



Project Hosting

Projectplan

Bachelor in de Toegepaste Informatica...

Naam van studenten
Wout Wynen, Frederik van Doren, Joey van
Eym, Barend van Lith, Kobe van Hasselt,
Jesse van Doninck

Academiejaar 2018-2019

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

INHOUDSTAFEL

INHOUDSTAFEL	2
1 INLEIDING	5
2 AANLEIDING EN ACHTERGROND	6
3 DOELSTELLINGEN.....	7
3.1 Prioritair.....	7
3.2 Operation report cards	7
3.2.1 Password safe	7
3.2.2 Een Post-mortem process.....	8
3.2.2.1 Inleiding	8
3.2.2.2 Document verslag doelen.....	8
3.2.2.3 Probleemgevallen identificeren, en hoe zijn deze opgelost.....	8
3.2.2.4 Welke lessen hebben we geleerd?	8
3.2.3 Monitoring.....	9
3.2.4 Do you have a pager rotation schedule?	9
3.2.5 Can a user's account be disabled on all systems in 1 hour?.....	9
3.2.6 Zijn gebruikers verzoeken traceerbaar via een ticket systeem?	9
3.2.7 Een database van alle machines.....	9
3.2.8 Automatisch software updaten.	10
3.2.9 Automatiseren van de backups.	10
3.2.10 Op een afstand werken.	10
3.2.11 Anti-malware software.	10
3.2.12 Security policy.	10
3.2.13 Reset privileged root passwords.	11
3.2.14 Veiligheid	11
3.2.15 Dataopslag	11
3.2.16 Hardware	11
3.3 Niet-Prioritair	11
3.3.1 Antwoordtijden	11
3.3.2 Schaalbaarheid	11
3.3.3 Testplan	12
3.3.4 Prijsberekening	12

4	STAKEHOLDERS EN BUSINESSCASE.....	13
4.1	Doelgroep.....	13
4.2	Voordelen.....	13
5	FASERING.....	14
6	VISUEEL PROJECTPLAN.	16
7	ONZE DOCKER-COMPOSE FILE.....	18
7.1	Lamp-stack.....	19
7.2	Bitwarden.....	20
7.3	Zabbix-server	21
7.4	Portainer	22
7.5	PHPmyAdmin.....	23
7.6	Watchtower.....	24
7.7	Anti-malware programma	24
7.8	Op afstand werken	25
7.9	Duplicati.....	25
7.10	DNS	26
7.11	VSFTPD.....	26
7.12	Github	27
7.13	Database van alle machines	27
7.14	Servicedesk plus	28
8	SECURITY POLICY	29
8.1	Introductie	29
8.1.1	Doelen	29
8.1.2	Bereik.....	29
8.2	Beleid.....	29
8.2.1	Systeem toegangscontrole.....	29
8.2.2	Personeels / infrastructuur wachtwoorden	29
8.3	Malware	30
8.4	Data en programma back-up	30
8.5	Bitwarden passwoorden.....	30
8.6	SSH	30
8.7	Software updates	31
8.8	Netwerk monitoring	31
9	PAGER ROTATION	32
10	HANDLEIDINGEN.....	33
10.1	Installing Ubuntu 18.04 and VM's	33
10.1.1	Dingen die men moet doen op de machine zelf.	37
10.1.2	Instellingen netwerk.	38
10.2	Installatie Docker.....	38
10.3	Installatie docker-compose.....	39
10.4	Installatie van de docker-compose file.....	39
10.5	ClamAV.....	40
10.5.1	Script ClamAV.....	41
10.6	VSFTPD.....	42
10.6.1	Installatie VSFTPD	42
10.7	Zabbix-agent installatie.....	43
10.8	VERANDEREN VAN PASSWOORDEN BINNEN HET UUR	47
10.8.1	Ubuntu root	47
10.8.2	Portainer	47
10.8.3	Bitwarden.....	48
10.8.4	Duplicati.....	48
10.8.5	MySQL & PHPmyAdmin	49

10.9	Service desk plus.....	50
10.9.1	Installatie.....	50
10.10	OpenSSH Server	57
10.10.1	Installatie.....	57
10.11	Volledig functionaliteitsverloop.....	58
10.12	DNS	69
10.12.1	Configuratie:	70
11	TROUBLE-SHOOTING.....	75
11.1	Ubuntu sources list.....	75
11.2	LAMP-stack	75
11.2.1	Logbestanden	75
11.2.2	Geblokkeerde poorten of conflicterende software.....	75
11.2.3	Andere mogelijke oorzaken.....	76
11.3	VSFTPD.....	76
11.3.1	Verbinding geweigerd	76
11.3.2	Andere fouten	76
11.4	ClamAV.....	77
11.4.1	Fout tijdens het updaten	77
11.4.2	ClamAV gebruikt telkens meer als 50% van de processor	77
11.5	Zabbix	77
11.6	Duplicati.....	78
11.7	DNS	79
12	TESTING.....	80
12.1	Zabbix	80
12.2	Service desk plus.....	80
12.3	Duplicati.....	81
12.5	Bitwarden.....	83
12.6	ClamAV.....	85
13	BIJLAGEN	87
13.1	Vergaderverslag 21/05	87
13.1.1	Wie staat waar?	87
13.2	Vergaderverslag 22/05	87
13.2.1	Wat is er gisteren gelukt?.....	87
13.2.2	Wat gaat er vandaag gebeuren:	87
13.3	Vergaderverslag 23/05/19	88
13.3.1	Wat is er gisteren gelukt?.....	88
13.3.2	Wat gaat er vandaag gebeuren:	88
13.4	Trello.....	88

1 INLEIDING

De leerlingen APP hebben opdracht gekregen om een PHP project te creëren. Het is wenselijk dat ze deze online kunnen hosten, zodat anderen deze ook kunnen benaderen. Het is onze taak om in dit verhaal de hosting te voorzien.

Het doel van dit project is om een shared web hosting omgeving op te zetten, waar de verschillende leerlingen een account kunnen maken. Hier kunnen ze via FTP inloggen en hun project uploaden. Het is tevens belangrijk dat de leerlingen toegang hebben tot hun MySQL databases.

Dit gaan we onder andere realiseren doormiddel van een LAMP stack (= linux, apache, MySQL, PHP). Zoals eerder aangegeven hebben de leerlingen toegang nodig tot een database. Dit doen we door PHPMyAdmin te installeren. Op deze manier kan men hun databases gemakkelijk beheren.

Verder maken we gebruik van verschillende technologieën zoals onder andere Zabbix, Docker, Portainer,... In dit project gaan we al deze software proberen te integreren met elkaar, om zo uiteindelijk tot een shared webhosting infrastructuur te kunnen raken.

In dit document vindt u onder meer ook de verschillende Operation report cards, die beschrijven hoe we met bepaalde situaties omgaan, of op welke manier we gaan handelen. Voorbeelden hiervan zijn bijvoorbeeld een post-mortem proces, of het hebben van een wachtwoord safe.

2 AANLEIDING EN ACHTERGROND

De studenten van de richting APP hebben nu enkel de mogelijkheid om hun projecten lokaal te bekijken, door middel van een lokale webserver. Wanneer ze in een groep samenwerken, kan men tegen problemen lopen omdat het niet allemaal even bereikbaar is. Uiteraard zijn er oplossingen zoals GitHub, maar deze zijn niet geschikt om op een vlotte manier het project weer te geven.

3 DOELSTELLINGEN

3.1 Prioritair

Het verwachte eindproduct moet een hosting platform worden waarmee we de websites van de studenten van 2APP kunnen op hosten met hun eigen database. De doelstellingen die nodig zijn voor dit project:

- De studenten moeten eenvoudig hun website op onze webserver kunnen plaatsen.
- De studenten moeten niet veel / niks meer extra installeren/ configureren om hun websites te kunnen hosten.
- Ze moeten ook toegang krijgen tot hun eigen database zodat hun PHP applicatie kan werken.
- Er moet een goed back-upprogramma zijn, zodat als er iets fout loopt men niet al zijn gegevens verloren is.

We hebben ook een aantal functionaliteiten in ons project gestopt, namelijk die van de Operation Report Cards.

3.2 Operation report cards

We hebben gekozen om ervoor te zorgen dat we minstens 12 operation report cards gaan integreren zoals beschreven in de website Opscards. Deze report cards zijn voor ons ook allemaal prioritaire functionaliteiten. Hieronder hebben we ze voor u even allemaal opgelijst.

3.2.1 Password safe

We gaan gebruik maken van een password safe waar dat de studenten al hun paswoorden veilig kunnen opslaan.

Als password safe willen we gebruik maken van Bitwarden. Bitwarden is een opensource en een cloud-gebaseerde tool voor wachtwoordbeheer voor persoonlijk en zakelijk gebruik. Het is een eenvoudige oplossing die is uitgerust met alle noodzakelijke functies voor het beheren en beveiligen van uw wachtwoorden, en het voert al deze functies goed uit.

We hadden hier ook voor Lastpass kunnen kiezen maar deze heeft de optie niet om zelf een database te maken van alle useraccounts/passwords. Dit leek ons wel een nuttige optie want zo kunnen we zelf alles gaan beheren.

3.2.2 Een Post-mortem process.

3.2.2.1 Inleiding

Om het project achteraf succesvol te kunnen beoordelen, hebben we ervoor gekozen een post-mortem document te voorzien. Het is de bedoeling dat de deelnemers van het project achteraf dit document invullen, om een beter idee te krijgen over de hoogte- en dieptepunten. Uiteindelijk hopen we op deze manier de volgende keer het aantal dieptepunten te verminderen.

3.2.2.2 Document verslag doelen

Identificeren van hoogtepunten en/of dieptepunten van het project. Een duidelijk beeld geven welke lessen er geleerd zijn, om hier in de toekomst rekening mee te houden

3.2.2.3 Probleemgevallen identificeren, en hoe zijn deze opgelost

Binnen de volgende tabel is het de bedoeling dat men de verschillende acties die er gedaan zijn om het project tot stand te brengen, opschrijven. Wanneer er iets fout ging, duidt men dit aan in de laatste kolom en markeren we deze rij.

Actie item	Type	Eigenaar	Fout
Ubuntu server	Proces	Kobe van Hasselt	Sources list niet uitgebreid genoeg
LAMP-stack	Proces	Kobe van Hasselt	Conflicterende poorten
VSFTPD	Proces	Jesse van Doninck	Verbinding geweigerd
ClamAV	Proces	Wout Wynen	Gebruikt veel CPU
Zabbix	Proces	Joey van Erum	Weigering inkomende verbinding
Duplicati	Proces	Frederik van Doren	Geen permissies om map te maken op externe server

3.2.2.4 Welke lessen hebben we geleerd?

Vul onder de onderstaande kopteksten in welke delen van het project waarin het goed of fout ging, maar ook waar er een factor van geluk heeft meegespeeld. Deze gegevens kunnen gemakkelijk zijn om in de toekomst zelfde fouten te vermijden.

Wat ging er goed?

Installeren van FTP server, LAMP-stack, Ubuntu server, ClamAv,...

Wat ging er fout?

Installeren van Bacula → deze hebben we verwisseld voor Duplicati

Installeren van een mailserver → vervangen voor een ticketing systeem

Waar hebben we geluk gehad?

3.2.3 Monitoring.

Natuurlijk willen we alles kunnen zien wat in ons netwerk gebeurt, daarom gaan we een monitoring tool installeren die heel ons netwerk zal monitoren.

Als monitoring tool hebben we een keuze gemaakt tussen Nagios en Zabbix, het zijn beide uitstekende monitoring tools maar hebben toch de keuze gemaakt voor Zabbix.

We hebben voor Zabbix gekozen omdat de configuratie in een grafische omgeving wordt gedaan en we dus niet sukkelen in de CLI met configuratiebestanden. Ook gebruikt Zabbix een eigen database waar dat het al zijn gegevens in opslaat.

Zo kunnen we bijvoorbeeld gaan kijken in de database als er een crash is gebeurd waar dat het juist aan lag.

We hebben ook gebruik gemaakt van Portainer.io, dit leek ons een nuttige tool, omdat we gebruik gingen maken van Docker. Met Portainer.io kunnen we in een grafische omgeving werken met de verschillende containers.

3.2.4 Do you have a pager rotation schedule?

Per dag gaan we iemand de hele werkdag (8-17u) beschikbaar stellen. Dit is per dag verschillend, een schema kan men vinden in hoofdstuk 8.

3.2.5 Can a user's account be disabled on all systems in 1 hour?

In hoofdstuk 9 wordt hier dieper op ingegaan. Specifieker kan men in hoofdstuk 9.7 een gedetailleerde handleiding vinden om alle wachtwoorden die gebruikt worden binnen ons systeem vlog aan te passen. Inclusief screenshots ter verduidelijking van het geheel.

3.2.6 Zijn gebruikers verzoeken traceerbaar via een ticket systeem?

Via een ticket systeem kunnen gebruikers ons eventuele verzoeken sturen.

Indien het over een probleem gaat, proberen we deze uiteraard zo snel mogelijk op te lossen. Als de ticket over een verzoek gaat voor bijvoorbeeld een feature te implementeren in ons huidig systeem, zullen we als team bekijken of deze feature echt nuttig is. Als dit het geval is, zullen we zeker ons best doen om naar de wensen van de klant te luisteren.

3.2.7 Een database van alle machines.

Er komen databanken met alle informatie van onze machines. Deze informatie omvat het RAM, processorsnelheid, type, jaar van aankoop, locatie en prijs. Deze databanken worden handmatig gemaakt en bewerkt omdat we momenteel maar met een beperkt aantal machines werken.

Wanneer onze omgevingen groter worden gaan we uitbreiden naar een automatisch systeem dat telkens de databanken update bij een wijziging.

3.2.8 Automatisch software updaten.

We willen ook gebruik maken van een patchsoftware, deze software zal alles automatisch updaten als er een nieuwe update van een bepaald programma is. Als patchsoftware gaan we gebruik maken van Watchtower, dit is een gratis en opensource applicatie waarmee we draaiende Docker-containers kunnen controleren en deze automatisch kunt bijwerken als er wijzigingen in hun basic images worden gevonden.

3.2.9 Automatiseren van de backups.

We hebben een programma nodig dat automatisch snapshots & back-ups maakt, om te voorkomen dat er bestanden verloren gaan bij het falen van de hardware of als iemand intern in het bedrijf per ongeluk iets heeft verwijderd. Hiervoor gaan we gebruik maken van Duplicati. Om het configureren te vereenvoudigen hebben we in dit geval gebruik gemaakt van een grafische interface, die bereikbaar is op poort 8200.

3.2.10 Op een afstand werken.

We gaan op een afstand connecteren met onze machines via SSH. De SSH die we hebben gekozen is openSSH omdat dit aan encryptie doet en hierdoor veiliger is dan gelijkaardige software (telnet, rlogin). Het is tevens ook mogelijk om met public en private keys te werken om zo het gebruik van wachtwoorden te vermijden en de beveiliging nog te verhogen.

3.2.11 Anti-malware software.

De veiligheid in ons systeem is ook zeker een must, we willen niet dat er malware of andere gevaarlijke zaken op onze servers/pc's komen. Daarom zullen wij ook een anti-malware programma installeren op onze apparaten. Als antimalware programma gaan wij ClamAV gebruiken dit is een simpel stukje software die wij dagelijks gaan laten runnen en deze scant dan alle bestanden op malware.

3.2.12 Security policy.

Het is belangrijk voor een bedrijf om toch minstens enkele vormen van beveiliging in te bouwen. Dit kan onder andere bestaan uit een handleiding voor het personeel / klanten ten opzichte van phishing, maar ook verschillende criteria ten opzichte van het wachtwoord, bijvoorbeeld speciale karakters gebruiken, wachtwoord vervallen na x aantal dagen,...

Verder zullen er rechten moeten worden ingesteld, zodat elke gebruiker slechts toegang heeft tot de mappen waar hij thuis hoort. Verder zal er ook gewerkt moeten worden met encryptie, om ervoor te zorgen dat zelfs het personeel niet bij de bestanden van de klant kan komen. Dit zou ongewenst zijn.

Updaten zou volgens een gecontroleerd systeem werken. We testen de updates eerst met een paar computers, om te kijken hoe deze erop reageren. Daarna gefaseerd uitrollen zodat bij een fout er niet te veel computers in 1 keer "besmet zijn".

3.2.13 Reset privileged root passwords.

Voor dit te organiseren gebruiken wij de handleiding die u kunt vinden bij hoofdstuk 9. De procedure hiervan is duidelijk opgesteld, en is met 1 commando te realiseren.

3.2.14 Veiligheid

Dit is zeker een prioritair gegeven in ons hosting platform. We willen niet dat studenten in de database van een andere studenten kunnen komen en dingen kunnen aanpassen. Ook willen we niet dat van buitenaf er malware op onze servers kan gezet worden, dit willen we tegen gaan met een goed anti-malware systeem.

We willen ook dat de users van ons hostingplatform een password-safe gebruiken zodat al hun wachtwoorden beveiligd worden.

3.2.15 Dataopslag

Dit is ook zeker een prioritair gegeven in ons hosting platform. De studenten van 2APP moeten hun persoonlijke database kunnen raadplegen zodat ze aan hun PHP applicatie kunnen werken. Daarvoor gebruiken wij een MySQL-database, zodat ze hier hun database op kunnen installeren.

3.2.16 Hardware

Wat ook vrij belangrijk is in ons project is de hardware, we willen niet dat de servers continu uitvallen wegens overbelasting. Daarom moeten we servers hebben die genoeg resources hebben om onze VM's te kunnen draaien.

3.3 Niet-Prioritair

3.3.1 Antwoordtijden

Natuurlijk willen we dat het systeem zo snel mogelijk reageert als men een actie doet, maar aangezien het voor onze studenten is en niet voor effectieve klanten (waar dat snelheid een must is), zal het in dit geval niet uitmaken mocht de website wat later reageren.

3.3.2 Schaalbaarheid

Omdat het hosting platform alleen maar wordt gebruikt door studenten en misschien ook een paar docenten van IT Factory in Thomas More Geel is maximale kwantiteit van gelijktijdige connecties niet meer dan 300. Als het hosting platform wordt uitgebreid zal de hardware moeten worden aangepast. Momenteel is dit niet prioritair omdat het heel onwaarschijnlijk is dat dit platform uitgebreid moet worden.

3.3.3 Testplan

Nadat we alles netjes hebben kunnen configureren volgt er nog een testplan van elk onderdeel. We gaan ons systeem dus effectief testen. In dit testplan kunnen er voorbeelden gezien worden van de werking van het systeem, en hoe de verschillende onderdelen in samenwerken tot het einddoel komen.

3.3.4 Prijsberekening

We hebben alvast een voorspelling van de prijsberekening voorzien voor wanneer men deze oplossing zou willen gebruiken in de bedrijfswereld. Dit houdt een kostenraming van het project in voor de tijd van opzet van dit systeem in tabelvorm.

4 STAKEHOLDERS EN BUSINESSCASE

4.1 Doelgroep

Het eindproduct is voorzien voor de studenten en docenten van 2APP op Thomas More. Zij kunnen hier dan hun PHP webapplicatie hosten op onze hostomgeving.

4.2 Voordelen

De studenten van APP moeten door de implementatie van ons project zich geen zorgen meer maken over het beschikbaar stellen van hun project. Er kleven verschillende voordelen aan het project dat wij voorstellen. Zo integreert onze ftp-service vrijwel naadloos met ontwikkelomgevingen als PHPStorm, waardoor de productiviteit verhoogd wordt.

Tevens hoeven de leerlingen zich geen zorgen meer te maken om zo'n omgeving zelf op te zetten, wat aanzienlijk veel tijd kan kosten. Dit zal ervoor zorgen dat de studenten hun projecten op een zorgeloze, veilige manier in onze hostomgeving kunnen plaatsen.

5 FASERING

Dit project omvat 11 lesweken met telkens lesblokken van 3 uur en een projectweek van vier werkdagen.

Fases	Deadlines
Brainstormen	6 uren
Proof of Concept	9 uren
Projectplan	6 uren
Test fase	12 uren
Implementatie fase	32 uren
Documentatie fase	15 uren

Eerste fase: Brainstormen – deadline 20/02

Het project is begonnen met een aantal dagen te brainstormen. In deze fase hebben we gekeken naar welke onderdelen er allemaal aanwezig moeten zijn om deze opdracht te doen slagen. We denken na over elk onderdeel dat aanwezig zal zijn en overleggen met ons team of dit een goede bijdrage gaat zijn voor ons eindresultaat vooraleer we aan de volgende fase beginnen.

Tweede fase: Proof of concept – deadline 06/03

In deze fase gaan we aan de slag met het onderzoeken van de verschillende mogelijkheden. Iedereen heeft een apart gebied waarin hij onderzoek doet. Om dit correct te laten verlopen betrekken we altijd heel het team als iemand een oplossing heeft gevonden, met de bedoeling dat geen technologieën met elkaar botsten. Door grondig onderzoek te doen hebben we een mooie presentatie kunnen geven die in het algemeen goed is ontvangen en hiermee de goedkeuring hebben gekregen om het concept te kunnen testen en later te gaan implementeren.

Derde fase : Projectplan – deadline 03/04

Tijdens deze fase dient men de gekozen technologieën en de Ops Report Cards te documenteren en dient men te controleren of ze ook effectief als geheel samen kunnen functioneren. Deze documentatie zal zeer nuttig zijn achteraf bij de test fase en de implementatie fase. Met het projectplan komt ook een schematische voorstelling van onze opstelling die voor meer duidelijkheid zorgt naar de mensen buitenaf.

Vierde fase: Test fase – deadline 20/05

Om tot een goed eindresultaat te komen maken we eerst een testopstelling op onze eigen laptop. Hierdoor krijgen we een idee van wat goed en minder goed verloopt met onze opstelling. Voor de onderdelen die minder goed verlopen zoeken we oplossingen door samen met ons team te vergaderen. Moest er een bepaalde software zijn die toch niet compatibel is met de rest van onze opstelling, kunnen we deze nog altijd veranderen om te voorkomen dat de eindopstelling niet gaat werken. Een goede uitvoering van deze fase is cruciaal voor het verdere verloop van ons project.

Vijfde fase : Implementatie fase – 24/05

Tijdens de Projectweek gaan we het gehele project realiseren in een virtuele omgeving. We maken gebruik van een datacenter met VMWare. Door de voorafgaande testfase zouden er geen grote problemen mogen optreden bij het samenvoegen van de gekozen technologieën en software. Het doel is om een werkende server te bekomen om het project van 2 ITF APP op te hosten.

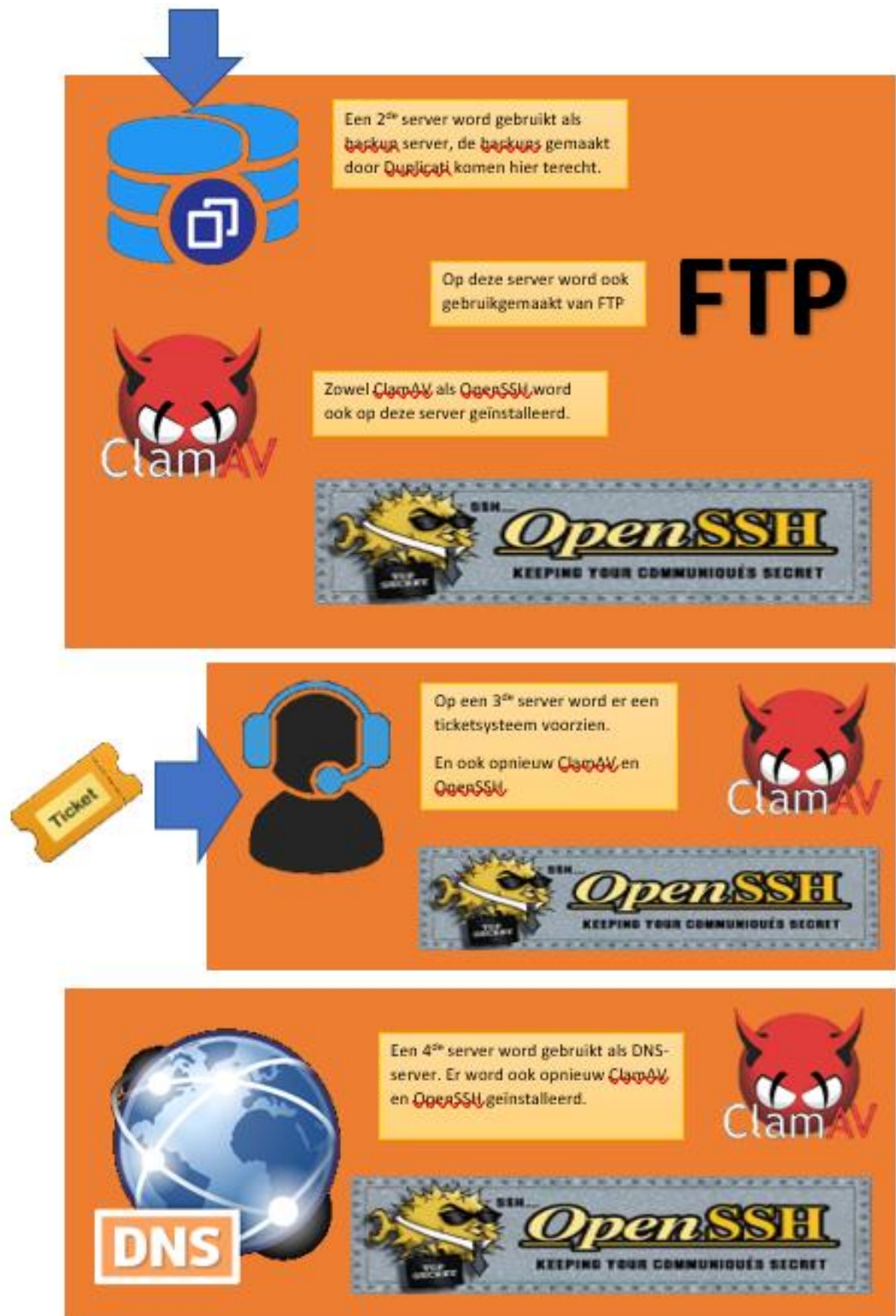
Zesde fase : Documentatie fase - 24/05

De laatste en één van de belangrijkste fases van het project is het documenteren van alle opgezochte en geïmplementeerde technologieën die we gebruikt hebben. Hier gaan we alles wat we hebben opgezocht en hebben uitgevoerd grondig documenteren. Zo kan men achteraf stap voor stap nagaan hoe we alles hebben samengevoegd en tot een werkend geheel hebben gebracht in de Ubuntu server. De documentatie is ook zeer handig voor achteraf, moesten er in de werkende fase toch nog grotere fouten optreden of om achteraf na te gaan of er eventueel kleine configuratiefouten of gelijkaardige fouten waren tijdens de implementatie fase.

6 VISUEEL PROJECTPLAN.



Afbeelding: visueel projectplan schema deel 1



Afbeelding: visueel projectplan schema deel 2

7 ONZE DOCKER-COMPOSE FILE.

Docker-compose is een hulpmiddel voor het definiëren en uitvoeren van Docker-toepassingen met meerdere containers. Met compose gebruikt u een YAML-bestand om de services van uw toepassing te configureren. Vervolgens maakt en start u met een enkele opdracht alle services uit uw configuratie.

Compose heeft opdrachten voor het beheer van de gehele levenscyclus van uw applicatie:

- Services starten, stoppen en opnieuw opbouwen
- Bekijk de status van actieve services
- Stream de loguitvoer van actieve services
- Voer een eenmalige opdracht uit voor een service

Docker-compose houdt ook al zijn gegevens van zijn services bij in bepaalde volumes, elke service heeft zijn eigen volume waar dat de data van die bepaalde service wordt opgeslagen.

Sommige services kunnen we bereiken via de webbrowser met een bepaalde poort, we hebben hieronder elke service besproken en hier hebben we dan ook de poorten bijstaan waarmee je een service kan bereiken.

Onze docker-compose file bestaat uit een aantal programma's die het voor de studenten van APP eenvoudiger zouden maken. Deze onderdelen leggen we kort even vast

```
version: "3.5"
services:
  www:
    build: .
    ports:
      - "8000:80"
    volumes:
      - ./www:/var/www/html/
    links:
      - db
    networks:
      - default
  bitwarden:
    image: mprasil/bitwarden
    restart: always
    ports:
      - 8004:80
    volumes:
      - ./bw-data:/data
    environment:
      WEBSOCKET_ENABLED: "true"
      SIGNUPS_ALLOWED: "true" # set to false to disable signups
  db:
    image: mysql:8.0
    ports:
      - "3305:3305"
    command: --default-authentication-plugin=mysql_native_password
    environment:
      MYSQL_DATABASE: myDb
      MYSQL_USER: user
      MYSQL_PASSWORD: test
      MYSQL_ROOT_PASSWORD: test
```

[Read 131 lines]

```

portainer:
  image: portainer/portainer
  command: -H unix:///var/run/docker.sock
  restart: always
  ports:
    - 9000:9000
  volumes:
    - /var/run/docker.sock:/var/run/docker.sock
    - portainer_data:/data

watchtower:
  image: v2tec/watchtower
  container_name: watchtower-compose
  privileged: true
  command: watchtower clusterman clusterman --interval 30
  restart: unless-stopped
  volumes:
    - /var/run/docker.sock:/var/run/docker.sock
    - /root/.docker/config.json:/config.json
dbzabbix:
  image: gcavalcante8808/zabbix-db-postgres:4.0.0
  restart: always
  environment:
    POSTGRES_DB: zabbix
    POSTGRES_USER: zabbix
    POSTGRES_PASSWORD: "zabbix"
  volumes:
    - zabbix-db-data:/var/lib/postgresql/data

```

Afbeelding: docker-compose bestand

7.1 Lamp-stack

In het eerste deel van de compose-file vinden we een paar services die nodig zijn om een PHP applicatie met de nodige database van de gebruiker toe te passen. De WWW service is eigenlijk onze Apache service, hier kan dan de PHP website op runnen. We gebruiken daaronder ook de DB service, dit is onze database van MySQL waar dat de studenten van APP hun persoonlijke database die ze nodig hebben voor hun applicatie in kunnen plaatsen. Met kan de WWW service bereiken op:

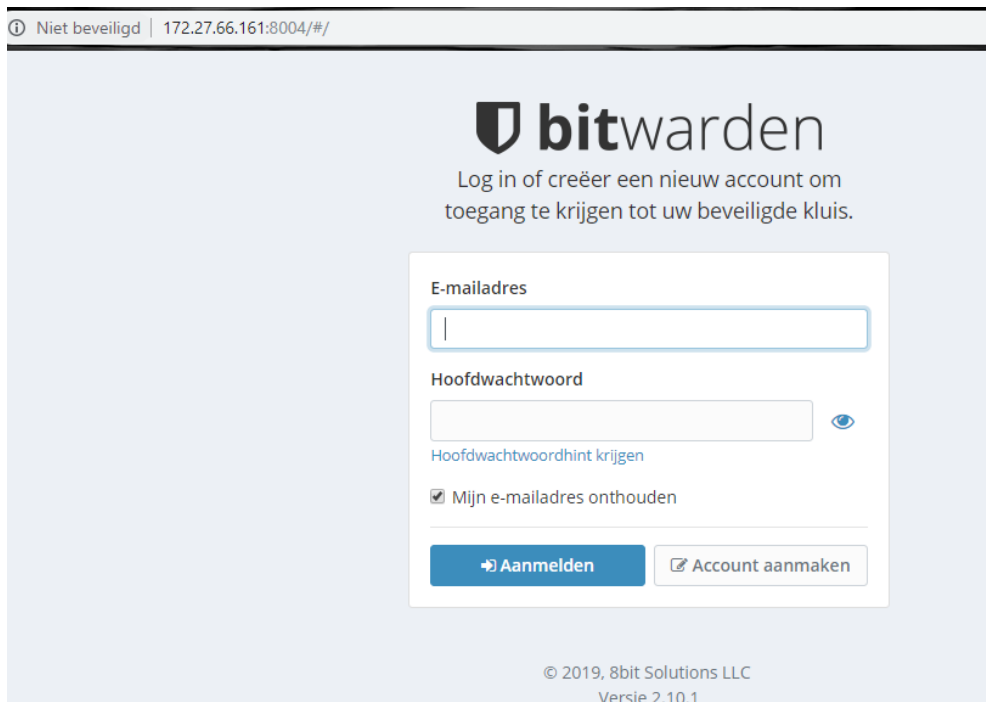
Poort: **80**



Afbeelding: Visueel schema van LAMP-stack

7.2 Bitwarden

Wachtwoorddiefstal is een serieus probleem. Daarom hebben wij ervoor gekozen om ook een wachtwoord manager toe te voegen aan onze docker-compose file. Deze zal alle wachtwoorden van de gebruiker bijhouden en beveiligen voor diefstal. Men kan deze wachtwoord manager bereiken op poort **8004** en hier kan men dan een account maken waar dat ze al hun wachtwoorden kunnen opslaan.



Niet beveiligd | 172.27.66.161:8004/#/

bitwarden

Log in of creëer een nieuw account om toegang te krijgen tot uw beveiligde kluis.

E-mailadres

Hoofdwachtwoord

Hoofdwachtwoordhint krijgen

☒ Mijn e-mailadres onthouden

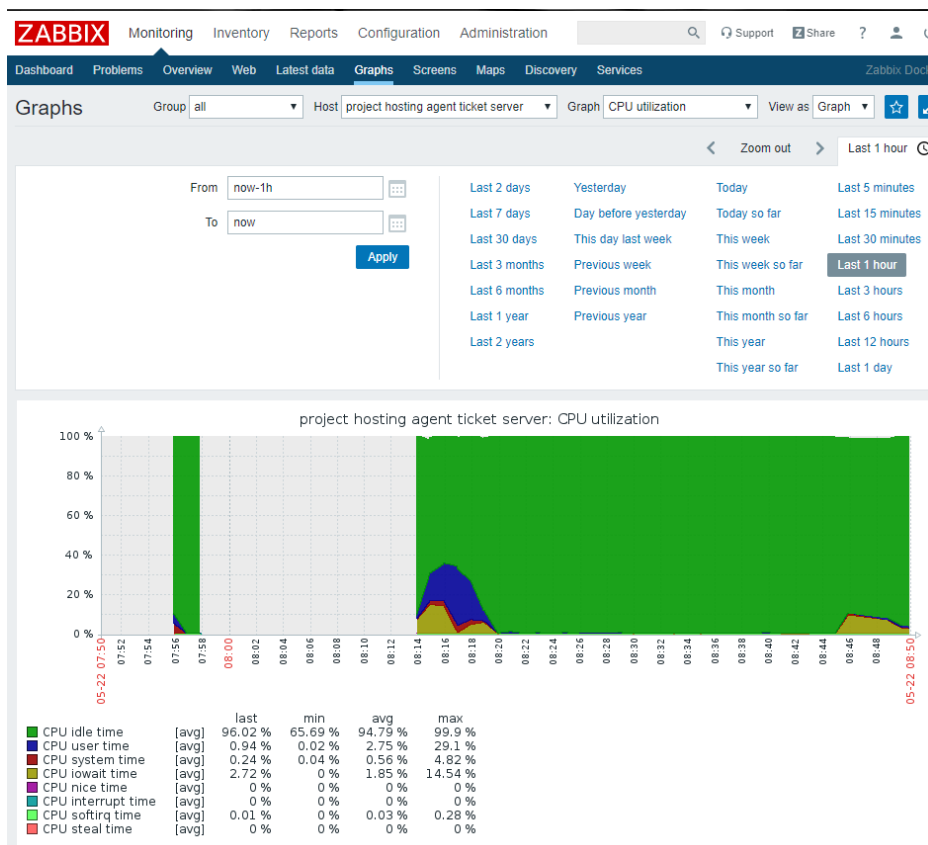
Aanmelden Account aanmaken

© 2019, 8bit Solutions LLC
Versie 2.10.1

Afbeelding: Bitwarden inlog scherm

7.3 Zabbix-server

Zabbix server is een opensource applicatie voor de monitoring van de servers en nog veel meer. Wij gebruiken deze tool om buiten de containers te monitoren op de hosting server waar dat onze docker-compose file staat, ook gaan we monitoren op de ticket server en de backup server mocht daar iets fout gaan. Deze server kunnen we bereiken op de poort **8080**. **Dit is wel een service die enkel voor de administrator bedoeld is. Hier mogen dus eigenlijk geen studenten aankomen!**

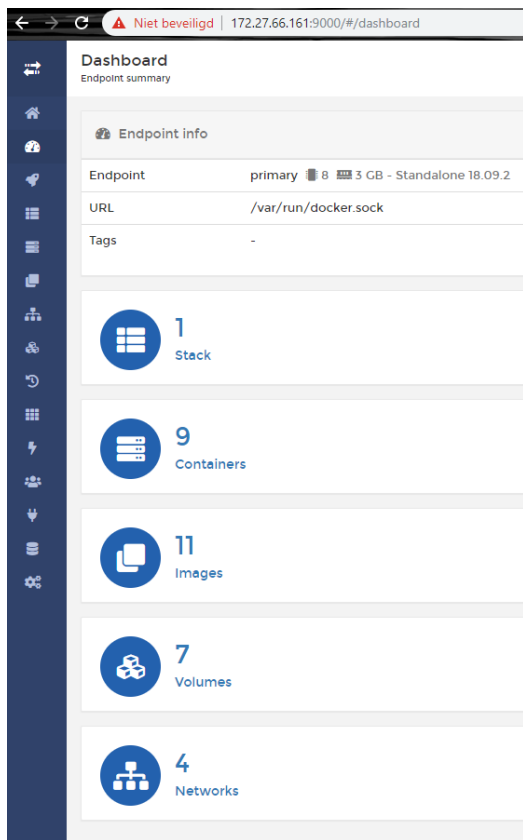


Afbeelding: Zabbix overzicht scherm

7.4 Portainer

Portainer is een krachtige open-source beheertools waarmee u eenvoudig Docker-omgevingen kunt bouwen, beheren en onderhouden. Ook een voordeel hier is de grafische omgeving waarmee Portainer werkt, deze interface is zeer geoptimaliseerd en ook zeer duidelijk.

Dit is een handige tool voor ons omdat we met docker werken en zo kunnen we in de containers zelf gaan kijken. Deze tool kunnen we bereiken op de poort **9000**. **Deze service is ook enkel voor de administrator waar dat hij of zij de containers van docker kan beheren.**



Afbeelding: Het dashboard van Portainer

7.5 PHPmyAdmin

PhpMyAdmin is een gratis softwaretool geschreven in PHP, deze tool is voor het beheren van onze MySQL databases via het internet. Vaak gebruikte bewerkingen zijn (beheren van databases, tabellen aanmaken, kolommen aanmaken, relaties toevoegen, indexen generen, gebruikers machtigingen geven, enz.) We kunnen de phpmyadmin bereiken op poort 8001.



Afbeelding: het logo van phpMyAdmin

7.6 Watchtower

Watchtower is een applicatie die je draaiende Docker-containers controleert en controleert op wijzigingen in de images waarvan die containers oorspronkelijk zijn gestart. Watchtower detecteert dat er een image is gewijzigd en zal dan ook de container automatisch opnieuw opstarten.

Met Watchtower kunt u de actieve versie van uw gecontaineriseerde app bijwerken door een nieuwe image naar de Docker Hub of uw eigen imageregister te pushen.



Afbeelding: logo van Watchtower

7.7 Anti-malware programma

Als anti-malware programma hebben we gekozen voor het programma ClamAV. ClamAV is een open source programma dat heel gemakkelijk te installeren is. We hebben hierbij ook een script geïnstalleerd dat elke dag een volledige scan zal uitvoeren en om het uur een scan zal uitvoeren over de belangrijkste files.

ClamAV is een open-source antivirus programma dat zorgt voor het scannen van het systeem op de server. Het is een programma dat op alle besturingssystemen werkt. Het draait op de achtergrond zonder grafische interface. Het is een flexibel programma dat met een goede documentatie zorgt voor een robuust antivirus.

ClamAV kan gemakkelijk bash scripts gebruiken in Linux. Deze scripts zorgen er in ons geval voor dat het antivirus om het uur de php projecten scant, en dagelijks heel het systeem scant.

Ondanks wat sommige mensen denken, is clamAV altijd actief op de server. Vanaf deze opstart tot hij terug stopt met werken. De scripts worden maar eenmaal per uur (of per dag) uitgevoerd, maar ondertussen blijft clamAV wel actief op scannen van antivirussen.

Een belangrijke anekdote is wel dat clamav redelijk veel harde schijf ruimte nodig heeft. Het is een antivirus zonder grafische interface maar toch moet je zeker 4-5 GB ruimte voorzien om een vlotte installatie te garanderen.

De voornaamste reden waarom we als antivirus voor ClamAV hebben gekozen, is omdat de service het beste werkt realtime op Linux.

Ook als de het anti-malware programma een virus vindt zal het een push bericht sturen naar een app die de pager dan op zijn smartphone zal hebben staan. Dit is zeer handig want zo weet de pager meteen dat er iets op de server staat wat er eigenlijk niet hoort te staan.



7.8 Op afstand werken

Het is gemakkelijker wanneer er ergens zich een probleem voordoet, dat men niet meteen naar de locatie van de server te gaan om het probleem op te lossen. Dit hebben we getracht eenvoudig op te lossen door middel van een installatie van een OpenSSH server. Deze tool laat ons toe om onze server op afstand te beheren, dus als er bijvoorbeeld problemen zijn met een van onze services, kan dit vrijwel direct geïnspecteerd worden.



Afbeelding: afbeelding dat openSSH weergeeft.

7.9 Duplicati

Als back-up programma maken we gebruik van Duplicati, Duplicati is een Open Source web based & command line interface back-up tool. Duplicati maakt gebruik van poort 8200 en 8201. Duplicati is nu ingesteld om naar onze externe back-up server "172.27.66.162" te back-uppen via FTP. Wij hebben er voor gekozen om dagelijks een volledige backup uit te voeren van heel de installatie en daarnaast om het uur de "home/project-hosting/www/" map met de php projecten te back-uppen.



Afbeelding: Logo van Duplicati

7.10 DNS

Voor de gebruiksvriendelijkheid hebben we er voor gekozen om een externe DNS server aan te maken. zo kunnen de studenten van APP gebruik maken van het domein "wserver.team6.com" in plaats van het IP "172.27.66.161" in te voeren. Ook voor ons ticket systeem kunnen de studenten gebruik maken van het domein "support.team6.com" in plaats van het IP "172.27.66.163". Het domein vertaald wordt dus automatisch naar het IP adres. De configuratie van DNS kan u terugvinden in "/etc/hosts/"



Afbeelding: Logo DNS

7.11 VSFTPD



Vsftpd is een FTP-server voor unix-achtige systemen, waaronder Linux. Dit hebben we bij onze servers geïnstalleerd om zo de users te laten inloggen in hun map. Deze map hebben we zo ingesteld dat de users niet boven hun map kunnen geraken waardoor dat ze ook niet in mappen kunnen geraken van andere studenten.

Afbeelding: Logo van VSFTPd

7.12 Github

Github is een open-source repository hostingsservice of eigenlijk een cloud voor code. Het hosts uw source projecten in verschillende programmeertalen en houdt dan de verschillende wijzigingen bij in elke iteratie. De service kan dit doen met behulp van git. Wij hebben dit gebruikt voor onze code van onze docker-compose file op te slaan. Hier hebben we dan een git repository gemaakt waar dat iedereen van onze groep dingen in kon gaan aanpassen.

Dit was ook handig voor de studenten van app want zo kunnen zij eenvoudig de link van onze github repository nemen en door een paar eenvoudige commando's hun LAMP stack creëren.



Afbeelding: Logo van Github

7.13 Database van alle machines

Om een goed overzicht te krijgen over de machines die we gebruiken hebben we een database gemaakt met een aantal tabellen. Dit is nodig als wij bijvoorbeeld nieuwe software gebruiken die niet werkt voor een bepaalde machine, dan zullen we deze machine moeten upgraden ofwel andere software gaan zoeken. In de database staat een software tabel met alle huidige versies van de software die wij gebruiken en die altijd up to date zal zijn. Ook zal er een tabel OS staan met de versie van het besturingssysteem van de server. Ook zal er instaan wat het geheugen van de server is en nog andere resources zoals RAM en Disk Size. Het ip van de server komt er ook bij te staan zodat iedereen altijd op de hoogte is met het nieuwste adres. Ondanks dat we een werkende DNS server hebben, is dit toch altijd handig om te weten.

De database gaat er als volgt uitzien:

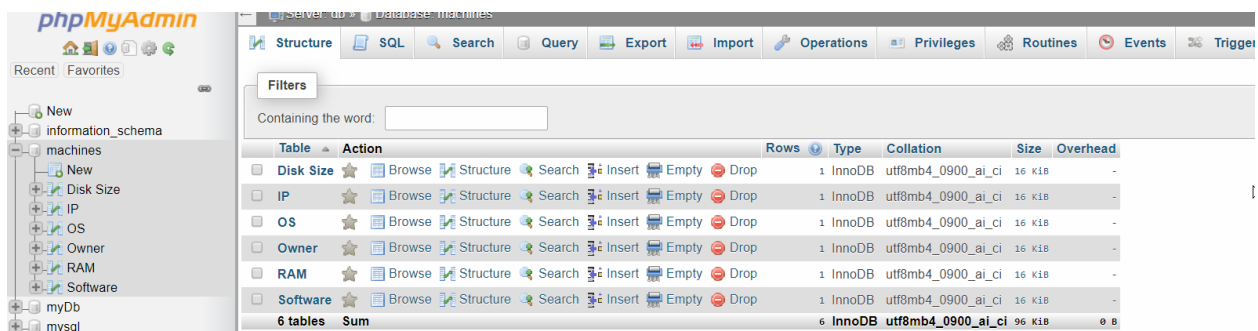


Table	Action	Rows	Type	Collation	Size	Overhead
Disk Size	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
IP	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
OS	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
Owner	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
RAM	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
Software	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_0900_ai_ci	16 K18	-
6 tables	Sum	6	InnoDB	utf8mb4_0900_ai_ci	96 K18	0 B

7.14 Servicedesk plus

Voor het opzetten van het ticketsysteem hebben we de software van ServiceDesk Plus gebruikt. Dit is een redelijk gemakkelijke oplossing dat zorgt voor een ticketsysteem met een uitgebreide interface en een live-chat systeem.

Het ticketsysteem van ServiceDesk Plus is een systeem dat niet open-source is, maar wel een gratis versie heeft. De gratis versie is verwoord als een 'trial' maar is eigenlijk blijvend gratis als je onder de 25 gebruikers blijft. Omdat we ons nu in een testomgeving bevinden, gaan we bij de gratis versie blijven. In de toekomst is het wel de bedoeling om uit te breiden.

ServiceDesk Plus biedt veel opties en is gratis, in tegenstelling tot andere servicedesk software. Het heeft ook een live-chat optie, dat heel handig kan zijn voor snel een antwoord te weten.

ManageEngine 
ServiceDesk Plus

8 SECURITY POLICY

8.1 Introductie

In deze policy wordt beschreven aan welke regels de werknemers / studenten zich dienen te houden. Zo sommen we een aantal regels op om ervoor te zorgen dat er onder andere geen malware, spyware of andere onveilige software kan worden geïnstalleerd.

8.1.1 Doelen

Het doel van dit beleid is onder andere om:

1. Uw bestanden veilig te houden;
2. Virussen, Malware en spyware te voorkomen;
3. Wachtwoorden veilig te houden.

8.1.2 Bereik

Deze policy is bedoeld voor iedereen die gebruik gaat maken van de server, dus in ons geval de studenten van 2 APP die hun project op onze server gaat hosten.

8.2 Beleid

8.2.1 Systeem toegangscontrole

8.2.2 Personeels / infrastructuur wachtwoorden

Team 6 heeft een verplichting om het intellectueel eigendom alsmede persoonlijke en financiële informatie die ons zijn toevertrouwd door de studenten en werknemers te beschermen. Door het gebruik van wachtwoorden die moeilijk te raden zijn, is een stap voorwaarts om deze verplichting te vervullen.

Elk wachtwoord die wordt gebruikt binnen de systemen die in het beheer zijn van Team 6 moeten ten minste 8 karakters lang zijn, bevat minstens 1 hoofdletter en 1 nummer of speciaal karakter.

Wachtwoorden vervallen elk jaar. Dit betekent dat alle wachtwoorden vervangen moeten worden die niet identiek zijn aan de voorgaande 3 wachtwoorden.

Wachtwoorden die ergens bewaard worden, mogen niet bewaard worden in een vorm dat onbevoegden deze kunnen lezen. Om het lezen te voorkomen, passen wij encryptie / hashes toe op de wachtwoorden, alvorens deze ergens bewaard worden

Wachtwoorden mogen nooit gedeeld worden met iemand anders buiten de bevoegde persoon.

Als er verdenking is dat een wachtwoord gelekt is, dient deze per direct veranderd te worden.

8.3 Malware

Alle gebruikers van Team 6 moeten goedgekeurde antivirussoftware gebruiken op hun computers. De software moet worden gebruikt om alle software / documenten te scannen, en moet worden gebeurd voordat het geopend wordt.

De gebruikers zijn verantwoordelijk als er schade ontstaat omdat er toch een virus op het systeem kon komen onder hun toezicht. Indien dit gebeurd moet men meteen de beheerder van Team 6 inschakelen zodat het zich niet verder kan verspreiden.

Er mag geen software geïnstalleerd worden welke van andere bronnen komen dan dat die zijn goedgekeurd door Team 6. Er kunnen uitzonderingen gemaakt worden mits de software uitvoerig wordt getest door Team6.

8.4 Data en programma back-up

Voor servers en communicatiesystemen is de systeem administrator verantwoordelijk voor het maken van periodische back-ups. In dit geval wordt dit verzorgd door Duplicati. Dit programma zal de back-ups voor zijn rekening nemen. Dat dit goed gebeurd is echter nog steeds de verantwoordelijkheid van de systeem administrator.

Om ervoor te zorgen dat kritische data is geback-upt, is het noodzakelijk dat deze op zowel servers staan in eigen beheer, alsmede een off-site back-up, welke verzorgd wordt door een vertrouwde partner.

8.5 Bitwarden passwords

Het programma Bitwarden slaat automatisch alle wachtwoorden op en als men gebruik wil maken van de betalende versie van Bitwarden verzekeren wij u dat we in geen enkel geval de wachtwoorden van de studenten mogen raadplegen. Uw wachtwoord is dus veilig in onze handen. Momenteel kan Bitwarden niet automatisch wachtwoorden invullen maar enkel wachtwoorden onthouden. Als u uw wachtwoord vergeten bent, dient men gewoon een nieuw wachtwoord in te stellen en dit wordt ook automatisch geüpdatet naar Bitwarden, hiervoor dient men dus geen contact met ons op te nemen.

8.6 SSH

Idealiter zou de computer beheerd kunnen worden van op afstand. Om dit ook op een veilige manier te kunnen doen, is encryptie noodzakelijk. We hebben ervoor gekozen om sowieso al SSH te gebruiken in plaats van Telnet. Dit verhoogt de beveiliging al grotendeels, om een nog veiligere manier van werken te kunnen aanbieden hebben we ook een sleutelpaar gegenereerd. Op deze manier zal een potentiële aanvaller zowel de public key moeten hebben, alsmede het wachtwoord.

Verder is de poort van SSH veranderd naar 2222, in plaats van de traditionele 22, dit maakt onze server minder vatbaar voor eventuele botnets die het

wachtwoord proberen te bruteforcen. Dit is echter maar een klein onderdeel van de beveiliging. Mocht een hacker toch onze server willen binnendringen, dan zou een simpele poortscan volstaan om de juiste poort te achterhalen.

8.7 Software updates

Om zoveel mogelijk beschermd te zijn tegen kwetsbaarheden, is het belangrijk dat de gebruikte software telkens wordt geüpdatet. Hiervoor hebben we een handige tool namelijk Watchtower. Deze zal dit voor zijn rekening nemen, en zal dit proces vrijwel geautomatiseerd worden. Op deze manier proberen we ook via deze invalshoek maximale beveiliging te bieden. De updates zullen eerst door de administrators worden geïnstalleerd om te kijken wat voor impact dit heeft op het systeem. Het is altijd mogelijk dat er een fout zit in de update, waardoor er een corrupt systeem kan ontstaan. Indien de updates zijn goedgekeurd door onze administrators, is het veilig om het uit te rollen naar de rest van het netwerk.

8.8 Network monitoring

Een netwerk monitoring tool is noodzakelijk voor elk netwerk. Hierbij is het mogelijk om bijvoorbeeld verdacht internetverkeer te identificeren, op deze manier is het mogelijk om snel te handelen en zo de eventuele hackers buiten te houden. Als er zich een probleem voordoet op het netwerk, zal Zabbix (onze keus op gebied van monitoring) automatisch een waarschuwing sturen naar de administrators. Dit kan zeer uiteenlopend zijn, van een server die misschien niet meer bereikbaar is, tot een nieuwe computer die op het netwerk geregistreerd wordt.

Tegelijkertijd kan een tool als deze ook ingezet worden om het netwerk performanter te maken. Men kan eenvoudig zien waar er bijvoorbeeld een vertraging is, waarbij er direct actie ondernomen kan worden.

9 PAGER ROTATION

Iedere dag gaat er op elk moment tussen 8u en 17u iemand van het team beschikbaar zijn voor eventuele problemen. Dit gaat van dag tot dag verschillen maar gaat grotendeels elke week hetzelfde zijn. De persoon die op het moment van een probleem de pager heeft, is ook verantwoordelijk voor de werking van het systeem en neemt die verantwoordelijkheid dan ook ten harte. De pager gaat in vorm van een telefoon ervoor zorgen dat het altijd beschikbaar is. Wanneer er iemand afwezig is op het moment dat hij de pager heeft (bv. ziekte, ongeval,..), laat deze persoon dit zo snel mogelijk weten zodat dit kan aangegeven worden binnen het team en de back-up persoon kan worden ingezet.

Het schema wordt elke week opnieuw uitgevoerd en wordt éénmaal per jaar aangepast.

Het huidig schema vindt u hieronder:

<u>Dag van de week</u>	<u>Maandag</u>	<u>Dinsdag</u>	<u>Woensdag</u>	<u>Donderdag</u>	<u>Vrijdag</u>
<u>Verantwoordelijke</u>	Wout Wynen	Joey Van Erum	Kobe Van Hasselt	Jesse Van Doninck	Barend Van Lith
<u>Back-up</u>	Joey Van Erum	Kobe Van Hasselt	Jesse Van Doninck	Barend van Lith	Wout Wynen

10 HANDLEIDINGEN

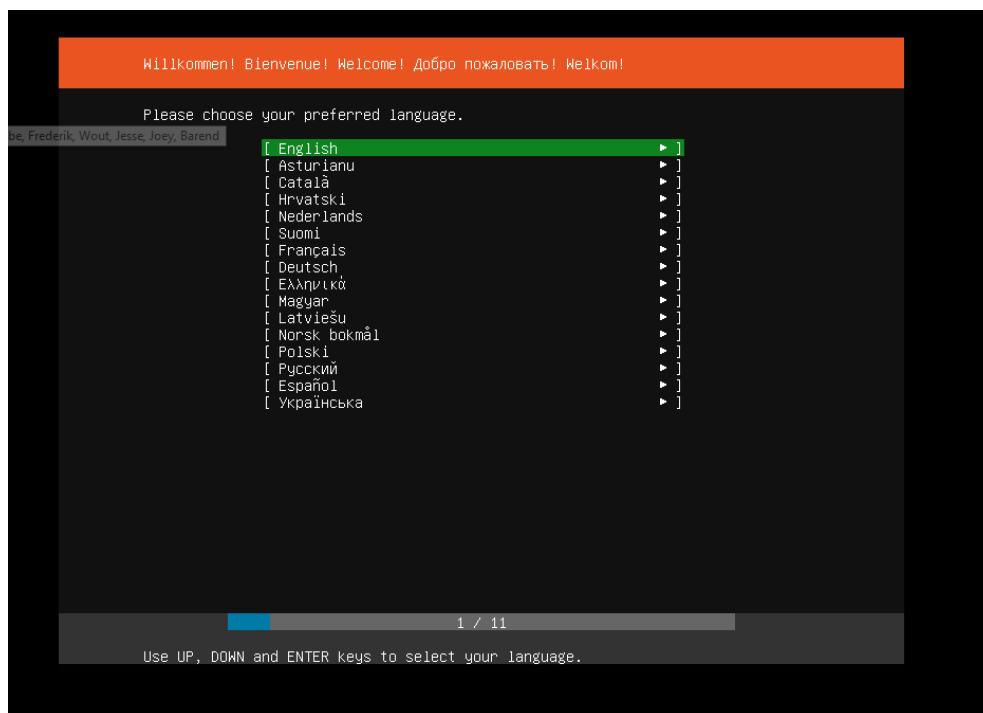
Tijdens dit hoofdstuk vind men de handleidingen van de verschillende applicaties die we gebruiken. Dit houdt concreet in dat de lezer een stappenplan ziet van de verschillende handelingen die we hebben moeten doen om een bepaalde applicatie draaiende te krijgen op ons systeem.

Normaliter als de lezer deze handelingen zelf uitvoert, zal deze hetzelfde resultaat bekomen als ons.

10.1 Installing Ubuntu 18.04 and VM's

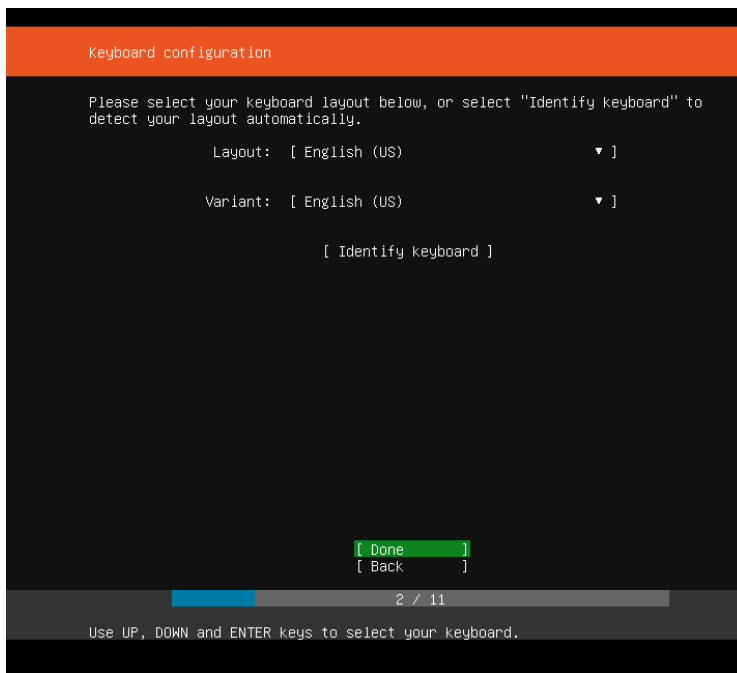
Als u uw machine opstart zal de VM eerst alles gaan configureren. Daarna zal u een paar dingen zelf moeten instellen, hierna een eerste stap die u dient te ondernemen.

Kies een taal waarin jij wilt werken. Ik kies hier zelf Engels



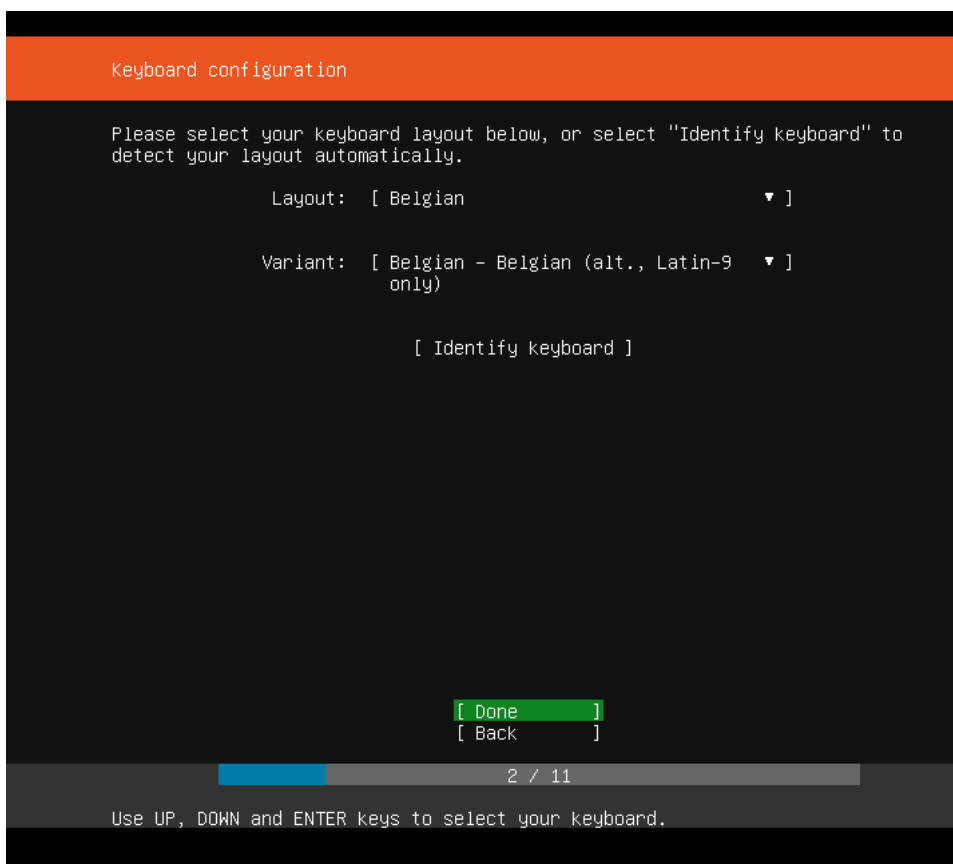
Afbeelding: kiezen van taal van besturingssysteem

1. Dan zal u uw keyboard layout moeten in geven. Als u een QWERTY toetsenbord heeft moet u het zo instellen als hieronder



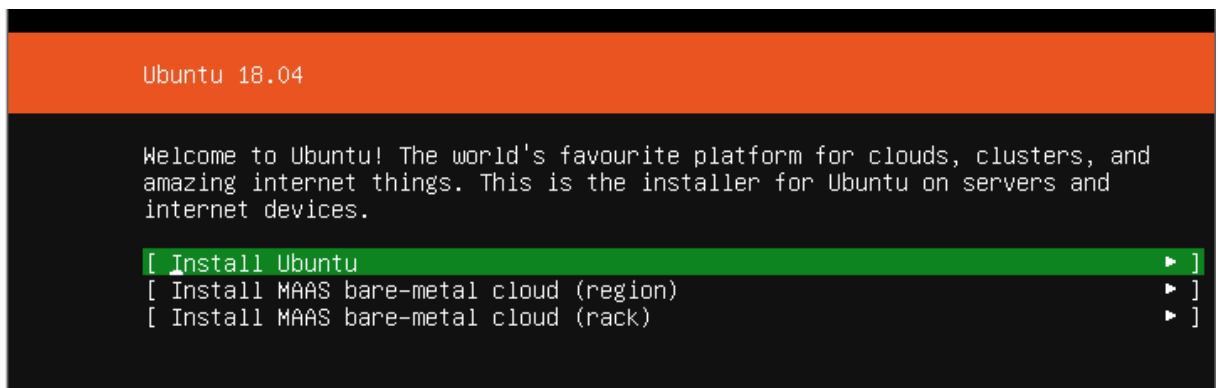
Afbeelding: Kiezen van toetsenbord layout

Als u een AZERTY toetsenbord heeft moet u het zo instellen.



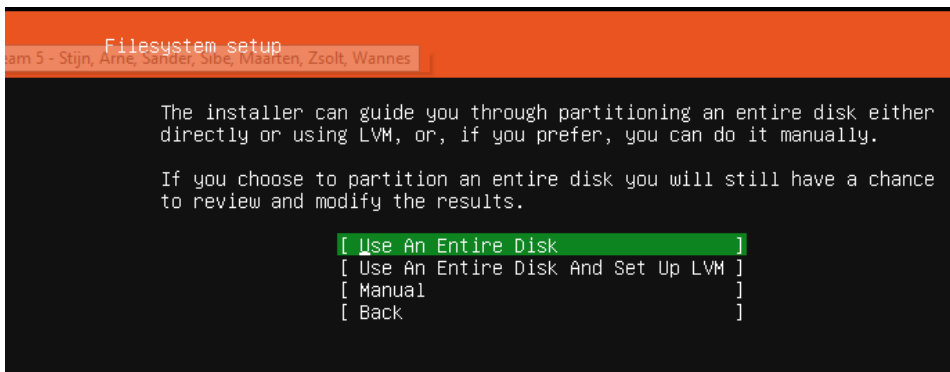
Afbeelding: selecteren van Belgisch toetsenbord

2. Kies hier voor "Install Ubuntu".



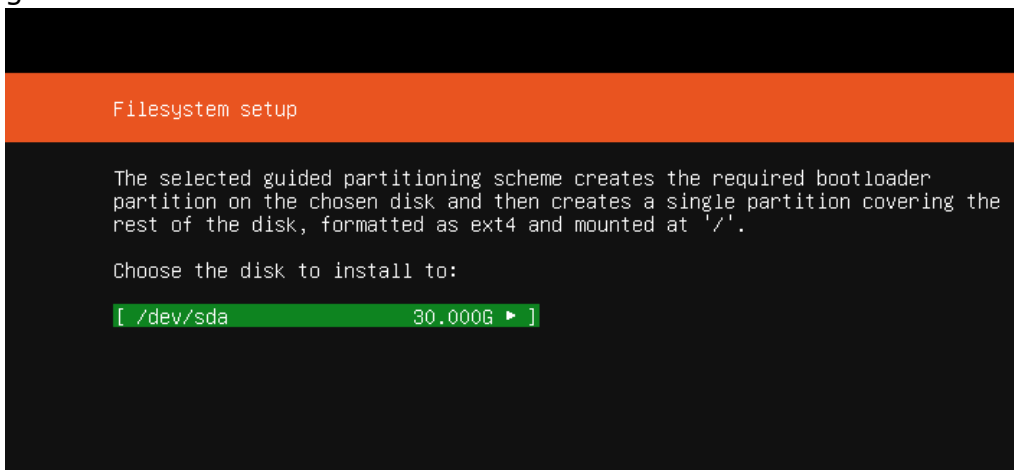
Afbeelding: kiezen van setup

3. Klik nu op 3 keer op "Done" tot dat je dit scherm ziet staan.



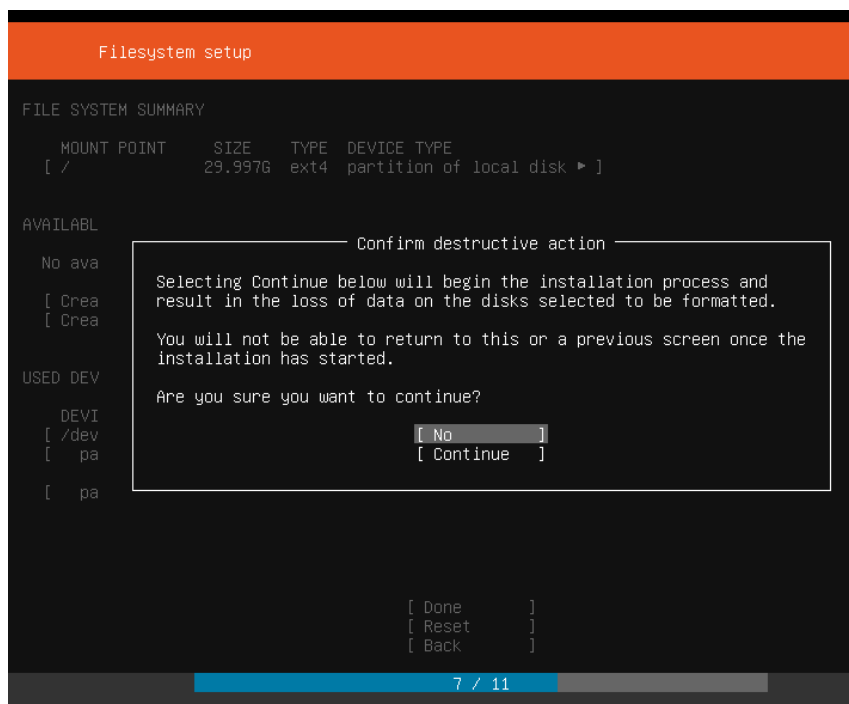
Afbeelding: kiezen van partities

4. Klik nu dan op "Use An Entire Disk"
5. Kies nu voor de disk die er staat. Als er meerdere staan kan je best de grootste nemen.



Afbeelding: selecteren van de harde schijf

6. Klik dan op "Done" en dan krijgt u een pop-up, kies hier voor "Continue"

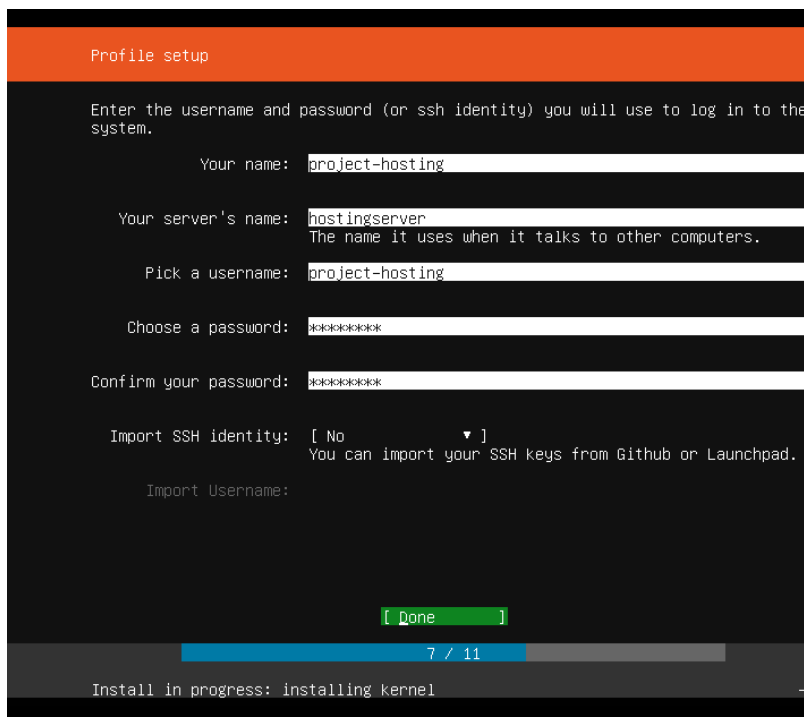


Afbeelding: bevestiging formatteren

Dan krijgt u een scherm waar dat u uw account en de naam van de server kan instellen.

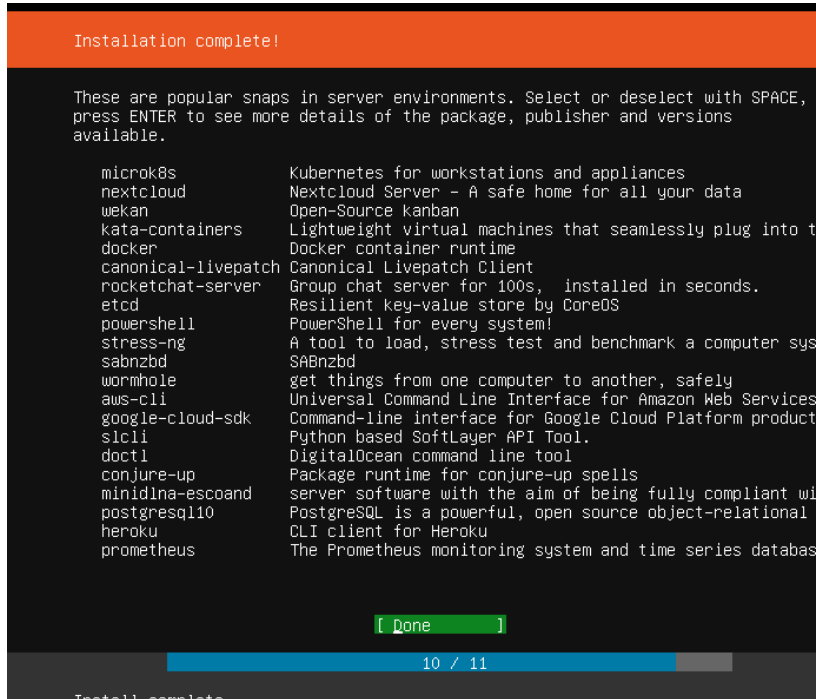
Zie dat al uw gegevens juist zijn en kies hier zeker een goed paswoord.

Als alles klaar is klik op "Done".



Afbeelding: instellen van (gebruikers)namen + wachtwoord

7. Scroll nu helemaal naar beneden en klik op "Done".



Afbeelding: eventueel nog extra packages installeren tijdens installatie

8. Op het einde klik dan op "Reboot Now"

10.1.1 Dingen die men moet doen op de machine zelf.

Als de machine is opgestart doet u best een update van al uw repository's.

Dit doet u met het commando: **sudo apt update** of **sudo apt-get update**

```
project-hosting@hostingserver:~$ sudo apt update
[sudo] password for project-hosting:
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease
Get:5 http://archive.ubuntu.com/ubuntu bionic/main Translation
```

Afbeelding: updaten van het systeem

10.1.2 Instellingen netwerk.

Om een statisch IP te krijgen in uw netwerkomgeving kan u de netwerkinstellingen gaan aanpassen. Dit doet u door het volgende commando in te geven.

```
project-hosting@hostingserver:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

Afbeelding: aanpassen van het bestand voor vast ip adres te krijgen

Als u dit commando ingeeft kan u het ip-adres van de verschillende netwerkkaarten gaan aanpassen.

Ik heb hier dit IP-adres gegeven omdat wij hier een range hadden van 172.27.66.160- 172.27.66.169

```
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    ens32:
      addresses: [172.27.66.161/24]
      gateway4: 172.27.66.254
      dhcp4: true
  version: 2
```

Afbeelding: het bestand om IP-adres aan te passen

10.2 Installatie Docker

1. Eerst zal je je apparaat moeten updaten dit doe je met de code:

- **Sudo apt-get update**

2. Indien nodig verwijder de oude docker versies door dit commando

- **Sudo apt-get remove docker-engine docker.io**

3. Nu gaan we docker installeren en dit doen we door het commando:

- **Sudo apt install docker.io**

10.3 Installatie docker-compose

Wij gebruiken een variant van docker, namelijk docker compose. Docker compose is een tool waarmee je via één file meerdere containers kan managen.

1. Download de docker compose binary in de "/usr/local/bin" map met het volgende commando:

```
sudo curl -L  
"https://github.com/docker/compose/releases/download/1.23.1/docker-  
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-  
compose
```

2. Eens deze download voltooid is verander je de rechten op de file met het volgende commando:

```
sudo chmod +x /usr/local/bin/docker-compose
```

3. Check of de installatie gelukt is met het volgende commando:

```
docker-compose --version
```

De output zo er ongeveer zo moeten uitzien:

```
docker-compose version 1.23.1, build b02f1306
```

10.4 Installatie van de docker-compose file

Dit houdt de installatie van onze docker-file in. Met deze docker-compose file heeft men een monitoring tool, een LAMP-stack, automatische update tool, een password safe, een database manager en een container manager.

Om de docker-file te installeren heeft men een Github link nodig en deze gaan we dan clonen. Dit doen we met het commando

- **Git clone <https://github.com/joeyve/project-hosting.git>**

```
root@joeyserver:~# git clone https://github.com/joeyve/project-hosting.git_
```

Afbeelding: het clonen van de GIT-repository

Dan gaan we in de map met het commando

- **cd project-hosting/**

```
root@joeyserver:~/project-hosting# _
```

Afbeelding: veranderen naar de map project-hosting

En om de docker-compose file nu te runnen geven we het volgende commando op

- **sudo docker-compose up**

- **sudo docker-compose up -d** (Dit is voor de compose file op de achtergrond te runnen)

```
root@joeyserver:~/project-hosting# sudo docker-compose up -d
```

Afbeelding: commando voor docker te starten

Wacht nu even tot dat de file helemaal is gedownload en geïnstalleerd, dit kan even duren.

10.5 ClamAV

Je kan ClamAV gratis downloaden omdat het een open-source programma is.

- Het installeren van de software: **apt-get install clamav clamav-freshclam**

```
kobe@ccs_server:~$ sudo apt-get install clamav
Pakketlijsten worden ingelezen... Klaar
Boom van vereisten wordt opgebouwd
De statusinformatie wordt gelezen... Klaar
clamav is reeds de nieuwste versie (0.100.3+dfsg-0ubuntu0.18.04.1).
De volgende pakketten zijn automatisch geïnstalleerd en zijn niet langer nodig:
  bridge-utils linux-headers-4.15.0-29 linux-headers-4.15.0-46
  linux-headers-4.15.0-46-generic linux-image-4.15.0-46-generic
  linux-modules-4.15.0-46-generic linux-modules-extra-4.15.0-46-generic
  ubuntu-fan
Gebruik 'sudo apt autoremove' om ze te verwijderen.
0 opgewaardeerd, 0 nieuw geïnstalleerd, 0 te verwijderen en 68 niet opgewaardeerd.
kobe@ccs_server:~$ sudo service clamav-freshclam start
```

- Het starten van de service: **service ClamAV-freshclam start**
- Virus definities worden elk uur gechecked. Je kan de configuratie aanpassen in de file **/etc/clamav/freshclam.conf**.

```
# Check for new database 24 times a day
Checks 24
```

- Je kan de hoeveelheid checks per dag aanpassen van 24 keer per dag naar:

```
# Check for new database 1 times a day
Checks 1
```

- Dit doen we nu niet omdat we 24 keer per dag een virusscan willen doen.

10.5.1 Script ClamAV

- We gaan nu een script invoeren voor het sturen van de virusdefinities naar onze pager. Als clamAV een verdacht programma heeft gevonden, gaat deze een simplepush bericht sturen met een waarschuwing. We doen dit op de volgende manier.
- We gaan eenmaal per dag een volledig scan van ons systeem maken. Om het uur gaan we een scan van onze /var/www map maken zodat alle php projecten worden gescanned.
- We maken het script aan: **sudo nano /root/clamscan_daily.sh**
- We plakken er de volgende code in:

```
#!/bin/bash
LOGFILE="/var/log/clamav/clamav-$(date +%Y-%m-%d').log";
DIRTOSCAN="/home";

for S in ${DIRTOSCAN}; do
    DIRSIZE=$(du -sh "$S" 2>/dev/null | cut -f1);

    echo "Starting a daily scan of "$S" directory.
    Amount of data to be scanned is "$DIRSIZE".";

    clamscan -ri "$S" >> "$LOGFILE";

    # get the value of "Infected lines"
    MALWARE=$(tail "$LOGFILE"|grep Infected|cut -d" " -f3);

    # if value is not equal to zero, a simplepush message will be sent to
    notify the user.
    if [ "$MALWARE" -ne "0" ];then
        # using simplepush

        sudo sh send-encrypted.sh -k "U4gT5v" -p "test123" -s "3fumfg9b" -t
        "Virus Alert!" -m "Opg$

    fi
done

exit 0
```

- We veranderen de rechten van het script zodat het altijd uitgevoerd kan worden.

```
chmod 0755 /root/clamscan_daily.sh
```

- We creëren een link zodat we het in de ClamAV directory het bestand zetten dat het dagelijks uitgevoerd kan worden.

In /root/clamscan_daily.sh /etc/cron.daily/clamscan_daily.

- Je kan het script testen met het commando: **sudo nano /root/clamscan_daily.sh**
- Als clamAV niks heeft gevonden, schrijft het een verslag in de logfile weg. Je kan dit bestand vinden op het pad **/var/log/clamav/**.

10.6 VSFTPD

We gebruiken VSFTPD om connectie te kunnen maken via winSCP zodat de studenten van 2APP hun php projecten op de server kunnen plaatsen. We hebben de users ook zo beveiligd zodat ze enkel in hun eigen map kunnen en dus ook niet in de mappen van andere studenten. Daarnaast gebruiken we het ook om connectie te maken met de back-up server via Duplicati.

10.6.1 Installatie VSFTPD

- Sudo apt-get update
- Sudo apt-get install vsftpd

Aanpassen van het configuratie bestand "/etc/vsftpd.conf"

```
GNU nano 2.9.3 vsftpd.conf
#
# You may fully customise the login banner string:
ftpd_banner=Welkom bij de FTP server van team6.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
allow_writeable_chroot=YES
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
```

Afbeelding: Screenshot van de vsftpd configuratiefile.

In de configuratie file staat een commando waardoor de map "/var/www/" de home map word van de gebruiker. Hierdoor word de gebruiker ook automatisch gechroot en de studenten hebben write rechten in deze map maar kunnen dus niet aan andere mappen.

10.7 Zabbix-agent installatie.

Bij een Zabbix-server moet er ook een Zabbix-agent gedownload worden, dit is nodig want via de Zabbix agent wordt alle data gehaald.

Hieronder vindt u wat uw moet doen om een Zabbix-agent te installeren.

1. Voeg als eerst de repositories toe. Dit doe je door het onderstaande commando's in te voeren.

- **wget**
http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.4-1+bionic_all.deb
- **sudo dpkg -i zabbix-release_3.4-1+bionic_all.deb**

2. Nu kan men de Zabbix-agent gaan installeren. Dit doet men door onderstaan commando te geven.

- **sudo apt-get install zabbix-agent**

3. Nu gaan we dit via een Zabbix-agent configureren. Editeer het volgende bestand met vim of sudo nano. Ik gebruik zelf nano.

Ga naar **sudo nano /etc/zabbix/zabbix_agentd.conf** verander het volgende. Zet het ip adres van de server hieronder.

```
# cat /etc/zabbix/zabbix_agentd.conf
# On line 97 - Specify Zabbix server IP Address
Server=192.168.10.2
# On line 138 - Specify Zabbix server ( For active
ServerActive=192.168.10.2
# Set server hostname reported by Zabbix agent
```

Afbeelding: Aanpassingen in de zabbix_agentd.conf

- Restart nu de zabbix-agent na dat je het hebt aangepast.

```
$ sudo systemctl restart zabbix-agent  
$ sudo systemctl status zabbix-agent
```

Afbeelding: Service restart Zabbix-agent

- Al je ufw hebt opstaan, vergeet dan niet poort 10050 en 10051 toe te staan door de firewall.

Dit doet u zo.

```
$ sudo ufw allow 10050/tcp
```

Afbeelding: Allow TCP-port 10050 in Firewall

- Nu moeten we een host gaan toevoegen aan de Zabbix-server. Als eerst moeten we inloggen in de zabbix interface, dit doen we door naar de browser te gaan en dan `http:jouwlocalhostaddress:8080` te gaan.

Hier log je in met username: Admin en wachtwoord: zabbix

Niet beveiligd | 172.27.66.161:8080/index.php?reconnect=1&form=default

ZABBIX

Username
Admin

Password
.....

☒ Remember me for 30 days

Sign in

or sign in as guest

[Help](#) • [Support](#)

Afbeelding: GUI Zabbix

Als je bent ingelogd ga dan naar de configuration tab dan naar Hosts en dan naar create host

7. Nu moet men de host ofwel de agent gaan instellen.

8. Als eerst configureer je de host.

Hosts

All hosts / project hosting agent Enabled ZBX SNMP JMX IPMI Applications 10 Items 63 Triggers 17 Graphs 19 Discovery rules 2 Web scenarios

Host Templates IPMI Macros Host inventory Encryption

* Host name project hosting agent

Visible name project hosting agent

* Groups Linux servers Virtual machines type here to search Select

* At least one interface must exist.

Agent interfaces

IP address	DNS name	Connect to	Port	Default
192.168.56.11		IP DNS	10050	<input checked="" type="radio"/> Remove
127.0.0.1		IP DNS	10050	<input type="radio"/> Remove

Add

SNMP interfaces Add

JMX interfaces Add

IPMI interfaces Add

Description

Monitored by proxy (no proxy)

Enabled ☒

Update Clone Full clone Delete Cancel

- Host name of the server to be monitored
- Visible name for the server to be monitored.
- Select the group or add a new group for "Groups" field.
- IP address
- Zabbix agent service port -default is 10050 of 10051

Hosts

All hosts / project hosting agent Enabled ZBX SNMP JMX IPMI Applications 10 Items 63 Triggers 17 Graphs 19 Discovery rules 2 Web scenarios

Host Templates IPMI Macros Host inventory Encryption

Linked templates

Link new templates

Group Templates

☐ Name

☒ Template App Apache Tomcat JMX

☒ Template App FTP Service

☐ Template App Generic Java JMX

☒ Template App HTTP Service

☐ Template App HTTPS Service

☒ Template App IMAP Service

☒ Template App LDAP Service

☐ Template App NNTP Service

☐ Template App NTP Service

☐ Template App POP Service

☐ Template App SMTP Service

☒ Template App SSH Service

☒ Template App Telnet Service

☐ Template App Zabbix Agent

☐ Template App Zabbix Proxy

☐ Template App Zabbix Server

☐ Template DB MySQL

☐ Template Module Brocade_Foundry Performance SNMPv2

☐ Template Module Cisco CISCO-ENVMON-MIB SNMPv2

☐ Template Module Cisco CISCO-MEMORY-POOL-MIB SNMPv2

☐ Template Module Cisco CISCO-PROCESS-MIB IOS versions 12.0_3_T-12.2_3.5 SNMPv2

☐ Template Module Cisco CISCO-PROCESS-MIB SNMPv2

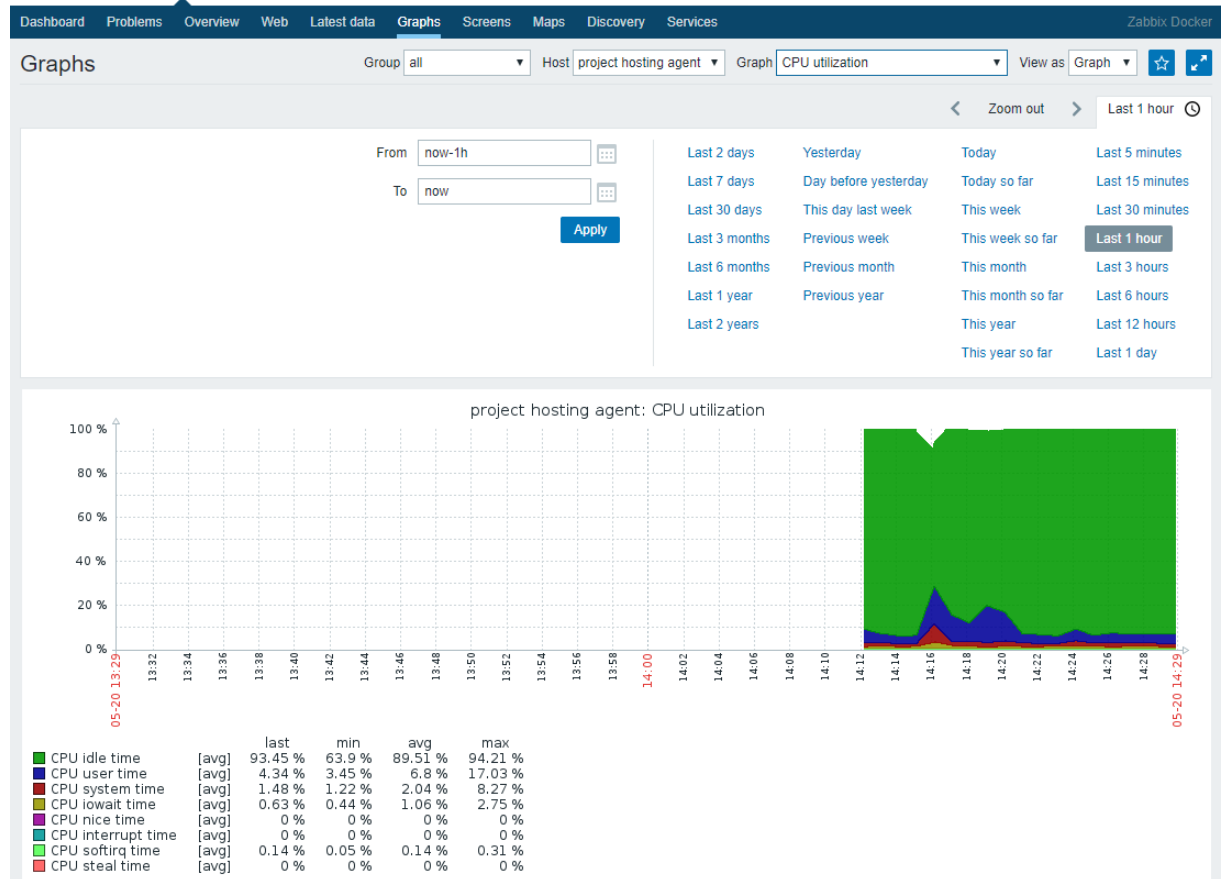
Ga dan naar het tabblad Sjablonen. Klik op de knop Selecteren en Nieuwe sjablonen koppelen. Selecteer de sjablonen die u wilt gebruiken.

Nadat u de sjablonen hebt geselecteerd, klikt u op de link Koppelingen toevoegen om sjablonen aan uw doelsysteem te koppelen.

Werk de instelling bij met de knop **Update** . Na enkele minuten worden meetgegevens verzameld en kunt u ze visualiseren met behulp van Zabbix-grafieken. Standaard hostgrafieken zijn toegankelijk op

Monitoring> Grafieken> <Host | Grafiek>

Hieronder staat de CPU-grafiek voor de host die we eerder hebben toegevoegd.



10.8 VERANDEREN VAN PASSWOORDEN BINNEN HET UUR

In deze handleiding kan je alle instructies terugvinden om gemakkelijk alle passwoorden te veranderen. De passwoorden die we gaan bespreken zijn: het Ubuntu root passwoord, het Portainer passwoord, het Bitwarden passwoord, het Duplicati passwoord, het MySQL passwoord en het PHPmyAdmin passwoord.

10.8.1 Ubuntu root

Eerst log je in met het root wachtwoord.

- `sudo -i`

Dan typ je het commando "passwd" in.

- `passwd`

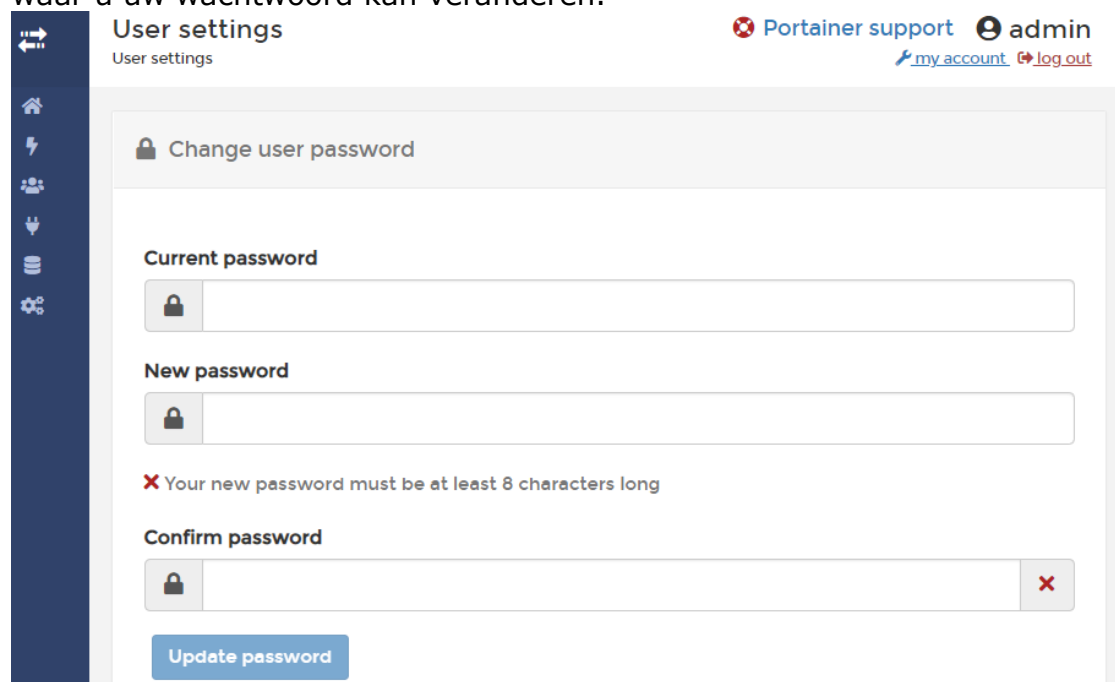
Bij het invoeren van het commando "passwd" word je gevraagd om een nieuw passwoord te kiezen.

```
root@linux:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@linux:~#
```

Afbeelding: invoeren van nieuw wachtwoord voor de root gebruiker

10.8.2 Portainer

Als u bij Portainer (poort 8002) klikt op "my account" krijgt u volgend scherm waar u uw wachtwoord kan veranderen.



The screenshot shows the 'User settings' page in Portainer. At the top right, there are links for 'Portainer support', 'admin', 'my account', and 'log out'. The main section is titled 'Change user password' and contains three password input fields: 'Current password', 'New password', and 'Confirm password'. Each field has a lock icon on the left. Below the 'New password' field, there is a red error message: 'X Your new password must be at least 8 characters long'. At the bottom of the form is a blue button labeled 'Update password'.

Afbeelding: nieuw wachtwoord ingeven voor Portainer

10.8.3 Bitwarden

Als u bij Bitwarden (poort 8004) naar instellingen gaat kan u onder de rubriek “Hoofdwachtwoord wijzigen” uw wachtwoord aanpassen.

Hoofdwachtwoord wijzigen

⚠ WAARSCHUWING

Doorgaan zal uw huidige sessie afmelden, waarna het nodig is terug aan te melden. Actieve sessies op andere apparaten kunnen mogelijks tot één uur actief blijven.

Huidig hoofdwachtwoord

••••••••

Nieuw hoofdwachtwoord

Bevestig nieuw Hoofdwachtwoord

☐ De versleuteling van mijn account ook draaien ?

Hoofdwachtwoord wijzigen

Afbeelding: nieuw wachtwoord invoeren voor Bitwarden

10.8.4 Duplicati

1. veranderen van het toegangswachtwoord

Door bij Duplicati (poort 8200) naar instellingen te gaan kan u het wachtwoord van de gebruikersinterface veranderen.

Instellingen

Toegang tot gebruikersinterface

☐ Wachtwoord

☒ Remote toegang toestaan (herstart vereist)

Afbeelding: toegang tot gebruikersinterface instellen van Duplicati

2. Veranderen van het wachtwoord van een back-up

Eerst klikt u op de back-up waarvan u het wachtwoord wenst te veranderen. Vervolgens klikt u bij configuratie op “bewerken ...”. Hier kan je een nieuw wachtwoord instellen.

Algemene back-upinstellingen

Naam	<input type="text" value="volledigebakup"/>
Versleuteling	<input type="text" value="AES-256 encryption, built in"/>
Wachtwoordzin	<input type="password" value="....."/>
Herhaal wachtwoordzin	<input type="password" value="....."/>

[Tonen](#) | [Genereer](#) | [Strength: Zwak](#)

Afbeelding: wachtwoorden voor backups aanpassen

10.8.5 MySQL & PHPmyAdmin

Als u in de map "docker-lamp" het bestand "docker-compose.yml" opent kan u in de .yml file de wachtwoorden van MySQL en PHPmyAdmin simpelweg aanpassen.

```
command: --default-authentication-plugin=mysql_native_password
environment:
  MYSQL_DATABASE: myDb
  MYSQL_USER: user
  MYSQL_PASSWORD: test
  MYSQL_ROOT_PASSWORD: test
volumes:
  - ./dump:/docker-entrypoint-initdb.d
  - ./conf:/etc/mysql/conf.d
  - persistent:/var/lib/mysql
networks:
  - default
phpmyadmin:
  image: phpmyadmin/phpmyadmin
  links:
    - db:db
  ports:
    - 8000:80
  environment:
    MYSQL_USER: user
    MYSQL_PASSWORD: test
    MYSQL_ROOT_PASSWORD: test
```

Afbeelding: aanpassen van wachtwoord voor MySQL

10.9 Service desk plus

Als ticketsysteem gebruiken we service desk plus. Het is een programma dat zichzelf uitwijst en een gemakkelijke grafische interface heeft. Je kan bij elk ticket een priority en een reden meegeven. Er is ook een chat voorzien dat zorgt voor de interactie tussen de 'technician' en de 'client'.

10.9.1 Installatie

De installatie van de Servicedesk Plus bestaat uit een aantal onderdelen. Het eerste deel van de configuratie is op de commandprompt, het tweede deel van de configuratie is op de grafische interface van het programma zelf.

- Het downloaden van de software in zip file:
Hiermee download je het 64 bit bestand dat bestemt is voor Linux.
- Het veranderen van de rechten van het bestand doe je zo:
chmod +xManageEngine_ServiceDesk_Plus_MSP_64bit.bin
- Nu kan je het bestand uitvoeren, dit doe je met het ./ commando.
Sudo ./xManageEngine_ServiceDesk_Plus_MSP_64bit.bin
- Het bestand wordt nog niet uitgevoerd omdat we op een Linux werken zonder GUI, om dit te omzeilen schrijf je het vorig commando met -
console erachter.

project-hosting@host1:~\$ server: ~/Ticket-systeem

This License Agreement details the policy for license of ManageEngine ServiceDesk Plus ("Licensed Software") on the following topics:

- * Evaluation License
- * Commercial License
- * Technical Support

Please read the following license carefully, before either (i) completing the electronic order or download of the Licensed Software from an authorised website, or (ii) installing the Licensed Software from media that was delivered after being ordered by alternative order process, as applicable. You acknowledge that you have read this License Agreement, have understood it, and agree to be bound by its terms. If you do not agree to the terms and conditions of this Agreement, either (i) exit the web site page without continuing the ordering process, or (ii) return the provided unused media and documentation within thirty (30) days from the date of shipment of the Licensed Software for a full refund of your payment, as applicable.

THE following terms constitute a binding agreement between you and Zoho with

PRESS <ENTER> TO CONTINUE: █

De tutorial gaan we verder maken aan de hand van cijfers. Typ 1 en ga verder met de tutorial.

De rechten en licensies worden aangehaald, druk op enter om verder te gaan.

13. GENERAL:

If you are a resident of the United States or Canada, this Agreement shall be governed by and interpreted in all respects by the laws of the State of California, without reference to conflict of laws' principles, as such laws are applied to agreements entered into and to be performed entirely within California between California residents. If you are a resident of any other country, this Agreement shall be governed by and interpreted in all respects by the laws of the Republic of India without reference to conflict of laws' principles, as such laws are applied to agreements entered into and to be

PRESS <ENTER> TO CONTINUE:

performed entirely within the Republic of India between residents of the Republic of India. If you are a resident of the United States or Canada, you agree to submit to the personal jurisdiction of the courts in the Northern District of California. If you are a resident of any other country, you agree to submit to the personal jurisdiction of the courts in Chennai, India. This Agreement constitutes the entire agreement between the parties, and supersedes all prior communications, understandings or agreements between the parties. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this Agreement is found invalid or unenforceable, the remainder shall be interpreted so as to reasonable effect the intention of the parties. You shall not export the Licensed Software or your application containing the Licensed Software except in compliance with United States export regulations and applicable laws and regulations.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): █

```

Choose Edition
-----

Choose Service Desk Plus Edition ..

->1- Enterprise Edition
   2- Standard Edition
   3- Professional Edition

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
PRESS <ENTER> TO ACCEPT THE DEFAULT: 2

=====

Standard Edition Panel
-----

->1- Trial Edition
   2- Free Edition

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
PRESS <ENTER> TO ACCEPT THE DEFAULT: 2

=====

Registration Technical Support
-----

Name: 

```

Nu komen we aan het echte installeren. We moeten een versie kiezen dat we gaan gebruiken. We kiezen momenteel voor de Standard Edition, omdat we in een niet commerciële omgeving zitten.

- We kiezen voor de Free Edition.
- Bij de naam geven we Team 6.
- Bij de telefoon geven we de pager in van ons team.

Registration Technical Support

Name: 2

Phone: 1

E-Mail Id: r0687075@student.thomasmore.be

Country: BE

Company Name: TM

Choose options

By Selecting 'Next', you agree to our privacy policy in below url

<https://www.manageengine.com/privacy.html>

->1- Next

2- Skip

3- Cancel

4- Back

Select option to continue: 1

We gaan verder.

- We moeten nu een pad meegeven, we gaan hiervoor het pad /home/project-hosting/Ticket-systeem gebruiken.

```

=====
Choose Install Folder
-----

Where would you like to install?

  Default Installation Folder: /root/ManageEngine/ServiceDesk

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: /home/project-hosting/Ticket-systeemENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO
T THE DEFAULT

INSTALL FOLDER IS: /home/project-hosting/Ticket-systeemENTER AN ABSOLUTE
PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
IS THIS CORRECT? (Y/N): n

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: /home/project-hosting/Ticket-systeem/

INSTALL FOLDER IS: /home/project-hosting/Ticket-systeem
IS THIS CORRECT? (Y/N): Y

=====

=====

Choose port
-----
Enter requested information

Enter WebServer Port (Default: 8080): 8008

```

Als poort gebruiken we 8008 omdat er ook andere systemen zijn die andere poorten gebruiken. Default is dit de 8080 poort maar deze is al in gebruik door onze Zabbix.

```

=====
Choose port
-----

Enter requested information

Enter WebServer Port (Default: 8080): 8008

=====

DB Info
-----

POSTGRESQL(Default)

NOTE: Other databases like MSSQL can be configured after installing the
application by executing the <Installation
Folder>/ServiceDesk/bin/changeDBServer.sh file.

PRESS <ENTER> TO CONTINUE: █

```

De database veranderen we naar MYSQL nadat we de installatie hebben gedaan:

- We drukken nogmaals op Enter om ver te gaan en de folder te controleren.

```

=====
Ready To Install
-----

InstallAnywhere is now ready to install ServiceDesk onto your system at the
following location:

    /home/project-hosting/Ticket-systeem/ServiceDesk

PRESS <ENTER> TO INSTALL:

=====

Installing...
-----

[=====|=====|=====|=====]
[-----|-----|-----|-----]

=====

Pgsql Err Msg
-----

Problem in Initializing Postgres !!! Kindly check logs...

PRESS <ENTER> TO AGREE THE FOLLOWING (OK):

```

- Nu installeert het programma zich.
- Om de poort aan te passen, gebruiken we het bestand changeWebServerPort.sh. Dit is momenteel niet nodig

- We starten het programma door naar de /bin map te gaan van de servicedesk map, en hier **sudo sh run.sh** uit te voeren.
- De service start nu op en geeft de poort waarop de grafische interface draait.
- We kunnen nu beginnen met het configureren van de grafische interface.

10.10 OpenSSH Server

We gebruiken OpenSSH voor een connectie met de server. Dit is een veilige software die zorgt voor een geëncrypteerde verbinding. Hier volgt een korte handleiding die zorgt voor een installatie van OpenSSH op de server.

10.10.1 Installatie

```
$ sudo apt update
$ sudo apt install openssh-server
```

Installatie van openSSH-server:

Met het commando "sudo systemctl status ssh" kunnen we de status van openSSH controleren.

In de het bestand "sshd_config" in de mappenstructuur "/etc/ssh" hebben we de instellingen van de poort en de verdere configuratie geconfigureerd. We hebben er voor gekozen om poort 2222 te gebruiken omdat de standaard poort 22 niet veilig is.

```
GNU nano 2.9.3 sshd_config

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none
```

Herstarten van de SSH service kan met "sudo systemctl restart ssh.service".

10.11 Volledig functionaliteitsverloop

Stap 1: user aanmaken

De admin moet de user aanmaken. Dit doet hij door via ssh in te loggen op de server en het bijhorende script te gebruiken. Er zijn 2 opties: scriptUser of scriptCsv.

Scriptuser

Dit script gebruikt men als men een enkele user wilt toevoegen. Men opent het script met de volgende code:

Sudo bash /home/project-hosting/project-hosting/scriptUser

Er wordt vervolgens een usernaam gevraagd:

```
[sudo] password for project-hosting:  
Geef de username : █
```

Daarna een paswoord:

Als de user al bestaat meldt het script dit en gebeurt er niets. Als deze niet bestaat dan zal het script zeggen dat de user is toegevoegd en vervolgens alles gereed maken voor de user: de www map, ftp toegang, e.d.

```
[sudo] password for project-hosting:  
Geef de username : Barend  
Geef het paswoord : User is toegevoegd  
project-hosting@hostingserver:~/project-hosting$ █
```

ScriptCSV

Om users in grote hoeveelheden aan te maken hebben we een script geschreven dat gelijkaardig loopt als het vorige. Het enige verschil is er dat in plaats van de usernaam, wordt er gevraagd achter het pad naar de csv file. Deze csv file moet volgende opbouw hebben:

Naam,wachtwoord

Ook dit script wordt gestart met de volgende code:

Sudo bash /home/project-hosting/project-hosting/scriptCsv

```

project-hosting@hostingserver:~/project-hosting$ sudo bash scriptCsv
Geef het pad naar de CSV filecsv.csv
scriptCsv: line 8: [0: command not found
useradd: user 'naam' already exists
User naam toevoegen mislukt
mkdir: cannot create directory '/home/project-hosting/project-hosting/www/naam': File exists
usermod: no changes
scriptCsv: line 8: [0: command not found
useradd: user 'gunter' already exists
User gunter toevoegen mislukt
mkdir: cannot create directory '/home/project-hosting/project-hosting/www/gunter': File exists
usermod: no changes
scriptCsv: line 8: [0: command not found
useradd: user 'louis' already exists
User louis toevoegen mislukt
mkdir: cannot create directory '/home/project-hosting/project-hosting/www/louis': File exists
usermod: no changes
scriptCsv: line 8: [1: command not found
User 'ronny' is toegevoegd
project-hosting@hostingserver:~/project-hosting$ █

```

(de foutmeldingen die u ziet gebeuren er als de user al bestaat)

Stap 2: Docker runnen

Je kan docker runnen door het uitvoeren van volgende code:

Cd /home/project-hosting/project-hosting

Sudo docker-compose up -d

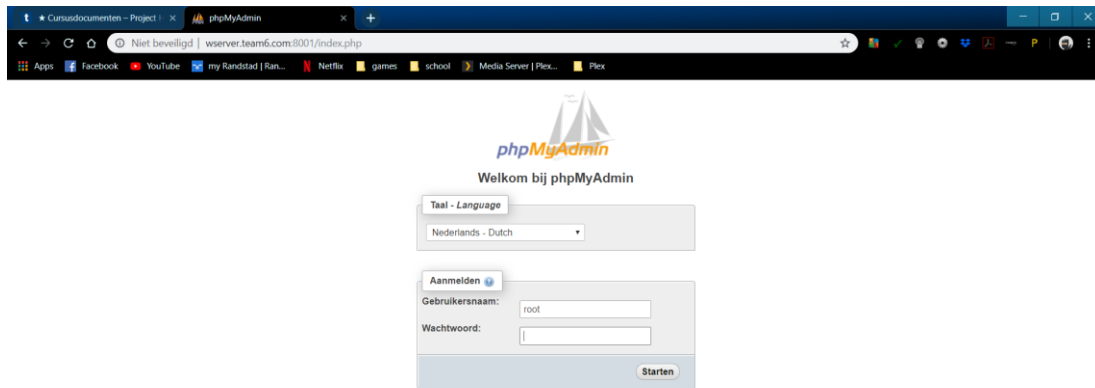
```

project-hosting@hostingserver:~$ cd /home/project-hosting/project-hosting/
project-hosting@hostingserver:~/project-hosting$ sudo docker-compose up -d
Starting project-hosting_dbzabbix_1_13a122ebc749 ... done
Starting project-hosting_db_1_1e9cd2cc7a62 ... done
Starting watchtower-compose ... done
Starting project-hosting_portainer_1_47c983fd91a2 ... done
Starting project-hosting_bitwarden_1_c5c5b59138d8 ... done
Starting project-hosting_server_1_1fab4b4efa2 ... done
Starting project-hosting_frontend_1_cab3fc393f42 ... done
Starting project-hosting_phpmyadmin_1_c832d36ee5b5 ... done
Starting project-hosting_www_1_6d7dac0f040a ... done
project-hosting@hostingserver:~/project-hosting$ █

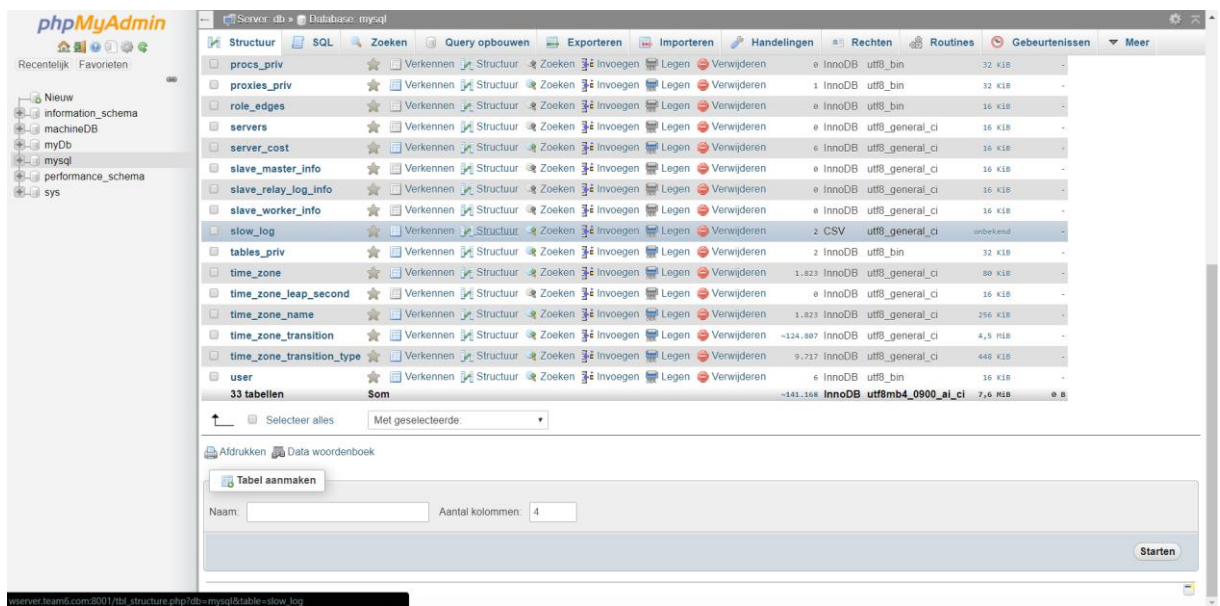
```

Stap 3: Gebruikers aanmaken in PHPMyAdmin

Om gebruikers aan te maken in PHPMyadmin moet de admin deze semi-handmatig aanmaken in de browser. De admin surft naar het volgende webadres: <http://wserver.team6.com:8001> en logt hier in met de root.



Eens deze ingelogd is kiest hij links in het vester voor SQL en vervolgens de userdatabase die onderaan staat.



Vervolgens kiest men bovenaan voor importeren

Server: db » Database: mysql » Tabel: user "Users and global privileges"

Verkennen Structuur SQL Zoeken Invoegen Exporteren Importeren Rechten Handelingen Triggers

✓ Weergave van records 0 - 5 (6 totaal, Query duurde 0.0012 seconden)

SELECT * FROM 'user'

Profiling [Online bewerken] [Wijzig] [Verklaar SQL] [Genereer PHP-code] [Ververs]

Toon alles Aantal rijen: 25 Filter rijen: Zoek in deze tabel Sorteren op sleutel: Geen

Opties

	Host	User	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reload_priv	Shutdown_priv	Process_priv
Wijzig Kopieren Verwijderen	%	root	Y	Y	Y	Y	Y	Y	Y	Y	Y
Wijzig Kopieren Verwijderen	%	user	N	N	N	N	N	N	N	N	N
Wijzig Kopieren Verwijderen	localhost	mysql.infoschema	Y	N	N	N	N	N	N	N	N
Wijzig Kopieren Verwijderen	localhost	mysql.session	N	N	N	N	N	N	N	N	N
Wijzig Kopieren Verwijderen	localhost	mysql.sys	N	N	N	N	N	N	N	N	N
Wijzig Kopieren Verwijderen	localhost	root	Y	Y	Y	Y	Y	Y	Y	Y	Y

Selecteer alles Met geselecteerde: Wijzig Kopieren Verwijderen Exporteren

Toon alles Aantal rijen: 25 Filter rijen: Zoek in deze tabel Sorteren op sleutel: Geen

Handelingen voor queryresultaat

Afdrukken Kopieer naar klembord Exporteren Grafiek weergeven VIEW aanmaken

Console

Men gebruikt het lokaal opgeslagen powershell script en de bijhorende bestanden om de gebruikers in te lezen via een CSV file en een sql entry te maken. Deze gaat Users.sql heten en wordt lokaal opgeslagen.

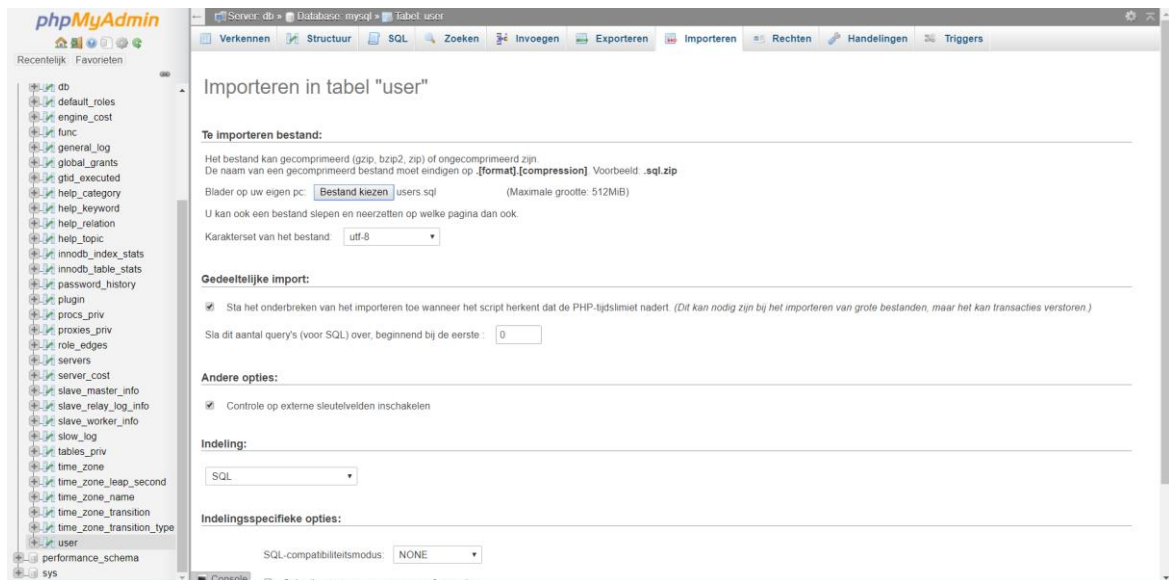
```
PS C:\WINDOWS\system32> E:\school\jaar 2\Semester 2\Project hosting\script users\script.ps1

Directory: C:\

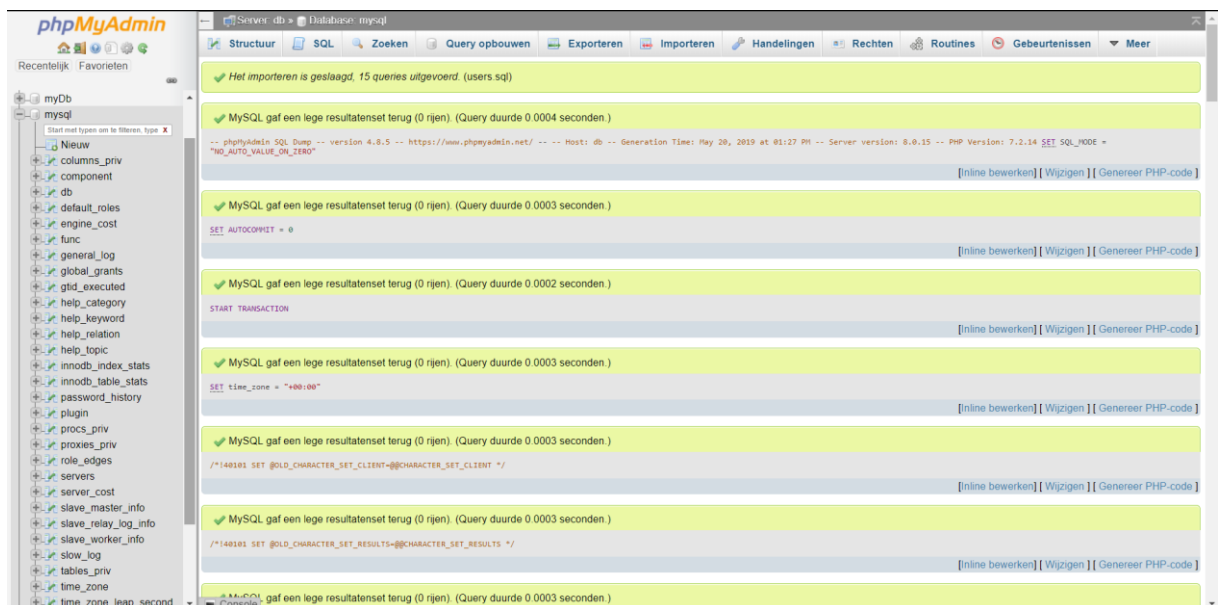
Mode                LastWriteTime         Length Name
----                -
-a----           23/05/2019   13:41             0 users.sql
Geef hier het pad naar het CSV bestand:: E:\csv.csv

PS C:\WINDOWS\system32>
```

Vervolgens voegt de admin de users toe door eerst de database users te verwijderen en daarna het nieuwe SQL bestand te importeren.



En als dit gelukt is krijgt men volgend scherm:



Om alle veranderingen door te voeren herstart je vervolgens de docker via de volgende commando's:

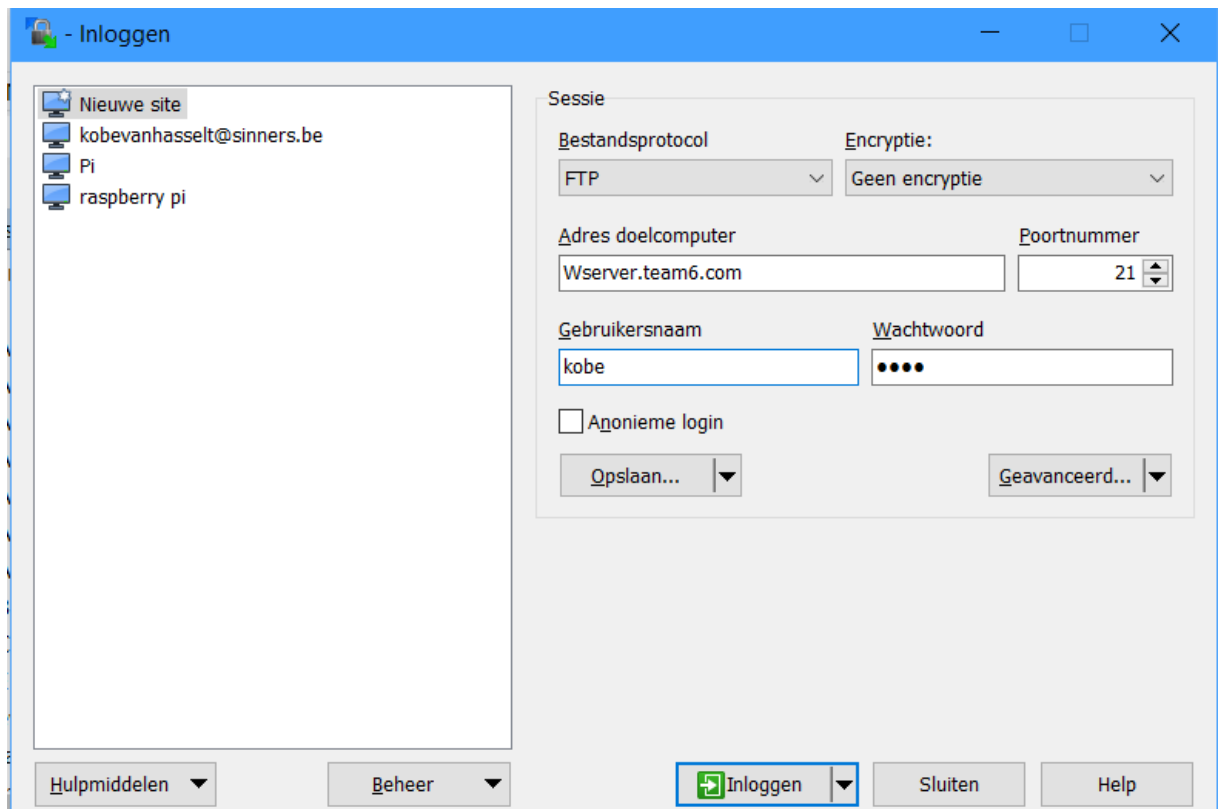
Cd /home/project-hosting/project-hosting

Sudo docker-compose down

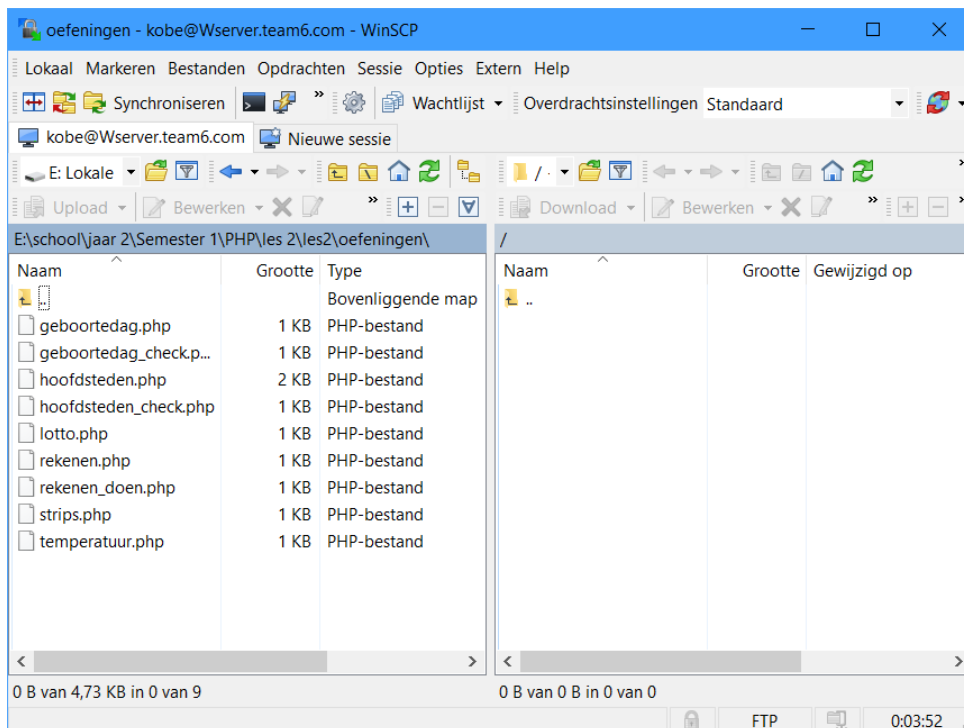
Sudo docker-compose up -d

Stap 4: Projecten uploaden via FTP

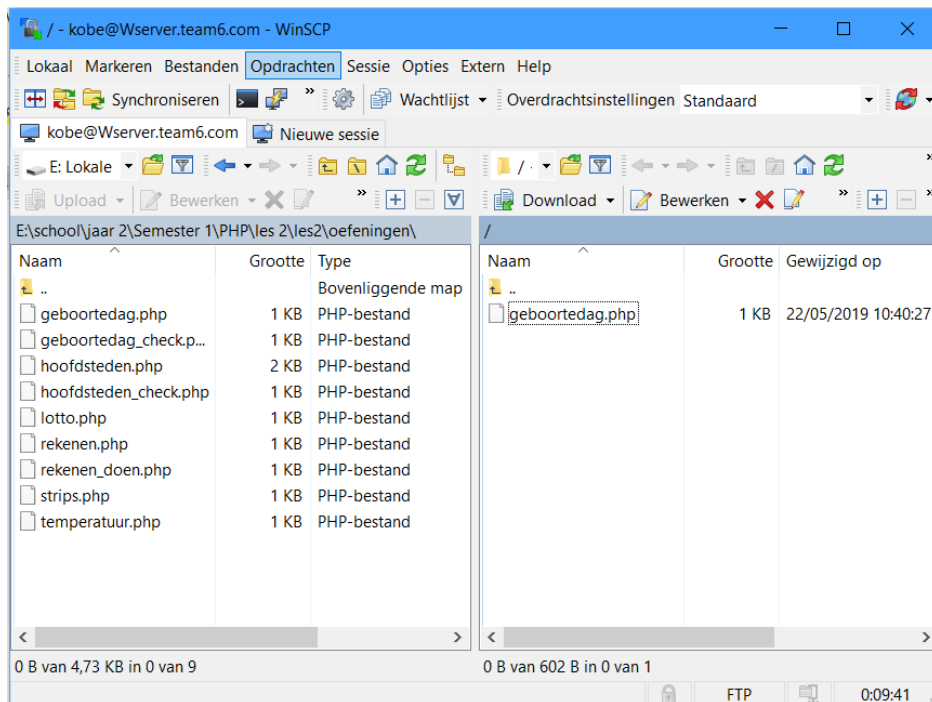
Om projecten te uploaden kan de user gebruik maken van FTP. Het programma dat we gebruiken hiervoor is WinSCP. Een gratis tool van Microsoft. Hierop kan de user inloggen en bestanden in zijn eigen map uploaden.



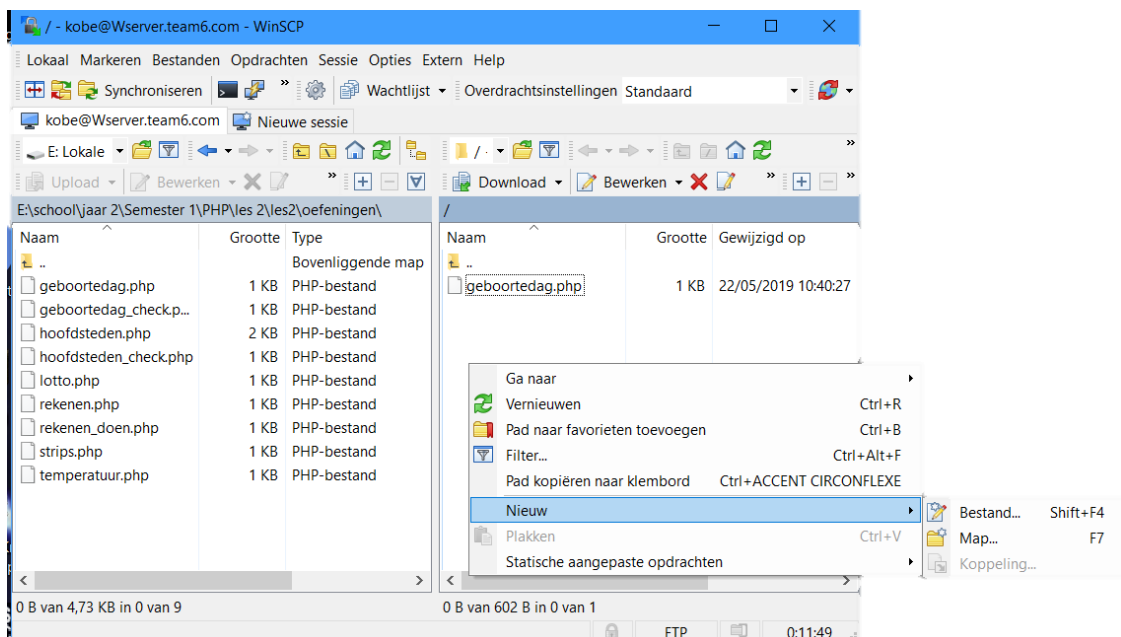
Als de login correct is krijg je het volgende scherm, hier ziet u links de lokale bestanden en rechts de bestanden op de server. De user komt terecht in de www map van de docker en kan niet naar de bovenliggende map gaan o.w.v. veiligheidsredenen.



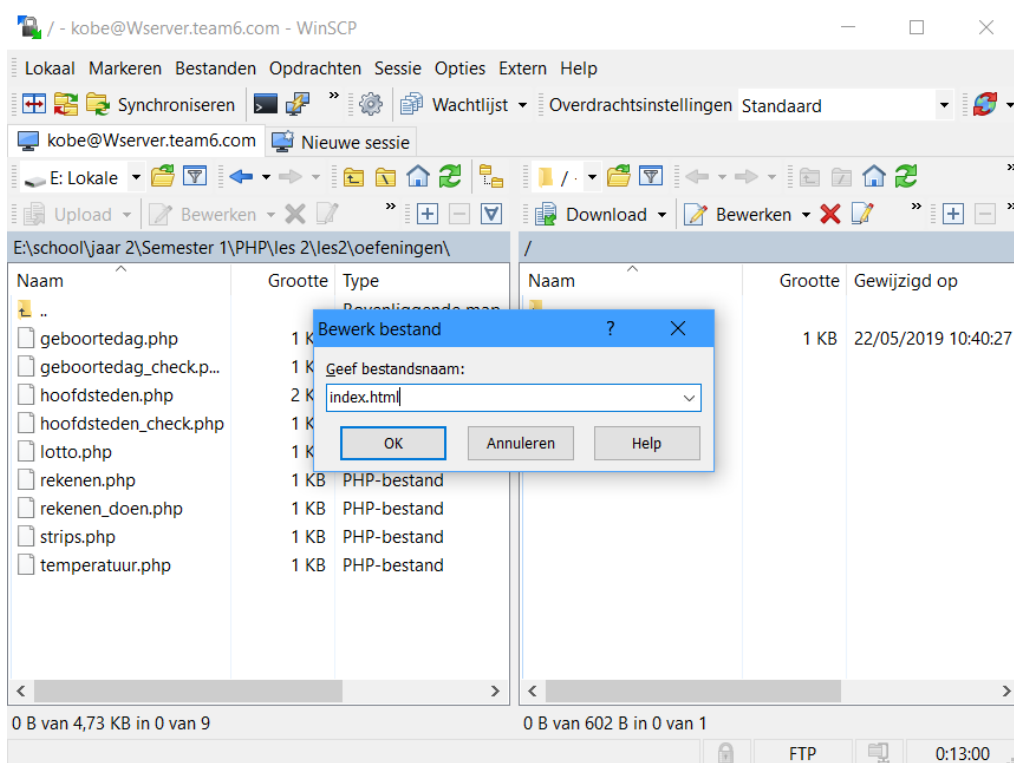
De gebruiker kan bestanden uploaden door het bestand vanuit het linkse scherm te verslepen naar rechts. Zoals hieronder gebeurt is:



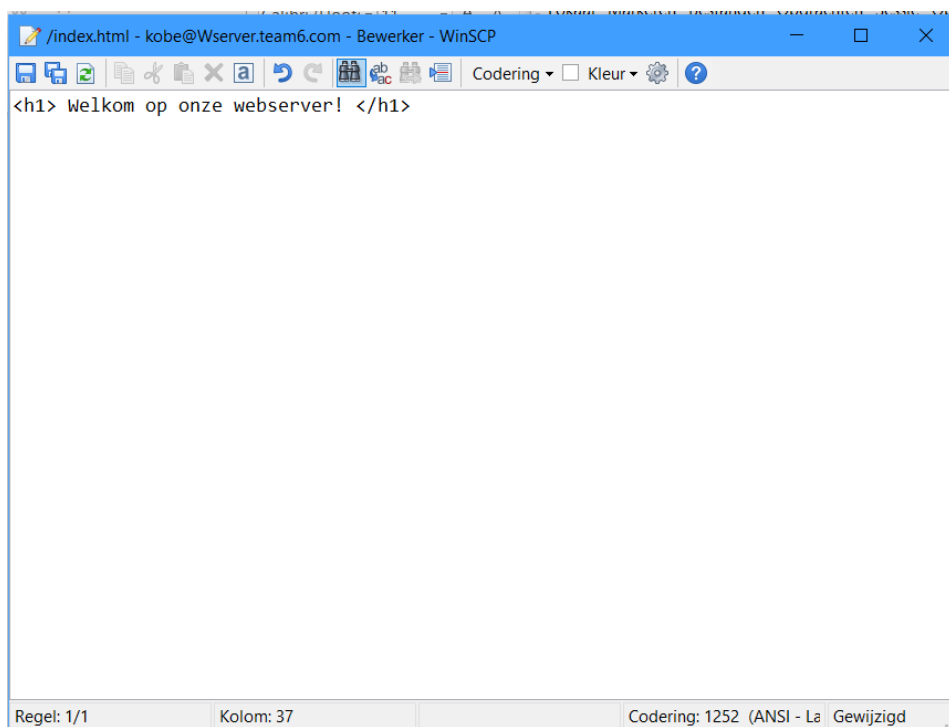
Men kan ook rechtstreeks nieuwe files maken door in het rechtse scherm een rechtermuisklik te doen en te kiezen voor de optie "nieuw". Hierna vraagt het systeem de naam en kan je het direct bewerken.



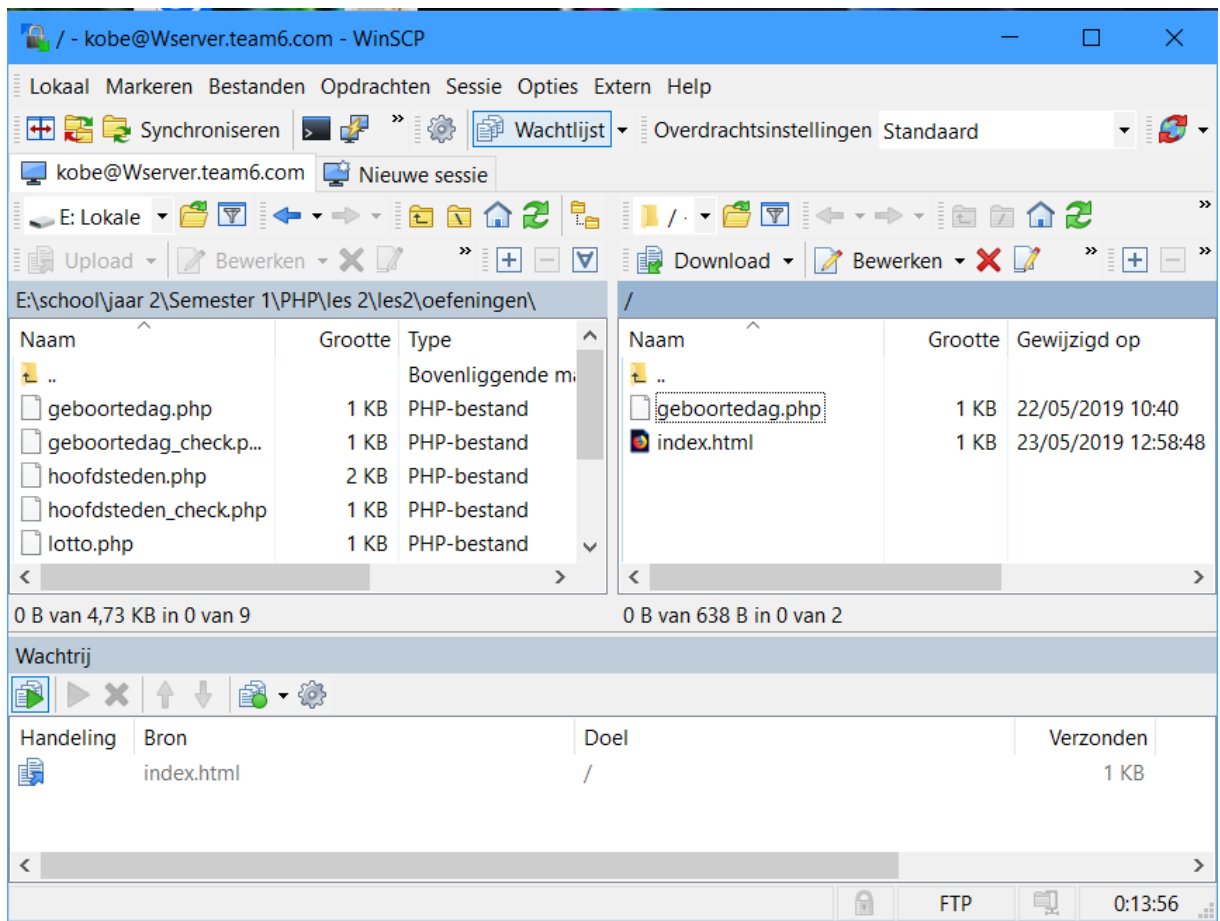
Nieuwe file toevoegen



Naam kiezen van het nieuwe bestand



Inhoud toevoegen

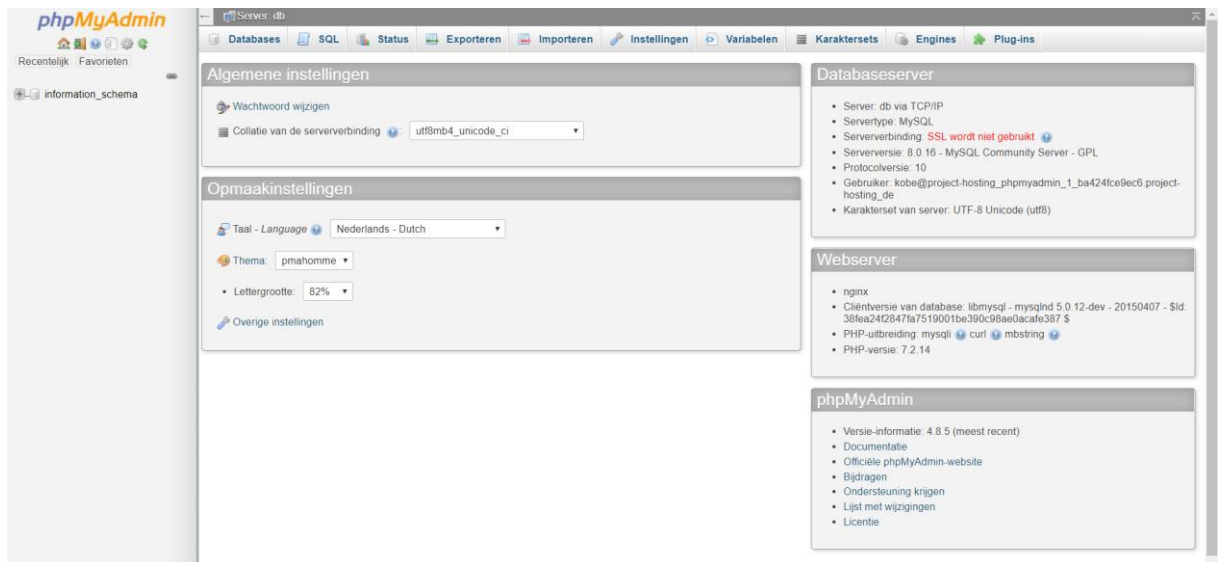


Checken of het toegevoegd is

Step 5: Databases toevoegen via PHPmyAdmin

PHPmyadmin is een PHP tool die het gebruik van de mysql database vergemakkelijkt. Je kan hier naar surfen via de webpagina <http://wserver.team6.com:8001>. Hier kan de gebruiker zich inloggen via zijn gebruikersnaam en paswoord. Hij kan er zijn eigen databases aanmaken en beheren zodat zijn applicaties deze kunnen gebruiken.





Vervolgens kan de gebruiker links databases en tabellen aanmaken naar wens.

En vervolgens de tabel aanmaken



Console

En vervolgens kolommen aanmaken in deze tabel.

The screenshot shows a database management tool interface with a menu bar at the top: Verkennen, Structuur, SQL, Zoeken, Invoegen, Exporteren, Importeren, Rechten, and Handelingen. Below the menu bar, there is a section for table configuration with fields for 'Tabelnaam' (containing 'test'), 'Toevoegen' (set to 1), and 'Kolom(men)' (set to 1), along with a 'Starten' button.

The main area displays a table structure configuration table with the following columns: Naam, Type, Lengte/Waarden, Standaardwaarde, Collatie, Attributen, Leeg, Index, A_, and Opmerkingen. There are four rows, each representing a column of type 'INT' with a length of 11, no default value, and no index.

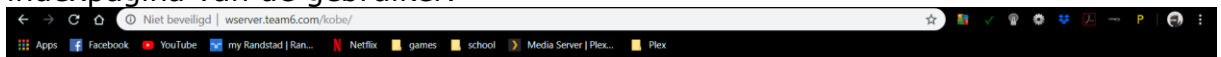
Below the table, there are fields for 'Tabelopmerkingen', 'Collatie', and 'Opslag-engine' (set to InnoDB). At the bottom right, there are buttons for 'SQL-voorbeeld' and 'Opslaan'.

En vervolgens klinkt je op opslaan onderaan en wordt de database opgeslagen.

Stap 5: online de pagina's bekijken

De gebruiker kan zijn eigen pagina's bekijken via het webadres:
 "http://Wserver.team6/'xxx'"

Met xxx als gebruikersnaam. Hier zal men verwezen worden naar de indexpagina van de gebruiker.



Welkom op onze webserver!

10.12 DNS

Installatie DNS pakketten:

Allereerst zorgen we ervoor dat we met de laatste versie van DNS pakketten aan de slag gaan. Daarom updaten we onze lijst van beschikbare pakketten via volgende code:

- **sudo apt-get update**
- **sudo apt-get upgrade**

Voer het volgende commando uit, om het DNS pakket te installeren:

- **sudo apt install bind9**

Daarnaast installeren we ook het pakket dnsutils.

Dit is een zeer interessant pakket ontwikkeld voor het testen en troubleshooten van DNS problemen.

Vaak zijn deze tools reeds aanwezig, controleer dit. Is het nog niet aanwezig, installeren we tevens dit pakket.

- **sudo apt install dnsutils**

De daemon horende bij de DNS-server heet "named".

Om na te gaan of de juiste versie van DNS geïnstalleerd is (BIND9), kan je het volgende commando uitvoeren:

- **named -v**

10.12.1 Configuratie:

1. Installeer DNS

Om ervoor te zorgen dat `/etc/resolv.conf` aangevuld wordt met de DNS-server afkomstig uit de file `/etc/netplan/.... .yaml`, dient u de volgende stappen door te voeren:

- **Pas allereerst de file `/etc/systemd/resolved.conf` aan als sudoer.**

Bijvoorbeeld in ons geval:

DNS=172/27.66.166 8.8.8.8 8.8.4.4

Neem hier het IP-adres op van je server

- **Annuleer de huidige symbolic link naar `/etc/resolv.conf`**

Hoe? Remove de file `/etc/resolv.conf`

- **We maken nu een nieuwe symbolic link "`/etc/resolv.conf`" aan die verwijst naar `/run/systemd/resolve/resolv.conf`.**

Hoe? Voer de volgende regel uit:

`sudo ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf`

- **Herstart de `system-resolved` service:**

`sudo service systemd-resolved restart`

- **Bekijk nu opnieuw de `/etc/resolv.conf` file.**

Deze zou nu de correcte nameservers moeten omvatten.

- **Test via `nslookup`!**

We maken door het uitvoeren van de bovenstaande regels nu gebruik van custom dns in plaats van de lokale aanwezige `systemd-resolved` cache. Ga na of in de file `/etc/nsswitch.conf`, de volgende regel voorkomt:
hosts: files dns

- Ja?Ok, geen probleem!
- Neen? Voeg deze regel toe!

Zorg dat in de file `/etc/host.conf` ook de juiste volgorde (order) wordt ingesteld!

order hosts,bind

Reboot nogmaals de `systemd` service:

- **`sudo service systemd-resolved restart`**

Start de naamserver of de DNS-daemon "named".

- **sudo systemctl restart bind9.service**
- **Vervolgens willen we een nslookup uitvoeren.**
Voer bv. een nslookup uit van www.google.com.

nslookup <te resoluten domeinnaam> <ip-adres van onze DNS server>

Jouw DNS-server dient hierop nu te antwoorden, namelijk als eerst vermelde IP-adres moet het IP-adres van onze server verschijnen:

```
project-hosting@hostingserver:~$ nslookup www.google.com
Server:      172.27.66.166
Address:     172.27.66.166#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.17.68
Name:   www.google.com
Address: 2a00:1450:400e:805::2004

project-hosting@hostingserver:~$
```

Configuratie van een forward lookup zone

We gaan ons eigen domein creëren, namelijk: "team6"

In de printscreens is het IP-adres van de DNS-server 172.27.66.166

Dit kan op jouw systeem verschillend zijn. .

Let dus op: neem de IP-adressen niet "klakkeloos" over!

Werkwijze:

Stap 1 – aanmaken zone in named.conf.local:

We passen /etc/bind/named.conf.local aan

```
project-hosting@hostingserver:~$ sudo cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "team6.com" {
    notify no;
    allow-update {none;};
    type master;
    file "/etc/bind/team6";
};
project-hosting@hostingserver:~$
```

De bovenstaande regels:

- definiëren een nieuwe zone
- ze geven aan dat de huidige server voor deze zone master is
- ze geven aan dat de data voor deze zone terug te vinden is in het bestand `"/etc/bind/team6"`

Dit bestand zal handmatig moeten worden aangemaakt.

- Met `"notify no"`
wordt aangegeven dat er geen slave-naamserveren zijn voor deze zone.
↔ `"notify yes"`
- Met `allow-update`
bepaal je of **dynamic DNS** wordt gebruikt of niet.

Stap 2 – aanmaken zonebestand:

We maken het volgende bestand `"/etc/bind/team6"` aan.

Als vertrekbasis gebruiken we een reeds bestaande zone file.

In de `/etc/bind` directory vinden we de file `db.local` terug.

Deze file gebruiken we als vertrekbasis en hier zullen we aanpassingen aan doorvoeren.

Voer hiervoor het copy commando uit:

- **`sudo cp /etc/bind/db.local /etc/bind/team6`**

```
cv@ccs4server:/etc/bind$ ls -l
total 56
-rw-r--r-- 1 root root 2761 okt 10 17:33 bind.keys
-rw-r--r-- 1 root root 237 okt 10 17:33 db.0
-rw-r--r-- 1 root root 271 okt 10 17:33 db.127
-rw-r--r-- 1 root root 237 okt 10 17:33 db.255
-rw-r--r-- 1 root root 353 okt 10 17:33 db.empty
-rw-r--r-- 1 root root 270 okt 10 17:33 db.local
-rw-r--r-- 1 root root 3171 okt 10 17:33 db.root
-rw-r--r-- 1 root bind 357 feb 5 10:51 ITF_linux
-rw-r--r-- 1 root bind 463 okt 10 17:33 named.conf
-rw-r--r-- 1 root bind 490 okt 10 17:33 named.conf.default-zones
-rw-r--r-- 1 root bind 265 feb 5 10:41 named.conf.local
-rw-r--r-- 1 root bind 890 feb 5 10:28 named.conf.options
-rw-r----- 1 bind bind 77 feb 5 09:53 rndc.key
-rw-r--r-- 1 root root 1317 okt 10 17:33 zones.rfc1918
cv@ccs4server:/etc/bind$
```


We passen de nieuwe zonefile aan als volgt:

```
project-hosting@hostingserver:~$ sudo cat /etc/bind/team6
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      Nserver.team6.com      root.team6.com (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 )      ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
Nserver   IN      A        172.27.66.166
Wserver   IN      A        172.27.66.161
support   IN      A        172.27.66.163
project-hosting@hostingserver:~$
```

Stap 3 – rechten aanpassen:

Hierna dienen we de rechten van de net aangemaakte zonefile aan te passen.

Dit doen we via het commando:

- **chmod 644 /etc/bind/team6**

Stap 4 – herstarten DNS-server:

Nadat de zonefile op een correcte manier is aangepast; dienen we de DNS-server te herstarten.

Dit dien je te doen telkens als er wijziging wordt doorgevoerd aan de zonefile.

- **sudo systemctl restart bind9.service**

Stap 5 – testen van de forward lookup zone op de server zelf + eventuele fouten uit de zonefile halen:

Bij fouten in de zonefile; krijg je niet onmiddellijk een error.
Hoe kan je dan nagaan of de zonefile correct werkende is; door de zonefile te testen.

We testen onze zonefile via het commando "nslookup".
Bv. nslookup Nserver.team6.com

Wanneer dit niet het gewenste resultaat oplevert; staan er waarschijnlijk oftewel fouten in de net aangemaakte zonefile oftewel in de file named.conf.local.
In de logfile /var/log/syslog kan je nagaan waar de fout zich precies bevindt.
In deze logfile wordt duidelijk de regel aangegeven waar de fout zich bevindt!

Nadat alles op een correcte manier is ingegeven en de DNS-server herstart is; zou je het volgende moeten verkrijgen bij uitvoering van het commando nslookup:

```
project-hosting@hostingserver:~$ nslookup wserver.team6.com
Server:          172.27.66.166
Address:         172.27.66.166#53

Name:   Wserver.team6.com
Address: 172.27.66.161

project-hosting@hostingserver:~$ nslookup Nserver.team6.com
Server:          172.27.66.166
Address:         172.27.66.166#53

Name:   Nserver.team6.com
Address: 172.27.66.166

project-hosting@hostingserver:~$ nslookup support.team6.com
Server:          172.27.66.166
Address:         172.27.66.166#53

Name:   support.team6.com
Address: 172.27.66.163

project-hosting@hostingserver:~$ █
```

WERKT HET NIET?

Bekijk /var/log/syslog via commando tail -60 op eventuele fouten in de named.conf file!!

11 TROUBLE-SHOOTING

In elk project zijn er problemen waar men uiteindelijk tegenaan zal lopen. Zo is dit project geen uitzondering, en ook wij zijn verschillende problemen tegengekomen in dit traject.

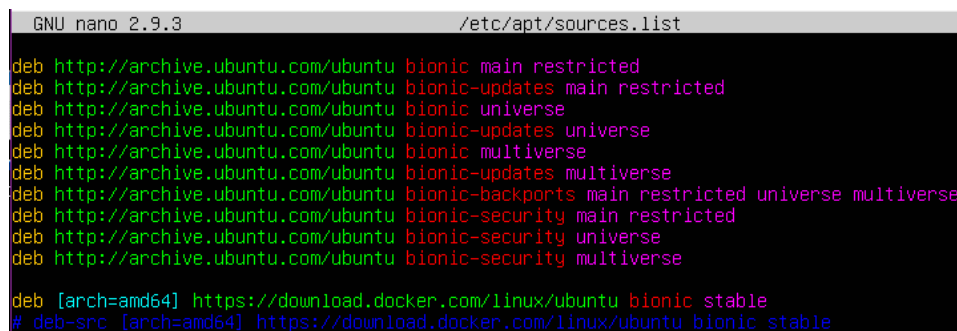
Dit hoofdstuk gaat dieper in op deze problemen, en laat tegelijkertijd zien hoe we deze opgelost hebben.

11.1 Ubuntu sources list

Als er tijdens het proberen van verkrijgen van installatie packages geen gevonden kunnen worden, ga dan zeker na of de sources list uitgebreid genoeg is. Maak gebruik van het volgende commando om de sources list te bekijken en aan te passen.

Sudo nano /etc/apt/sources.list

Een voorbeeld:



```
GNU nano 2.9.3 /etc/apt/sources.list
deb http://archive.ubuntu.com/ubuntu bionic main restricted
deb http://archive.ubuntu.com/ubuntu bionic-updates main restricted
deb http://archive.ubuntu.com/ubuntu bionic universe
deb http://archive.ubuntu.com/ubuntu bionic-updates universe
deb http://archive.ubuntu.com/ubuntu bionic multiverse
deb http://archive.ubuntu.com/ubuntu bionic-updates multiverse
deb http://archive.ubuntu.com/ubuntu bionic-backports main restricted universe multiverse
deb http://archive.ubuntu.com/ubuntu bionic-security main restricted
deb http://archive.ubuntu.com/ubuntu bionic-security universe
deb http://archive.ubuntu.com/ubuntu bionic-security multiverse

deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable
# deb-src [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable
```

Afbeelding: sources lijst van Ubuntu.

Hierna moeten we natuurlijk het commando "sudo apt-get update" uitvoeren om hier nut uit te halen.

11.2 LAMP-stack

11.2.1 Logbestanden

Er kan altijd iets misgaan tijdens het configureren van apache, of wanneer de bestanden allemaal al geconfigureerd zijn, maar de website bijvoorbeeld niet bereikbaar is. De eerste stap die we dan kunnen uitvoeren is het bekijken van logbestanden.

Deze kunnen gevonden worden op de locatie **"/var/log/apache2/error_log"**. Dit is een tekstbestand, die men gewoon kan bekijken doormiddel van nano of tail.

11.2.2 Geblokkeerde poorten of conflicterende software

Het is ook mogelijk dat apache geblokkeerd wordt door een andere applicatie. Standaard gebruikt apache poorten 80 en 443 voor https. Er zijn ook andere

applicaties die gebruik maken van deze poort. Hierdoor zal de apache service niet starten, en tegelijkertijd komt er ook geen melding van in het logbestand.

Dit kunnen we gemakkelijk controleren door het volgende commando uit te voeren: `"netstat -an | grep ':80:' of ':443'"` uit te voeren. Uiteindelijk kan men dit proces killen, zodat apache wel kan starten. Eventueel kan men de poorten aanpassen van de applicaties, waardoor dit probleem niet meer zal toetreden.

11.2.3 Andere mogelijke oorzaken

De mogelijkheid bestaat dat het probleem niet opgelost is met de bovenstaande opties. Indien dit het geval is, kan de oorzaak ergens anders liggen, bijvoorbeeld in de configuratie.

Daarom is het aan te raden om de configuratiebestanden van apache na te lopen, al zal men dit meestal wel in de logbestanden terug vinden. Een andere oorzaak kan bijvoorbeeld zijn dat er bestanden zijn die verwijderd zijn, een verkeerde naam hebben, of de bestanden beschadigd zijn. In dat geval zal men wat moeten zoeken, of in het slechtste geval apache opnieuw installeren.

Een laatste oorzaak kan zijn dat het logbestand vol zit. Wanneer je een logbestand hebt met een grootte van enkele gigabytes, kan dit ervoor zorgen dat apache crasht of niet kan starten. Om dit te kunnen bekijken kan men het commando `"cd /var/log/httpd | ls -ls | less"`.

11.3 VSFTPD

11.3.1 Verbinding geweigerd

Controleer of de FTP service wel draait. Je kan in het configuratiebestand `"/etc/vsftpd/vsftpd.conf"` kijken of er `"listen=YES"` staat, en uit commentaar gehaald is. Vervolgens kun je vsftp starten met `"service vsftp start"`.

De FTP server werkt standaard met poort 21. Je kan in netstat kijken of er een applicatie poort 21 gebruikt, en deze zo nodig afsluiten.

11.3.2 Andere fouten

Wanneer poort 21 nog niet open gezet is in de firewall, kunnen er verschillende fouten optreden wanneer er geprobeerd wordt te connecteren. Enkele van deze fouten zijn o.a.

- Long delay on command after ftp login
- Ftp: connection timed out
- Ftp: connect: no route or host
- Security: bad ip connecting
- 606: no socket

In het bestand `/etc/vsftpd/vsftpd.conf` moet men enkele regels uit commentaar halen als dit nog niet gebeurd is.

- Pasv_enable = yes
- Pasv_min_port = 11000
- Pasv_max_port = 11010

11.4 ClamAV

11.4.1 Fout tijdens het updaten

Het kan ooit gebeuren dat een virusscan fabrikant een update van de definities uitstuurt, terwijl deze een fout bevat. In het ergste geval kan dit ervoor zorgen dat de virusscanner zijn werk niet meer doet. Dit is ook al eens gebeurd bij ClamAV. De enigste manier om dit op te lossen is door een update van het systeem uit te voeren, daarna de ClamAV service te herstarten, om vervolgens de update opnieuw uit te voeren. Hou hierbij rekening dat men daar best een dag over heen laat, zodat de fabrikant ook de tijd heeft om de fout op te lossen.

11.4.2 ClamAV gebruikt telkens meer als 50% van de processor

Dit kan enkele oorzaken hebben, bijvoorbeeld wanneer het definitiebestand te groot is. Soms kan het helpen om het commando "**sudo rm /var/lib/clamav/daily.cld**" uit te voeren. Hierna is een herstart van ClamAV vereist. Dit zorgt ervoor dat de definities worden verwijderd. ClamAV krijgt hierdoor de kans om de nieuwe definities te downloaden, deze zullen aanzienlijk kleiner zijn in bestandsgrootte. Dit zorgt op zijn beurt weer op snelheidswinst.

11.5 Zabbix

Tijdens het installeren en configureren van Zabbix zijn we tegen enkele problemen aangelopen. Af en toe kwam er de melding dat de connectie geweigerd was. Om dit op een eenvoudige manier op te lossen was het belangrijk dat we in de logbestanden gingen kijken. Deze zijn te vinden in "**/var/log/zabbix/zabbix_agentd.log**"

```
96573:20190522:090259.474 failed to accept an incoming connection: connection from "172.19.0.4" re$
96572:20190522:090359.495 failed to accept an incoming connection: connection from "172.19.0.4" re$
96571:20190522:090459.517 failed to accept an incoming connection: connection from "172.19.0.4" re$
96573:20190522:090559.539 failed to accept an incoming connection: connection from "172.19.0.4" re$
96572:20190522:090659.559 failed to accept an incoming connection: connection from "172.19.0.4" re$
96572:20190522:090759.579 failed to accept an incoming connection: connection from "172.19.0.4" re$
96572:20190522:090859.600 failed to accept an incoming connection: connection from "172.19.0.4" re$
```

Afbeelding: screenshot van het zabbix logbestand

We hebben dit opgelost door het ip-adres in het agent.conf bestand te plaatsen.

```
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=172.27.66.161,172.19.0.4,127.0.0.1

### Option: ListenPort
#
#   Agent will listen on this port for connections from the server
#
```

Afbeelding: Toevoegen van ip adres aan agent.conf bij Server.

```
#
#   Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:3001
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=172.27.66.161,172.19.0.4,127.0.0.1

### Option: Hostname
#
#   Unique, case sensitive hostname.
#   Required for active checks and must match hostname as configured in the server.
#   Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=
```

Afbeelding: Toevoegen van ip-adres aan agent.conf bij ServerActive

Hierna is het belangrijk dat we de zabbix agent service opnieuw starten.

```
project-hosting@hostingserver:~$ sudo systemctl restart zabbix-agent.service _
```

Afbeelding: herstarten van de zabbix service

Zabbix accepteert nu de inkomende verbindingen op het ingestelde ip-adres.

11.6 Duplicati

Tijdens het installeren en configureren van Duplicati hadden we slechts last van 1 probleem. Het was onmogelijk om opnieuw te verbinden met de web interface op poort 8200.

```
kobe@ccs_server:~$ duplicati-server --web-service-interface=any
A serious error occurred in Duplicati: System.Exception: Unable to open a socket for listening, tried ports: 8200
   at Duplicati.Server.WebServer.Server..ctor (System.Collections.Generic.IDictionary`2[TKey,TValue] options) [0x002cf] in <a6c0c2089b9a44ec9be5057a44f12116>:0
   at Duplicati.Server.Program.RealMain (System.String[] args) [0x00564] in <a6c0c2089b9a44ec9be5057a44f12116>:0
Invalid type Microsoft.WindowsAzure.Storage.Blob.BlobEncryptionPolicy for instance field Microsoft.WindowsAzure.Storage.Blob.BlobRequestOptions:<EncryptionPolicy>k__BackingField
Invalid type Microsoft.WindowsAzure.Storage.Queue.QueueEncryptionPolicy for instance field Microsoft.WindowsAzure.Storage.Queue.QueueRequestOptions:<EncryptionPolicy>k__BackingField
Invalid type Microsoft.WindowsAzure.Storage.Table.TableEncryptionPolicy for instance field Microsoft.WindowsAzure.Storage.Table.TableRequestOptions:<EncryptionPolicy>k__BackingField
```

Afbeelding: Starten van duplicati met de verkeerde parameters

De oorzaak bleek uiteindelijk deels logisch te zijn. Omdat een backup service cruciaal is, sluit de service zichzelf nooit volledig af, er blijft altijd iets draaien. Dit heeft als gevolg dat poort 8200 bezet is gebleven. De oplossing is dan ook voordehand liggend, we moeten de poort veranderen. In dit geval kunnen we met het commando "duplicati-server -web-service-port=8201" de poort veranderen naar 8201.

11.7 DNS

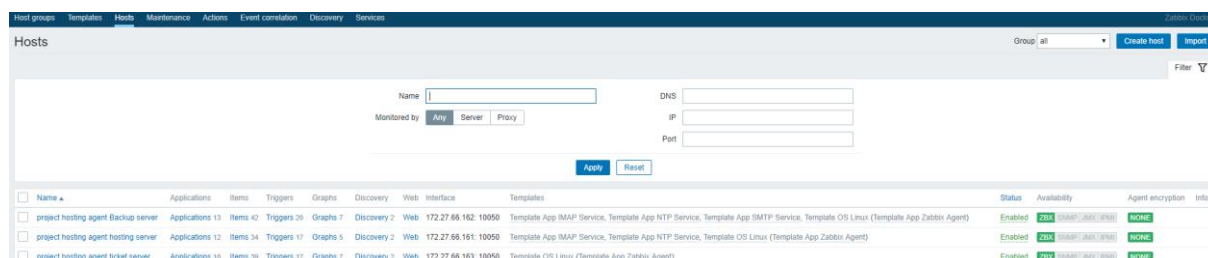
Zie titel voor troubleshooting van DNS.

Zie handleiding DNS.

12 TESTING

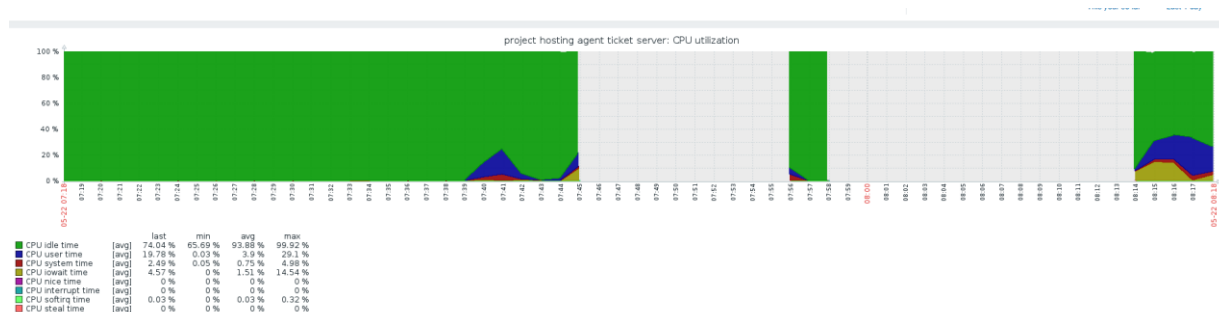
12.1 Zabbix

Voor het deel van Zabbix te testen hebben we een paar Zabbix agents geïnstalleerd op de backup server en de ticket server. In de eerste screenshot ziet u de agents staan en helemaal links ziet u dat deze online zijn (ze zijn groen wat betekend available).



Afbeelding: overzicht van zabbix hosts

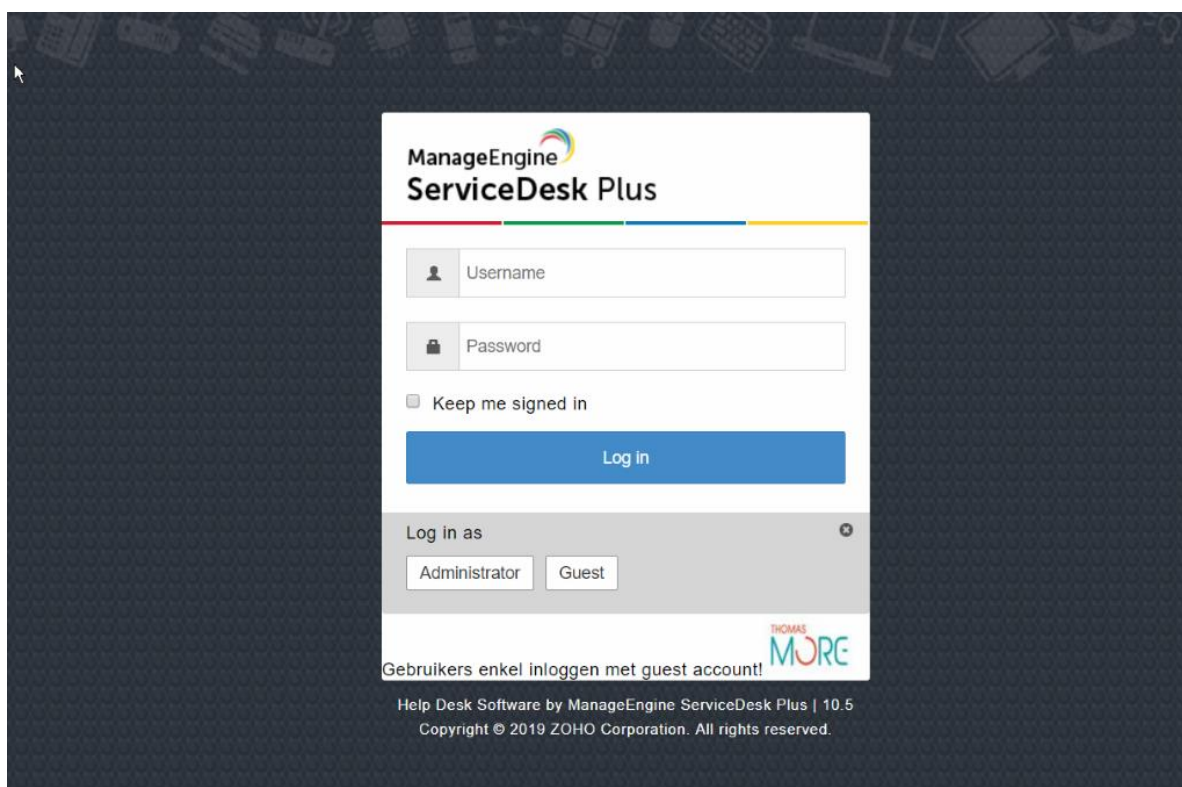
Hieronder heb ik dan de CPU usage van de ticket server gemeten. De blanco stukken zijn de stukken waar dat de server een reboot heeft gemaakt maar anders dan dat zie je hier mooi wat de CPU waardes zijn en wanneer dat de server een "Heavy CPU load" heeft.



Afbeelding: overzicht van CPU gebruik van de hosts

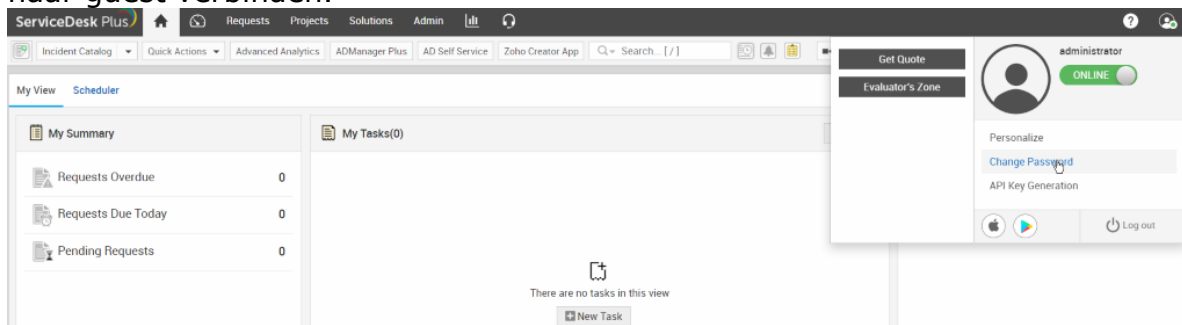
12.2 Service desk plus

Het systeem werkt uiteraard met een grafische interface waarin gebruikers en administrators op kunnen werken. Hierin kunnen de gebruikers inloggen met een guest account (login: guest, passwd: guest) en een ticket verzenden. De administrator heeft een veranderd wachtwoord om te voorkomen dat er gewone gebruikers op dit account gaan. Bij de grafische interface kunnen we met het administrator account inloggen, uiteraard willen we het default wachtwoord wijzigen.



Afbeelding: inlogscherm ticket systeem

We hebben het wachtwoord van 'administrator' naar 'teamzes6' veranderd. Het online chat systeem werkt ook, en je kan dus met administrator naar guest verbinden.



Afbeelding: dashboard van het ticket systeem

Een guest kan een ticket verzenden naar de administrator doormiddel van een 'request' in te dienen.

12.3 Duplicati

Om te testen of de back-up ook effectief werkt hebben we 2 back-ups aangemaakt. 1 back-up die dagelijks heel de map home met alle configuratiebestanden in gaat back-uppen en 1 back-up dat ieder uur de map "home/project-hosting/www/" back-upt. We back-uppen onze bestanden naar een externe back-up server namelijk "172.27.66.162" via het FTP protocol.

Afbeelding: het testen van Duplicati

Hieronder ziet u dat we het back-up doel instellen en vervolgens de verbinding testen:

Volgende geplande taak: Backup1Hour vandaag om 14:00

HoofdBackupDaily ▾

Laatste succesvolle back-up: vandaag om 10:38 (duurde 00:00:34) [Nu uitvoeren](#)

Volgende geplande uitvoering: vandaag om 17:00

Bron: 47,25 MB

Back-up: 21,16 MB / 1 Versie

Backup1Hour ▾

Laatste succesvolle back-up: vandaag om 10:33 (duurde 00:00:02) [Nu uitvoeren](#)

Volgende geplande uitvoering: vandaag om 14:00

Bron: 1,83 KB

Back-up: 9,33 KB / 1 Versie

Afbeelding: geslaagde backup van Duplicati

Als we dan de back-up gaan terugzoeken op de back-up server dan zien we onder het path "home/testmap/" dat de files effectief aanwezig zijn. Deze kunnen we in Duplicati ook zeer simpel terugplaatsen via de web-based interface.

```
project-hosting@hostingserver:~$ cd testmap/
project-hosting@hostingserver:~/testmap$ ls
duplicati-20190523T083304Z.dlist.zip.aes      hallo
duplicati-b74a46e4591794a8bbe83b7f4851afd6c.dblock.zip.aes  test.txt
duplicati-i8f65960ad2924e8db16ba6a90a8dd35a.dindex.zip.aes
project-hosting@hostingserver:~/testmap$
```

Afbeelding: ge-encrypteerde backup van Duplicati op andere server

Voor de volledige back-up hebben we dit ook getest.

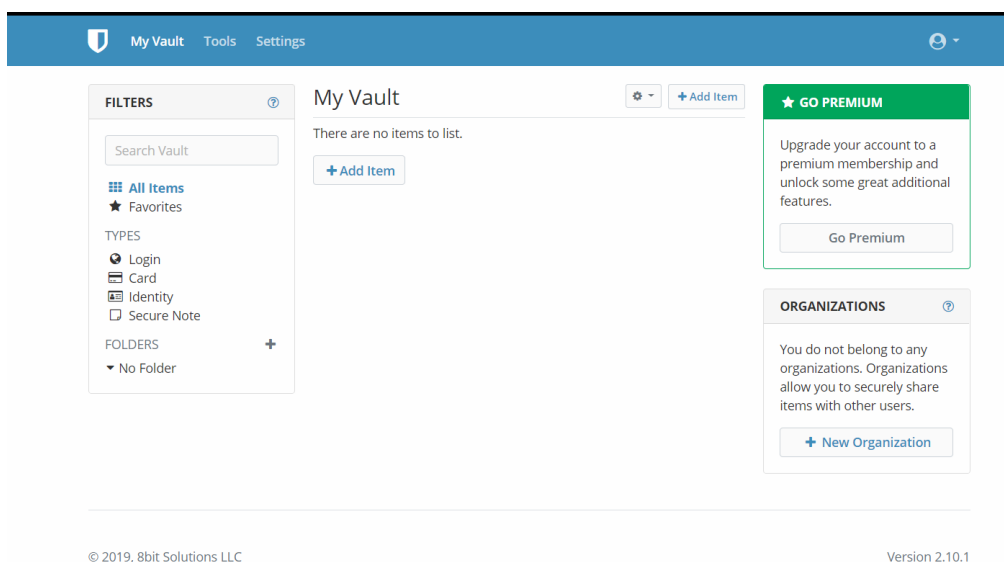
```
project-hosting@hostingserver:~$ cd testmapvolledig/
project-hosting@hostingserver:~/testmapvolledig$ ls
duplicati-20190523T083802Z.dlist.zip.aes
duplicati-b24b29a350e1c4f2984d6a4facb2e92bc.dblock.zip.aes
duplicati-ic13338ae2e5944f89b28216315623200.dindex.zip.aes
project-hosting@hostingserver:~/testmapvolledig$
```

Afbeelding: volledige backup van server

12.5 Bitwarden

Bitwarden kunnen we testen door op de hoofserver naar poort 8004 te gaan. We maken gebruik van poort 8004 omdat de standaard poort 8000 al bezet is.

Hieronder ziet u de homepage van Bitwarden. Hierin kan u simpelweg nieuwe accounts toevoegen door op "add item" te klikken.



Hieronder ziet u dat we een website URL, een gebruikersnaam en een wachtwoord moeten opgeven.

ITEM TOEVOEGEN

Welk soort item is dit?

Aanmelden

Naam

Map

Geen map

Gebruikersnaam

test@test.com

Wachtwoord

••••••••

Authenticatiegeheim (TOTP)

URI 1

bijv. https://google.com

Match detectie

Standaard match detectie

+ Nieuwe URI

Notities

Omdat we gebruik maken van de gratis host versie van Bitwarden kunnen we deze gegevens niet automatisch laten invullen op de website deze Chrome & Firefox plug-in is betalend maar Bitwarden is wel al voldoende geconfigureerd om hiervan gebruik te kunnen maken.

12.6 ClamAV

ClamAV bevat geen grafische interface. Dit komt omdat ClamAV een robuust antivirus is dat draait op de achtergrond. Het wordt enkel op de terminal beheerd.

Met het commando **sudo clamav-freshclam status** kunnen we details zien van het antivirus. Dit wil concreet zeggen dat we kunnen zien of clamAV draait, en voor hoelang al. Dit is handig omdat er niet altijd in het 'top' commando een service actief is van clamav en daardoor het kan lijken dat de antivirus niet meer actief is.

Hieronder bevindt zich een afbeelding waarin het commando getoond is:

```
kobe@ccs_server:~$ sudo apt-get install clamav
[sudo] password for kobe:
Pakketlijsten worden ingelezen... Klaar
Boom van vereisten wordt opgebouwd
De statusinformatie wordt gelezen... Klaar
clamav is reeds de nieuwste versie (0.100.3+dfsg-0ubuntu0.18.04.1).
De volgende pakketten zijn automatisch geïnstalleerd en zijn niet langer nodig:
  bridge-utils ubuntu-fan
Gebruik 'sudo apt autoremove' om ze te verwijderen.
0 opgewaardeerd, 0 nieuw geïnstalleerd, 0 te verwijderen en 68 niet opgewaardeerd.
kobe@ccs_server:~$ sudo service clamav-freshclam status
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2019-05-23 19:36:01 UTC; 2min 8s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://www.clamav.net/documents
   Main PID: 1128 (freshclam)
    Tasks: 1 (limit: 4695)
   CGroup: /system.slice/clamav-freshclam.service
           └─1128 /usr/bin/freshclam -d --foreground=true

mei 23 19:36:01 ccs_server systemd[1]: Started ClamAV virus database updater.
mei 23 19:36:31 ccs_server freshclam[1128]: Thu May 23 19:36:31 2019 -> ClamAV update process starte
mei 23 19:36:36 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> ^Your ClamAV installation is
mei 23 19:36:36 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> ^Local version: 0.100.3 Reco
mei 23 19:36:36 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> DON'T PANIC! Read https://ww
mei 23 19:36:36 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> main.cvd is up to date (vers
mei 23 19:36:36 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> daily.cld is up to date (ver
mei 23 19:36:37 ccs_server freshclam[1128]: Thu May 23 19:36:36 2019 -> bytecode.cvd is up to date (
lines 1-19/19 (END)
```

Bovendien wordt er ook nog een log getoond van wat de clamAV momenteel aan het doen is.

Verder is er ook nog een log bestand waarin clamAV de logs zet die hij heeft gemaakt. In deze map komen ook onze log bestanden die wij zelf hebben gemaakt met het script.

Je kan dus, wanneer er iets mis is met het antivirus, een kijkje gaan nemen in het log bestand om zo de oorzaak te weten te komen.

De logbestanden zijn te vinden in **/var/log/clamav/**.

Logbestand van ons script:

```
Scanned directories: 117
Scanned files: 129
Infected files: 0
Data scanned: 0.64 MB
Data read: 205.10 MB (ratio 0.00:1)
Time: 44.845 sec (0 m 44 s)

----- SCAN SUMMARY -----
Known viruses: 6136447
Engine version: 0.100.3
Scanned directories: 117
Scanned files: 129
Infected files: 0
Data scanned: 0.64 MB
Data read: 205.10 MB (ratio 0.00:1)
Time: 43.666 sec (0 m 43 s)

----- SCAN SUMMARY -----
Known viruses: 6136447
Engine version: 0.100.3
Scanned directories: 117
Scanned files: 129
Infected files: 0
Data scanned: 0.64 MB
Data read: 205.10 MB (ratio 0.00:1)
Time: 40.333 sec (0 m 40 s)

----- SCAN SUMMARY -----
Known viruses: 6136447
Engine version: 0.100.3
Scanned directories: 117
Scanned files: 129
Infected files: 0
Data scanned: 0.64 MB
Data read: 205.10 MB (ratio 0.00:1)
Time: 38.538 sec (0 m 38 s)
kobe@ccs_server:/var/log/clamav$
```

Logbestand van clamav zelf:

```
Thu May 23 19:36:31 2019 -> Running as user clamav (UID 111, GID 114)
Thu May 23 19:36:31 2019 -> Log file size limited to 4294967295 bytes.
Thu May 23 19:36:31 2019 -> Reading databases from /var/lib/clamav
Thu May 23 19:36:31 2019 -> Not loading PUA signatures.
Thu May 23 19:36:31 2019 -> Bytecode: Security mode set to "TrustSigned".
Thu May 23 19:37:42 2019 -> Loaded 6136447 signatures.
Thu May 23 19:37:47 2019 -> LOCAL: Unix socket file /var/run/clamav/clamd.ctl
Thu May 23 19:37:47 2019 -> LOCAL: Setting connection queue length to 15
Thu May 23 19:37:47 2019 -> Limits: Global size limit set to 104857600 bytes.
Thu May 23 19:37:47 2019 -> Limits: File size limit set to 26214400 bytes.
Thu May 23 19:37:47 2019 -> Limits: Recursion level limit set to 16.
Thu May 23 19:37:47 2019 -> Limits: Files limit set to 10000.
Thu May 23 19:37:47 2019 -> Limits: MaxEmbeddedPE limit set to 10485760 bytes.
Thu May 23 19:37:47 2019 -> Limits: MaxHTMLNormalize limit set to 10485760 bytes.
Thu May 23 19:37:47 2019 -> Limits: MaxHTMLNoTags limit set to 2097152 bytes.
Thu May 23 19:37:47 2019 -> Limits: MaxScriptNormalize limit set to 5242880 bytes.
Thu May 23 19:37:47 2019 -> Limits: MaxZipTypeRcg limit set to 1048576 bytes.
Thu May 23 19:37:47 2019 -> Limits: MaxPartitions limit set to 50.
Thu May 23 19:37:47 2019 -> Limits: MaxIconsPE limit set to 100.
Thu May 23 19:37:47 2019 -> Limits: MaxRechWp3 limit set to 16.
Thu May 23 19:37:47 2019 -> Limits: PCREMatchLimit limit set to 10000.
Thu May 23 19:37:47 2019 -> Limits: PCRERecMatchLimit limit set to 5000.
Thu May 23 19:37:47 2019 -> Limits: PCREMaxFileSize limit set to 26214400.
Thu May 23 19:37:47 2019 -> Archive support enabled.
Thu May 23 19:37:47 2019 -> BlockMax heuristic detection disabled.
Thu May 23 19:37:47 2019 -> Algorithmic detection enabled.
Thu May 23 19:37:47 2019 -> Portable Executable support enabled.
Thu May 23 19:37:47 2019 -> ELF support enabled.
Thu May 23 19:37:47 2019 -> Mail files support enabled.
Thu May 23 19:37:47 2019 -> OLE2 support enabled.
Thu May 23 19:37:47 2019 -> PDF support enabled.
Thu May 23 19:37:47 2019 -> SWF support enabled.
Thu May 23 19:37:47 2019 -> HTML support enabled.
Thu May 23 19:37:47 2019 -> XMLDOCs support enabled.
Thu May 23 19:37:47 2019 -> HWP3 support enabled.
Thu May 23 19:37:47 2019 -> Self checking every 3600 seconds.
kobe@ccs_server:/var/log/clamav$
```

13 BIJLAGEN

13.1 Vergaderverslag 21/05

Afwezig : Barend -> hersenschudding

13.1.1 Wie staat waar?

Joey

- server installatie

Frederik

- Security policy, Puppet

Wout

- ClamAV script aan het schrijven
- Puppet

Kobe

- Helpen met server installatie
- Handleiding docker
- DNS configureren

Jesse

- Puppet installeren

Doel van de dag

- Alles op de VM workstation krijgen.
- Puppet afkrijgen
- DNS configureren
- Handleidingen verder uitschrijven (optioneel)

13.2 Vergaderverslag 22/05

13.2.1 Wat is er gisteren gelukt?

Server configuratie:

- Docker
- LAMP stack
- openSSH (beveiligingen nog niet)
- Scripts
- Zabbix
- Duplicati (enkel geïnstalleerd)
- ClamAV
- Ubuntu
- 2^{de} server voor backups
- FTP (behalve chrooten)

13.2.2 Wat gaat er vandaag gebeuren:

- Zabbix agent op backup server
- Nieuwe ticket server
- Duplicati configureren
- FTP chrooten

13.3 Vergaderverslag 23/05/19

13.3.1 Wat is er gisteren gelukt?

Server configuratie:

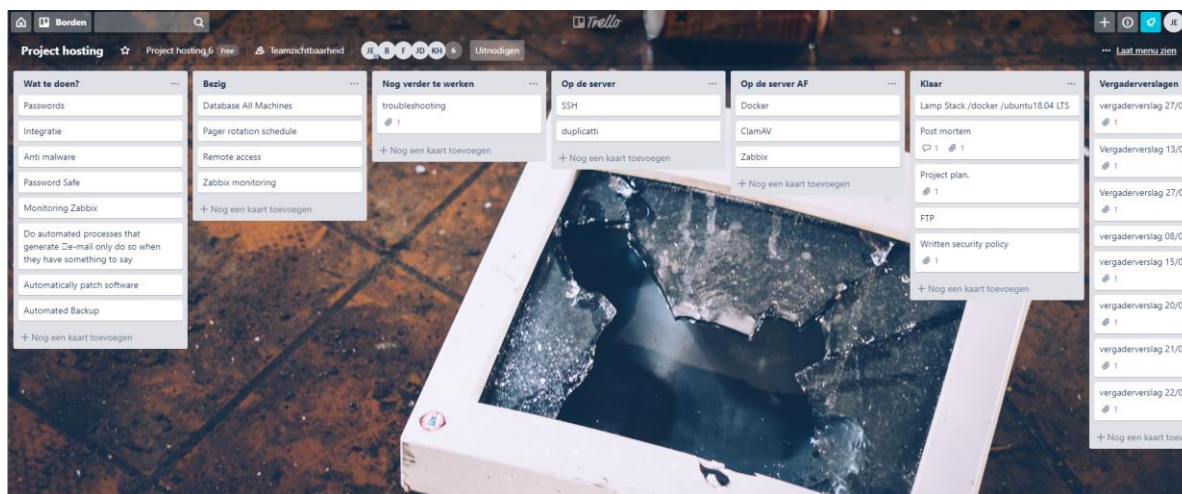
- Docker
- LAMP stack
- openSSH (beveiligingen nog niet)
- Scripts
- Zabbix
- Duplicatti (enkel geïnstalleerd)
- ClamAV
- Ubuntu
- 2^{de} server voor backups
- FTP (behalve chrooten)

13.3.2 Wat gaat er vandaag gebeuren:

- Frederik test Duplicati op de hosting server.
- Kobe stelt de dns server in.
- De rest van het groepje is bezig aan de documentatie en presentatie.

13.4 Trello

Tijdens de lessen Project hosting hebben we ook gebruik gemaakt van Trello. Dit was een gemakkelijke manier om alles mooi bij te houden en gestructureerd te houden. Zo wist ook iedereen waar iedereen mee bezig was waardoor het ook gemakkelijk was om samen te werken. Elke les of soms om de twee weken hebben we dan een vergaderverslag gemaakt om zo te checken hoe ver iedereen met zijn deel is gekomen en wat er nog moest gedaan worden.



Afbeelding: overzicht van onze trello