Oefeningen Infrastructuur

Oefen Verslag

Adam Nunes – 2022

Inhoudsopgave

Voorwoord 3

Requirements 4

Netwerkspecificaties5/6

Gemaakte keuzes tijdens de proftaak 7/10

OpenVpn 11

Ldap 12

Realisatie 13

Overige Opdrachten 14-20

Reflectie 21

Analyse

Voorwoord

Met dit document hoop ik aan te tonen dat ik voldoende kennis heb om een verdiepende challenge te maken. De meeste leerdoelen zullen niet allen maal op zichzelf worden aangetoond. Maar in een groter samenhangend netwerk. De losse leerdoelen zullen aan het einde van dit document getoond worden. Verder ik een klein gefaalde projectje aantonen. Tot slot zal dit document eindigen met een reflectie.

Overzicht van het netwerk

Dit netwerk bevat toegang voor meerdere gebruikers voor wie verschillende rollen gelden. Daarnaast kunnen bepaalde gebruikers op afstand inloggen op het netwerk door middel van LDAP. Verder is het netwerk verbonden aan anderen netwerken met behulp van een site to site vpn. Bovendien beschikt het netwerk over een webserver die zich bevind in een docker container. Tot slot is het netwerk op een bevredigend niveau beveiligd.

Overzicht losse leerdoelen

Aan het einde van dit verslag zal een reeks losse leerdoelen aan bod komen. Dit zijnde : raid configuratie , het maken van een docker image en Twee statische routers met elkaar laten pingen.

Gefaalde projectje

Het is mij niet gelukt om een image te maken van een apache/nginx server.

Analyse

Requirments voor de oefeningen

De Vcenter - Is de virtuele omgeving waarin de servers en netwerk componenten geplaatst worden
De virtuele router - Die we gaan gebruiken heet Pfsense. Het is gratis en “open source” wat inhoud dat het continue bijgeschaafd wordt.
De clientserver - Is de server waarop de werknemer zij arbeid zal verrichten
De domaincontroller - Is de server die de regels en instellingen van de clientserver beheerd
D.M.Z - Is een kundigheid die het lokale netwerk beveiligd. Door de bijvoorbeeld een webserver voor de firewall van het lokale netwerk te plaatsen.
Vlans - Zorgen ervoor dat de verschillende netwerken op een keurige manier gescheiden worden
DHCP - Server is de server die ip adressen uitdeelt
NAT - Is ontworpen voor het behoud van IP-adressen. Het stelt IP-netwerken in staat die niet-geregistreerde IP-adressen gebruiken om verbinding te maken met internet.
Poort forwarding - Proces waarbij je twee verschillende Vlans met elkaar kan verbinden
Docker – Dient als een gereedschap die bestandsystemen kan vitaliseren op een zeer handige manier

OpenVpn – Dit is een opensource programma waarmee een beveiligde data verbinding in stand word gezet

Site-to-Site vpn – Deze vpn dient voor meerdere clients

Azure/Aws – Dit zijn cloudservers platvormen die gebruikt kunnen worden om data in op te slaan

Kubernetes – Dient voor het automatiseren van container objecten

De requirments worden gerangschikt op de “M.o.S.C.o.W” methode.

M	S	C	W
Vcenter	Rdp	Cloud	Kubernetes
Vrouter	Image		Arduino met webserver
	Webserver		
Domaincontroller	Sit-to-site VPN		
Clientserver			
D.M.Z			
Vlans			
DHCP server			
NAT			
VPN			
Docker			
Webserver			

Netwerk specificatie’s

R1

CPU : 2

Memory : 2 GB

Hard disk : 50 GB

Network adapter 1 : DHCP

Network adapter 2 : VlanA

R2

CPU : 2

Memory : 2 GB

Hard disk : 15 GB

Network adapter 1 : VlanA

Network adapter 2 : VlanB

Domain controller

CPU : 2

Memory : 2 GB

Hard disk : 15 GB

Network adapter 1 : VlanA

Network adapter 2 : VlanB

Windows machine

CPU : 2

Memory : 4 GB

Hard disk : 100 GB (RAID)

Network adapter 1 : VlanA

Linux client

CPU : 4

Memory : 3 GB

Hard disk : 16 GB

Network adapter 1 : VlanA

Windows werkstation

CPU : 2

Memory : 4 GB

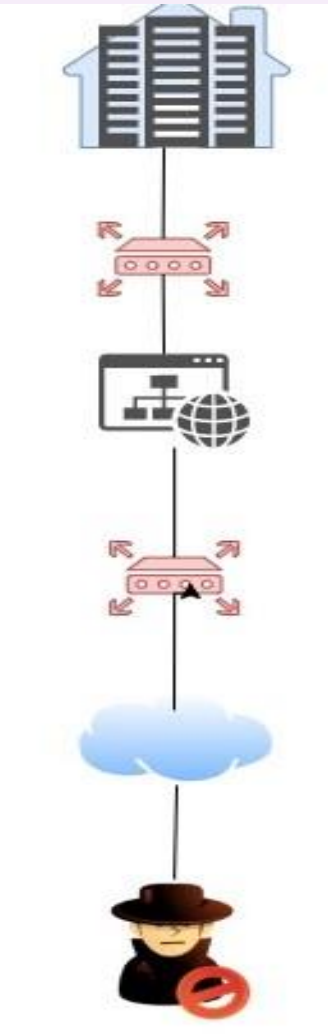
Hard disk : 48 GB

Network adapter 1 : VlanB

Ontwerp

Gemaakte keuzes tijdens de opdracht

De webserver wordt in een DMZ zone geplaatst. Dit houd in dat het netwerk op dusdanige wijzen gescheiden wordt dat het heel lastig is voor indringers om toegang te verschaffen tot gevoelige servers. Dit zal met twee routers gedaan worden om de beveiliging te vergroten. **Voorbeeld :**

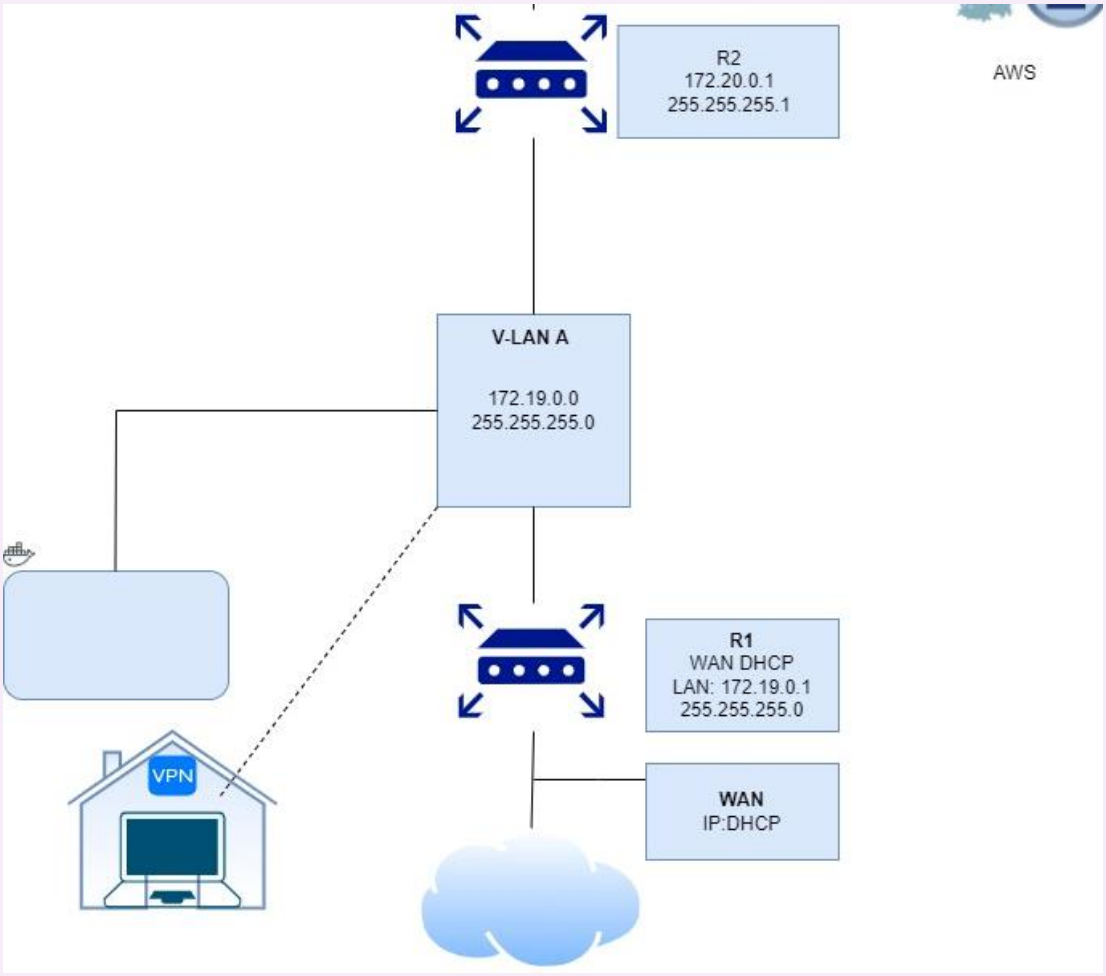


Wanneer er van buiten af verbinding gemaakt word met het netwerk wordt dit gedaan met een vpn. Een vpn zorgt ervoor dat er op een veilige manier verbinding gemaakt kan worden.

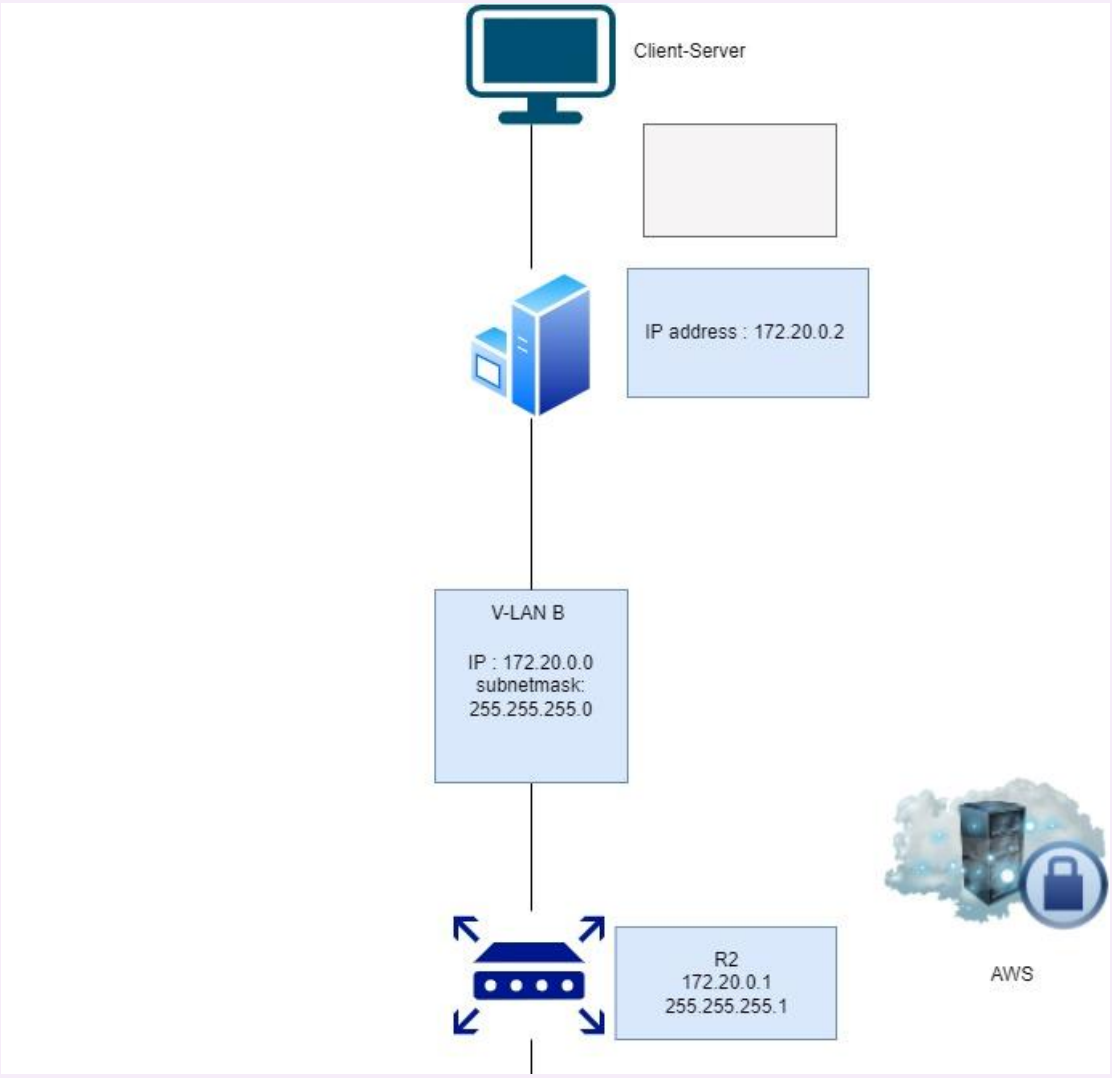
Ontwerp

De scheiding van mijn netwerk heb ik met twee V-lans gedaan A & B.

In het subnet van V-lan A staat de DMZ met daarin een docker container waarin een webserver zit. Verder zijn er twee routers die verbonden zijn aan V-lan A namelijk, de wan kant van router 2 en de lan kant van router 1.



In V-lan B staat de domain controller en de werkstation.



Hier is een overzicht van allen ip adressen, V-lans en subnetmaskers.

IP PLAN			
Device	IP	Subnet	V-lans
R1	172.19.0.1	255.255.255.0	A
R2	172.20.0.1	255.255.255.0	A & B
WAN	192.168.56.39	255.255.255.0	
VLAN A	172.19.0.0	255.255.255.0	
VLAN B	172.20.0.0	255.255.255.0	
Domain Controller	172.20.0.15	255.255.255.0	B
DMZ netwerk kaart	172.19.0.2	255.255.255.0	
Windows Client	172.20.0.35	255.255.255.0	B
Linux client	172.19.0.11	255.255.255.0	A

Twee routers in een netwerken

Om een netwerk te maken waarin twee routers zitten moet het wan adres van router 2 worden ingevuld bij het lan adres van router 1.

Wanneer je dit doet kunnen de routers elkaar pingen maar kan je werkstation van v-lan B nog niet het internet bereiken hier ging ik de fout in.

Dat komt omdat router 1 niet weet wat er zich achter router 2 bevind.

Er moet dus een any regel worden toegevoegd bij source.

In router 2 moet NAT worden uitgezet

Docker

Docker installeer je met het volgende script

```
curl -fsSL https://get.docker.com -o get-docker.sh
$ sudo sh get-docker.sh
```

Om te controleren of alles werkt doen we het volgende:

Pull de whale say image

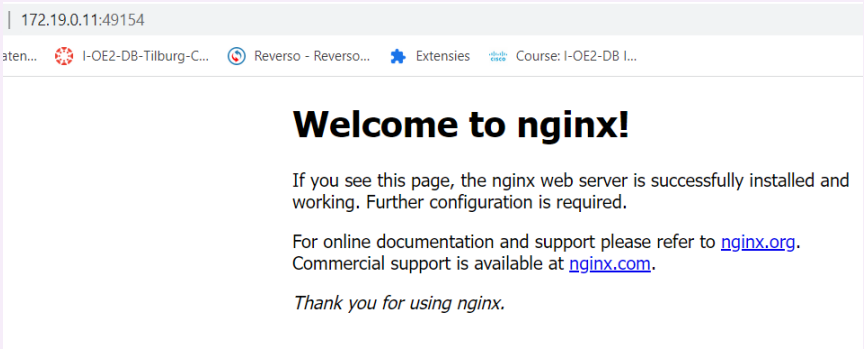
Run de image

Oefeningen Infrastructuur

```
sudo docker run -d -p 8000:8000 -p 9000:9000 --name=portainer --r
```

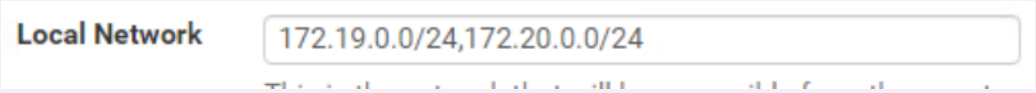
Vervolgens doen hetzelfde met de portcontainer image. Want we willen een gui gebruiken zodat we meer overzicht hebben over Docker. De portainer server gaat door poort 9000.

In Docker heb ik een nginx webserver staan. Die door poort 49154:80 gaat.



Open Vpn

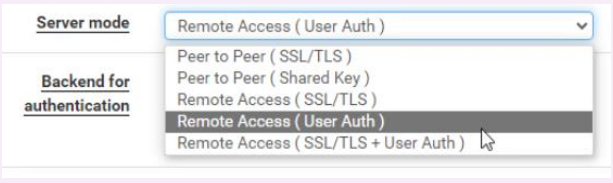
Ik wil graag vanaf mijn eigen werkmachine remote toegang krijgen tot mijn netwerk. Dit doe ik door Open vpn te downloaden in mijn router.
Daarna vul ik de adressen van mijn subnet in.



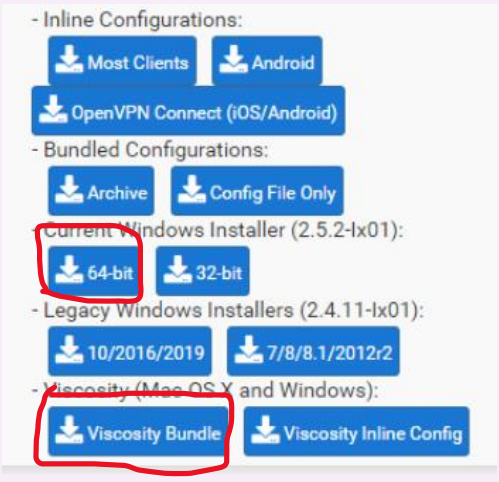
Daarna maak ik een gebruiker aan in User manager

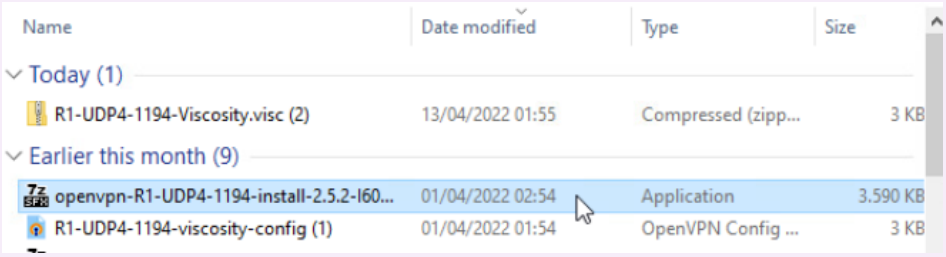
Gebruiksnaam	Test
Wachtwoord	*******

Vervolgens ga ik terug naar mijn vpn en doe ik de volgende instelling.

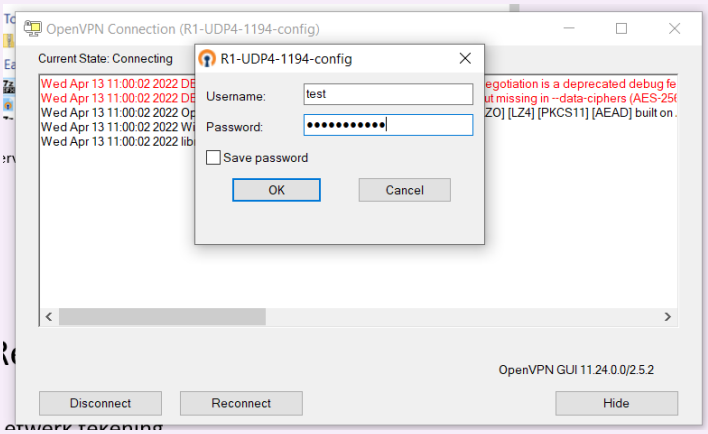


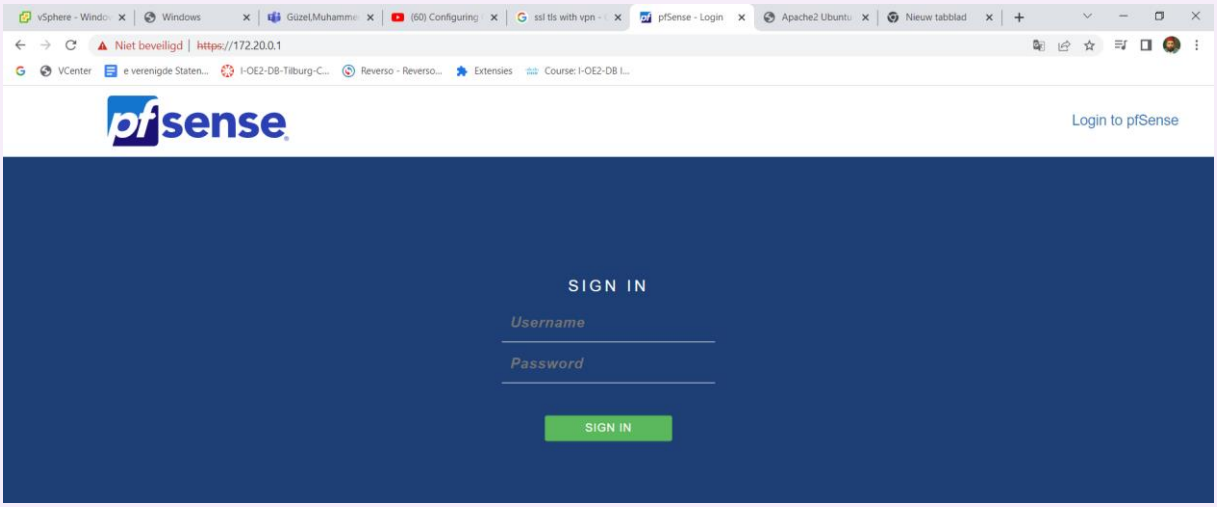
Daarna downloaden we de open vpn client





Vervolgens stuur je deze installer naar je eigen werkmachine waar je hem opnieuw download.

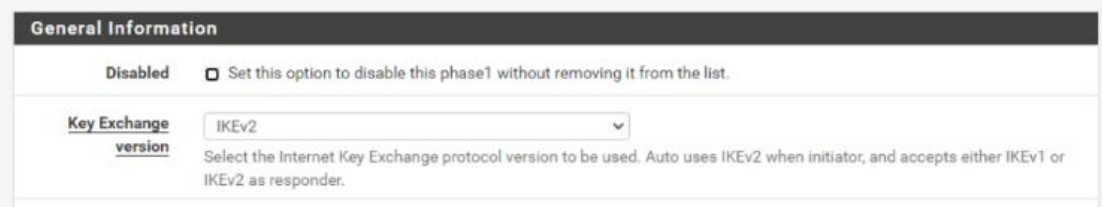




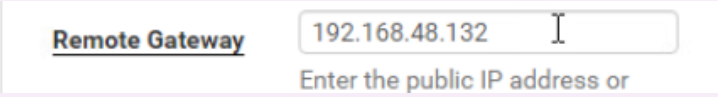
Router bereikt zonder vm dus vanaf remote werkmachine

Site to Site vpn

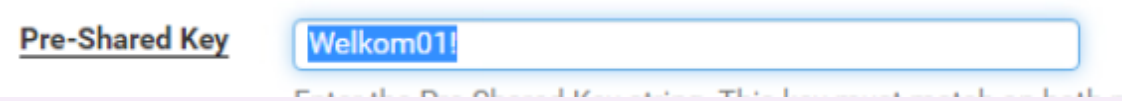
Dit is het soort vpn dat ik gebruikt heb om mijn netwerk te verbinden aan een mede student.



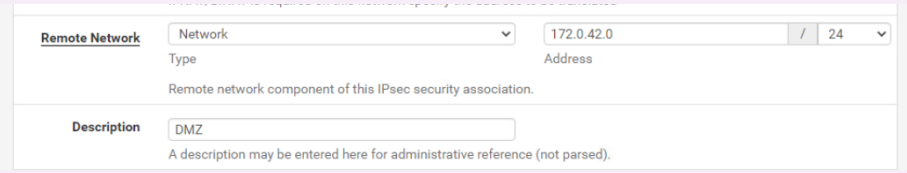
Beiden routers moeten dezelfde protocol aanhouden



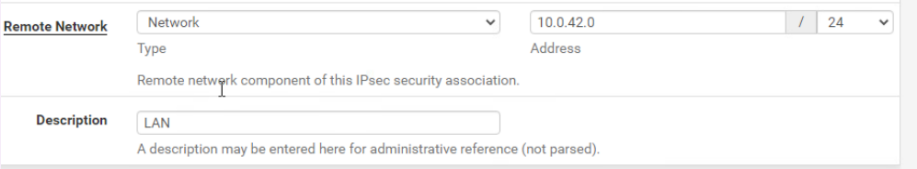
Dit is het wan adres van Muhamed Ali want het is zijn netwerk waar ik verbinding mee wil maken.
En in zijn router staat mijn remote gateway van mijn router 1.



De pre shared key moet bij beiden router hetzelfde zijn.



Hier laat ik zien naar welk gedeelte van zijn netwerk ik verbinding wil maken namelijk zijn DMZ



En hier maak ik verbinding met zijn lan

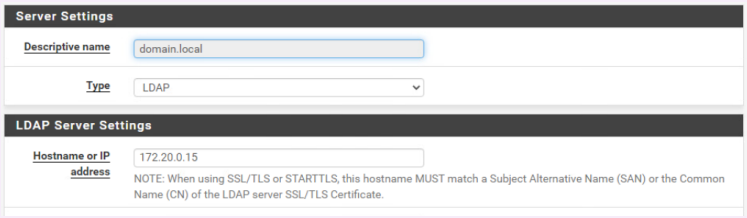
Test

```
C:\Users\Adam>ping 172.0.42.1

Pinging 172.0.42.1 with 32 bytes of data:
Reply from 172.0.42.1: bytes=32 time=1ms TTL=62
Reply from 172.0.42.1: bytes=32 time=1ms TTL=62
Reply from 172.0.42.1: bytes=32 time=1ms TTL=62
Reply from 172.0.42.1: bytes=32 time=1ms TTL=62

Ping statistics for 172.0.42.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Adam>ping 10.0.42.1

Pinging 10.0.42.1 with 32 bytes of data:
Reply from 10.0.42.1: bytes=32 time=1ms TTL=125
Reply from 10.0.42.1: bytes=32 time=1ms TTL=125
Reply from 10.0.42.1: bytes=32 time=1ms TTL=125
Reply from 10.0.42.1: bytes=32 time=1ms TTL=125

Ping statistics for 10.0.42.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

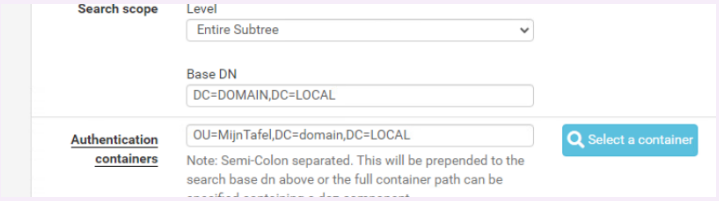
Test

LDAP

Ik maak gebruik van LDAP omdat ik graag wil dat de gebruikers in mijn active directory toegang krijgen tot het netwerk.
Eerst verbind ik mijn domain controller met mijn router.



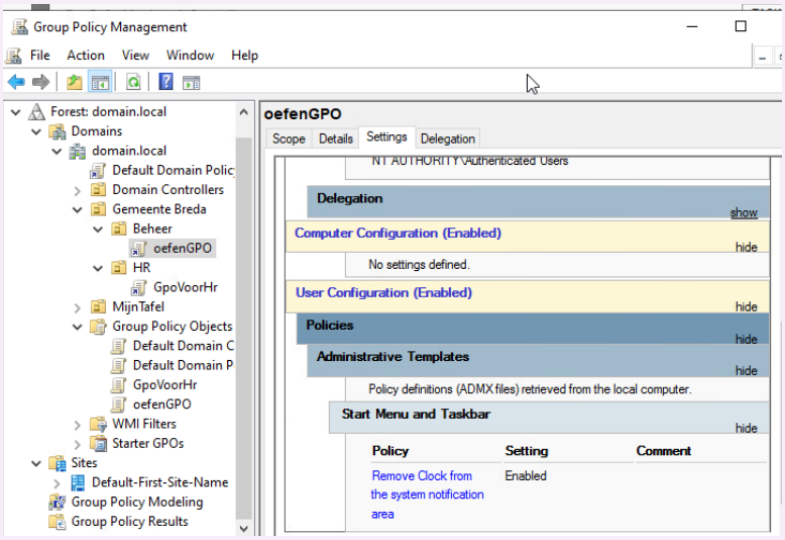
Bij hostname vul ik de ip van mijn domain controller in.



Vervolgens vul ik in welk gedeelte van mij AD verbinding maakt.

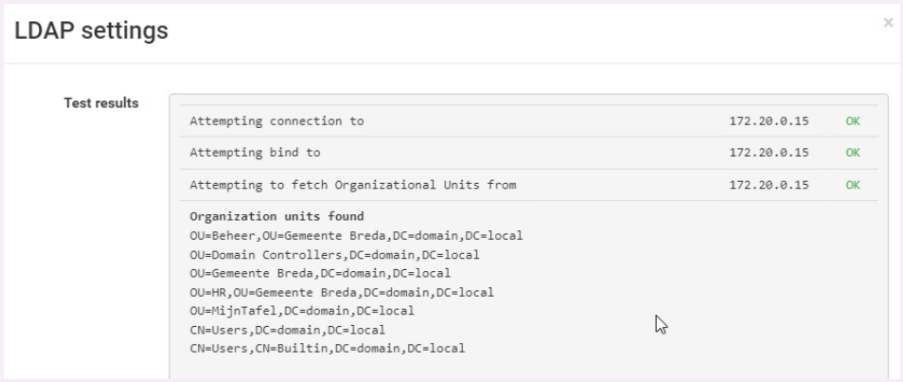
Voor mijn andere groep namelijk Beheer heb ik een policy ingesteld die de klok verbergt.

Oefeningen Infrastructuur



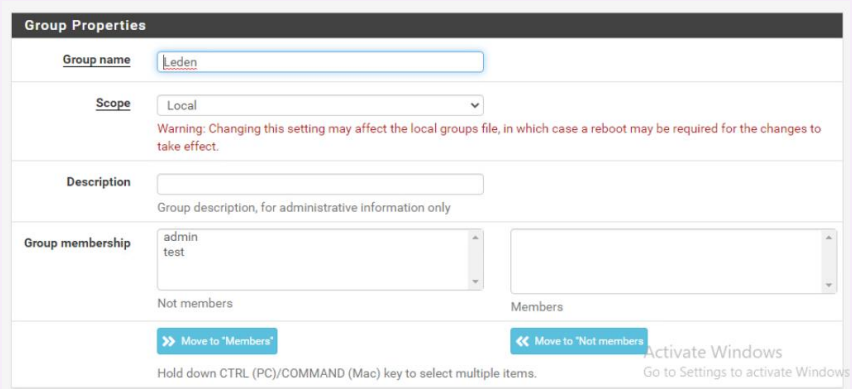
Wanner ik inlog

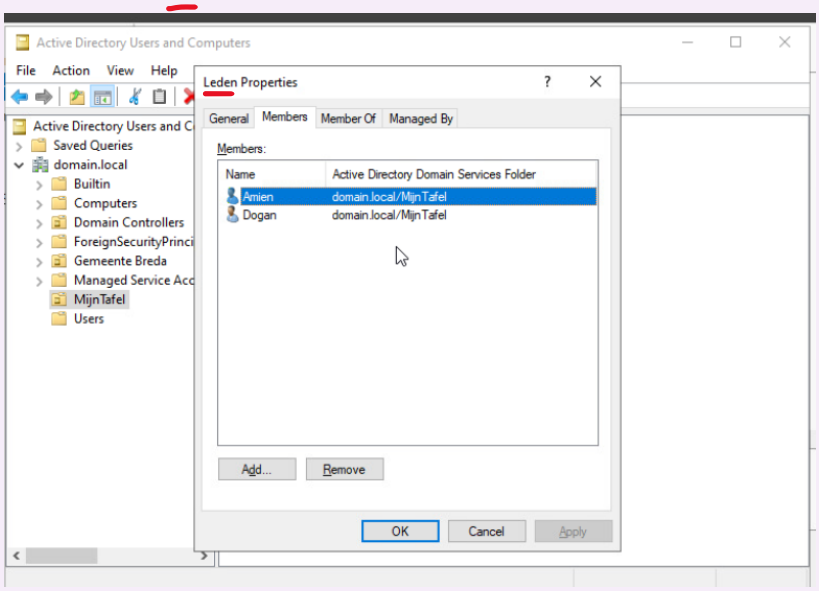
Zie ik geen klok



Test

Verder voeg ik een groep aan gebruikers toe.

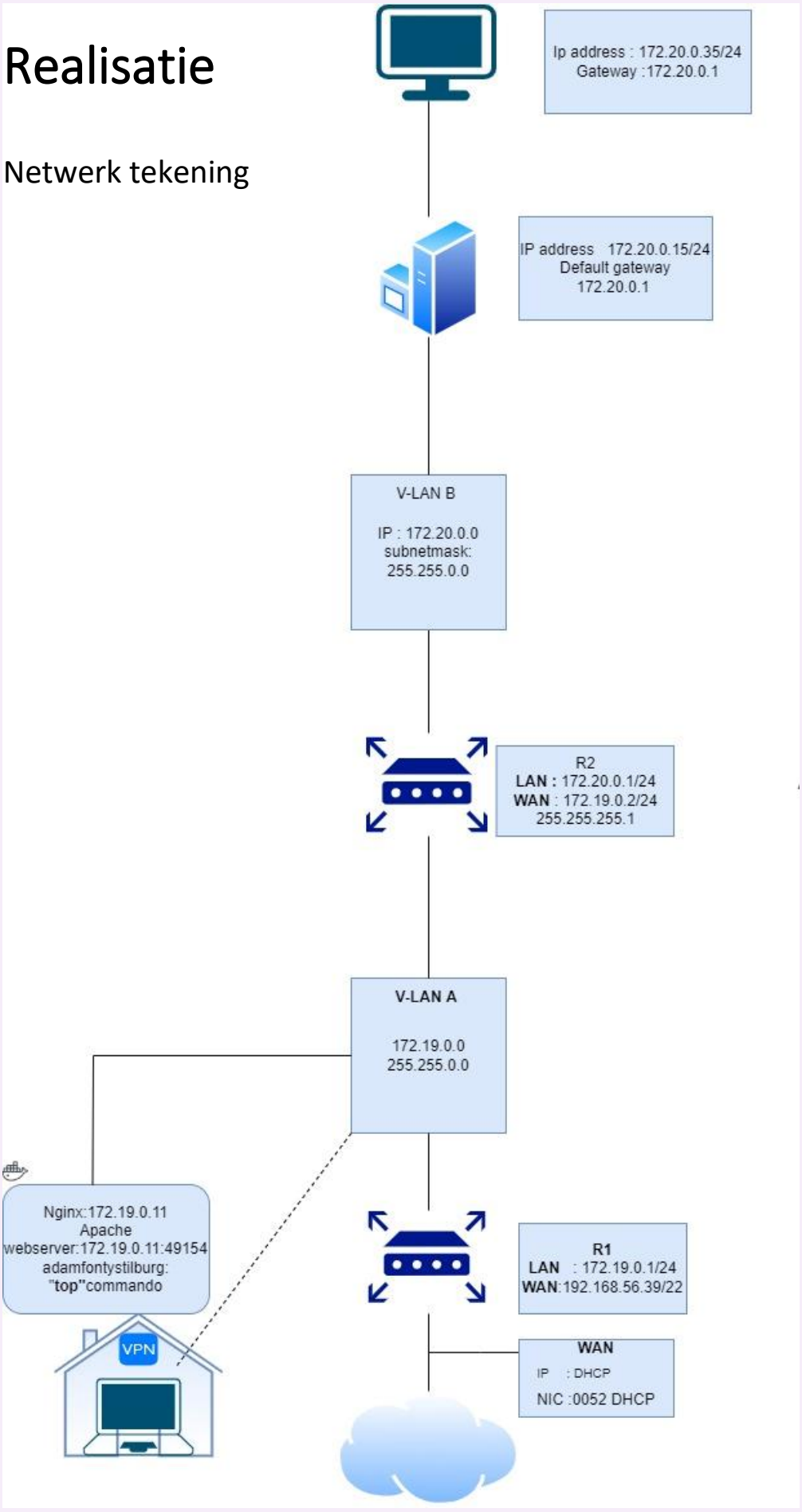




De gebruikte naam voor de groep moet gelijk zijn

Realisatie

Netwerk tekening



Overige opdrachten

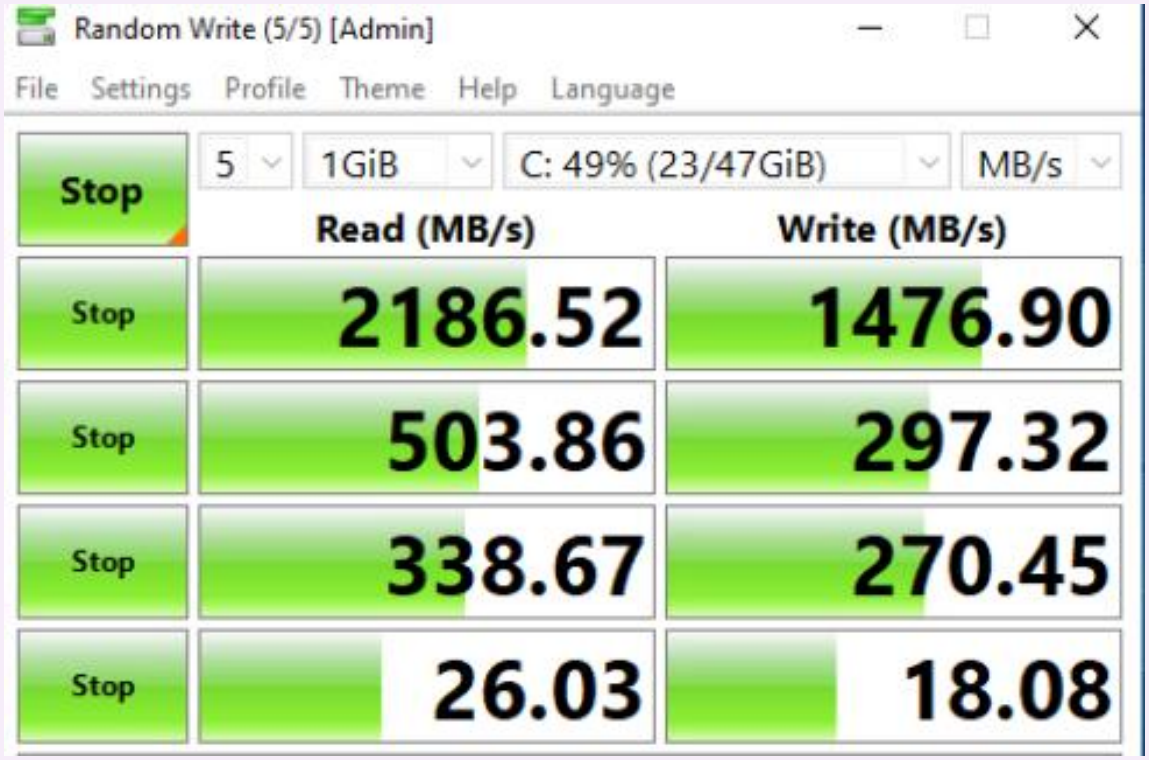
RAID configuratie

Werkt raid met SSD?

Antwoord: Het is zeker mogelijk en het heeft zelfs voordelen over de HDD. Namelijk HDDs hebben een lagere performance, verder krijgen HDDs sneller failure ’s.

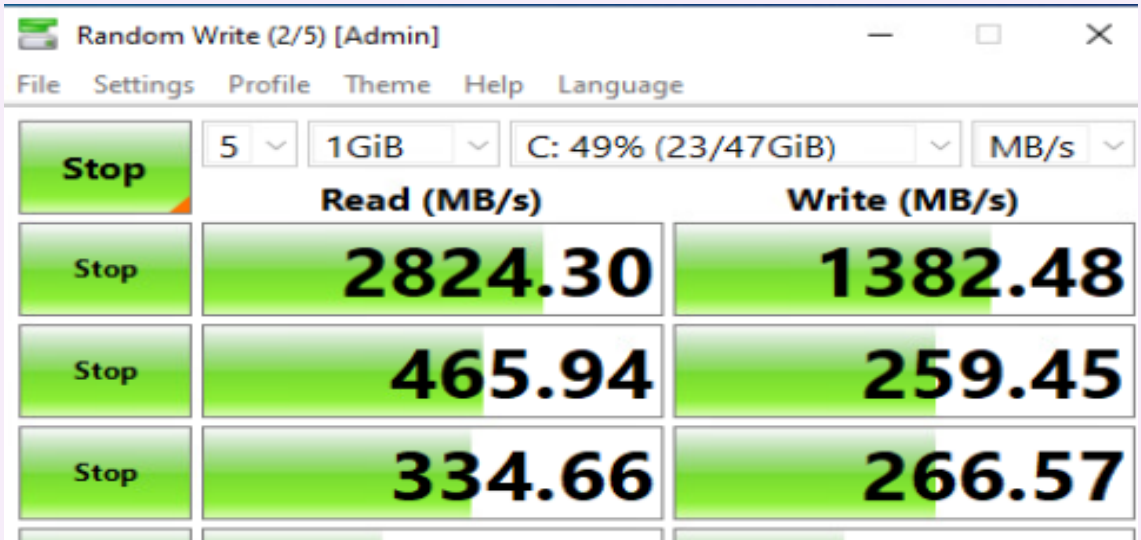
Bron: https://www.enterprisestorageforum.com/hardware/ssd-raid-boosting-ssd-performance-with-raid/

Zonder Raid



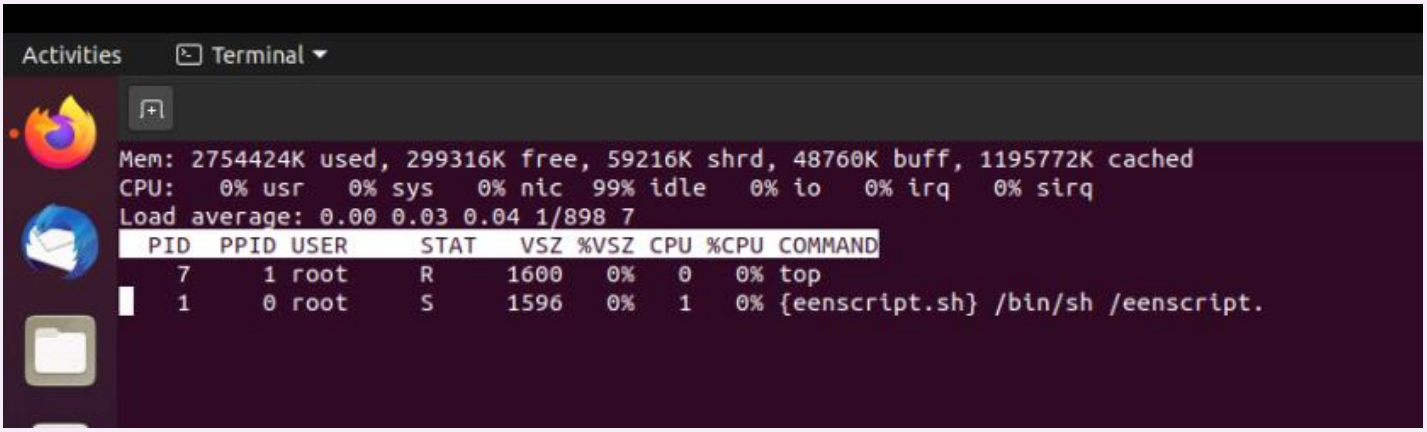
Met Raid

Het lezen van data gaat iets sneller maar het schrijven van data gaat juist slomer.



Oefeningen Infrastructuur

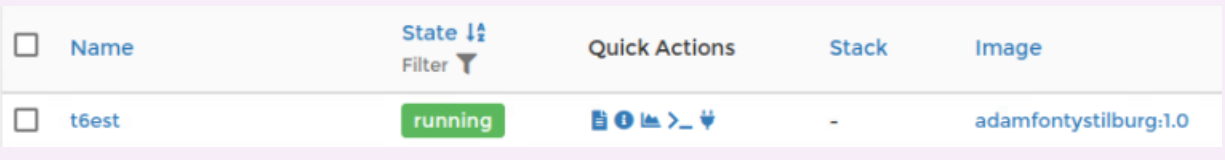
Het maken van een docker image



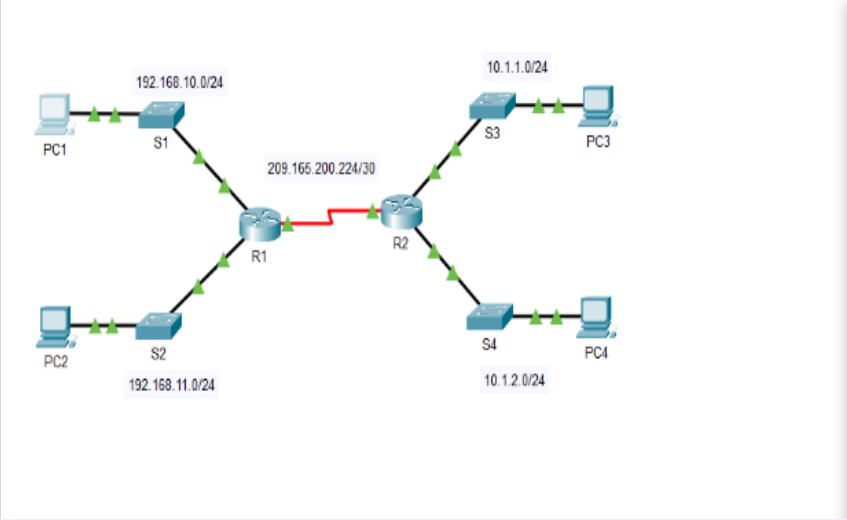
Hier heb ik een image gemaakt van het TOP commando.

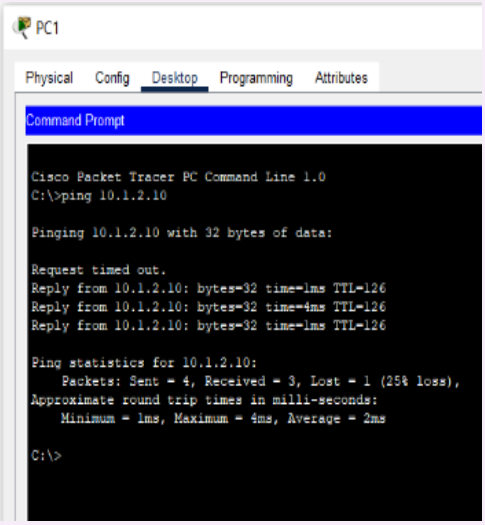
Gebruikte commando's

#! /bin/sh (hiermee geef je aan dat het een shell commando is)
top (checkt de specificaties van de werkmachine)
sudo Docker build -t adamfontystilburg:1.0 (Build maakt een image -t geeft de image een naam)
touch Dockerfile (met Touch maak je een nieuwe file die we Docker noemen)
nano Dockerfile (Nano is een teksteditor vi zou ook kunnen)



2 statische routers





In deze opdracht heb ik nogmaals geoefend met het verbinden van statische routers oefening baart kunst.

Gefaalde project

Ik wilde graag meer experimenteren met het maken van image’s dus ik kwam op het idee om een apache webserver in een image te plaatsen.

In talloze verschillende tutorial kwamen de volgende punten steeds terug

FROM UBUNTU :latest (dit houd in dat de ubuntu image van Dockerhub word gehaald) (latest houd in dat de nieuwste image opgehaald moet)

RUN apt-get -y update (allen pakketjes worden hierdoor geüpdatet)

RUN apt-get install -y apache2 curl (-y execute Allen commando's automatisch) (curl zorgt ervoor dat de de surver draait)

EXPOSE 80 (Dit is de poort waar de apache server op draait)

CMD ["-D", "FOREGROUND"] (de entrypoint gaat het cmd vlags gebruiken als commando)

Wat ik best vreemd vind is dat in allen tutorials die ik tegen ben gekomen de vi editor gebruikt word. Dit is een ouderwetse en zeer frustrerende editor die niet werk als een normale toestenboord. Om dat ik kwakkeloos de tutorials deed volgen heb ik de volgende commando's moeten gebruiken

VI Editing commands

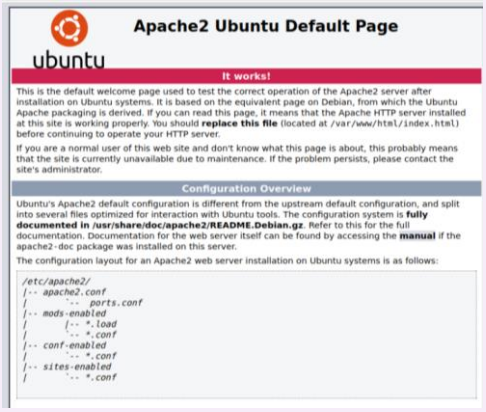
- i – Insert at cursor (goes into insert mode)
- a – Write after cursor (goes into insert mode)
- A – Write at the end of line (goes into insert mode)
- ESC – Terminate insert mode
- u – Undo last change
- U – Undo all changes to the entire line
- o – Open a new line (goes into insert mode)
- dd – Delete line
- 3dd – Delete 3 lines.
- D – Delete contents of line after the cursor
- C – Delete contents of a line after the cursor and insert new text. Press ESC key to end insertion.
- dw – Delete word
- 4dw – Delete 4 words
- cw – Change word
- x – Delete character at the cursor
- r – Replace character
- R – Overwrite characters from cursor onward
- s – Substitute one character under cursor continue to insert
- S – Substitute entire line and begin to insert at the beginning of the line
- ~ – Change case of individual character

De Nano tekst editor was ook voldoende geweest.

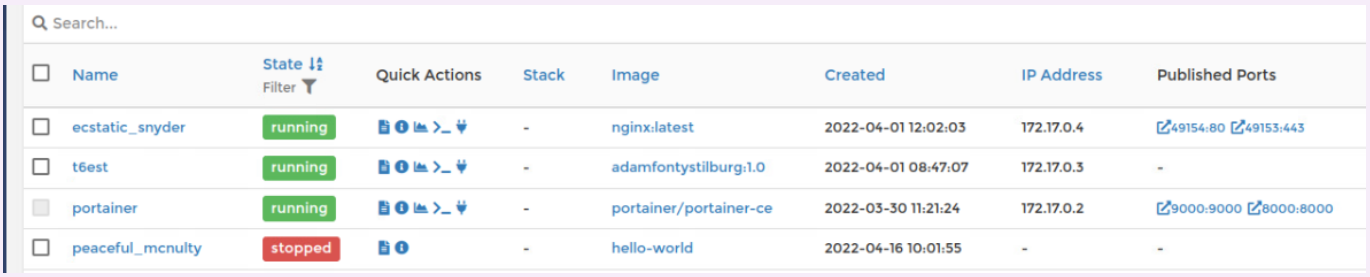
De foutmelding die ik steeds krijg is dat de image niet lokaal is opgeslagen wat raar is aangezien de image gewoon in mijn editor is aangemaakt net zoals hoe dat ging bij de tutorial die op teams staan en de tutorial van het internet.

```
adem@adem-virtual-machine:~$ sudo docker run --name myapache -d -p 80:80 apache_image:1.0
Unable to find image 'apache_image:1.0' locally
docker: Error response from daemon: pull access denied for apache_image, repository does not exist or may require 'docker login': denied: requested access to the resource is denied.
See 'docker run --help'.
adem@adem-virtual-machine:~$
```

Het gekste van allemaal is het volgende,



De apache-container runt terwijl ik geen container heb met apache erin



Search...

Name	State / Filter	Quick Actions	Stack	Image	Created	IP Address	Published Ports
ecstatic_snyder	running		-	nginx:latest	2022-04-01 12:02:03	172.17.0.4	49154:80 49153:443
t6est	running		-	adamfontystilburg:1.0	2022-04-01 08:47:07	172.17.0.3	-
portainer	running		-	portainer/portainer-ce	2022-03-30 11:21:24	172.17.0.2	9000:9000 8000:8000
peaceful_mcnulty	stopped		-	hello-world	2022-04-16 10:01:55	-	-

Dit zijn de enige containers die bij mij runnen. Overginds is de container genaamd t6est slechts een linux top commando. Dus eigenlijk werkt het een beetje aangezien de server wel draait?

Reflectie

Ik vond het wel een leuke acht weken omdat ik nu steeds meer begrijp over hoe infra werkt. Wat ik ook gemerkt heb is dat er meer gelet moet worden op de leer uitkomsten in plaats van de opdrachten aanzich. In het begin dacht ik bijvoorbeeld met Docker dat als ik een paar containers liet runnen dat het dan wel genoeg is omdat ik dan feitelijk de opdracht heb gehaald. Hier leer je niet zo veel van en het is ook niet wat de leerdoel aantoont. Door in mijn geval dan steeds meer Docker te bestuderen toon je wel de leerdoelen aan terwijl je wellicht geen specifieke opdracht aankaart. Het volgende semester zal ik mijn projecten meer richten op de leerdoelen en dan zal ik dit combineren met datgene waarin ik mij graag in wil verdiepen.

Voor de volgende keer ga ik mijzelf aanleren om eerst een plan te maken voordat ik iets doe. Eerst onderzoek doen en nadenken dan uitvoeren. Ik heb gemerkt dat ik tekort schiet in deze gestructureerde professionelen mindset.