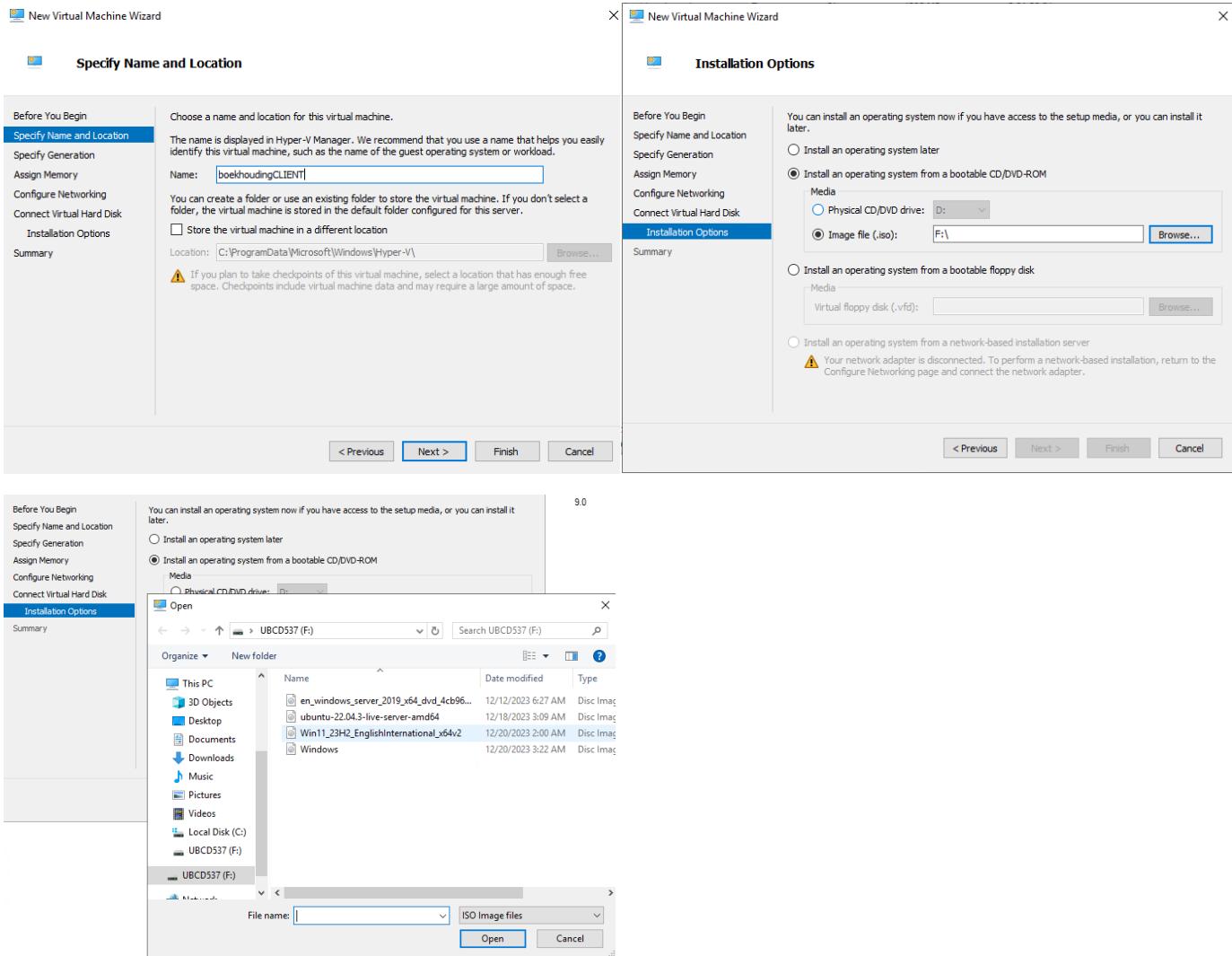
interface Port-channel1
!
interface GigabitEthernet3/0/1
switchport access vlan 10
switchport mode access
!
interface GigabitEthernet3/0/2
switchport access vlan 20
switchport mode access
!
interface GigabitEthernet3/0/3
switchport access vlan 30
switchport mode access
!
interface GigabitEthernet3/0/4
switchport access vlan 40
switchport mode access
!
interface GigabitEthernet3/0/5
switchport access vlan 50
switchport mode access
!
interface GigabitEthernet3/0/6
switchport access vlan 60
switchport mode access
!
interface GigabitEthernet3/0/7
switchport access vlan 70
switchport mode access
!
interface GigabitEthernet3/0/8
switchport access vlan 80
switchport mode access
!
interface GigabitEthernet3/0/9
switchport access vlan 90
switchport mode access
!
interface GigabitEthernet3/0/10
switchport access vlan 100
switchport mode access
!
interface GigabitEthernet3/0/11
switchport access vlan 110
switchport mode access
!
interface GigabitEthernet3/0/12
switchport access vlan 120
switchport mode access
!
interface GigabitEthernet3/0/13
switchport access vlan 130
switchport mode access
!
interface GigabitEthernet3/0/14
switchport access vlan 140
switchport mode access
!
interface GigabitEthernet3/0/15
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-140
switchport mode trunk
!
interface GigabitEthernet3/0/16
switchport access vlan 130
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-140
switchport mode trunk
!
interface GigabitEthernet3/0/21
channel-group 1 mode passive
!
interface GigabitEthernet3/0/22
channel-group 1 mode passive
!
```

Voor de resterende poorten dat we niet gebruiken is het ook beter om deze in shut down te plaatsen omdat open poorten een securityprobleem kunnen worden. Bij de EtherChannel moet je ook 2 kabels voorzien die van de ene switch zo gelinkt zijn aan de andere switch.

2.3 Virtuele machines

Voor de VM's aan te maken hebben we hiervoor Rufus gebruikt om USB compatibel te maken. Dit zorgt ervoor dat de ISO-bestanden gebruikt kunnen worden voor installatie. Voor elke VM moet je ook gaan zien wat de beste memory is om deze zonder probleem te laten runnen bijvoorbeeld de clients vragen minder memory dan de domain controllers.

Eens je de VM hebt aangemaakt kan je nog de settings naar wens aanpassen.

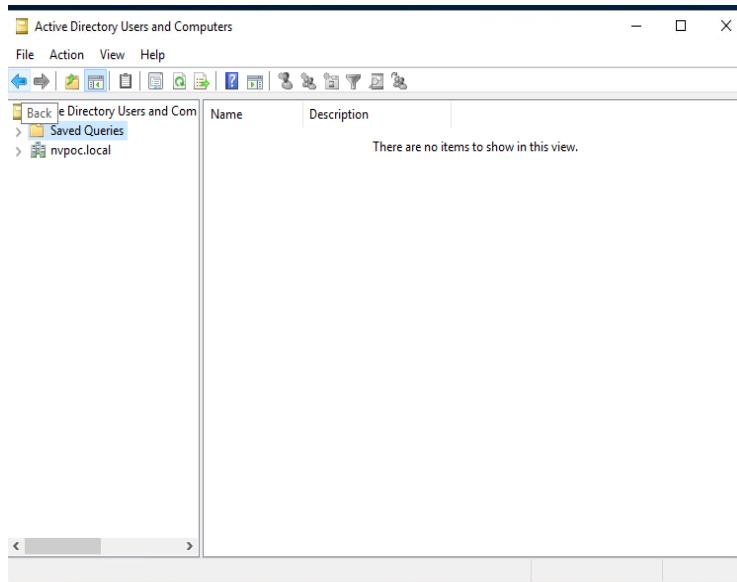
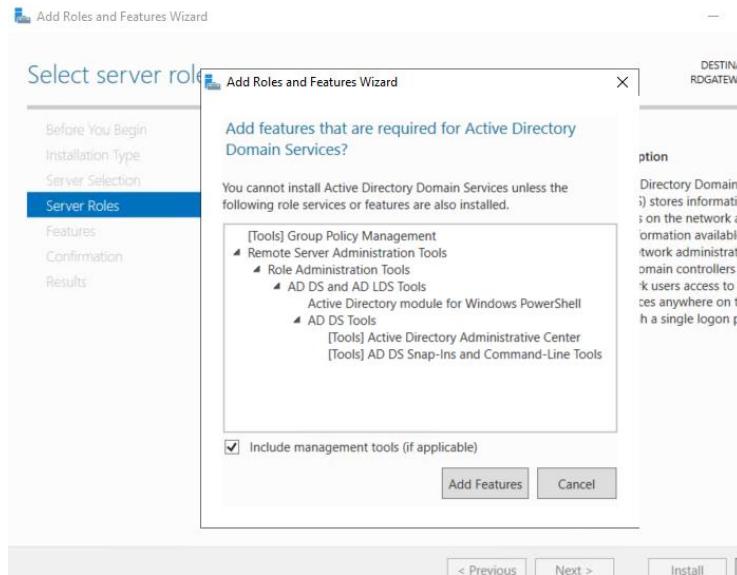


2.4 Domain Controller 1

Op de DC1 hebben we Active directory services en DNS server geïnstalleerd. Dit moet als eerst gedaan worden omdat dit de basis is van een domain controller.

2.4.1 Active Directory

Active Directory is een belangrijk Microsoft-hulpmiddel voor bedrijven. Het helpt bij het organiseren en beheren van gebruikers en computers. We maken een nieuwe forest aan met als domein naam nvpoc.local



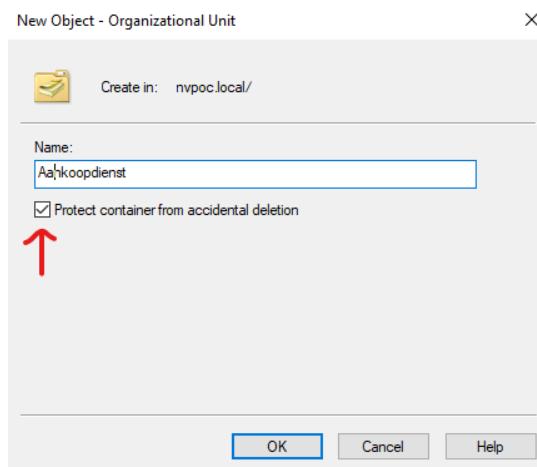
Als domeinnaam hebben we nvpoc.local gebruikt. Deze domeinnaam gaan we geven aan elke client. Ze gaan hierdoor ook tevoorschijn komen in de computerfolder op onze Active Directory en gaan we deze kunnen gebruiken voor latere toepassingen.

The screenshot shows the Active Directory Users and Computers interface. The left pane displays a tree view of the domain structure under 'nvpoc.local'. The right pane lists objects with columns for Name, Type, and Description. Objects shown include RDGATEWAY, TRUENAS-LAB, DIENSTNAVERKOOP, and BOEKHOUDING.

Name	Type
RDGATEWAY	Computer
TRUENAS-LAB	Computer
DIENSTNAVERKOOP	Computer
BOEKHOUDING	Computer

2.4.1.1 Aanmaak van OU's

Elke departement is aangemaakt geweest als OU. We zorgen ook dat bij het aanmaken van een OU je protect from accidental deletion aan staat dit is zeer belangrijk.



The screenshot shows the Active Directory Users and Computers interface. The left pane displays the domain structure. The right pane lists objects, including the newly created 'Aankoopdienst' organizational unit, which is described as 'Default container for up...'. Other objects listed include Aankoopdienst, Boekhouding, Builtin, Computers, Dienst na verkoop, Directie, Dispatching, Domain Controllers, ForeignSecurityPrincipals, Fortigate-Users, Groups, IT-dienst Infrastructuur, IT-dienst Ontwikkeling, Kader, Keys, LostAndFound, Magazijn, Managed Service Accounts, powershell, Program Data, Raad van bestuur, System, Users, Verkoopdienst, NTDS Quotas, TPM Devices, and Infrastructure.

Name	Type	Description
Aankoopdienst	Organizational Unit	Default container for up...
Boekhouding	Organizational Unit	
Builtin	builtinDomain	
Computers	Container	
Dienst na verkoop	Organizational Unit	
Directie	Organizational Unit	
Dispatching	Organizational Unit	
Domain Controllers	Organizational Unit	
ForeignSecurityPrincipals	Container	
Fortigate-Users	Organizational Unit	
Groups	Organizational Unit	
IT-dienst Infrastructuur	Organizational Unit	
IT-dienst Ontwikkeling	Organizational Unit	
Kader	Container	
Keys	Container	
LostAndFound	Container	
Magazijn	Organizational Unit	
Managed Service Accounts	Container	
powershell	Organizational Unit	
Program Data	Container	
Raad van bestuur	Organizational Unit	
System	Container	Builtin system settings
Users	Container	
Verkoopdienst	Organizational Unit	
NTDS Quotas	msDS-QuotaContainer	
TPM Devices	msTPM-InformationObjectsContainer	
Infrastructure	infrastructureUpdate	Quota specifications co...

2.4.1.2 Users

Bij het aanmaken van mijn users heb ik een CSV-bestand gebruikt die ik online heb aangemaakt. Al de users in dit bestand zijn dan ook automatische op mijn Active Directory toegevoegd. Elke paswoord van deze users gaan veranderd moeten worden wanneer ze er de eerste keer gaan op inloggen.

```
# Import required modules
Import-Module ActiveDirectory

# Define CSV file path
$csvFilePath = "\\\$vnuenas-lab\\Shared\\Bestanden\\downloads\\csv_file\\300_useraccounts_unicode.csv"

# Check if the CSV file exists
if (Test-Path $csvFilePath) {
    # Import CSV data
    $csvData = Import-Csv -Path $csvFilePath

    # Hashtable to track processed SamAccountNames
    $processedAccounts = @{}

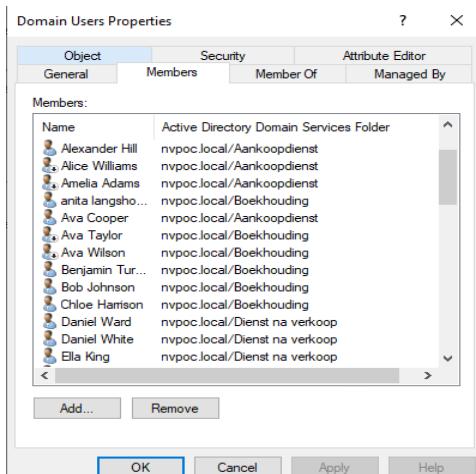
    # Iterate through each row in the CSV data
    foreach ($userData in $csvData) {
        # Assign values to variables
        $Name = $userData.SamAccountName
        $Surname = $userData.Surname
        $SamAccountName = $userData.SamAccountName
        $DisplayName = $userData.DisplayName
        $Name = $userData.Name
        $StreetAddress = $userData.StreetAddress
        $City = $userData.City
        $PostalCode = $userData.PostalCode
        $CountryCode = $userData.CountryCode
        $Country = $userData.Country
        $OU = $userData.OU
        $csvUsersPath = "[\\powershell,DC=nvpoc,DC=local]"
        $EmailAddress = $userData.EmailAddress
        $Username = $userData.Username
        $AccountPassword = $userData.AccountPassword
        $MobilePhone = $userData.MobilePhone
        $TelephoneCountryCode = $userData.TelephoneCountryCode
        $MothersMaiden = $userData.MothersMaiden
        $Birthday = $userData.Birthday
        $Age = $userData.Age
        $Company = $userData.Company

        # Check if SamAccountName has already been processed
        if ($processedAccounts.ContainsKey($SamAccountName)) {
            Write-Host "User with SamAccountName $SamAccountName already processed. Skipping."
        } else {
            # Build user parameters
            $parameters = @{
                Name = $Name
                GivenName = $FirstName
                Surname = $Surname
                SamAccountName = $SamAccountName
                EmailAddress = $EmailAddress
                DisplayName = $DisplayName
                MobilePhone = $MobilePhone
                Company = $Company
                AccountPassword = (ConvertTo-SecureString "$AccountPassword" -AsPlainText -Force)
                Path = $csvUsersPath # Corrected variable name
                Enabled = $true
                ChangePasswordAtLogon = $true
            }

            # Create user in Active Directory
            New-ADUser $parameters

            # Add SamAccountName to the processed hashtable
            $processedAccounts[$SamAccountName] = $true
        }
    }

    Write-Host "User accounts created successfully."
} else {
    Write-Host "CSV file not found at path: $csvFilePath"
}
}
```



2.4.1.3 User rechten

Voor elke OU dat we hebben in ons domein, hebben we een domain local group aangemaakt. Voor iedere group zijn er ook rechten toegepast, bijvoorbeeld Full-control (FC), Read (R) en Write (W). Zo krijgen alle users de juiste rechten toegekend. We hebben daarna elke rechten gegeven aan de juiste folders op onze File Share.

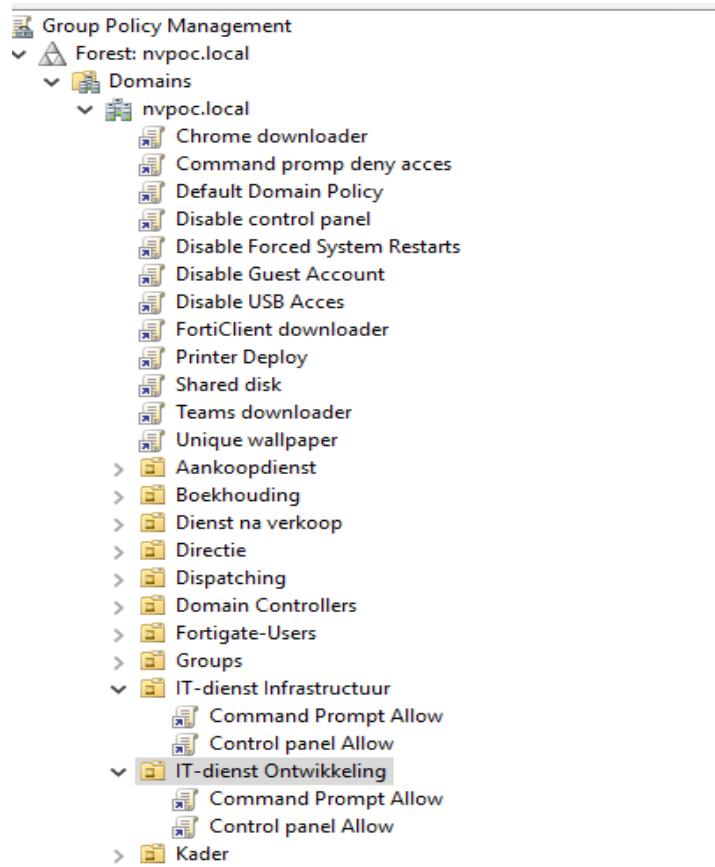
The screenshot displays three windows illustrating the configuration of user permissions:

- Active Directory Users and Computers:** Shows the structure of the domain, including various OUs like 'Aankoopdienst', 'Boekhouding', 'Dienstniveaukoop', 'Directie', 'IT', 'Magazijn', 'Raadvanbestuur', and 'Verkoopdienst'. Each OU contains several security groups (e.g., 'Aankoopdienst-FC', 'Boekhouding-R', etc.).
- File Explorer View:** Shows a folder structure under 'Shared'. The 'Boekhouding' folder is selected, displaying its contents and properties. The folder was created on 1/6/2024 at 4:27 AM.
- Security Properties Dialog:** A detailed view of the 'Boekhouding' folder's security settings. It shows the object name as '\\truenas-lab\Shared\Bestanden\Boekhouding'. The 'Group or user names' list includes 'Boekhouding-R (NVPOC\Boekhouding-R)', 'Boekhouding-W (NVPOC\Boekhouding-W)', and 'Boekhouding-FC (NVPOC\Boekhouding-FC)'. The 'Permissions for wheel' section lists 'Full control', 'Modify', 'Read & execute', 'List folder contents', and 'Read'. The 'Edit...' button is visible above the permission list.

2.4.2 GPO's

In een bedrijf is het belangrijk om GPO's te hebben. GPO's zorgen ervoor dat niet alle users alles kunnen doen of aanpassen. Je kan met GPO's ook ervoor zorgen dat alles direct geïnstalleerd is bij elke domain user zonder dat dit 1 per 1 wordt gedaan. Voor security van het bedrijf is dit een must. Op DC1 hebben we de volgende GPO's aangemaakt:

- Chrome downloader → Chrome gaat automatisch bij de users gedownload en geïnstalleerd worden.
- Teams downloader → Teams gaat automatisch bij de users gedownload en geïnstalleerd worden.
- FortiClient downloader → FortiClient gaat automatisch bij de users gedownload en geïnstalleerd worden.
- Command prompt deny acces → sommige users hebben geen recht op Command prompt. Maar iT krijgt een GPO dat ze wel acces hebben hierop
- Disable control panel → sommige users hebben geen recht op control panel. Maar iT krijgt een GPO dat ze wel acces hebben hierop
- Disable Forced system restart → computer gaat niet automatisch herstarten.
- Disable guest account → niemand buiten iT kan accounts aanmaken voor andere.
- Disable USB-acces → geen USB-acces zodat er geen security issue kunnen gebeuren. Maar iT krijgt een GPO dat ze wel acces hebben hierop
- Monitor changes to your GPO-settings → belangrijk om uw GPO-logs in oog te houden.
- Printer Deploy → users krijgen ook de printers te zien.
- Restrict software installations → buiten de software die er worden meegegeven als GPO kunnen er geen andere worden geïnstalleerd.
- Shared disk → elke user heeft toegang tot file share met daarin ieder elk departement.
- Unique wallpaper → iedereen in het domein krijgt dezelfde achtergrond wallpaper.



2.4.3 DNS

In forward Lookup voegen we elke computer toe met hun IP. We hebben hier de clients, NAS, RD-gateway en DC2 toegevoegd als A-record. Bij het toevoegen is het ook handig om Create PTR record aanvinken zodat deze in de reverse lookup worden gezet.

The screenshot shows the Windows DNS Manager interface. On the left, the navigation pane shows the DNS tree with the 'nvpoc.local' zone selected. On the right, a table displays the records for this zone. The table has columns for Name, Type, Data, and Timestamp. The data includes the Start of Authority (SOA) record, Name Server (NS) records, and numerous Host (A) records for various servers and clients. At the bottom of the table, there is a checked checkbox labeled 'Create associated pointer (PTR) record'.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[85], domaincontroller1.nv...	static
(same as parent folder)	Name Server (NS)	dc2.nvpoc.local.	static
(same as parent folder)	Name Server (NS)	domaincontroller1.nvpoc.l...	static
(same as parent folder)	Host (A)	10.10.16.20	1/15/2024
(same as parent folder)	Host (A)	10.0.0.4	1/17/2024
boekhouding	Host (A)	172.16.10.2	static
DC2	Host (A)	10.0.0.4	static
dienstNaVerkoop	Host (A)	172.16.40.2	static
domaincontroller1	Host (A)	10.10.16.20	static
domaincontroller2	Host (A)	10.0.0.4	static
NAS	Host (A)	10.10.16.9	static
RDGATEWAY	Host (A)	10.10.16.21	1/8/2024 7
truenas-lab	Host (A)	10.10.16.9	1/1/2024 7

Create associated pointer (PTR) record

The screenshot shows the Windows DNS Manager interface. On the left, the navigation pane shows the DNS tree with the 'Reverse Lookup Zones' node under 'nvpoc.local'. On the right, a table displays the records for this zone. The table has columns for Name, Type, and Status. The data includes four Standard Primary zones for the ranges 0.0.10.in-addr.arpa, 10.16.172.in-addr.arpa, 16.10.10.in-addr.arpa, and 40.16.172.in-addr.arpa, all of which are running.

Name	Type	Status
0.0.10.in-addr.arpa	Active Directory-Integrated Pr...	Running
10.16.172.in-addr.arpa	Active Directory-Integrated Pr...	Running
16.10.10.in-addr.arpa	Standard Primary	Running
40.16.172.in-addr.arpa	Active Directory-Integrated Pr...	Running

2.5 Printer server

Een printserver heeft als doel het efficiënt beheren en delen van printers binnen een netwerkomgeving.

We hebben een nieuwe printer toegevoegd met als naam Printer-NVPOC1 en deze gelinkt dan aan onze GPO zodat het zichtbaar is voor iedereen.

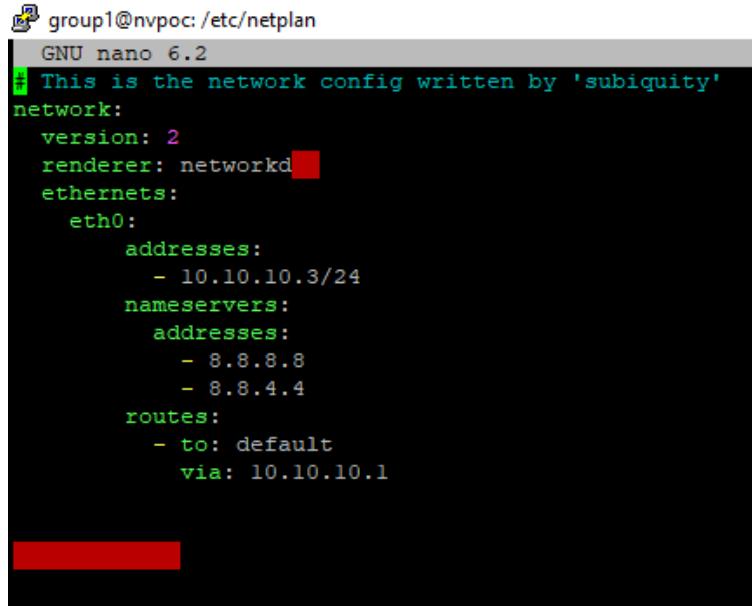
The screenshot shows the Windows Print Management console. The left navigation pane shows 'Print Management' with 'Printers' selected. Under 'Printers', 'domaincontroller1 (local)' is expanded, showing 'Drivers', 'Forms', 'Ports', and 'Printers'. A 'Deployed Printers' icon is highlighted. The main pane displays a table with columns: 'Printer Name', 'Server Name', and 'Per-User GPO'. One row is shown: 'Printer-NVPOC1', 'domaincontrol...', and 'Printer Deploy'. The right pane is titled 'Actions' with 'Deployed Printers' selected. Below the table, a tree view under 'Group Policy Objects' lists various policies, with 'Printer Deploy' also highlighted.

The screenshot shows the Windows Settings app with 'Printers & scanners' selected in the sidebar. It displays a list of printers, including 'Printer-NVPOC1 on DOMAINCONTROLLER'. An 'Add device' button is visible. Below the list, a message says 'The printer that I want isn't listed'. At the bottom, there's another 'Printers & scanners' section showing 'Fax' and 'Microsoft Print to PDF'.

2.6 Webserver

2.6.1 ubuntu Linux

Voor onze webserver maken we gebruik van een Ubuntu Linux machine. Deze geven we ook een Statisch IP adres mee, met toebehorende DNS adressen. Wat zeer belangrijk is, is het enablen van SSH en het disabelen van automatische DHCP.

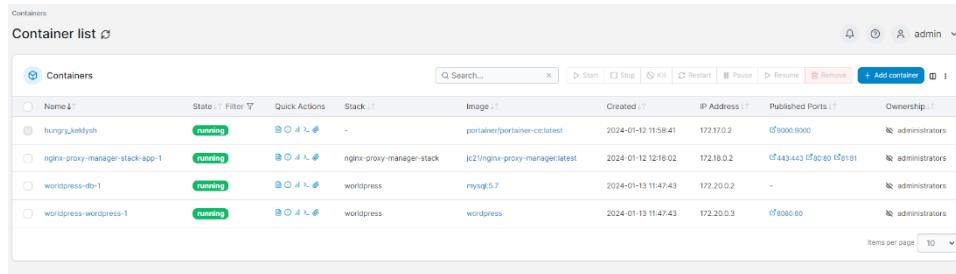


```
group1@nvpoc: /etc/netplan
GNU nano 6.2
This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      addresses:
        - 10.10.10.3/24
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
      routes:
        - to: default
          via: 10.10.10.1
```

2.6.2 Portainer.io

Voor de Webserver maken we gebruik van een GUI van Docker, Portainer.io. Dit is een gebruiksvriendelijke manier om containers op te zetten. Containers gebruiken is zeer Efficiënt voor het opzetten van webservers. In deze container zit onze database, Nginx Proxy Manager en Wordpress.

URL: 10.10.10.3:9000 op deze URL kom je op portainer daar voegen we onze containers aan.



Name	State	Quick Actions	Stack	Image	Created	IP Address	Published Ports	Ownership
hungry_keldysh	running		-	portainer/portainer-ce-latest	2024-01-12 11:58:41	172.17.0.2	9000:9000	administrators
nginx-proxy-manager-stack-app-1	running		nginx-proxy-manager-stack	jk21/nginx-proxy-manager:latest	2024-01-12 12:16:02	172.18.0.2	443:443 80:80 81:81	administrators
wordpress-db-1	running		wordpress	mysql:5.7	2024-01-13 11:47:43	172.20.0.2	-	administrators
wordpress-wordpress-1	running		wordpress	wordpress	2024-01-13 11:47:43	172.20.0.3	8000:80	administrators

2.6.3 Domain name

We kochten een domein aan via combell.com. We hebben onze domeinnaam niet gehost op Combell, maar op Cloudflare. Dit doen we door de nameservers te veranderen naar de nameservers die Cloudflare ons heeft gegeven.

nvpoc.com	
Expiration date	30/12/2024 (in 11 months)
<input checked="" type="checkbox"/> Renew automatically	
Registrant	Yusuf Coban Nijverheidskaai 170 1070 Anderlecht Belgium E-mail: yusuf.coban@student.ehb.be Phone: +32 2 523 37 37
Edit registrant	
Name servers	alec.ns.cloudflare.com carol.ns.cloudflare.com
Edit name servers	

Op Cloudflare zie je dan dat de domeinnaam actief is en je hier alles kan beheren.

nvpoc.com

Active

2.6.4 CloudFlare DNS records

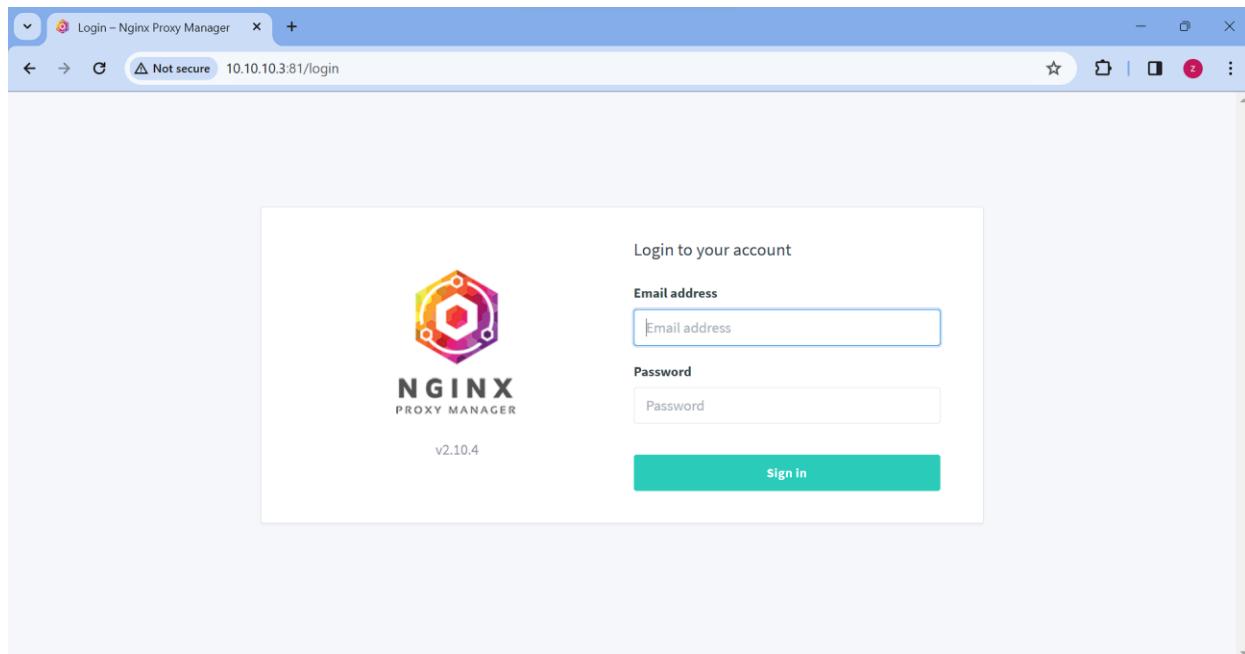
Om onze domeinnaam te koppelen aan het IP-adres, maken we een A-record aan. Hierbij gebruiken we ons publiek IP-adres om deze aan elkaar te koppelen.

DNS management for nvpoc.com					
Review, add, and edit DNS records. Edits will go into effect once saved.			Import and Export Dashboard Display Settings		
<input type="button" value="Add filter"/> <input type="text" value="q"/> <input type="button" value="Search"/> <input type="button" value="Add record"/>					
Type	Name	Content	Proxy status	TTL	Actions
A	nvpoc.com	193.191.183.42	DNS only	1 hr	Edit

2.6.5 Nginx Proxy manager

Voor onze webserver maken we gebruik van Nginx. Dit is een open source webserver en reverse proxyserver. Het staat bekend om zijn efficiëntie en schaalbaarheid.

URL: 10.10.10.3:81



Proxyhost

Voor onze Website bereikbaar te maken hebben we een proxy host aangemaakt. Ook hebben we een redirection host aangemaakt voor ons “www” subdomein, anders werd je doorverwezen naar de default page van Nginx.

Edit Proxy Host

Details Custom locations SSL Advanced

Domain Names *

Scheme * **Forward Hostname / IP *** **Forward Port ***

Cache Assets Block Common Exploits

Websockets Support

Access List

NV POC

Edit Proxy Host

✖

↳ Details ⚒ Custom locations ⚒ SSL ⚒ Advanced

SSL Certificate

nvpoc.com, *.nvpoc.com

Force SSL HTTP/2 Support

HSTS Enabled ? HSTS Subdomains

Redirection host

New Redirection Host

✖

↳ Details ⚒ SSL ⚒ Advanced

Domain Names *

www.nvpoc.com

Scheme * Forward Domain *

https nvpoc.com

HTTP Code *

308 Permanent redirect

Preserve Path Block Common Exploits

NV POC

Let's Encrypt Certificate

Bij het aanmaken van onze proxy host, hebben we een SSL-certificaat nodig. Deze kunnen we verkrijgen via Cloudflare. Een [reddit blog](#) vertelt ons hoe we deze certificaat moeten aanmaken.

Create Custom Token

Token name
Give your API token a descriptive name.
NVPOC-LETSENCRYPT

Permissions
Select edit or read permissions to apply to your accounts or websites for this token.
Zone DNS Edit
+ Add more

Zone Resources
Select zones to include or exclude.
Include All zones
+ Add more

Client IP Address Filtering
Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.
Operator Value
Select item... e.g. 192.168.1.88
+ Add more

TTL
Define how long this token will stay active.
Start Date → End Date

Add Let's Encrypt Certificate

Domain Names *
.nvpoc.com nvpoc.com
⚠ These domains must be already configured to point to this installation

Email Address for Let's Encrypt *
soufyannaimi@student.ehb.be

Use a DNS Challenge

⚠ This section requires some knowledge about Certbot and its DNS plugins. Please consult the respective plugins documentation.

DNS Provider *
Cloudflare

Credentials File Content *

```
# Cloudflare API token
dns.cloudflare_api_token = 0123456789abcdef0123456789abcdef01234567
```

ⓘ This plugin requires a configuration file containing an API token or other credentials to your provider
⚠ This data will be stored as plaintext in the database and in a file!

Propagation Seconds

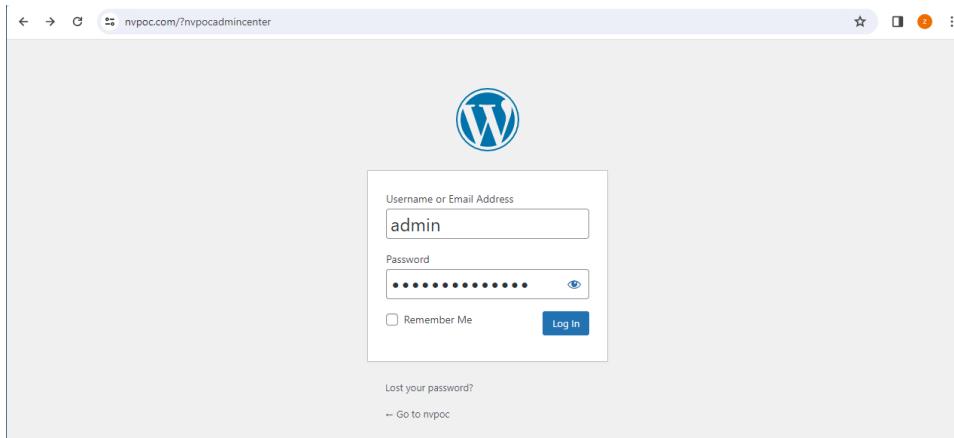
ⓘ Leave empty to use the plugins default value. Number of seconds to wait for DNS propagation.

I Agree to the [Let's Encrypt Terms of Service](#) *

SSL Certificates			<input type="text"/> Search Certificate...	<input type="button"/>	<input type="button"/> Add SSL Certificate
NAME	CERTIFICATE PROVIDER	EXPIRES			
 *.nvpoc.com nvpoc.com Created: 13th January 2024	Let's Encrypt - Cloudflare	12th April 2024, 12:33 pm			

2.6.6 WordPress

Hier zie je de WordPress login om aan te melden met je default login <https://nvpoc.com/wp-admin>. Voor security redenen is die default login URL niet veilig. Dit kunnen we veranderen via een plugin.



Security plugin

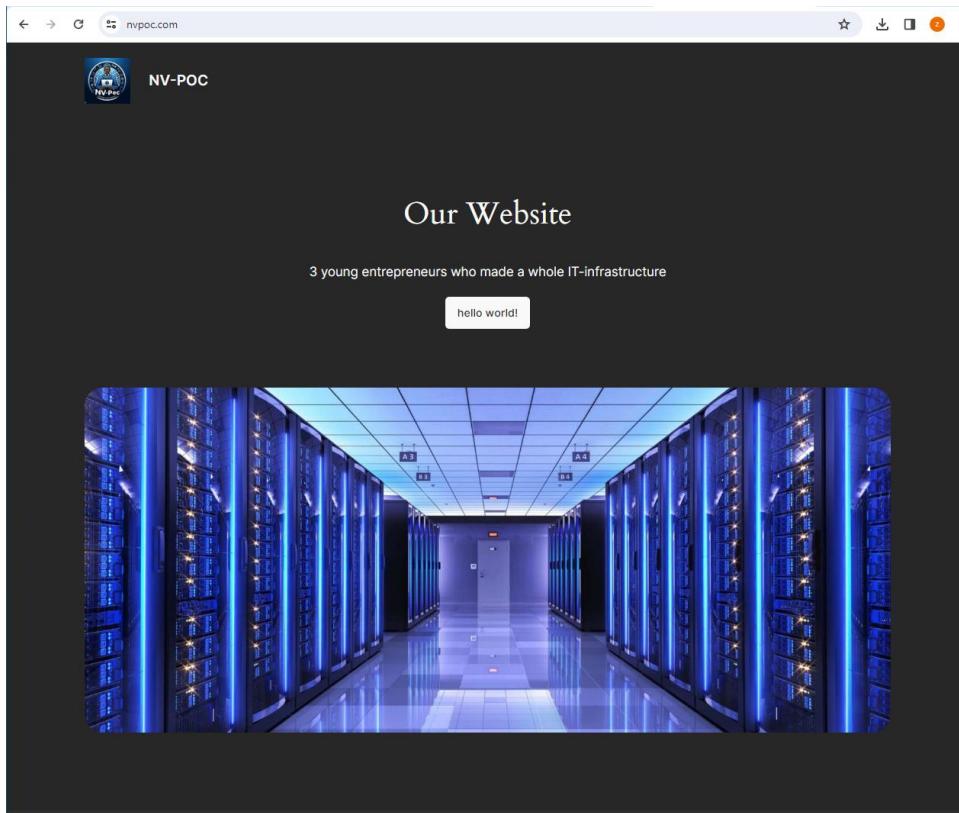
Via deze plugin kan je “wp-admin” veranderen naar een zelfgekozen URL. We veranderen dit naar <https://nvpoc.com/?nvpocadmincenter>.

WPS Hide Login
Settings | Deactivate
Protect your website by changing the login URL and preventing access to wp-login.php page and wp-admin directory while not logged-in
Enable auto-updates
Version 1.9.11 | By WPSServeur, NicolasKulka, wpformation | View details
There is a new version of WPS Hide Login available. [View version 1.9.12 details](#) or [update now](#).

WPS Hide Login
Need help? Try the [support forum](#). This plugin is kindly brought to you by [WPSServeur](#) (WordPress specialized hosting)
Discover our other plugins: the plugin [WPS Bidouille](#), the plugin [WPS Cleaner](#) and [WPS Limit Login](#)
Login url: https://nvpoc.com/?nvpocadmincenter
Protect your website by changing the login URL and preventing access to the wp-login.php page and the wp-admin directory to non-connected people.
Redirection url: https://nvpoc.com/?404
Redirect URL when someone tries to access the wp-login.php page and the wp-admin directory while not logged in.

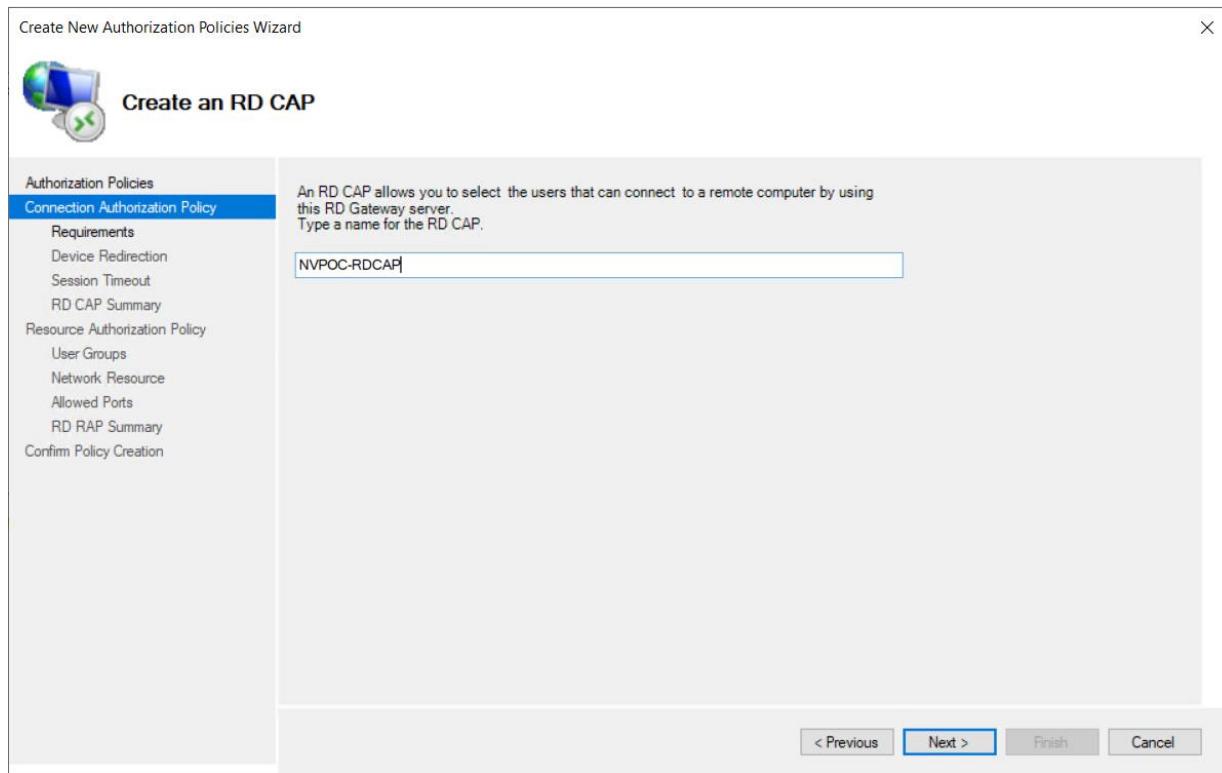
2.6.7 Website

Hier zie je onze website die we hebben aangepast naar onze wens via WordPress.

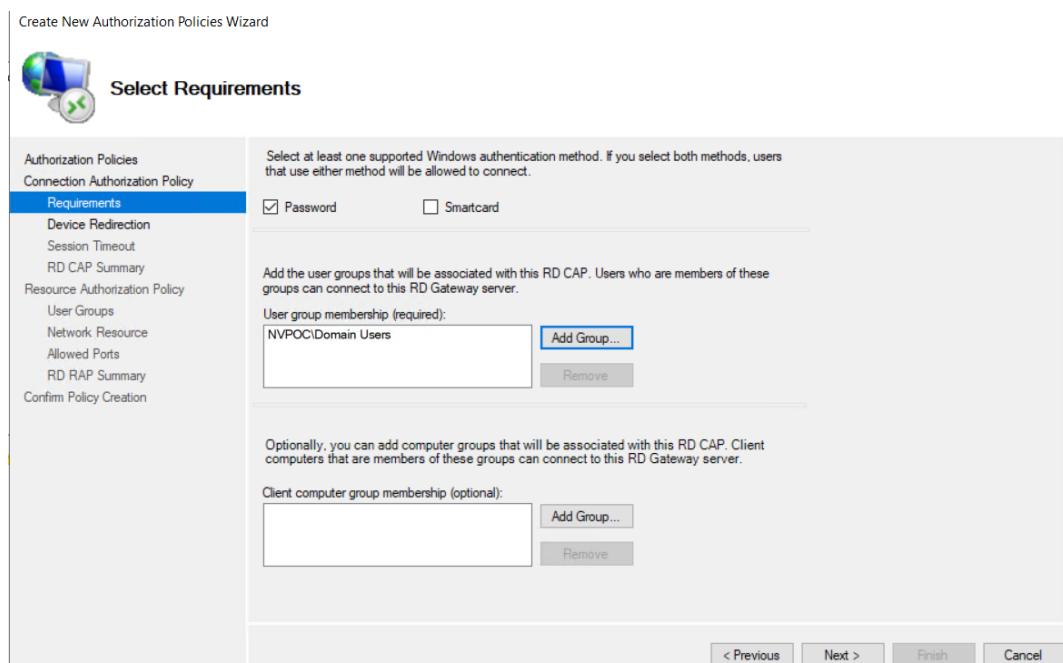


2.7 RD gateway server

Nu gaan we de RD-gateway server opbouwen. We maken een nieuwe windows server aan en configureren deze naar wens van de RD-gateway server. Dit doen we door op remote desktopmanager te drukken in het tabblad van tools. Daar gaan we naar connection authoriazation policies en maken we gebruik van de Wizard. We geven dit een naam en gaan door naar de volgende stap.



Hier connecteren wij de users op het domein aan de RD-gateway server.



Als volgende stap duiden we aan dat we de devices van de users toelaten om verbinding te kunnen maken.

Create New Authorization Policies Wizard X

Enable or Disable Device Redirection



Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation

Specify whether to enable or disable access to local client devices and resources in your remote session for clients that connect by using RD Gateway.

RD Gateway device redirection should only be used for trusted clients running Remote Desktop Connection .

Enable device redirection for all client devices
 Disable device redirection for the following client device types:

- Drives
- Clipboard
- Printers
- Ports (COM and LPT only)
- Supported Plug and Play devices

Only allow client connections to Remote Desktop Session Host servers that enforce RD Gateway device redirection.

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

Dit is een overzicht van al wat u hebt geconfigureerd op de RD CAP.

Create New Authorization Policies Wizard X

RD CAP Settings Summary



Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation

You have specified that an RD CAP with the following settings be created:

If the user is a member of any of the following user groups:
NVPOC\Domain Users

If the client computer is a member of any of the following computer groups:
Not applicable (no computer group is specified)

If the user uses the following supported Windows authentication methods:
Password

Allow the user to connect to this RD Gateway server and disable device redirection for the following client devices:
Not applicable (device redirection is allowed for all client devices)

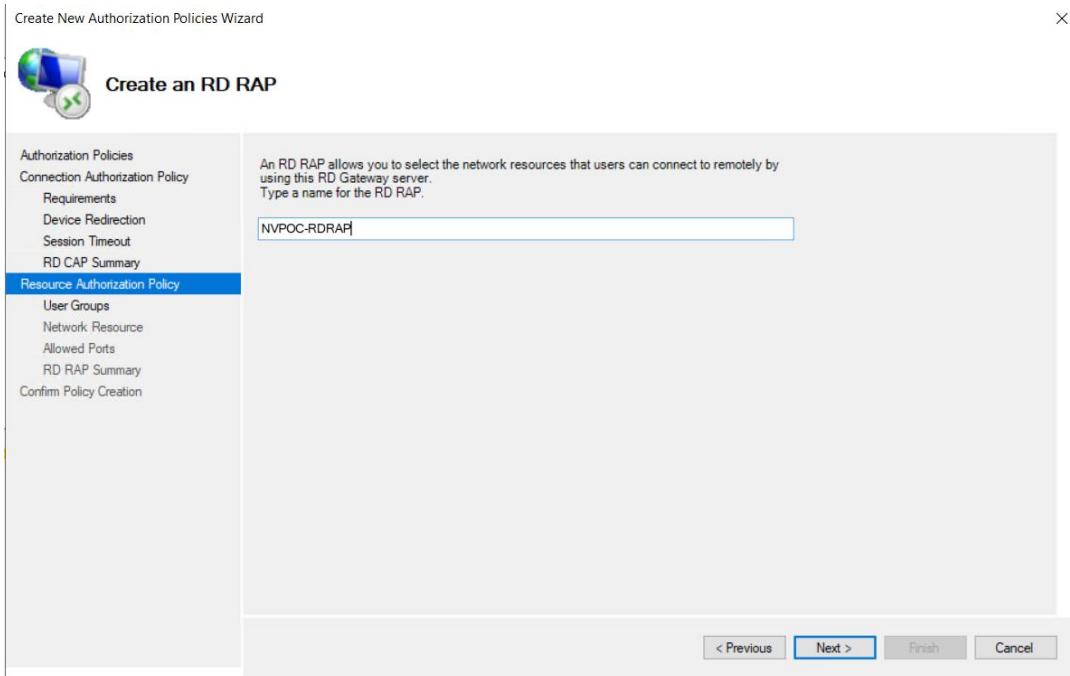
After the idle timeout is reached:
- Not applicable (no idle timeout)

After the session timeout is reached:
- Not applicable (no session timeout)

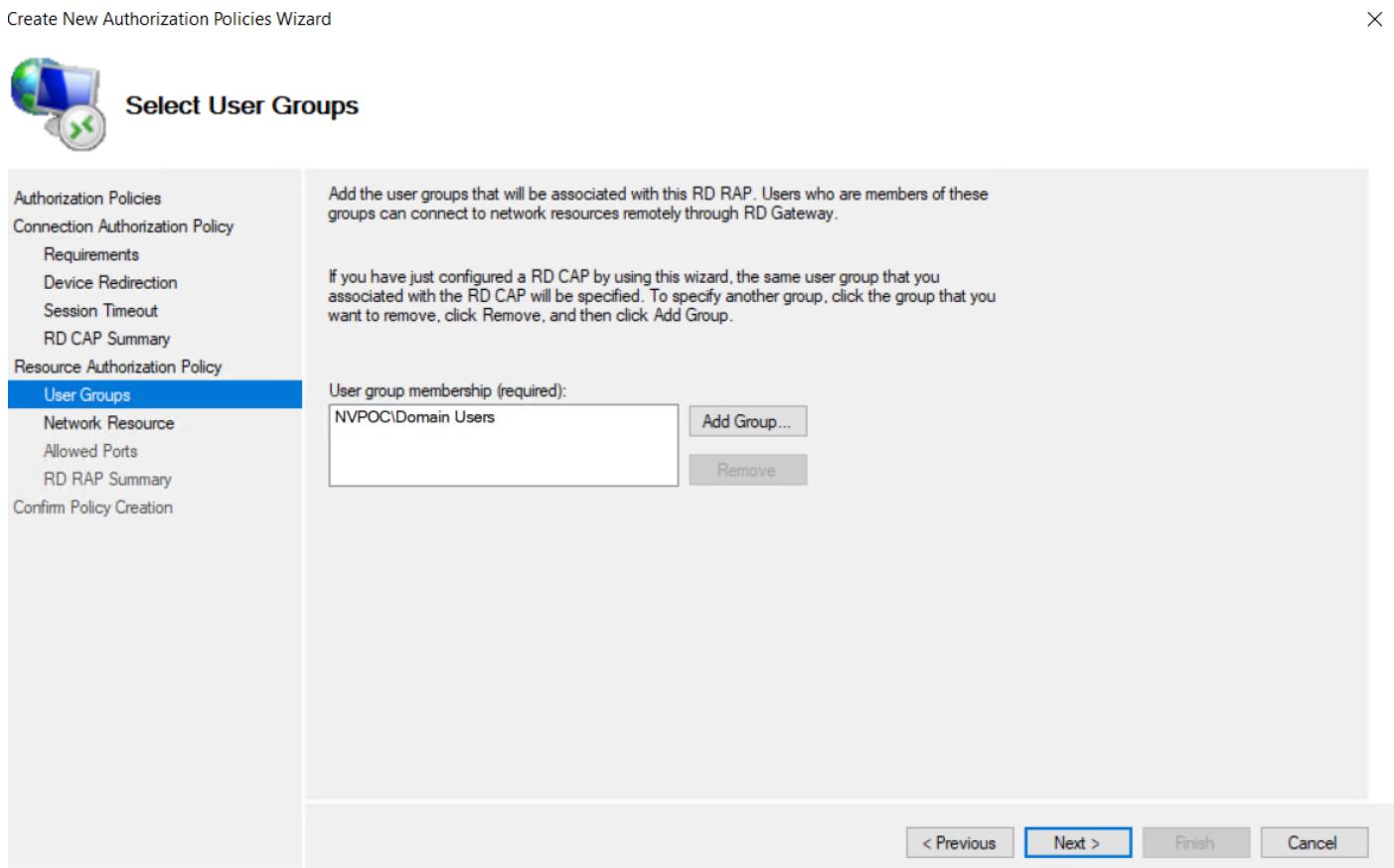
[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

NV POC

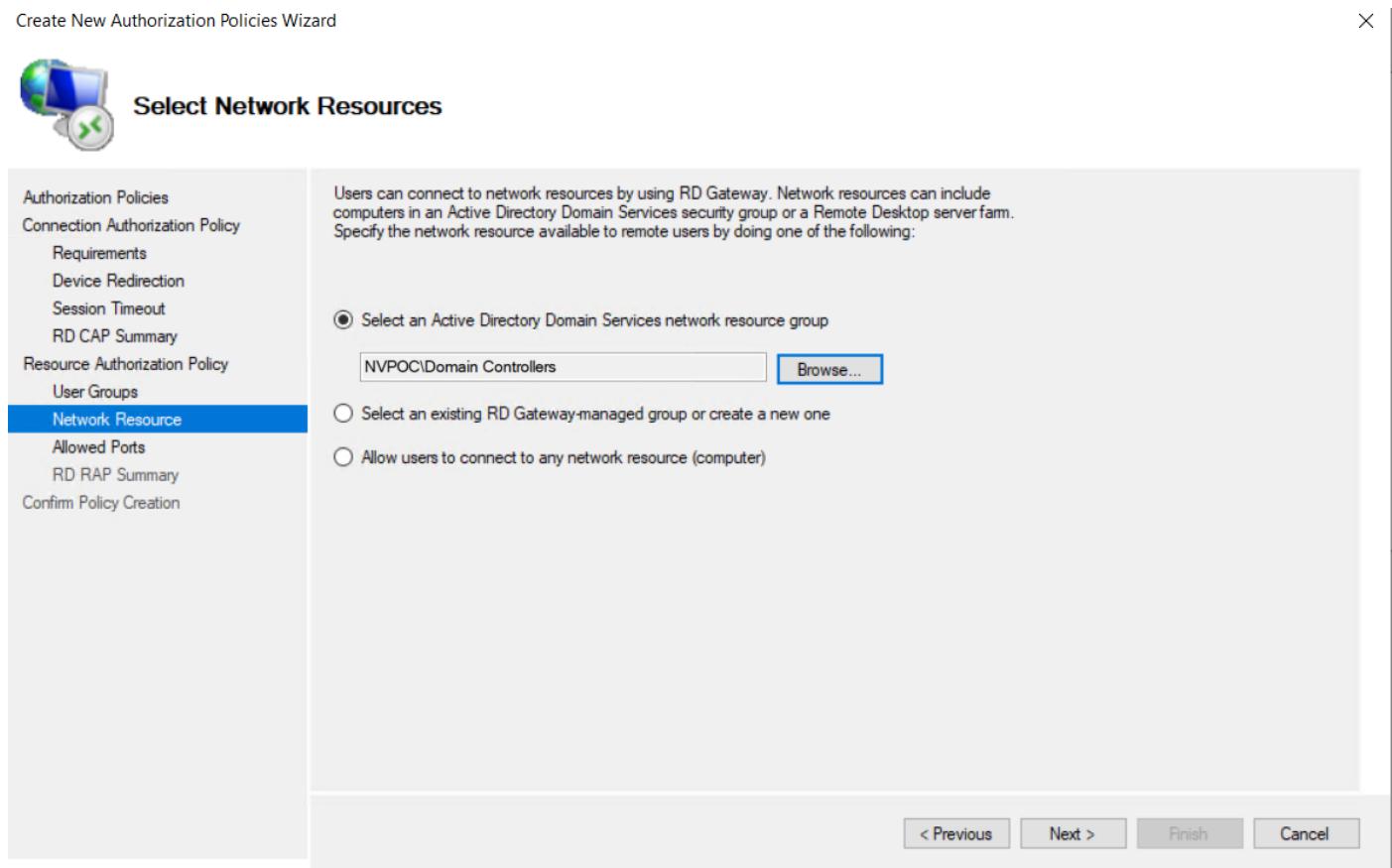
Eenmal dit klaar is gaan we door naar het configureren van de RD RAP.



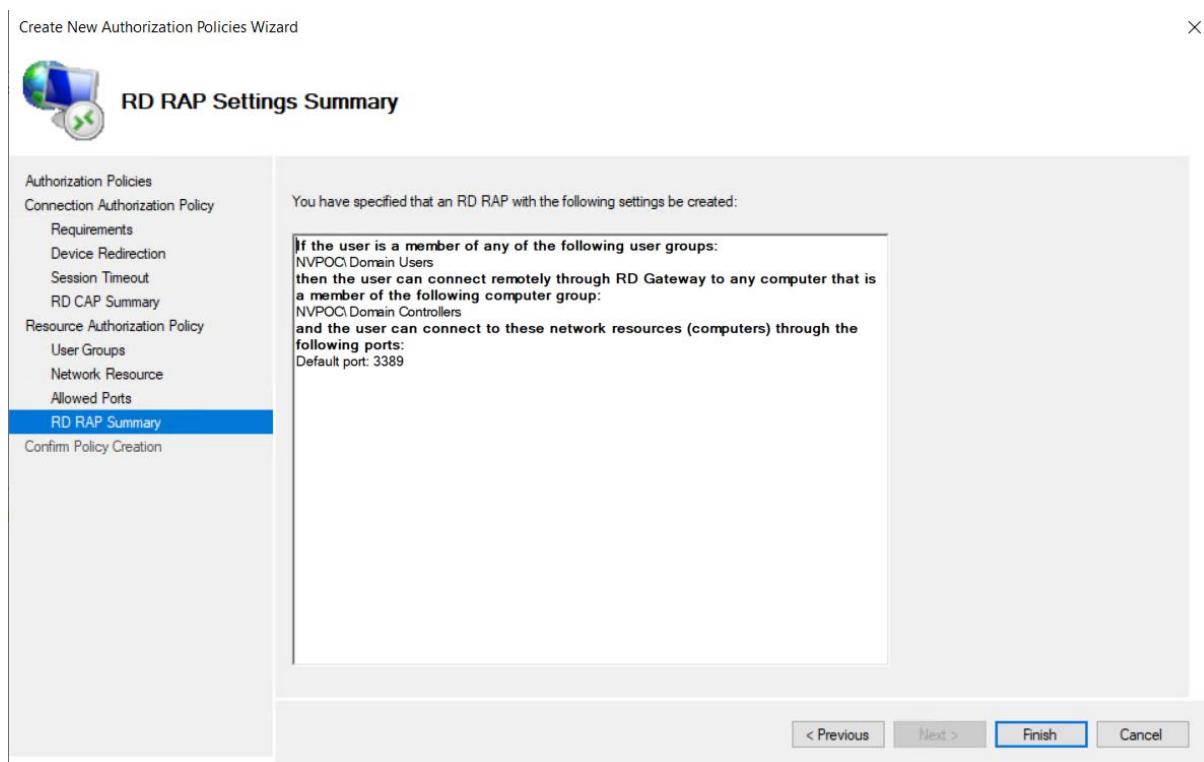
Hier kiezen we weer voor de users van ons domein.



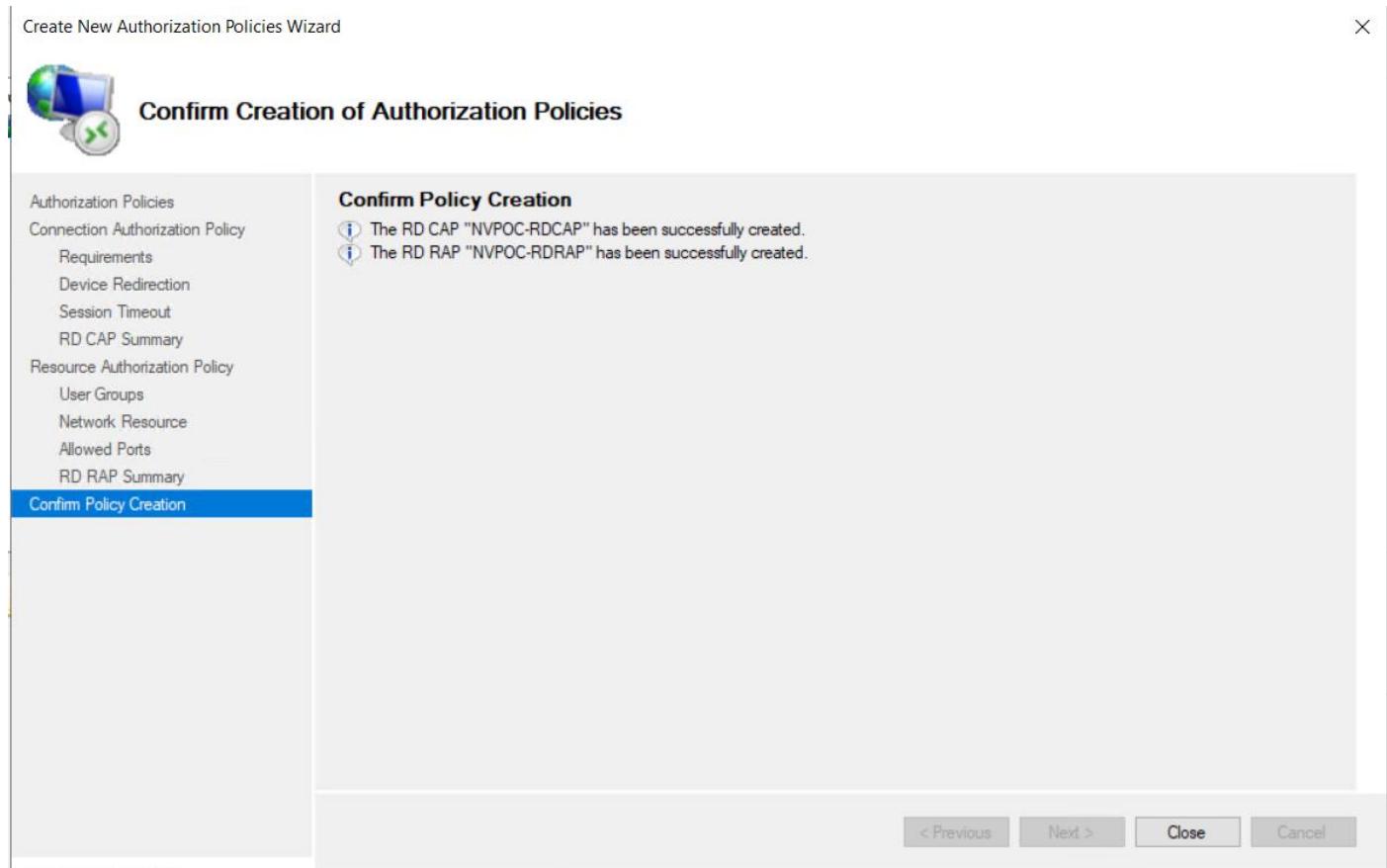
Bij network resource kiezen wij voor de bestaande domain controllers toe te voegen. En geven wij standaard poort 3389 toe bij "allowed ports".



Hier zien we wij een overzicht van de RD RAP die we net hebben geconfigureerd.



Hier krijgen we een bevestiging dat alles goed is geconfigureerd.

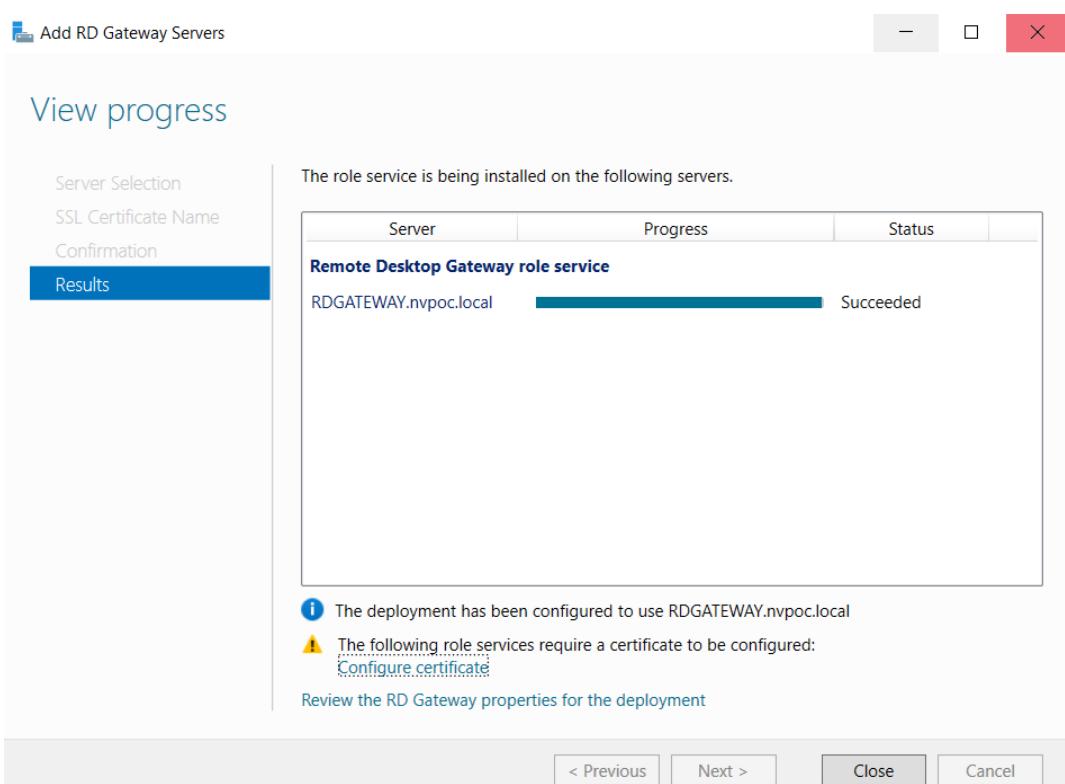
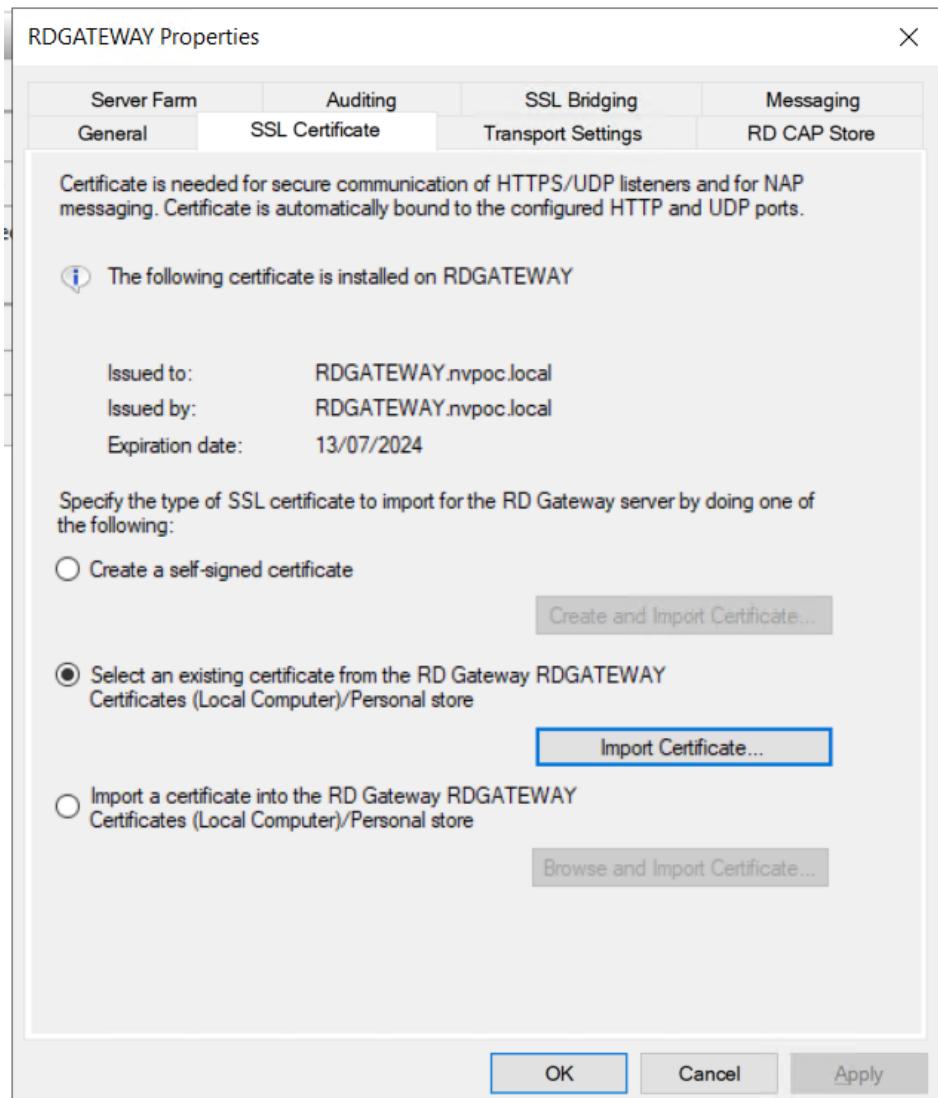


Vervolgens importeren wij een certificaat die we hebben aangemaakt.

Order	Policy (Applied in Order Listed)	User Groups	Client Computer Groups	Status
1	NVPOC-RDCAP	NVPOC\Domain Users	Not applicable (no computer gr...)	Enabled

NVPOC-RDCAP
Policy Status: Enabled
Apply this policy when a user attempts to connect to the RD Gateway server:

- If the user is a member of any of the following user groups:
NVPOC\Domain Users
- If the client computer is a member of any of the following computer groups:
Not applicable (no computer group is specified)
- If the user uses the following supported Windows authentication methods:
Password
- Allow the user to connect to this RD Gateway server and disable device redirection for the following client devices:
Not applicable (device redirection is allowed for all client devices)
- After the idle timeout is reached:
- Not applicable (no idle timeout)
- After the session timeout is reached:
- Not applicable (no session timeout)



2.8 TrueNAS

Voor opslag gebruiken wij de virtuele versie van een NAS, TrueNAS. Via [deze video](#) hebben wij een TrueNAS geconfigureerd. Wij gebruiken dit om een shared folder te maken, die beschikbaar is voor heel het domein.

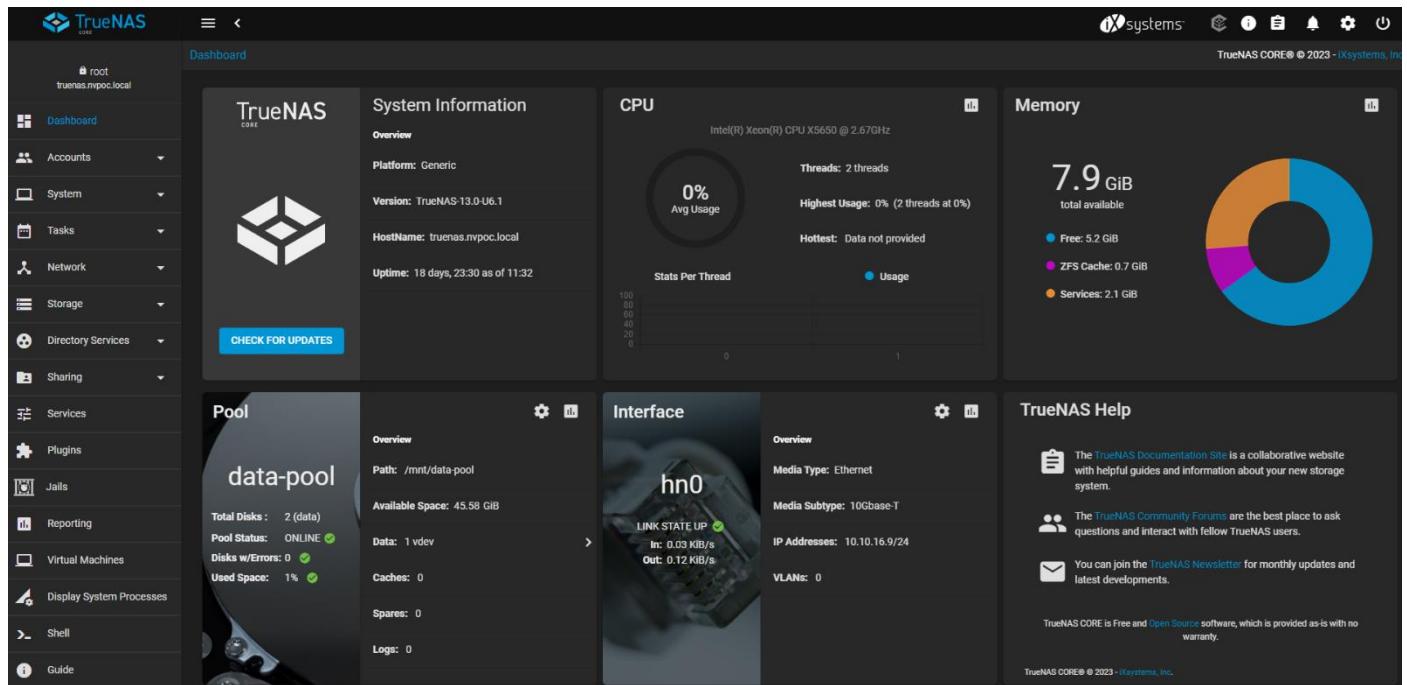
```
88 -- restrict: ignoring line 12, address/host '2.freebsd.pool.ntp.org' unusabl
e.

Console setup
-----
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:
http://10.10.16.9
https://10.10.16.9

Enter an option from 1-11: ■
```

Bij het configureren hebben we een IP meegegeven dat uit de range komt van onze server VLAN. Hierna kan je browsen naar 10.10.16.9 om op de TrueNAS GUI te komen voor verdere configuraties.



NV POC

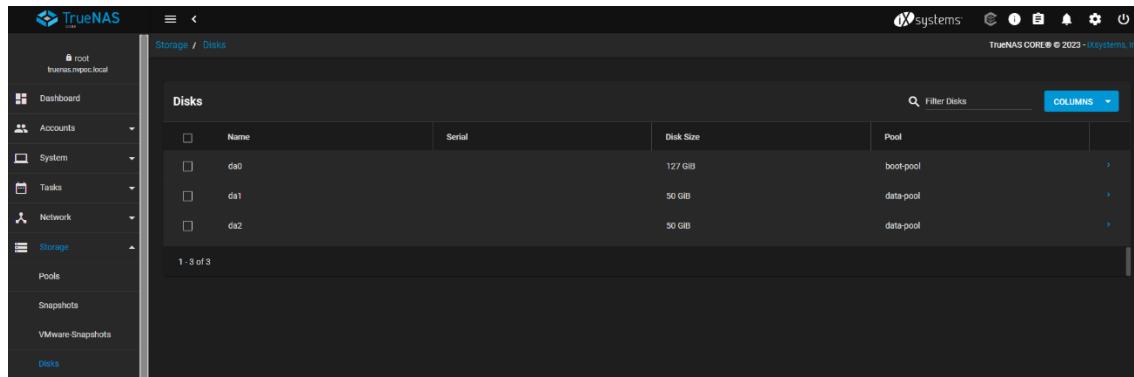
Het toewijzen naar domein nvpoc.local en naar onze DC1 als DNS moet gedaan worden, om de TrueNAS aan de Active Directory toe te voegen.

The screenshot shows the 'Global Configuration' section under 'Network'. It includes fields for Hostname (truenas), Domain (nvpoc.local), and Additional Domains. Under 'Service Announcement', 'mDNS' and 'WS-Discovery' are checked. 'DNS Servers' lists Nameserver 1 (10.10.16.20) and Nameserver 2. 'Default Gateway' shows IPv4 Default Gateway as 10.10.16.1. 'Other Settings' includes an 'HTTP Proxy' section with a checkbox for 'Enable Netwait Feature'.

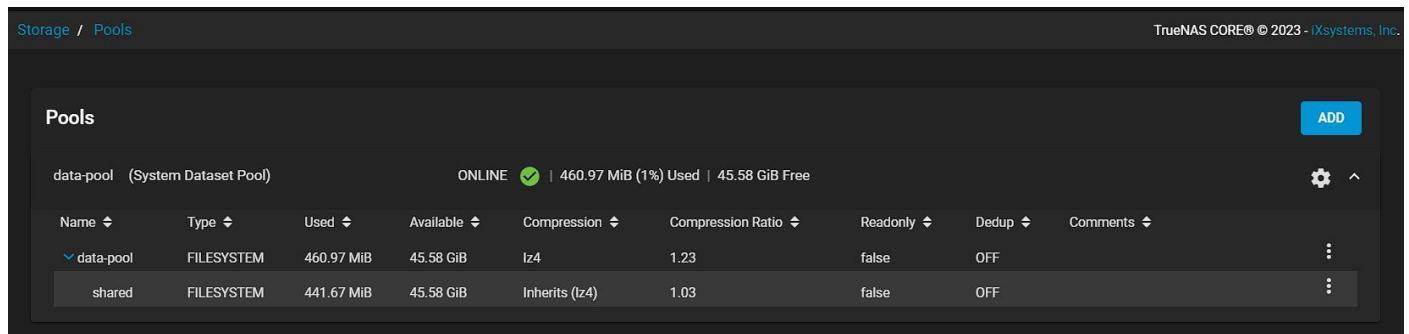
The screenshot shows the 'Network Summary' section under 'Network'. It displays the 'Interfaces' table with one entry for 'hn0' with an IPv4 address of 10.10.16.9/24. The 'Default Routes' table shows a single route to 10.10.16.1. The 'Nameservers' table lists a nameserver at 10.10.16.20.

NV POC

Het is belangrijk om op een Nas een storage methode te gebruiken dit doe je aan de hand van een RAID. TrueNAS draait op een virtueel disk we hebben hierop een data pool aangemaakt die onze disk in mirror gaan zetten (RAID 1).

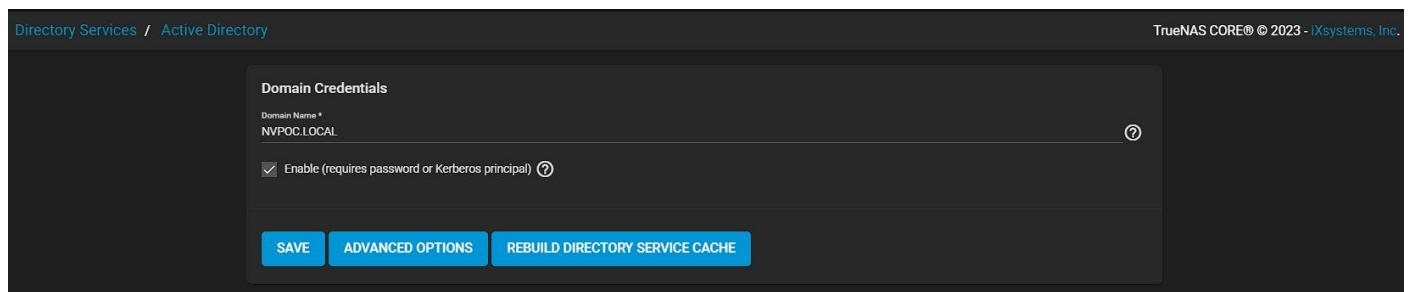


The screenshot shows the 'Disks' section of the TrueNAS web interface. It lists three physical disks: da0 (127 GiB), da1 (50 GiB), and da2 (50 GiB). Each disk is associated with a pool: boot-pool for da0, data-pool for da1, and data-pool for da2. The interface includes a search bar and a 'COLUMNS' dropdown.



The screenshot shows the 'Pools' section of the TrueNAS web interface. It displays the 'data-pool' pool, which is an online system dataset pool. The table shows two datasets: 'shared' (FILESYSTEM, 441.67 MiB used, 45.58 GiB free) and 'data-pool' (FILESYSTEM, 460.97 MiB used, 45.58 GiB free). The 'data-pool' dataset inherits its compression settings from its parent pool.

Bij Directory services ga je naar Active Directory. Domain Name wordt toegevoegd en het kan ook zijn dat je account credentials moet meegegeven. Na het drukken op save komt de Truenas op Active directory te staan bij computers.



The screenshot shows the 'Active Directory' configuration page. It includes fields for 'Domain Name' (NVPOC.LOCAL) and a checked checkbox for 'Enable (requires password or Kerberos principal)'. At the bottom are buttons for 'SAVE', 'ADVANCED OPTIONS', and 'REBUILD DIRECTORY SERVICE CACHE'.

NV POC

Voor een shared folder aan te maken en te linken met uw Windows shares (SMB) nodig. Daarna ga je de folder meegegeven dat gedeeld moet worden. Het is ook belangrijk dat de folder voor Everyone op full control staat omdat deze later gaan aanpassen op DC1 Volgens AGDLP principe.

The image consists of three vertically stacked screenshots from the TrueNAS CORE web interface.

Screenshot 1: Active Directory Configuration

This screenshot shows the "Domain Credentials" section under "Active Directory". It includes fields for "Domain Name" (set to "NVPOC.LOCAL") and a checked "Enable" checkbox. Below the form are buttons for "SAVE", "ADVANCED OPTIONS", and "REBUILD DIRECTORY SERVICE CACHE".

Screenshot 2: Sharing Settings

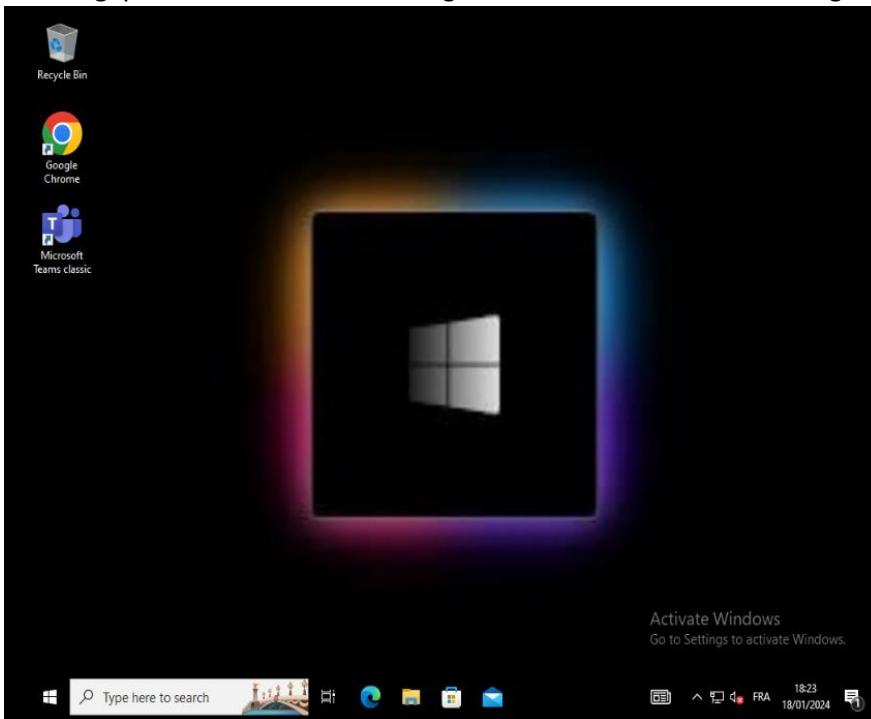
This screenshot shows the "Sharing" page with a sidebar containing links for Apple Shares (AFP), Block Shares (iSCSI), Unix Shares (NFS), WebDAV Shares, and Windows Shares (SMB). The "Windows Shares (SMB)" link is highlighted. The main area shows a "Basic" configuration for a share named "Shared" with path "/mnt/data-pool/shared". The "Enabled" checkbox is checked. Buttons for "SAVE", "CANCEL", and "ADVANCED OPTIONS" are at the bottom.

Screenshot 3: Samba Share List

This screenshot shows the "Samba" share list. A single share named "Shared" is listed with path "/mnt/data-pool/shared", description "", and enabled status "yes". The list includes a header row with columns for "Name", "Path", "Description", and "Enabled". Buttons for "COLUMNS" and "ADD" are at the top right.

2.9 Windows Client

Na alle GPO's uitgevoerd te hebben, kijken we of alles in orde is op onze client. We loggen in op onze user en zien het aangepaste bureaublad met Google Chrome en Microsoft Teams geïnstalleerd en aanwezig op ons bureaublad.



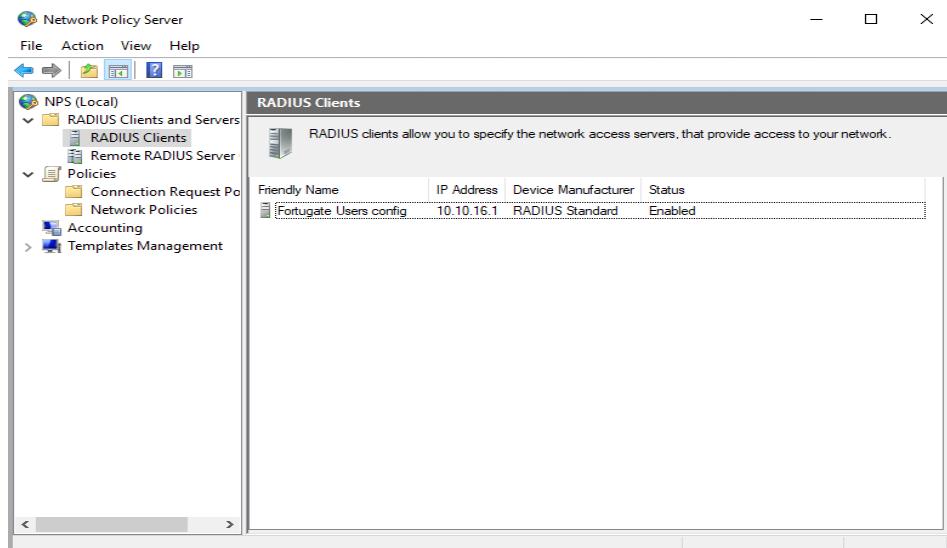
We zien dat onze fileshare die we hebben aangemaakt is voor onze client. Deze client kan enkel de downloads zien en zijn toegewezen directory, die van "boekhouding". Dit is belangrijk mocht de gebruiker iets willen van bestanden kan hij aan zijn files via zijn toegewezen directory.

Name	Date modified	Type	Size
Boekhouding	06/01/2024 12:27	File folder	
Downloads	04/01/2024 15:20	File folder	

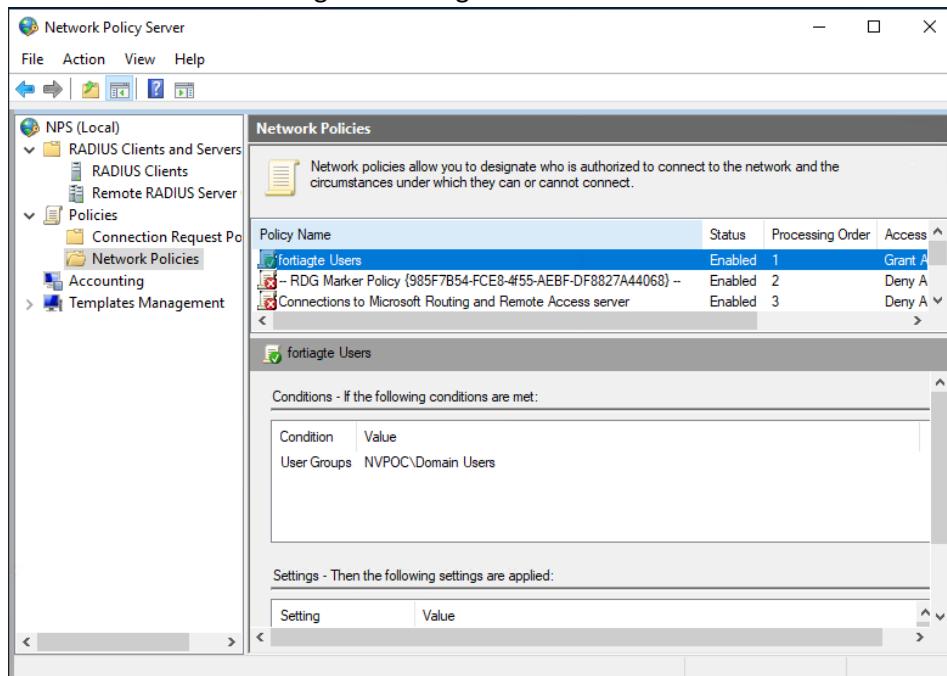
2.10 Radius Server

Voor de radius is het belangrijk dat elke users in het domein ook op het netwerk kan verbinding. Voor security is dit ook een groot pluspunt dat iedereen zijn eigen login heeft. Je kan users deleten van het domein en hebben ze zo geen access meer.

Eerst maken we een radius client en geven we de default gateway van on server IP. We zorgen er ook voor dat we de secret onthouden omdat we dit ook gaan moeten ingeven op de firewall.



Bij policies heb ik als Access client ipv4 adres meegegeven. Je moet een nieuwe network policy aanmaken waar we dan ook de domain users gaan toevoegen.



Via [Fortinet Community](#) kan je de stappen terugvinden hoe dat je radius moet instellen alsook op de Fortigate firewall.

3. Cloud

Voor een IT-bedrijf is werken in de Cloud zeer belangrijk. Van Active Directory tot licenties geven aan users. Zonder Cloud ben je als bedrijf niet echt voorbereid op het falen van hardware on premise.

3.1 Azure

We hebben besloten om een 2^{de} domain controller te configureren in de cloud. Dit zorgt voor redundantie aangezien we de Domain controller gaan gebruiken als back-up. Met een gelimiteerde Azure Portal saldo hebben wij een site to site VPN opgebouwd en deze geconnecteerd aan onze firewall on premise. Hier maakten we gebruik van de [fortigate cookbook](#) om deze link te leggen tussen on premise en cloud.

3.1.1 Terraform

Om onze VPN en Windows server aan te maken gebruiken wij een Terraform script. Deze software kan een hele Azure omgeving laten opbouwen via een script. Het voordeel hier van is dat we dit later kunnen hergebruiken. Als eerst maken we een directory aan genaamd "projectoncampuscloud". Daarna gaan we via volgend commando in de command prompt een main.tf file aanmaken.

```
C:\Users\Zacha\projectoncampuscloud>type nul > main.tf
```

We loggen in met "az login", en melden ons aan met ons Azure account waar we mee gaan werken.

```
C:\Users\Zacha\projectoncampuscloud>az login
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue the login in the web
b browser fails to open, use device code flow with `az login --use-device-code`.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "c2a59f2b-5d20-4b2a-a9a3-7a8605b14e3f",
    "id": "0fd680ca-276e-411d-971d-cc0f966b1959",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Azure for Students",
    "state": "Enabled",
    "tenantId": "c2a59f2b-5d20-4b2a-a9a3-7a8605b14e3f",
    "user": {
      "name": "zacharias.osselaer@student.ehb.be",
      "type": "user"
    }
  }
]
```

"Terraform init" zorgt ervoor dat je werkomgeving correct geconfigureerd is en klaar is voor andere Terraform commando's zoals 'terraform plan' of 'terraform apply'. Nu edit je je .tf file in je favoriete tekst-editor, ik gebruik visual studio code.

```
C:\Users\Zacha\projectoncampuscloud>terraform init
Initializing the backend...
Initializing provider plugins...
- Reusing previous version of hashicorp/azurerm from the dependency lock file
- Using previously-installed hashicorp/azurerm v3.87.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

NV POC

```
main.tf
C: > Users > Zacha > projectoncampuscloud > main.tf > resource "azurerm_network_interface" "cloud-windowsserver686_z3" > ip_configuration > private_ip_address
1 provider "azurerm" {
2   features {}
3 }
4
5 resource "azurerm_resource_group" "cloud-RG" {
6   name     = "cloud-RG"
7   location = "East US"
8 }
9
10 resource "azurerm_virtual_network" "cloud-VN" {
11   name          = "cloud-VN"
12   address_space = ["10.0.0.0/16"]
13   location      = azurerm_resource_group.cloud-RG.location
14   resource_group_name = azurerm_resource_group.cloud-RG.name
15 }
16
17 resource "azurerm_subnet" "default" {
18   name          = "default"
19   resource_group_name = azurerm_resource_group.cloud-RG.name
20   virtual_network_name = azurerm_virtual_network.cloud-VN.name
21   address_prefixes = ["10.0.0.0/24"]
22 }
23
24
25 resource "azurerm_subnet" "GatewaySubnet" {
26   name          = "GatewaySubnet"
27   resource_group_name = azurerm_resource_group.cloud-RG.name
28   virtual_network_name = azurerm_virtual_network.cloud-VN.name
29   address_prefixes = ["10.0.1.0/24"]
30 }
31
32 resource "azurerm_public_ip" "cloud-PIP" {
33   name          = "cloud-PIP"
34   location      = azurerm_resource_group.cloud-RG.location
35   resource_group_name = azurerm_resource_group.cloud-RG.name
36
37   allocation_method = "Dynamic"
38 }
39
40 resource "azurerm_virtual_network_gateway" "cloud-VNG" {
41   name          = "cloud-VNG"
42   location      = azurerm_resource_group.cloud-RG.location
43   resource_group_name = azurerm_resource_group.cloud-RG.name
44
45   type    = "Vpn"
46   vpn_type = "RouteBased"
47
48   active_active = false
49   enable_bgp   = false
50   sku         = "VpnGw1"
51
52   ip_configuration {
53     name          = "vnetGatewayConfig"
54     public_ip_address_id = azurerm_public_ip.cloud-PIP.id
55     private_ip_address_allocation = "Dynamic"
56     subnet_id      = azurerm_subnet.GatewaySubnet.id
57   }
58 }
59
60 resource "azurerm_local_network_gateway" "OnPremiseGateway" {
61   name          = "OnPremiseGateway"
62   resource_group_name = azurerm_resource_group.cloud-RG.name
63   location      = azurerm_resource_group.cloud-RG.location
64   gateway_address = "193.191.183.42"
65   address_space = ["10.10.16.0/24"]
66 }
```

NV POC

```
67
68 resource "azurerm_virtual_network_gateway_connection" "VPN" {
69   name          = "VPN"
70   location      = azurerm_resource_group.cloud-RG.location
71   resource_group_name = azurerm_resource_group.cloud-RG.name
72
73   type          = "IPsec"
74   virtual_network_gateway_id = azurerm_virtual_network_gateway.cloud-VNG.id
75   local_network_gateway_id  = azurerm_local_network_gateway.OnPremiseGateway.id
76
77   shared_key = "student123"
78 }
79
80 resource "azurerm_public_ip" "cloud-windowsserver-ip" {
81   name          = "cloud-windowsserver-ip"
82   location      = azurerm_resource_group.cloud-RG.location
83   resource_group_name = azurerm_resource_group.cloud-RG.name
84   allocation_method = "Dynamic"
85 }
86
87 resource "azurerm_network_interface" "cloud-windowsserver686_z3" {
88   name          = "cloud-windowsserver686_z3"
89   location      = azurerm_resource_group.cloud-RG.location
90   resource_group_name = azurerm_resource_group.cloud-RG.name
91
92   ip_configuration {
93     name          = "internal"
94     subnet_id    = azurerm_subnet.default.id
95     private_ip_address_allocation = "Static"
96     private_ip_address = "10.0.0.4"
97     public_ip_address_id = azurerm_public_ip.cloud-windowsserver-ip.id
98   }
99 }
```

```
100
101
102 resource "azurerm_network_security_group" "cloud-windowsserver-nsg" {
103   name          = "cloud-windowsserver-nsg"
104   location      = azurerm_resource_group.cloud-RG.location
105   resource_group_name = azurerm_resource_group.cloud-RG.name
106
107   security_rule {
108     name          = "rdpport"
109     priority      = 100
110     direction     = "Inbound"
111     access        = "Allow"
112     protocol      = "Tcp"
113     source_port_range = "*"
114     destination_port_range = "3389"
115     source_address_prefix = "*"
116     destination_address_prefix = "*"
117   }
118
119   tags = {
120     environment = "Testing"
121   }
122 }
123
124 # Associate security group with network interface
125 resource "azurerm_network_interface_security_group_association" "cloud-association" {
126   network_interface_id    = azurerm_network_interface.cloud-windowsserver686_z3.id
127   network_security_group_id = azurerm_network_security_group.cloud-windowsserver-nsg.id
128 }
```

NV POC

```
129
130 resource "azurerm_windows_virtual_machine" "cloud-windowsserver" {
131   name           = "cloud-windowsserver"
132   resource_group_name = azurerm_resource_group.cloud-RG.name
133   location        = azurerm_resource_group.cloud-RG.location
134   size            = "Standard_B2s"
135   admin_username  = "NVPOC"
136   admin_password  = "Nvpoc2023"
137   network_interface_ids = [
138     azurerm_network_interface.cloud-windowsserver686_z3.id,
139   ]
140
141   os_disk {
142     caching          = "ReadWrite"
143     storage_account_type = "Standard_LRS"
144   }
145
146   source_image_reference {
147     publisher = "MicrosoftWindowsServer"
148     offer     = "WindowsServer"
149     sku       = "2019-Datacenter"
150     version   = "latest"
151   }
152 }
```

Na het schrijven van het script, typ je “terraform apply” om dit script te launchen.

```
C:\Users\Zacha\projectoncampuscloud>terraform apply
[Output]
Apply complete! Resources: 13 added, 0 changed, 0 destroyed.
```

3.1.2 Virtual Network

Hier zien we ons aangemaakte Virtueel netwerk.

Resource group (move) : cloud-RG	Address space : 10.0.0.0/16
Location (move) : East US	DNS servers : Azure provided DNS service
Subscription (move) : Azure for Students	Flow timeout : Configure
Subscription ID : 0fd680ca-276e-411d-971d-cc0f966b1959	BGP community string : Configure
	Virtual network ID : f4cd70aa-dfb0-4715-afe2-62ba2580c79c

Wat belangrijk is, is het aanmaken van een default subnet en een gateway subnet. Gateway subnet is belangrijk om een virtual network gateway aan te maken.

Name ↑	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	...
default	10.0.0.0/24	-	251	-	-	-	...
GatewaySubnet	10.0.1.0/24	-	availability dependent on d...	-	-	-	...

3.1.3 Virtual Network Gateway

De volgende stap is de aanmaak van een virtual network gateway. Dit is één van de belangrijkste zaken om een connectie te maken tussen on premise en de Cloud. Hierbij maak je ook een nieuw publiek IP aan die we nodig hebben voor te configureren langs de firewall kant. Let op deze deployment duurt 30-45 minuten!

Resource group (move) : cloud-RG	SKU : VpnGw1
Location : East US	Gateway type : VPN
Subscription (move) : Azure for Students	VPN type : Route-based
Subscription ID : 0fd680ca-276e-411d-971d-cc0f966b1959	Virtual network : cloud-VN/GatewaySubnet
	Public IP address : 172.172.179.7 (cloud-PIP)

3.1.4 Local Network Gateway

Om de connectie te vervolledigen heb je een local network gateway nodig. Dit is onze on premise kant. Hierbij geven we ons publiek IP van onze firewall en onze IP van onze server.

Resource group (move) : cloud-RG	IP address : 193.191.183.42
Location : East US	Address Space(s) : 10.10.16.0/24
Subscription (move) : Azure for Students	
Subscription ID : 0fd680ca-276e-411d-971d-cc0f966b1959	

3.1.5 Connection

Om een connectie aan te maken, moet je “connection” aanmaken waar je je lokale gateway en je virtuele gateway aangeeft.

	:	
Data in	:	0 B
Data out	:	0 B
Virtual network	:	cloud-VN
Virtual network gateway	:	cloud-VNG
Local network gateway	:	OnPremiseGateway (193.191.183.42)

3.1.6 Tunnel in Firewall (on premise)

Nu we een connectie hebben gemaakt via Azure, moeten we nu ook één maken via de firewall. Hier geven wij het publiek IP van Azure aan en geven we de juiste shared key en algorithms mee volgens de fortigate cookbook.

3.1.7 Adresses in Firewall (on Premise)

Het aangeven van ons virtueel netwerk op Azure is een must. Wij geven dit aan en verwijzen naar de juiste interface.

3.1.8 Policies in Firewall (on Premise)

Zonder policies gaat er geen connectie zijn tussen firewall en Azure. We maken 2 policies tussen de server (10.10.16.0/24) en de tunnel interface. Hierbij gaan wij de eerder aangemaakt adres van Azure aangeven.

Name: ToAzureVPN

Incoming Interface: Server

Outgoing Interface: ToAzureVPN

Source: all

IP/MAC Based Access Control:

Destination: AzureVirtualNetwork01

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT:

Protocol Options: PROT default

Server → ToAzureVPN ①

ToAzureVPN → all

AzureVirtualNetwork01 → always

ALL → ALL

✓ ACCEPT → ✓ ACCEPT

✗ Disabled → ✗ Disabled

SSL no-inspection → SSL no-inspection

UTM → UTM

0 B → 0 B

Name: FromAzureVPN

Incoming Interface: ToAzureVPN

Outgoing Interface: Server

Source: AzureVirtualNetwork01

IP/MAC Based Access Control:

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT:

Protocol Options: PROT default

ToAzureVPN → Server ①

FromAzureVPN → AzureVirtualNetwork01

all → all

always → always

ALL → ALL

✓ ACCEPT → ✓ ACCEPT

✗ Disabled → ✗ Disabled

SSL no-inspection → SSL no-inspection

UTM → UTM

0 B → 0 B

3.1.9 Static route in Firewall (on Premise)

Een static route maken is van groot belang. Het zegt hoe de firewall het verkeer moet doorsturen tussen het lokale netwerk en de Cloud.

Automatic gateway retrieval

Destination

Subnet	Internet Service
10.0.0.0/255.255.0.0	
Interface	ToAzureVPN <input type="button" value="x"/>
<input type="button" value="+"/>	
Administrative Distance <input type="button" value="i"/>	2
Comments	Write a comment... <input type="text" value=""/> 0/255
Status	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>

Hier hebben we een Ubuntu VM gemaakt op de Cloud om eens te testen of we konden pingen naar onze gateway van onze server.

```
azureuser@cloud-ubuntu:~$ ping 10.10.16.1
PING 10.10.16.1 (10.10.16.1) 56(84) bytes of data.
64 bytes from 10.10.16.1: icmp_seq=1 ttl=255 time=90.4 ms
64 bytes from 10.10.16.1: icmp_seq=2 ttl=255 time=90.1 ms
64 bytes from 10.10.16.1: icmp_seq=3 ttl=255 time=90.0 ms
64 bytes from 10.10.16.1: icmp_seq=4 ttl=255 time=90.9 ms
```

3.1.10 Domain Controller 2

Na het opbouwen van de Virtuele machine krijgen wij een publiek IP voor te connecteren met onze Virtuele machine. We krijgen een .rdp file van Azure waar we makkelijk mee kunnen connecteren. Voor kosten te besparen stop ik mijn virtuele machine na gebruik, want de kosten kunnen zo makkelijk opstapelen.

The screenshot shows the Azure portal interface for managing a virtual machine named 'cloud-windowsserver'. The machine is currently stopped. Key details include:

- Resource group:** cloud-RG
- Status:** Stopped (deallocated)
- Location:** East US (Zone 3)
- Subscription:** Azure for Students
- Public IP address:** 20.55.37.91
- Virtual network/subnet:** cloud-VN/default
- DNS name:** Not configured
- Health state:** -
- Tags:** Add tags

The portal also displays the VM's properties, networking settings (including a public IP of 20.55.37.91), size (Standard B2s), and disk information.

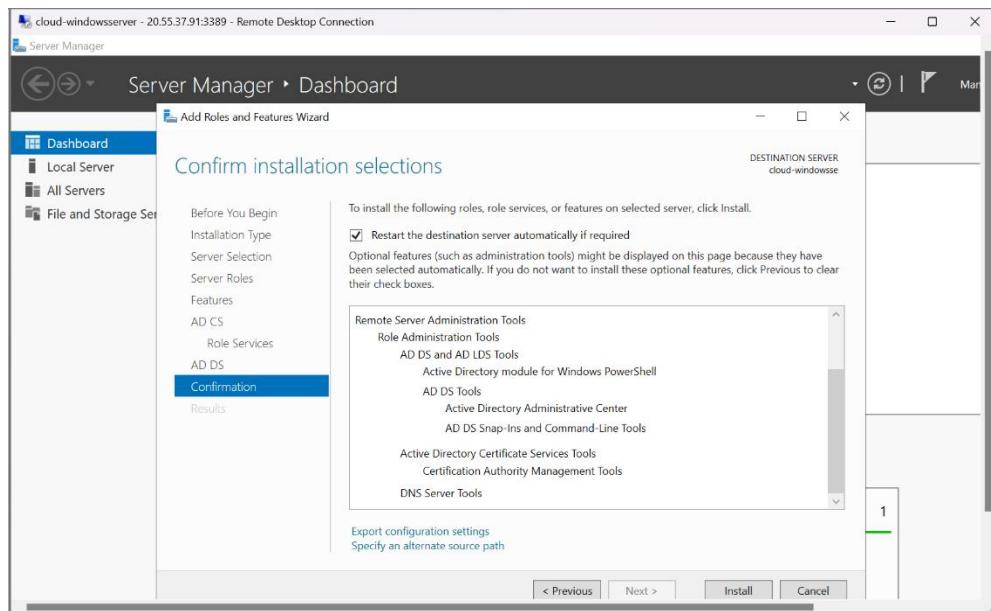
Het eerste wat we gaan doen is via de advanced adapter options zorgen dat we een statisch IP-adres krijgen. Ook geven we onze IP van onze 1^{ste} domain controller mee als DNS server.

```
Ethernet adapter Ethernet:

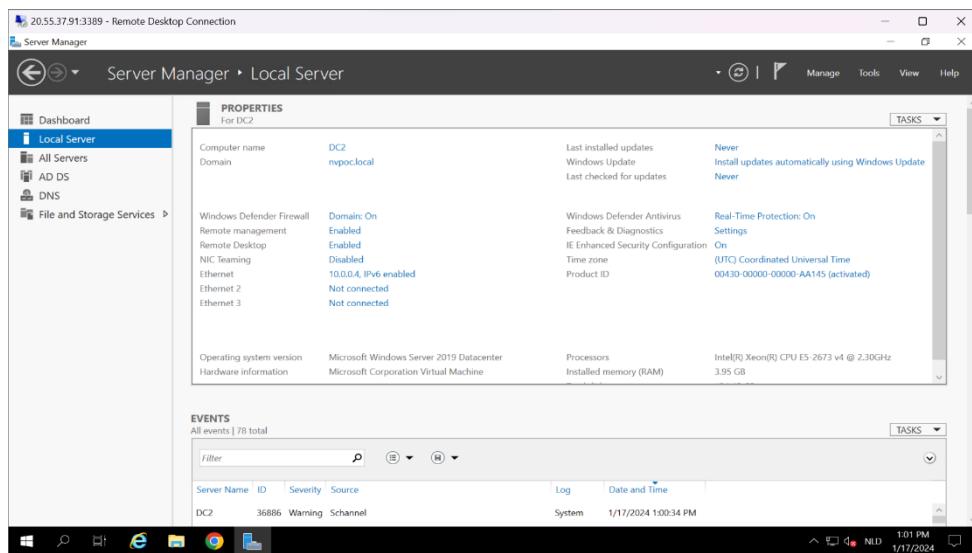
Connection-specific DNS Suffix . . . .
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address . . . . . : 60-45-BD-FE-7F-7B
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2fa4:1b95:8524:d0f5%5(Preferred)
IPv4 Address. . . . . : 10.0.0.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1
DHCPv6 IAID . . . . . : 106972605
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-38-D1-E9-60-45-BD-FE-7F-7B
DNS Servers . . . . . : ::1
                           10.10.16.20
                           127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

NV POC

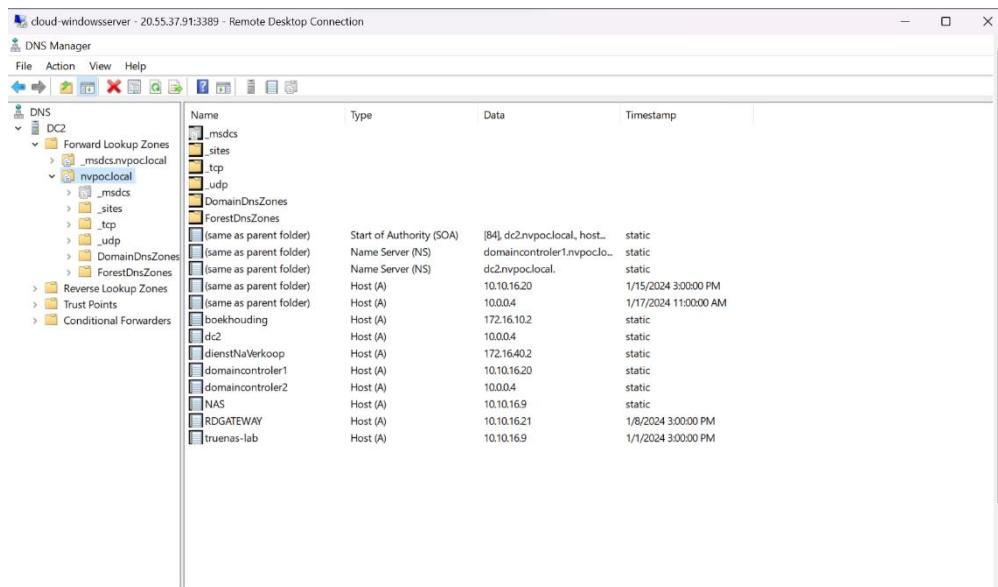
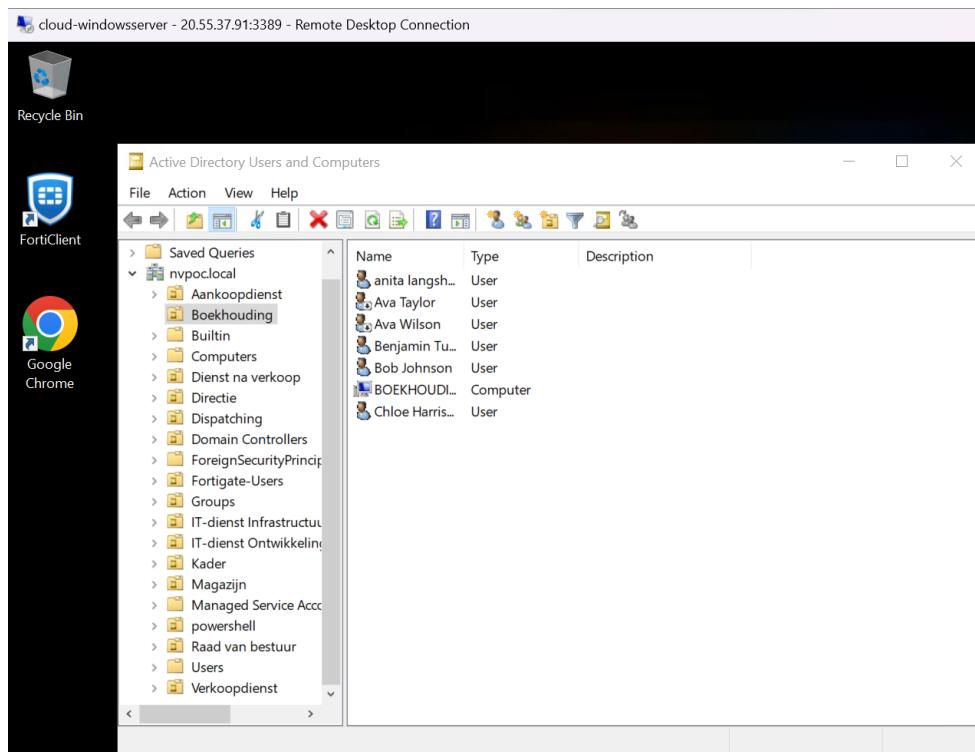
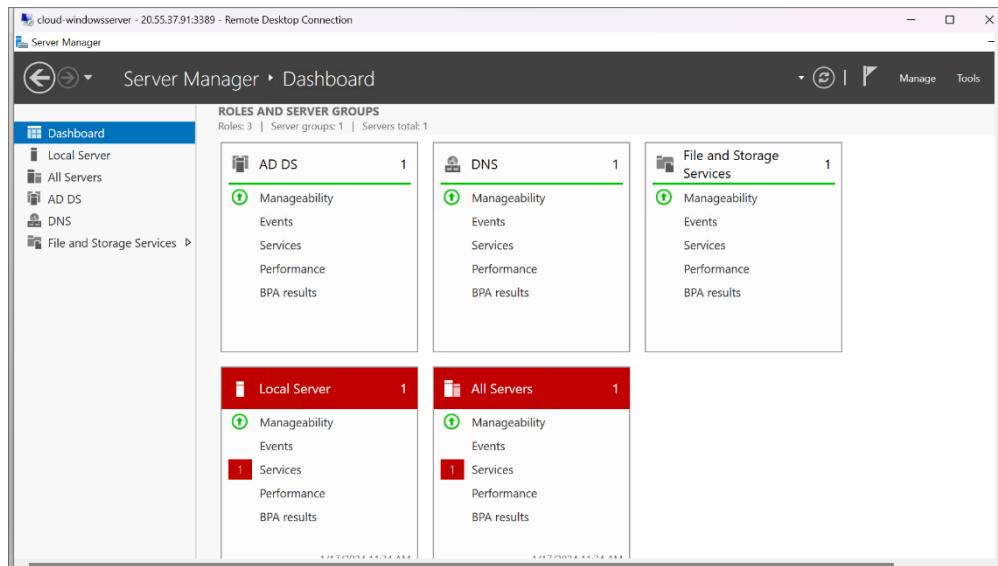
Eenmaal aangekomen in de Windows server manager installeren we Active Directory DS. Zo kunnen we onze server upgraden naar een 2^{de} Domain controller. We verwijderen AD CS terug aangezien we dit niet nodig hebben.



Na de ‘WORKGROUP’ te veranderen naar “nvpoc.local”, kunnen we deze server promoten naar een domain controller. [Deze link](#) laat zien hoe je een nieuwe domain controller maakt. Na het aanmaken van de domain controller zien we dat users, groups, GPO’s,.. allemaal zijn aangemaakt.



NV POC



3.1.11 Microsoft Defender for cloud

Microsoft Defender for cloud is belangrijk als je voor een hybride IT-infrastructuur kiest. Aangezien wij een domain controller op Azure hebben gebruiken wij hiervoor een trial.

The screenshot shows the Microsoft Defender for Cloud security posture dashboard. At the top, there's a green shield icon with a lock and the text "Microsoft Defender for Cloud" followed by "Secure your apps and infrastructure". Below this, there are three sections: "Security posture" (with a shield icon), "Unassigned secure score recommendations" (4/4), and "Overdue secure score recommendations" (0/0). There are also sections for "Attack paths" (0) and a "Secure score" chart comparing Azure (100%), AWS (~50%), and GCP (~50%). A large blue circular progress bar indicates a 100% secure score. At the bottom, a link says "Explore your security posture >".

Microsoft Defender for Cloud

Secure your apps and infrastructure

Security posture

4/4 Unassigned secure score recommendations

0/0 Overdue secure score recommendations

0 Attack paths

Azure 100%

AWS ~50%

GCP ~50%

100% SECURE SCORE

Explore your security posture >

3.2 Microsoft

3.2.1 Intune

Nu gaan we een Microsoft 365 tenant aanmaken. We gebruiken hiervoor een trial. Na het opzetten van deze tenant kunnen we inloggen in de admin center.

Office 365 E5

Office 365 E5 is a cloud-based suite of Microsoft 365 productivity apps combined with advanced voice, analytics, security, and compliance services.

- Install Microsoft 365 for mobile on up to five PCs or Macs, five tablets, and five phones per user.
- Make, receive, and transfer business calls from anywhere, using any device.
- Make informed decisions with data analytics and visualization.
- Safeguard your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.
- Assess your compliance risks, govern and protect sensitive data, and effectively respond to regulatory requirements.

[System requirements >](#)

Talk with an expert

To speak with a sales expert, call 1-855-270-0615. Available Mon to Fri from 6:00 AM to 6:00 PM Pacific Time.

\$38.00 user/month

Annual subscription—auto renews¹

[Buy now](#)

[Try for free >](#)

[See trial terms²](#)

[Contact Sales >](#)

Or

[Compare enterprise plans](#)

[Full comparison \(PDF\) >](#)

Office 365 E5 Trial

One month free with payment details

About you Sign-in details Payment info and finish

Let's get you started

You are signed in with admin@nupoc.com

This account already exists with another Microsoft Service. Continue purchase Office 365 ES Trial for your organization

[Continue](#) Logout and create new account instead

What is Office 365 E5 Trial?

Fully installed Office apps for PC and Mac



(PC Only) (PC Only)

Premium services



Other benefits

- Unlimited personal cloud storage with qualifying plans
- Email hosting with 100 GB mailbox
- Online & desktop versions of Office applications
- Free FastTrack deployment support with 150+ seats

Trial details

- Add up to 25 users during trial
- The free trial will be automatically converted to a paid annual subscription after one month

In order to avoid charges, cancel by 2/16/2024 at the Microsoft 365 Admin Center

3.2.2 Domeinnaam toevoegen

De eerste stap na het aanmaken van de tenant, is het linken van ons eigen domein aan de microsoft365 admin center. Dit doen we door DNS records aan te maken in Cloudflare net zoals Microsoft ons heeft verteld.

The screenshot shows the Microsoft 365 Admin Center with the URL 'https://admin.microsoft.com'. The left sidebar has a tree view with 'Domeinen' selected, which is further expanded to show 'DNS en sub-domeinen'. The main content area is titled 'DNS-records toevoegen' (Add DNS records). It contains a note about adding MX, CNAME, and TXT records for Exchange Online Protection. Below this, there are three tabs: 'CSV-bestand downloaden' (Download CSV file), 'Zoekresultaat downloaden' (Download search results), and 'Afsluiten' (Close). A note at the bottom says 'Als u geen e-mail wilt instellen, wissel u de selectie en ga u verder zonder DNS-records toe te voegen.' (If you don't want to set up email, switch the selection and continue without adding DNS records.)

The screenshot shows the Cloudflare DNS management interface for the domain 'nvpoc.com'. The top bar includes 'Import and Export' and 'Dashboard Display Settings'. The main table lists five DNS records:

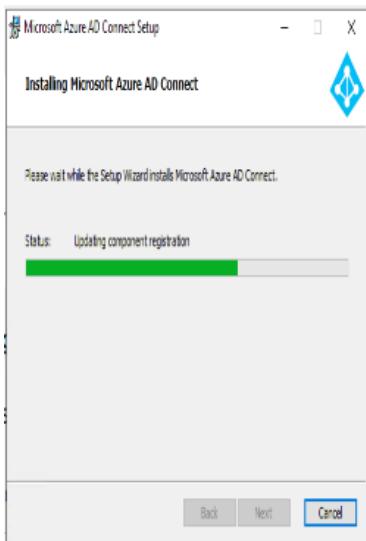
Type	Name	Content	Proxy status	TTL	Actions
TXT	nvpoc.com	v=spf1 include:spf.protection.outlook.co...	DNS only	1 hr	Edit
CNAME	autodiscover	autodiscover.outlook.com	DNS only	1 hr	Edit
MX	nvpoc.com	nvpoc-com.mail.protection.outlook.com	DNS only	1 hr	Edit
A	nvpoc.com	193.191.183.42	Proxied	Auto	Edit
CNAME	www	nvpoc.com	Proxied	Auto	Edit

Na het toevoegen van deze DNS records, kunnen we nieuwe gebruikers aanmaken en deze ons eigen domein meegeven.

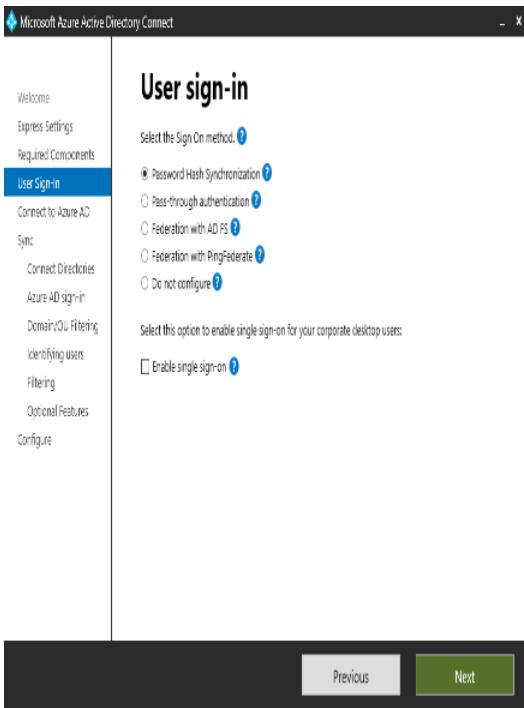
The screenshot shows the Microsoft 365 Admin Center user creation interface. The left sidebar has a tree view with 'Gebruiker toevoegen' selected. The main content area is titled 'Basisinformatie instellen' (Set basic information). It includes fields for 'Voornaam' (First name) containing 'yusuf', 'Achternaam' (Last name) containing 'coban', 'Weergavenaam' (Display name) containing 'Yusuf Coban', 'Gebruikersnaam' (User name) containing 'yusuf.coban', 'Domeinen' (Domains) containing 'nvpoc.com', and several checkboxes for password generation and distribution. A note at the bottom says 'Nieuw wachtwoord per e-mail verzenden naar de volgende geadresseerden' (Send new password by email to the following recipients) with 'group1.nvpoc@hotmail.com' listed.

3.2.3 AD Connect

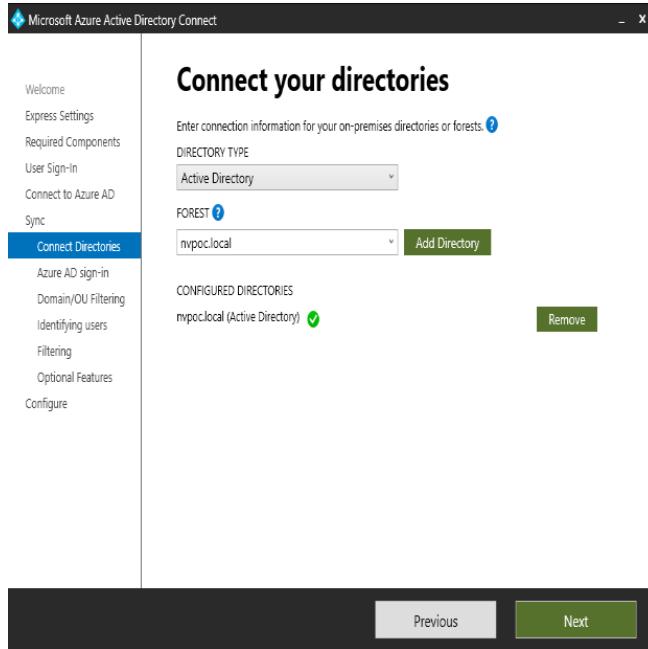
Voor Active directory te synchroniseren met onze Azure AD gebruiken wij AD connect. We volgen deze wizard voor de configuratie.



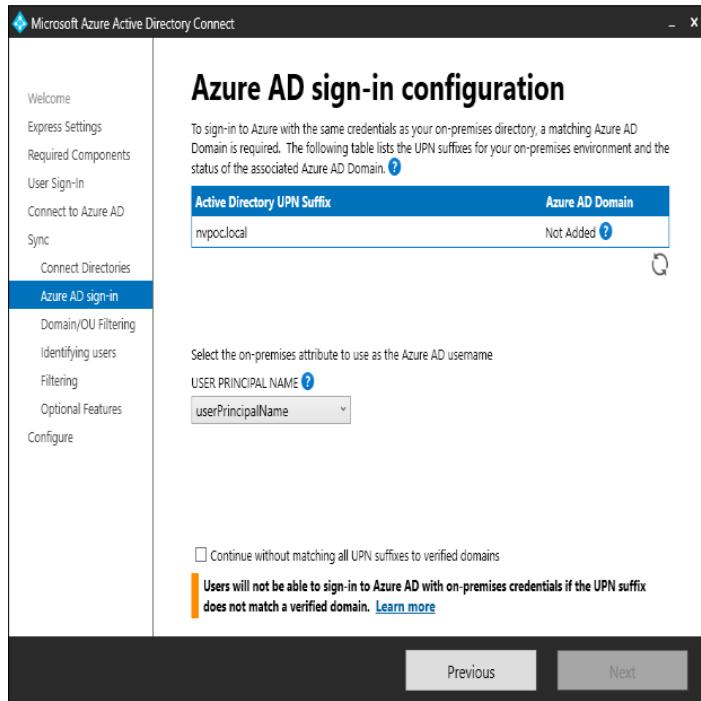
We kiezen hier voor password Hash Synchronisation. De manier waarop het werkt is dat wanneer een wachtwoord lokaal wordt gewijzigd, de password-hash van Active Directory wordt gesynchroniseerd met Microsoft Entra ID. Daarna connecteren we met onze Azure AD.



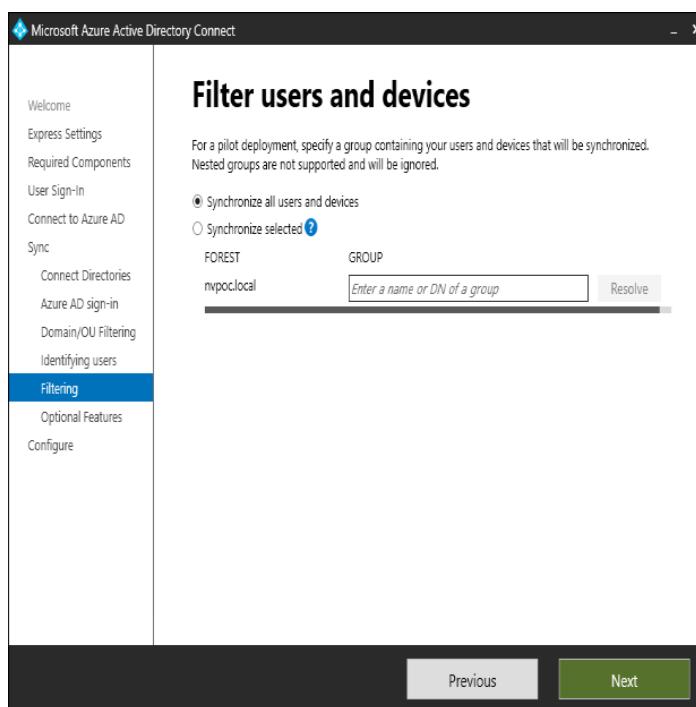
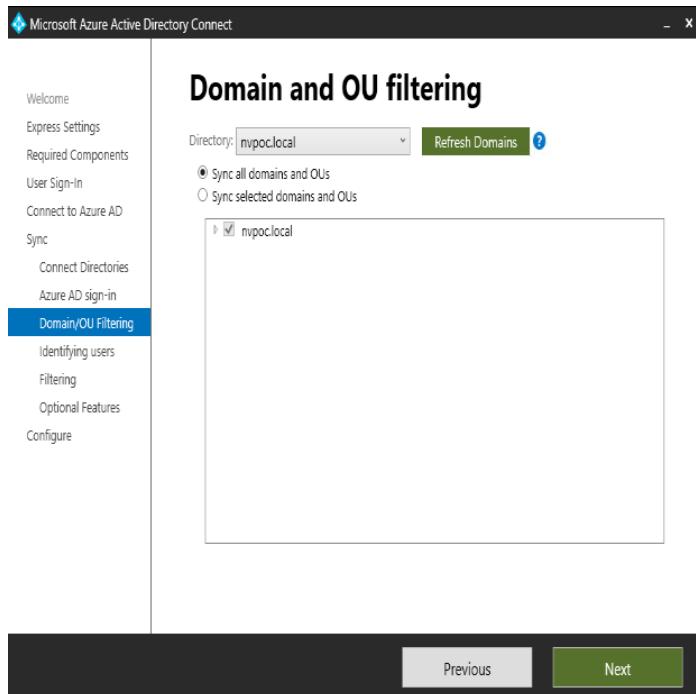
Hier kiezen we onze eigen active directory.



We zien dat ons Azure AD domein niet toegevoegd is, maar dit zou geen probleem veroorzaken voor de volgende stappen.

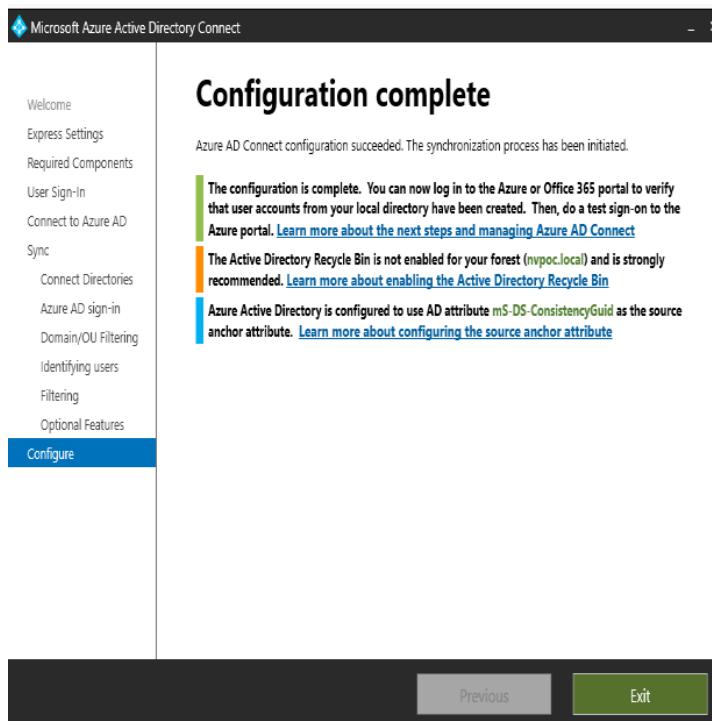
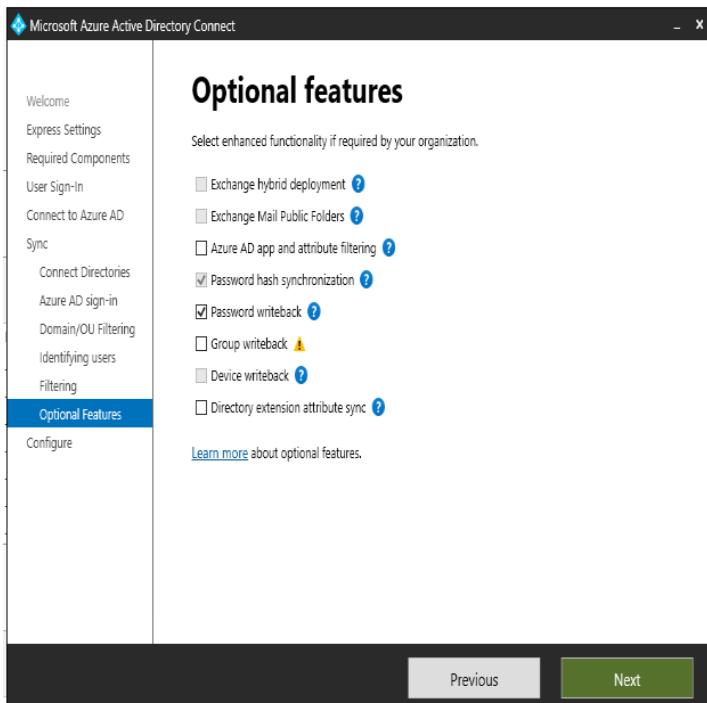


We kiezen hier voor alle domeinen en OU's te synchroniseren & ook de users en groups.



NV POC

We duiden hier password writeback aan. Dit zorgt ervoor dat we via Azure een wachtwoord reset kunnen doen.



Hier zie je dat ik als admin het paswoord kan resetten via Microsoft Entra Admin center.

The screenshot shows a user profile in the Microsoft Entra Admin center. The user is named 'anita.langhoffeld'. On the right side of the profile card, there is a 'Reset password' button. A tooltip for this button explains: 'The user "anita.langhoffeld" will be assigned a temporary password that must be changed on the next sign-in. To change the password, go to the "Forgot password?" page or use SSO and SCA. Note: This password is valid for 14 days.' Below the profile card, there are sections for 'My Profile', 'Sign In', and 'Invitations'.

NV POC

Na het synchroniseren van Active directory met Cloud, kunnen we alle users en groepen zien.

Microsoft Entra admin center

Home > Users > [Search] > [New user] > Download data > [bulkoperations] > [Actions] > Manage view > [Delete] > [Pause MFA] > [Get feedback]

Users

Search: [Search] > [Advanced]

33 users found

Display name	User principal name	User type	On premises	Identity	Company name	Creation type
administrator2	administrator2@inspectemirosoft.com	Member	No	inspectemirosoft.com		
alecason	alecason@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Corporation	
alexander8	alexander8@inspectemirosoft.com	Member	No	inspectemirosoft.com	123 Corp	
alexandra5	alexandra5@inspectemirosoft.com	Member	No	inspectemirosoft.com	X99 Corp	
alexandras	alexandras@inspectemirosoft.com	Member	No	inspectemirosoft.com	3942 Inc	
alexlangford	alexlangford@inspectemirosoft.com	Member	No	inspectemirosoft.com		
alexcooper	alexcooper@inspectemirosoft.com	Member	No	inspectemirosoft.com	X99 Corp	
alexhyde	alexhyde@inspectemirosoft.com	Member	No	inspectemirosoft.com	397 Corporation	
alexwilson	alexwilson@inspectemirosoft.com	Member	No	inspectemirosoft.com	X92 Inc	
alexturner	alexturner@inspectemirosoft.com	Member	No	inspectemirosoft.com	122 Industries	
alexjohansen	alexjohansen@inspectemirosoft.com	Member	No	inspectemirosoft.com	122 Industries	
alexcharleson	alexcharleson@inspectemirosoft.com	Member	No	inspectemirosoft.com	X97 Ltd	
alexdevon	alexdevon@inspectemirosoft.com	Member	No	inspectemirosoft.com	123 Corp	
alexwhite	alexwhite@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Ltd	
alexslater	alexslater@inspectemirosoft.com	Member	No	inspectemirosoft.com	X94 Corp	
alexjackson	alexjackson@inspectemirosoft.com	Member	No	inspectemirosoft.com	X92 Ltd	
alexvernon	alexvernon@inspectemirosoft.com	Member	No	inspectemirosoft.com	397 Inc	
alexsmith	alexsmith@inspectemirosoft.com	Member	No	inspectemirosoft.com	X97 Ltd	
alexchristian	alexchristian@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Company	
alexwerner	alexwerner@inspectemirosoft.com	Member	No	inspectemirosoft.com	394 Corporation	
alexabel	alexabel@inspectemirosoft.com	Member	No	inspectemirosoft.com	123 Corp	
alexturnell	alexturnell@inspectemirosoft.com	Member	No	inspectemirosoft.com		
alexjones	alexjones@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Corporation	
alexconner	alexconner@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Company	
alexscott	alexscott@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Company	
alexjohnson	alexjohnson@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Company	
alexsmith2	alexsmith2@inspectemirosoft.com	Member	No	inspectemirosoft.com	X92 Corporation	
alexwright	alexwright@inspectemirosoft.com	Member	No	inspectemirosoft.com		
alexwhite2	alexwhite2@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Ltd	
alexyoung	alexyoung@inspectemirosoft.com	Member	No	inspectemirosoft.com	ABC Ltd	
alexwerner2	alexwerner2@inspectemirosoft.com	Member	No	inspectemirosoft.com	X92 Inc	

3.2.4 Licenties

Qua licenties hebben we er verschillenden nodig. We sommen ze even op met uitleg:

Office 365 E3/E5

Deze licenties geven we aan de users/admins van het bedrijf. Hier staat al het nodige in voor de werknemers van het bedrijf.



Microsoft Entra ID P2

Wat vroeger Active directory Premium Plan 2 was, is nu Microsoft Entra ID P2. Deze geven we aan de administrator van het bedrijf. Deze licentie gebruiken we om onze on premise active directory te connecteren met onze cloudomgeving.



Microsoft Defender for office 365 (Plan 2)

Deze licentie geven we ook enkel aan de administrator van het bedrijf. Dit zorgt voor een veilige omgeving tegen cyberaanvallen, spam of phishing.



Intune

Voor de defender van VM's hebben we een Intune licentie nodig. Deze assignen we dan ook aan de admin van het bedrijf.



Via licenses kunnen we verschillende licenties assignen aan users en groepen. Dit is makkelijk om meerdere gebruikers een licentie te geven via groepen.

A screenshot of the Microsoft Azure portal's Licenses page. It shows a table with two rows: 'Windows' and 'Microsoft 365 Business Standard'. The 'Assigned' column shows values of 1 and 1 respectively, while the 'Available' column shows values of 11 and 11. The 'Expiring soon' column shows values of 0 and 0. The left sidebar includes sections for Overview, Devices and other problems, Manage (with options like License entitlements, Get service health products, Activity, and Audit log), Troubleshooting + Support, and Help support needed.

A screenshot of the Microsoft Entra admin center's Assign license page. It shows a list of users and groups under the 'Add users and groups' section. A specific group named 'TechnoHolding' is selected. The left sidebar lists various identity-related services and management tools such as Identity, Conditional Access, Applications, Intune, Identity governance, External identities, User risk, Protection, Identity governance, Verified ID, and Permissions Management. At the bottom, there are buttons for 'Next: Assign', 'Previous', and 'Post - Assignment options'.

3.3.5 Microsoft Teams

Door een GPO is Teams al geïnstalleerd. Aangezien elke gebruiker Microsoft Teams heeft kunnen we nu voor elke afdeling een teams groep maken.

3.3.6 Microsoft Defender

Bij het aanmelden bij onze security van M365, zien we onze security score staan. Dit daalde tot 20%. Dit is zeer laag voor een bedrijf van onze grote. Deze score kan je verbeteren via “recommended actions” en maken we al deze tasks.

The screenshot shows the Microsoft Secure Score dashboard. At the top, it displays a secure score of 40% with 4/10 points achieved. Below this, there's a chart showing the breakdown of points by category: Apps (40%), Identity (30%), and Devices (30%). A section titled "Top recommended actions" lists several items:

- Only invited users should be automatically admitted to ... - 20% (Status: To address, Category: Apps)
- Configure which users are allowed to present in Teams meetings - 20% (Status: To address, Category: Apps)
- Ensure modern authentication for SharePoint applications - 10% (Status: To address, Category: Apps)
- Restrict anonymous users from joining meetings - 10% (Status: Completed, Category: Apps)
- Sign out inactive users in SharePoint Online - 10% (Status: Completed, Category: Apps)
- Limit external participants from having control in a Team meeting - 10% (Status: Completed, Category: Apps)
- Restrict anonymous users from starting Teams meetings - 10% (Status: Completed, Category: Apps)

On the right side, there are sections for "Comparison" (showing a slight decrease from 13 Jan. 2024), "History" (listing recent score changes), and "Resources" (links to learn about Secure Score capabilities and partner experience updates).

Na verschillende taken gedaan te hebben, zien we dat onze score tot bijna 54% komt. Dit is al een serieuze verbetering.

The screenshot shows the Microsoft Secure Score dashboard again, but this time with a secure score of 53.72% and 154/192/287 points achieved. The "Actions" section now lists many more completed items:

- Only invited users should be automatically admitted to Teams meetings - 20% (Status: Completed, Category: Apps)
- Configure which users are allowed to present in Teams meetings - 20% (Status: Completed, Category: Apps)
- Ensure modern authentication for SharePoint applications is required - 10% (Status: Completed, Category: SharePoint Online)
- Restrict anonymous users from joining meetings - 10% (Status: Completed, Category: Identity)
- Sign out inactive users in SharePoint Online - 10% (Status: Completed, Category: SharePoint Online)
- Restrict stale users from bypassing a meeting lobby - 10% (Status: Completed, Category: Apps)
- Limit external participants from having control in a Teams meeting - 10% (Status: Completed, Category: Identity)
- Restrict anonymous users from starting Teams meetings - 10% (Status: Completed, Category: Apps)
- Ensure modern authentication is enabled for all external users - 10% (Status: Completed, Category: Identity)
- Turn off SSO for Microsoft 365 accounts - 10% (Status: Completed, Category: Identity)
- Ensure that Aad Identity Protection signs off on policies - 10% (Status: Completed, Category: Identity)
- Enable Aad Identity Protection user risk policies - 10% (Status: Completed, Category: Identity)
- Create new user risk policy for identities - 10% (Status: Completed, Category: Identity)
- Ensure that password hash is created for hybrid employees - 10% (Status: Completed, Category: Identity)
- Turn on Microsoft Defender for Office 365 (Identity, Compliance, and Threat) - 10% (Status: Completed, Category: Identity)
- Ensure DLP policies are enabled - 10% (Status: Completed, Category: Identity)
- Turn on daily discovery for office clients - 10% (Status: Completed, Category: Identity)
- Ensure the Cloud Protection Groups feature is enabled - 10% (Status: Completed, Category: Identity)
- Turn on automatic cleanup of cloud protection groups - 10% (Status: Completed, Category: Identity)
- Ensure that hybrid users are enabled - 10% (Status: Completed, Category: Identity)
- Ensure that Microsoft Entra is configured to match tenant risk levels - 10% (Status: Completed, Category: Identity)
- Create new user risk policy for hybrid employees - 10% (Status: Completed, Category: Identity)
- Set active take to bulk sync identities - 10% (Status: Completed, Category: Identity)
- Only invited users are allowed to present in Teams meetings - 10% (Status: Completed, Category: Identity)
- Configure which users are allowed to join in Teams meetings - 10% (Status: Completed, Category: Identity)
- Ensure that user identities are aligned for end user policies - 10% (Status: Completed, Category: Identity)
- Sign off inactive users in SharePoint Online - 10% (Status: Completed, Category: Identity)
- Ensure modern authentication for SharePoint applications is required - 10% (Status: Completed, Category: SharePoint Online)
- Ensure self-service password reset is enabled for all users - 10% (Status: Completed, Category: Identity)
- Restrict anonymous users from joining meetings - 10% (Status: Completed, Category: Identity)
- Allow inactive users from bypassing a meeting lobby - 10% (Status: Completed, Category: Identity)
- Limit external participants from having control in a Teams meeting - 10% (Status: Completed, Category: Identity)
- Restrict anonymous users from starting Teams meetings - 10% (Status: Completed, Category: Identity)
- Create new user risk policy for hybrid employees - 10% (Status: Completed, Category: Identity)
- Turn off SSO for Microsoft 365 accounts - 10% (Status: Completed, Category: Identity)
- Set maximum number of external requests that a user can send to a site per hour - 10% (Status: Completed, Category: SharePoint Online)
- Set maximum number of external requests that a user can send to a site per day - 10% (Status: Completed, Category: SharePoint Online)
- Set a daily message limit - 10% (Status: Completed, Category: SharePoint Online)

The screenshot shows the Microsoft Secure Score dashboard with a secure score of 53.72% and 154/192/287 points achieved. It includes a graph showing the secure score trend from 12-01 to 18-01, starting at 20%, dipping to 15%, then rising to 54%.

We maken ook een anti-spam en anti-phishing policy aan, die voor extra security zorgt voor gebruikers van ons domein.

Antiphishing

Microsoft 365 beschikt standaard over ingebouwde functies die helpen om gebruikers te beschermen tegen phishingaanvallen. Standaardbeleid is voor deze bescherming te verhogen, bijvoorbeeld door instellingen te wijzigen zodat aanvallen op basis van inhoud en adresverificatie beter kunnen worden gedetecteerd en voorkomen. Het standaardbeleid is van toepassing op alle gebruikers binnen de organisatie. U kunt een aangepast beleid maken met hogere prioriteit voor specifieke gebruikers, groepen of domeinen. [Meer informatie over antiphishingbeleid](#)

Naam	Status	Prioriteit	Laatste geüpdateld
antispam	Aan	0	13 jan. 2024
Anti-spam beleid voor inkomen...	Altijd aan	Laagst	13 jan. 2024
Verbindingsfilterbeleid (standaard)	Altijd aan	Laagst	13 jan. 2024
Anti-spam beleid voor uitgaande...	Altijd aan	Laagst	13 jan. 2024

Naam	Status	Prioriteit	Type
antispam	Aan	0	Aangepast anti-spambeleid
Anti-spam beleid voor inkomen...	Altijd aan	Laagst	
Verbindingsfilterbeleid (standaard)	Altijd aan	Laagst	
Anti-spam beleid voor uitgaande...	Altijd aan	Laagst	

3.3.7 Microsoft Exchange

Hier zie je dat de mailboxen zijn aangemaakt van onze users.

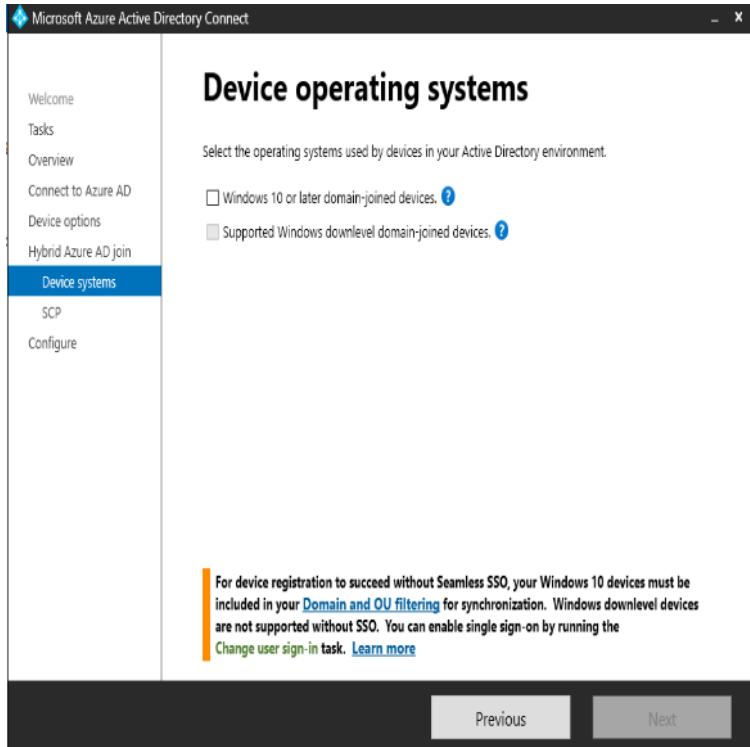
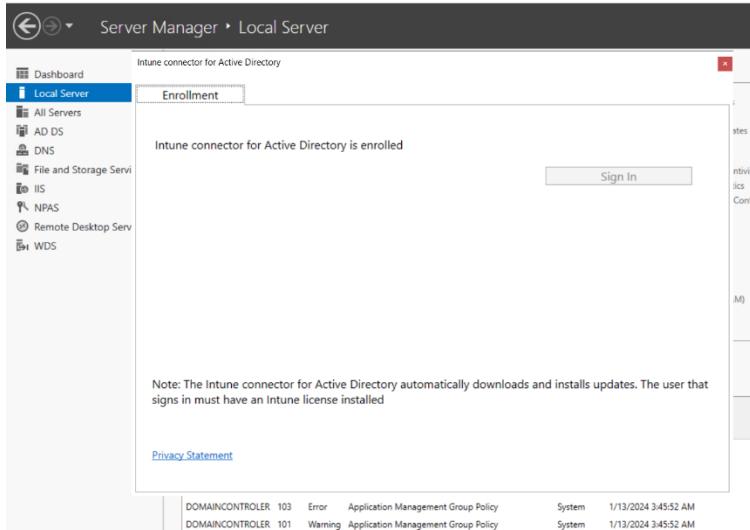
Manage mailboxes

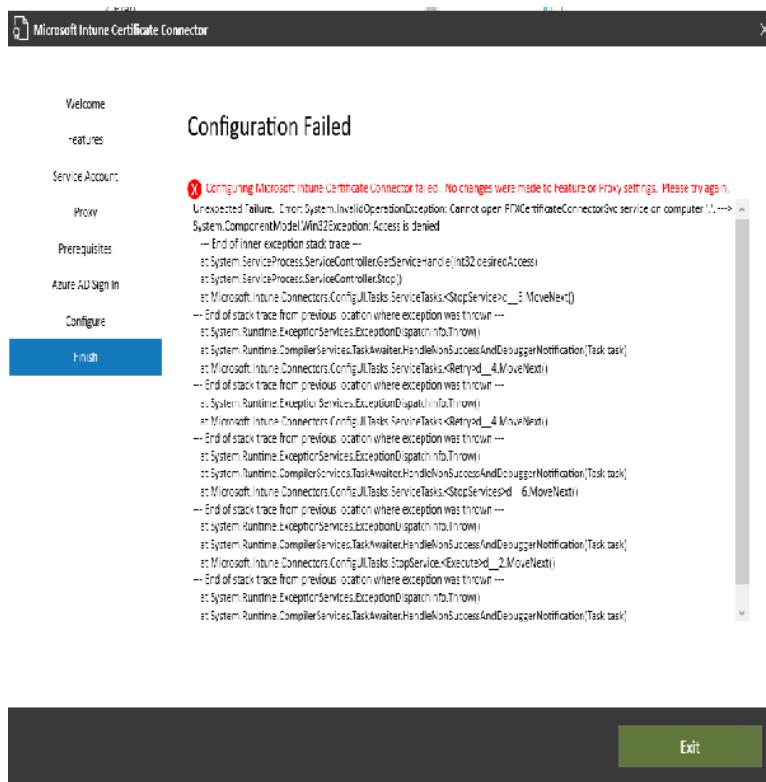
Create and manage settings for shared mailboxes. You can also manage settings for user mailboxes, but to add or delete them you must go to the Microsoft 365 admin center and do this on the [active users](#) page. [Learn more about mailboxes](#)

Display name ↑	Email address	Recipient type	Archive status	Last modified time	Choose columns
anita langhoofd	anita@nv poc.com	UserMailbox	None	1/11/2024, 5:46 PM	
Yusuf Coban	yusuf.coban@nv poc.com	UserMailbox	None	1/12/2024, 3:35 PM	
zacharias osselaer	admin@nv poc.com	UserMailbox	None	1/12/2024, 3:05 PM	

3.3.8 Defender voor Virtuele Machine

Endpoint manager lijkt vereist te zijn om Defender voor VM's te configureren. Hiervoor is het toevoegen van een Intune-licentie nodig. We kunnen die licentie toevoegen en configureren een device connection om toe te wijzen aan AD Active Directory connect. We installeren via domain controller 1 de certificate connector en proberen de apparaten te synchroniseren met AD Connect. Maar het werkt niet en er is geen tijd om het verder te onderzoeken.





4. Back-ups

Back-ups zijn zeer belangrijk voor als er iets misloopt kan je u gegevens terug halen, daarom hebben we besloten dat we onze back-ups zowel lokaal als op de Cloud gaan Back-uppen.

4.1 Local Backup

We gaan onze server helemaal back-uppen naar onze back-up folder.

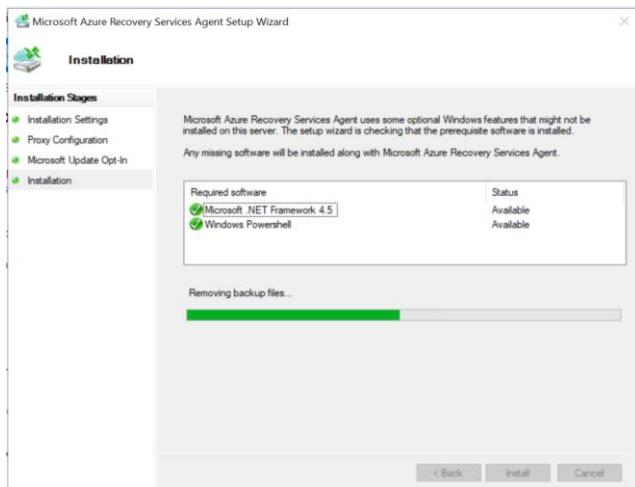
The screenshot displays the 'Backup Schedule Wizard' interface across four windows:

- Select Backup Configuration:** Shows options for 'Full server (recommended)' or 'Custom'. 'Full server' is selected. It also shows a backup size of 19.14 GB.
- Specify Backup Time:** Shows a schedule for 'Once a day' at 11:00 PM. It also allows for 'More than once a day' with a list of available times from 12:00 AM to 4:00 AM.
- Specify Destination Type:** Shows options for storing backups: 'Back up to a hard disk', 'Back up to a volume', or 'Back up to a shared network folder'. 'Back up to a shared network folder' is selected. A warning message states: 'When you use a remote shared folder as the storage destination for scheduled backups, each backup will erase the previous backup, and only the latest backup will be available.'
- Summary:** Displays the status: 'Status: You have successfully created the backup schedule. Your first scheduled backup will happen at 1/20/2024 11:00 PM.'

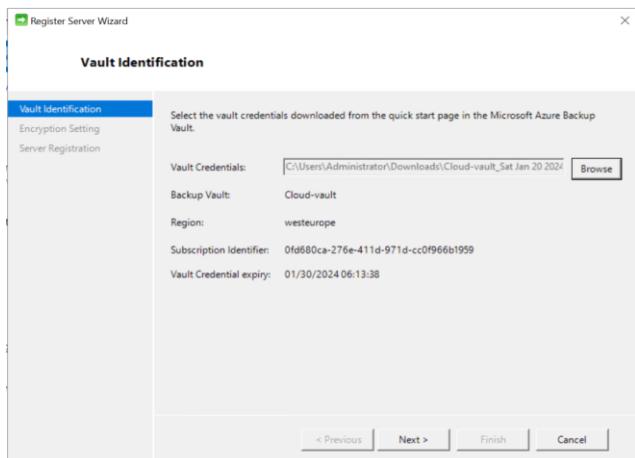
4.2 Cloud backup

Een backup op de cloud is zeer belangrijk voor een bedrijf. Via [deze link](#) hebben wij dan ook deze backup gedaan.

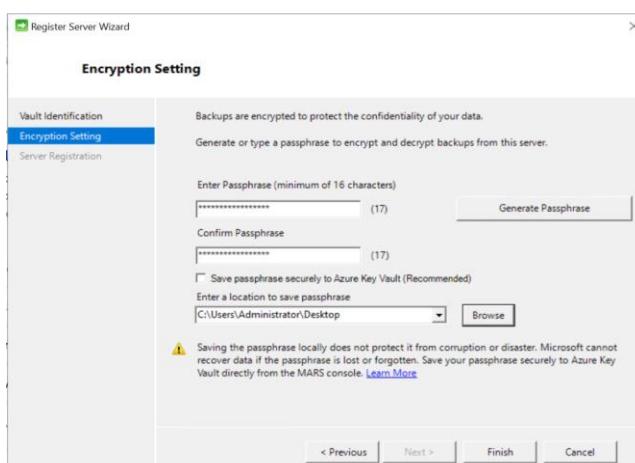
Eerst installeren wij via Azure Portal de Microsoft Azure Recovery services Agent. Dat verkrijg je bij het aanmaken van een vault. Deze wizard overlopen we even door.



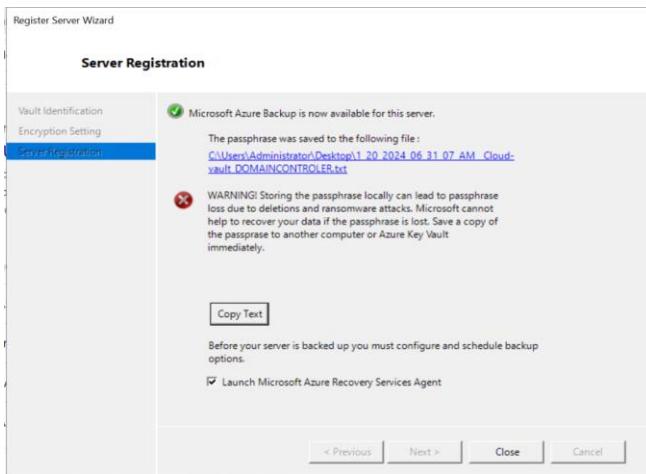
Daarna komen we op volgende tabblad waar we een key moeten meegeven. Deze key hebben we gekregen bij het aanmaken van onze vault in Azure krijgen wij een key die we moeten downloaden. Deze geven we hier mee.



We maken een paraphrase aan en deze kunnen we lokaal of op de cloud bewaren. We doen het nu lokaal om kosten te besparen.



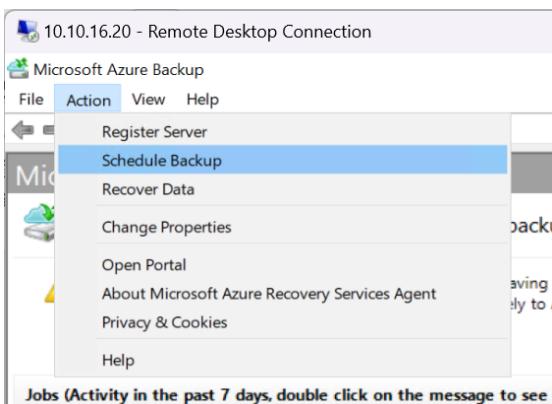
NV POC



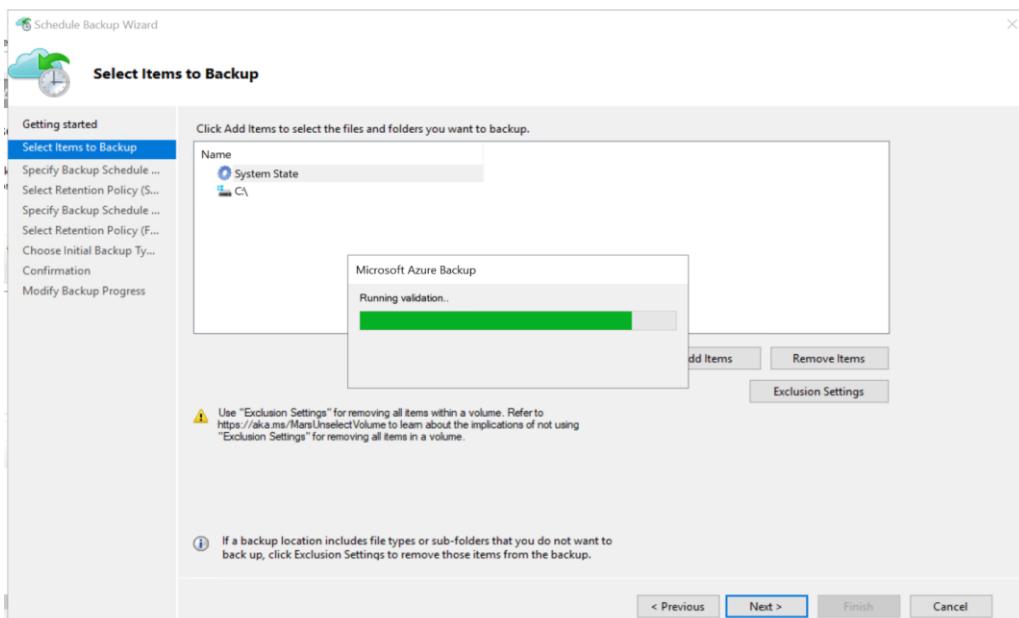
Server is geregistreerd dit zien we zowel op Azure als op onze Server.

The screenshot shows the Microsoft Azure portal's 'Protected Servers (Azure Backup Agent)' blade under the 'Cloud-vault' resource group. It lists a single server named 'DOMAINCONTROLLERINPOCLOGICAL' with an agent version of 2.0.9202.0 and a backup item count of 2. A progress bar indicates 'Fetching data from service completed.'

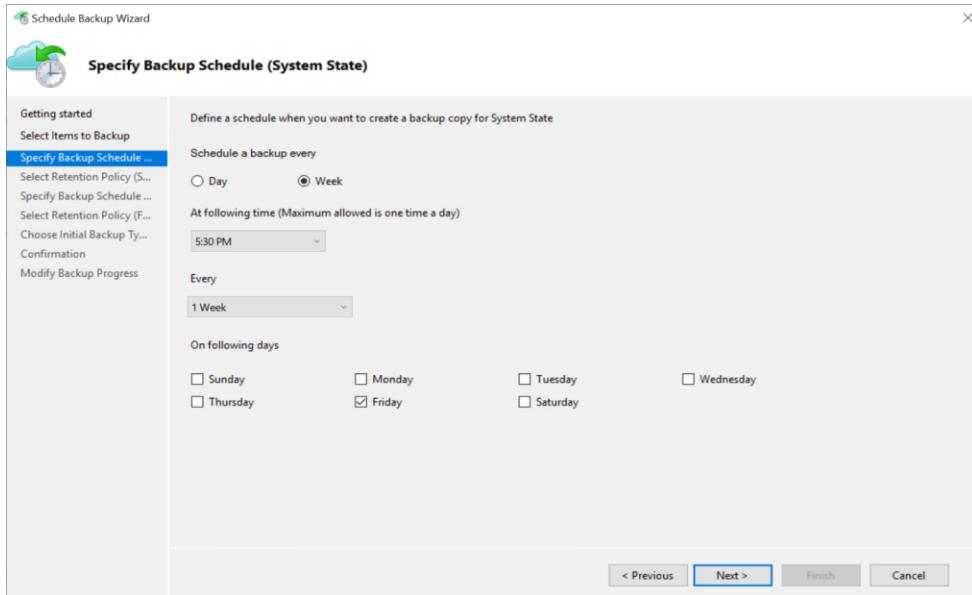
We gaan een backup schedule aanmaken, zodat we dit niet handmatig hoeven te doen.



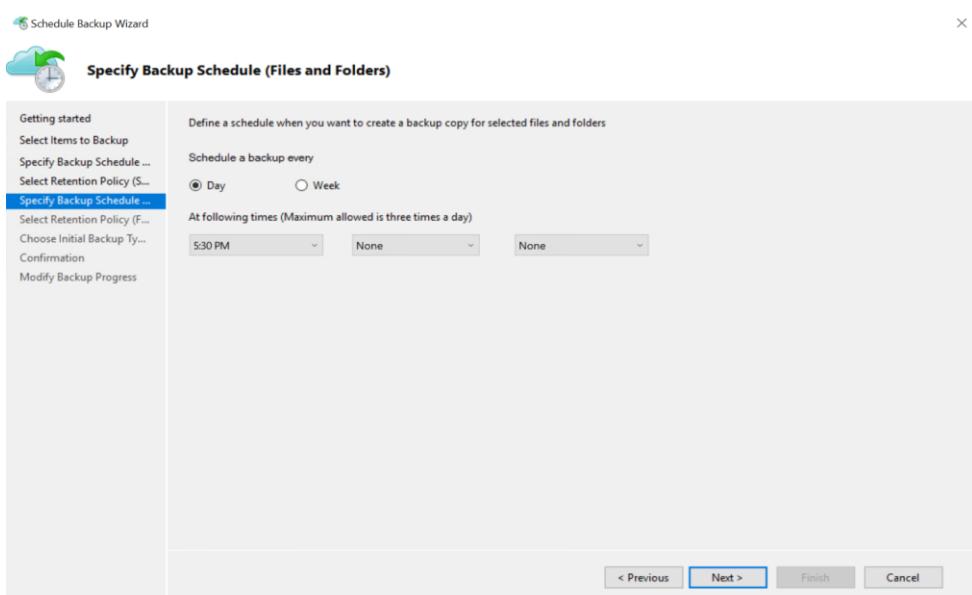
We kiezen hier voor system state en folders en files te backen uppren.



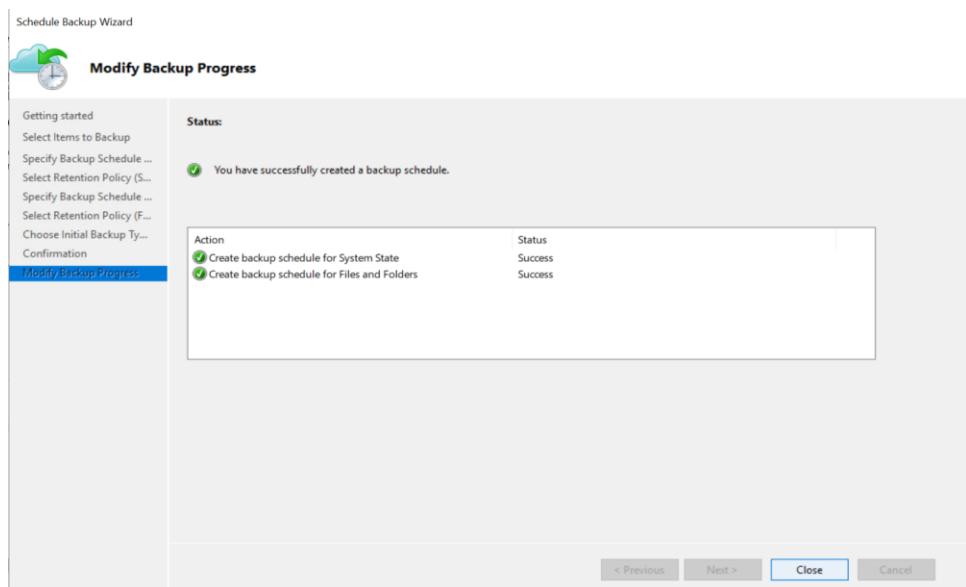
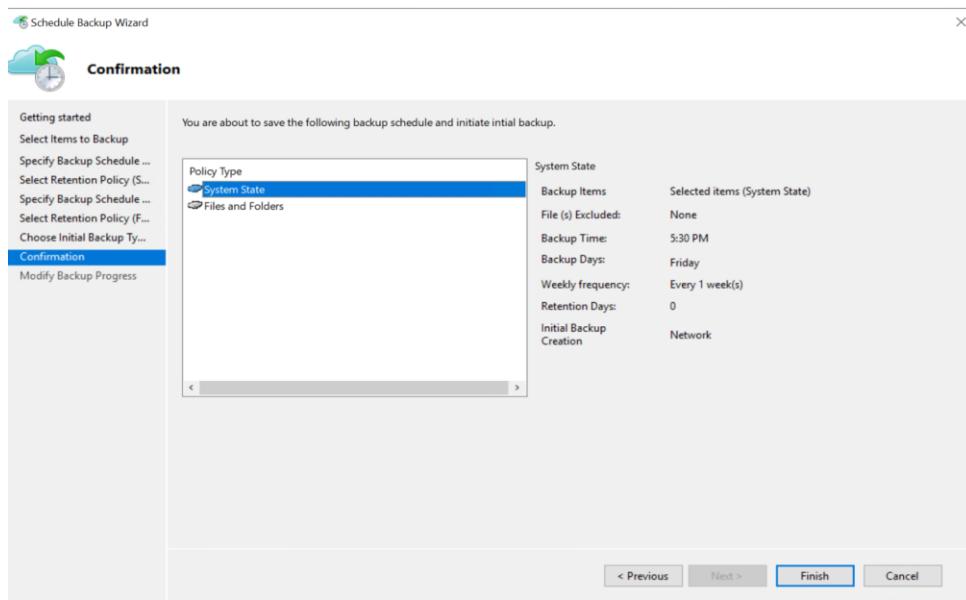
Systeem backup doen we wekelijks om 17u30 net na de werkweek.



Files en folders dooen we dan weer dagelijks om 17u30 zodat files altijd geback-up zijn.



NV POC

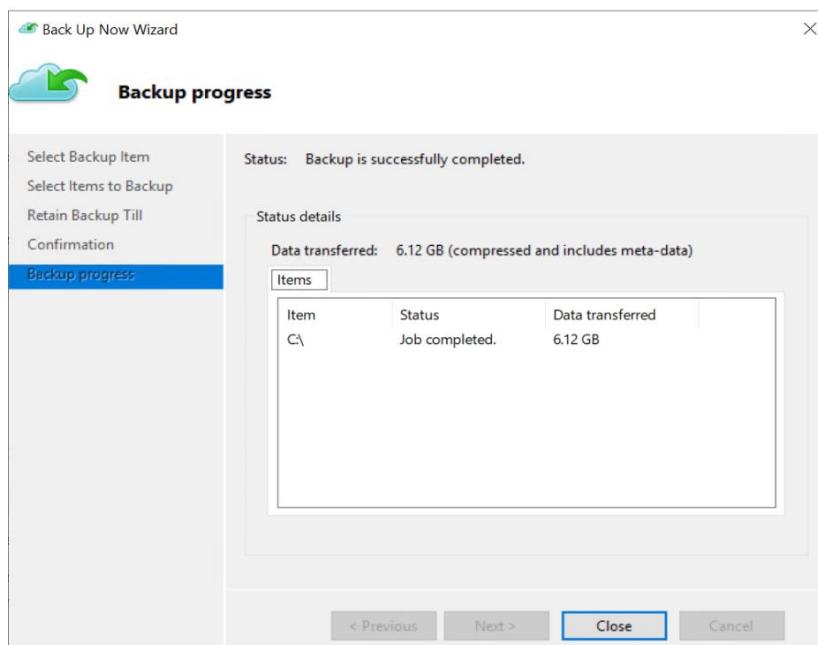
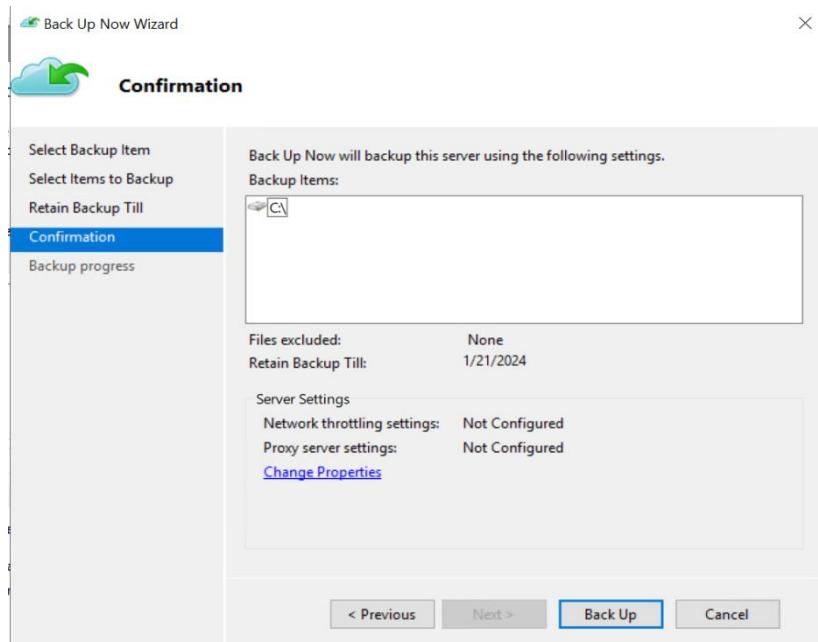


The screenshot shows the 'Backup Items (Azure Backup Agent)' page. The URL is 'Home > Cloud-vault | Backup items >'. The page has a header with 'Cloud-vault' and a search bar. It includes buttons for 'Refresh', 'Add', and 'Filter'. A message says 'All data fetched from the service.' Below is a table of backup items:

Backup item	Protected server	Last backup	Last backup time	Details
System State	domaincontroller.nvpoc.local	●	1/1/2021, 1:00:00 AM	View details
C:\	domaincontroller.nvpoc.local	●	1/20/2024, 3:30:00 PM	View details

NV POC

We proberen hier een back-up te maken van onze files en folders. We zien dan ook via Azure dat dit ons is gelukt.



domaincontroller.nvpooc.local Backup Completed Files and folders 1/20/2024 3:39:03 PM 00:11:25 [View details](#)

5. Zelfreflecties

5.1 Zelfreflectie Zacharias Osselaer

Het project was een leuke maar zware opdracht. Wat je leert in deze opleiding is de basis voor dit project maar ik kan nu wel zeggen dat “Google” mijn dikke vriend is. Dit heeft me dan extra veel bijgeleerd aangezien we nu al deze informatie in de praktijk moesten brengen. Alles zelf uitzoeken heeft ervoor gezorgd dat ik geïnteresseerd bleef. Dit heb ik gemerkt omdat ik nachtenlang niet kon slapen voordat ik een tutorial opzocht op YouTube.

Waar Google nog van pas kwam, was bij probleemoplossingen. Doorheen het traject werd probleemoplossing in ons brein gehamerd. Dit hebben we dan ook meer dan 1 keer ondervonden doorheen het project.

Bij het begin van het project was het allemaal nog vaag hoe alles te werk ging. Maar naar het einde toe was het plaatje compleet. Van een losse switch, een firewall en 2 servers naar een volledige IT-infrastructuur!

Doorheen heel de opleiding kregen we losse delen van kennis en dit project heeft ervoor gezorgd dat ik al deze kennis moet combineren. Waarvoor dank aan alle docenten van EHB.

Ik vind dat ik nu meer klaar ben om de echte IT-wereld in te gaan. Dit was de ultieme kans om te bewijzen dat ik daar klaar voor ben. Ondanks er nog veel valt te leren, blijf ik verder groeien qua kennis. Zoals we allemaal wel weten is er geen maximum aan kennis in de IT-wereld en daarom moeten we blijven kennis opdoen.

Ik ben blij dat ik dit met dit team kon afwerken. We vulden elkaar goed in en zorgden altijd dat er hulp was als één van ons even vast zat. Waar ik me meer focuste op alles omtrent Cloud en de lay-out van de documentatie focusten Yusuf en Soufyan weer meer on premise. Dit wil niet zeggen dat we afgesloten van elkaar werkten want we werkten goed samen en werkten bijna elke dag vanop Discord samen zodat we konden bijspringen bij problemen.

We hebben het project tot een goed eind kunnen brengen met dank aan mijn team. Zonder hen zou ik op zo een korte tijd dit niet allemaal tot een goed eind kunnen brengen. Daarvoor dank!

Mijn conclusie is dat ik dit project enorm boeiend en leerrijk vond. Ik ben trots op mezelf en mijn team en heb veel energie om mijn carrière in de IT verder te zetten!

5.2 Zelfreflectie Soufyan Naimi

Dit project was om te beginnen niet al te gemakkelijk. Het was zeker wel een compleet project waar onze kennis van zowel vorig jaar en dit jaar in samenwerking kwamen. Toen we ons project kregen met de doelstellingen had ik veel vragen over hoe ik juist moest beginnen en hoe dat ik sommige toepassingen moest aanpakken. Er waren wat aantal zaken waar ik niet veel van wist of niet wist hoe ze samen konden werken. En daardoor heb ik wel veel bijgeleerd samen met de rest van mijn groep. Voor heel veel zaken hebben we documentatie moeten zoeken zowel op google als op YouTube.

Het vinden van video's of documentatie was wel gemakkelijk maar het probleem was het in praktijk zelf brengen. We hebben meerdere keren zaken opnieuw moeten doen omdat ze niet werkten of zelfs VM's lieten crashen waardoor we veel tijd zijn verloren. Maar het is wel door dit soort fouten dat we veel hebben bijgeleerd. Ook dank aan de docenten die ons hebben geholpen wanneer we geen oplossingen vonden.

Doorheen onze opleiding hebben we geleerd dat probleemplossing zeker een belangrijk punt is in de IT-wereld. Dit hebben we ondervonden door meermaals online oplossingen te zoeken.

Wat ik wel ook goed heb gevonden aan dit project is dat we in groep werkten. Wanneer ik iets niet wist of mijn groep iets niets wist konden we altijd op elkaar rekenen want iemand had meestal wel een oplossing. Moest het niet zo zijn dan ging iedereen ook direct online zoeken om een oplossing te vinden voor ons probleem.

Heel veel zaken waarvan ik totaal geen kennis had zijn nu veel duidelijker. Sommige links zijn nu duidelijker en zeker hoe zowel hardware en software te werk gaan met elkaar, dit heb ik wel te danken aan dit project. Ik besef nu dat ik in mijn volgende jaren nog veel zaken ga bijleren omdat de IT-wereld heel complex is en dat er altijd wel iets nieuws bijkomt waardoor je altijd gaat moeten bijleren.

Samen met mij groepsleden zijn wel blij omdat we van niets naar iets werkend zijn kunnen gaan en dit op enkele weken. Ik heb zodanig veel tijd besteed met mijn groep dat het soms leek dat we onder hetzelfde dak woonden. Met veel dank aan mijn groep voor hun medewerking en hun doorzettingsvermogen doorheen dit project.

Mijn conclusie is dat ik door dit project besef hoe complex de IT-wereld is en dat ik er klaar voor ben om mij hierin te gaan verdiepen.

5.3 Zelfreflectie Yusuf Coban

Er is veel te zeggen over het project maar ik zal het kort houden. Eerst en vooral was het een boeiende en moeizame periode voor mij, want je leert er veel van uit maar langs andere kant steek je veel tijd en effort in en heb je soms geen tijd om activiteiten buiten school leven nog te doen. We zaten elke dag samen met groepsleden op Discord om aan ons project te werken zodat we tot een mooi einde zouden komen. Ik denk dat we als groep ons best gedaan hebben, met de kennis dat we op school hebben opgedaan is maar slechts de basis. Daarom moesten we ons vierdiepen op sommige zaken, hiervoor hebben we meestal YouTube filmpjes gekeken en google gebruikt.

Het viel soms erg tegen we zaten soms vast en moesten dagenlang zoeken naar een oplossing wat eigenlijk een leuke ervaring is, zo leer je hoe je moet handelen tijdens zo een situatie en kan ons helpen later op de werkvloer. Het was zeer belangrijk om te blijven proberen en testen tot totdat het werkte, maar soms moest je het laten en morgen terug proberen met een frisse hoofd. Maar ik kost rekenen op mijn team als ik met een probleem zat, we hielpen elkaar waar het moest.

In dit project heb ik geleerd hoe je in een groep moet werken eigenlijk, ik heb meerdere keren in groep gewerkt maar dit project was anders. Communicatie was belangrijk we wisten exact wie met wat bezig was, dit zorgde voor een goede vooruitgang.

Ik heb door dit project kunnen werken met nieuwe technologieën dat ik nog niet eerder mee had gewerkt, het was een aangename ervaring en kan van toepassing zijn later in mij carrière.

We hebben eigenlijk een grote puzzel gemaakt als je het zo bekijkt, alle zaken met elkaar verbonden en dit voor een mooi werkend project. Hierdoor kan ik nu wel zeggen dat ik klaar ben voor de toekomst. Leren ga ik heel mijn leven moeten doen, zeker als ik goed wil zijn in mijn domein.