HOGESCHOOL ROTTERDAM

BACHELOR SCRIPTIE

Verbetering van schaal- en onderhoudbaarheid in de infrastructuur van Developers.nl

Auteur:
Kaj de Munter
0911825

Begeleiders:
Tanja Ubert
Judith Lemmens

15/01/2020

`v0.6`

DEVELOPERS.NL

HOGESCHOOL ROTTERDAM

BACHELOR SCRIPTIE

Verbetering van schaal- en onderhoudbaarheid in de infrastructuur van Developers.nl

---

Auteur:
Kaj de Munter
0911825@hr.nl
k.demunter@developers.nl
06-81019142

Stagebegeleiders:
Tanja Ubert
t.ubert@hr.nl
Judith Lemmens
j.h.i.lemmens@hr.nl

Bedrijfsbegeleiders:
Maarten de Boer
m.deboer@developers.nl
Jelle van de Haterd
j.vandehaterd@developers.nl

Een scriptie ingediend ter voldoening aan de vereiste competenties voor de opleiding Informatica

Communicatie, Media, en Informatietechnologie

15/01/2020

`v0.6`


developers.nl
learn. code. share.


HOGESCHOOL
ROTTERDAM

Voorwoord

Voor u ligt het resultaat van een half jaar onderzoek naar schaal- en onderhoudbaarheid bij Developers.nl in de vorm van een afstudeerstage. Deze scriptie is ingediend ter voldoening aan de vereiste competenties voor de opleiding Informatica aan de Hogeschool Rotterdam.

Ik ben ongelofelijk trots op het eindresultaat. Ik ben altijd met plezier aan de slag gegaan met het onderzoek, en heb veel geleerd deze periode. Ik heb dit niet in mijn eentje kunnen bereiken, daarom wil ik graag een dankwoord uitschrijven.

Bedankt aan iedereen die mij in de afgelopen periode koffie heeft gebracht en geluisterd heeft naar mijn gesteun zodra het even tegenzat, maar ook naar mijn gejuich voor elke kleinste vordering. Ik wil graag mijn stage- en bedrijfsbegeleiders Tanja Ubert, Judith Lemmens, Jelle van de Haterd, en Maarten de Boer bedanken voor alle hulp en steun. Daarnaast wil ik alle collega's bij Developers.nl bedanken voor alle aanmoedigingen en gezelligheid. In het bijzonder mijn mede-stagiair Lex de Willigen, voor het aanhoren van al mijn ideeën, het meedenken, en zijn proeflezingen. Tevens gaat een dankwoord naar Maarten van der Heijden, voor zijn code-reviews en ideeën. Ook bedank ik mijn studiegenoten Steven Drost en Anthony Dijkhoff voor hun gezelligheid en aanmoediging. Tot slot wil ik mijn familie bedanken voor hun motiverende woorden gedurende mijn gehele opleiding.

Ik wens u evenveel leesplezier toe als dat ik plezier heb gehad tijdens het schrijven.

Kaj de Munter
Rotterdam, Januari 2020

HOGESCHOOL ROTTERDAM

Samenvatting

Communicatie, Media, en Informatietechnologie

Informatica

Verbetering van schaal- en onderhoudbaarheid in de infrastructuur van Developers.nl

door Kaj de Munter

Dit onderzoek heeft tot doel het verkrijgen van inzicht over de schaal- en onderhoudbaarheid van de website van Developers.nl, om vervolgens deze twee factoren in de praktijk te verbeteren.

De definitie van onderhoudbaarheid in de ogen van Developers.nl is het versnellen van de workflow, voornamelijk door het afdwingen van kwaliteitsstandaarden. De definitie van schaalbaarheid van Developers.nl is voornamelijk de mogelijkheid om te schalen, boven het daadwerkelijk schalen. Een manier om zowel schaal- als onderhoudbaarheid te realiseren is het implementeren van "feature-environments".

Feature environments zijn aparte deployments en omgevingen voor elke individuele nieuwe feature die wordt toegevoegd. Dit is gerealiseerd door middel van een reverse proxy, Traefik.

Verder is Codecov geimplementeerd om code-coverage te waarborgen, worden Docker images periodiek opgeruimd om ruimte op de server vrij te houden, is Grafana geïmplementeerd om monitoring data te visualiseren, en is Open Policy Agent gebruikt om beveiliging en kwaliteit van nieuwe toevoegingen te waarborgen.

UNIVERSITY OF APPLIED SCIENCES ROTTERDAM

Abstract

Communication, Media, and Information Technology

Computer Science

Improvement of scalability and maintainability in the infrastructure of Developers.nl

by Kaj de Munter

The purpose of this research is to gain insight into the scalability and maintainability belonging to the website of Developers.nl, in order to subsequently improve these two factors in practice.

The definition of maintainability through the eyes of Developers.nl is the improvement of the workflow, mainly through the enforcement of quality standards. The definition of scalability of Developers.nl is primarily the ability to scale, instead of actually scaling. One way to achieve both scalability and maintainability is to implement "feature environments".

Feature environments are separate deployments and environments for each individual new feature that is in process of being added. This has been achieved through a reverse proxy, Traefik.

Furthermore, Codecov has been implemented to ensure code-coverage, Docker images are periodically cleaned up to keep space free on the server, Grafana has been implemented to visualize monitoring data, and Open Policy Agent has been used to guarantee security and quality of new additions.

Inhoud

Figurenlijst

Begrippenlijst

Slack	Het communicatiemiddel waar Developers.nl gebruik van maakt.
Proxmox	Proxmox VE is a complete open-source platform for enterprise virtualization [1]
Service Discovery	Service discovery is the process of automatically detecting devices and services on a network [2]
Kubernetes	Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications [3].
Docker	Docker is a tool designed to make it easier to create, deploy, and run applications by using containers [4].
Ansible	Ansible is a radically simple IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs [5].
Docker Swarm	Docker Swarm provides native clustering functionality for Docker containers, which lets you turn a group of Docker engines into a single, virtual Docker engine [6].
Nginx	High performance load balancer, webserver, and reverse proxy [7].
Vagrant	Leverages a declarative configuration file which describes all your software requirements, packages, operating system configuration, users, and more [8].
Serverless Computing	En application defined as a set of event-triggered functions that execute without requiring the user to explicitly manage servers [9].
Infrastructure as Code	Infrastructure as code describes the idea of using a high-level programming language to control IT systems [10].
Chef	Deploy new code faster and more efficiently. Automate infrastructure and applications [11].
Puppet	Powerful infrastructure automation and delivery [12].
Terraform	Terraform is a tool for building, changing, and versioning infrastructure safely and efficiently. Terraform can manage existing and popular service providers as well as custom in-house solutions [13].

Cloud computing providers	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [14].
12-factor app	Een methodologie voor het bouwen van Software as a Service (SaaS) applications [15].
The Open Group Architecture Framework	A generic framework to build different IT architectures frameworks [16].
4+1 architectural view model	A model for describing the architecture of software-intensive systems, based on the use of multiple, concurrent views [17].
Jinja2	Ansible uses Jinja2 templating to enable dynamic expressions and access to variables. Ansible greatly expands the number of filters and tests available, as well as adding a new plugin type: lookups [18].
Ansible-vault	Ansible Vault is a feature of ansible that allows you to keep sensitive data such as passwords or keys in encrypted files, rather than as plaintext in playbooks or roles. These vault files can then be distributed or placed in source control [19].

Afkortingenlijst

MI	**M**aintainability **I**ndex
CI	**C**ontinuous **I**ntegration
CD	**C**ontinuous **D**eployment
CM	**C**onfiguration **M**anagement
VU	**V**irtual **U**ser
VM	**V**irtual **M**achine
CA	**C**ertificate **A**uthority
APM	**A**pplication **P**erformance **M**onitoring
EMS	**E**mployee **M**anagement **S**ystem
CMS	**C**ontent **M**anagement **S**ystem
QoS	**Q**uality **o**f **S**ervice
AWS	**A**mazon **W**eb **S**ervices
GCP	**G**oogle **C**loud **P**latform
OPA	**O**pen **P**olicy **A**gent
PaC	**P**olicies **a**s **C**ode
IaC	**I**nfrastructure **A**s **C**ode
K8s	**K**uberneteS
TCP	**T**ransmission **C**ontrol **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
CLI	**C**ommand **L**ine **I**nterface
IaaS	**I**nfrastructure **a**s **a** **S**ervice
PaaS	**P**latform **a**s **a** **S**ervice
SaaS	**S**oftware **a**s **a** **S**ervice
DDoS	**D**istributed **D**enial of **S**ervice
FQDN	**F**ully **Q**ualified **D**omain **N**ame
TOGAF	**T**he **O**pen **G**roup **A**rchitecture **F**ramework
FastCGI	**F**ast **C**ommon **G**ateway **I**nterface

Hoofdstuk 1

Inleiding

1.1 Aanleiding

"Een visitekaartje voor het bedrijf". Dat is het uitgangspunt van de interne software bij Developers.nl. Niet alleen qua uiterlijk, maar de code, de infrastructuur en de werkmethodes moeten van hoge kwaliteit zijn. Dit heeft te maken met het feit dat de code uit de website en infrastructuur van Developers.nl open-source wordt gemaakt gedurende deze stage. Het open-source maken van de website betekent dat elke potentiële klant en/of nieuwe medewerker de mogelijkheid heeft om te bekijken wat Developers.nl qua kennis in huis heeft. Het is dus van groot belang dat de kwaliteit gewaarborgd wordt, en dat zo veel mogelijk nieuwe en opkomende technieken worden gebruikt. Dit vereist constant onderhoudswerk. Daarnaast heeft Wheeler [20] geconcludeerd dat open-source software voordelen heeft als:

- Betere beveiliging
- Betere betrouwbaarheid
- Betere prestaties
- Betere schaalbaarheid
- Mindere onderhoudskosten

Developers.nl organiseert maandelijks een "TechNight". Op deze TechNight ontvangt de website van Developers.nl een piek aantal bezoekers, het is belangrijk dat deze pieken goed worden afgehandeld zonder enige downtime. Dit betekent dat onderzoek op de kwaliteit van de huidige website belangrijk is. Bovendien zijn er meerdere interne systemen dan alleen de website, zoals bijvoorbeeld het Employee Management System (EMS). Het onderhouden van deze systemen vereist veel tijd en moeite. Dit wordt voornamelijk door stagiairs of tijdelijke hulpkrachten uitgevoerd. In dit onderzoek wordt voornamelijk gefocussed op de website. Dit is de applicatie die het meest frequent gebruikt wordt, en dus de meeste aandacht verdiend.

1.2 Belang

De interne systemen zijn op eerste gezicht van de buitenkant vrij eenvoudig. Developers.nl wilt – om indruk te wekken op potentiële klanten en nieuwe medewerkers – onder water een applicatie draaien dat "te complex" is. Maar; omdat de ontwikkelaars óf "minder ervaren" stagiairs zijn, óf een tijdelijke hulpkracht zijn

kost het onderhouden – vooral met 5 verschillende systemen – erg veel tijd, moeite, en als gevolg hiervan: geld.

1.3 Doelstelling

Dit onderzoek heeft tot doel het verkrijgen van inzicht over de schaal- en onderhoudbaarheid van de website van Developers.nl, om vervolgens deze twee factoren in de praktijk te verbeteren.

1.4 Probleemstelling

Bij Developers.nl werken veel verschillende ontwikkelaars voor een erg variabele tijd aan de interne projecten. Dit heeft te maken met het feit dat de ontwikkelaars die eraan werken vaak tussen twee opdrachten in zitten. Dit betekent dat het van hoog belang is dat een ontwikkelaar de omgeving snel kan opzetten en op korte termijn een kwalitatieve toevoeging kan leveren die in productie staat. De workflow moet verder geoptimaliseerd worden om Developers.nl dit te beloven.

1.5 Hoofd- en Deelvragen

Hoofdvraag

Op welke wijze kan Developers.nl de architectuur van haar websites beter schaal- en onderhoudbaar maken?

Deelvragen

- Wat zijn de wensen en eisen van Developers.nl met betrekking tot de schaal- en onderhoudbaarheid van haar huidige websites?
- Welke standaarden en best-practices voor het waarborgen van schaal- en onderhoudbaarheid zijn relevant voor de eisen van Developers.nl?
- Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?
- Wat voor verbeteringen ten aanzien van schaal- en onderhoudbaarheid kunnen worden toegepast op de huidige websites van Developers.nl?
- Hoe kunnen de gekozen verbeteringen ten aanzien van schaal- en onderhoudbaarheid geïmplementeerd worden?
- Voldoen de verbeteringen aan de vereiste requirements?

1.6 Methodologie

Om antwoord te geven op de hoofdvraag "Op welke wijze kan Developers.nl de architectuur van haar websites beter schaal- en onderhoudbaar maken?" is voornamelijk kwalitatief onderzoek uitgevoerd. Vooronderzoek is uitgevoerd door bestaande literatuur te bestuderen om zo een beter beeld te verkrijgen en om een basis te leggen van de belangrijkste begrippen. Alle bronnen zijn handmatig gecontroleerd op kwaliteit en relevantie. Voor het definiëren van functionele schaalbaarheid is veel overlegd met verschillende software-ontwikkelaars, veel feedback gevraagd aan de community, en zijn zowel formele als informele bronnen samengevoegd om zo tot één concrete definitie te komen.

Om technieken te vinden die behoren bij schaal- en onderhoudbaarheid is deskresearch uitgevoerd door middel van interviews met ontwikkelaars en bestaande onderzoeken te verzamelen. Hierna zijn deze technieken afgebakend tot de meest relevante die bij dit onderzoek horen. Vervolgens is een beschrijvend onderzoek uitgevoerd op de huidige infrastructuur in hoofdstuk 5. Hier zijn bestaande kenmerken en elementen van de huidige infrastructuur tegen de gevonden standaarden en technieken uit hoofdstuk 4 afgewogen. Om verschillende verbeteringen te vinden is net als hoofdstuk 4 deskresearch uitgevoerd. Dit bevat voornamelijk interviews met senior ontwikkelaars die deze technieken in de praktijk gebruiken. Hierna zijn de gevonden methodes kwalitatief onderbouwd.

Voor de daadwerkelijke implementatie is allereerst exploratief onderzoek gedaan naar de bijbehorende technieken en hun best-practices. Het doel hiervan is vooral om ideeën op te doen naar mogelijke implementaties.

1.7 Planning

In tabel 1.1 is de vooraf opgestelde planning te vinden. Het is mogelijk dat hier vanaf is geweken tijdens het daadwerkelijke onderzoek, maar het geeft een ruw beeld van de tijdsverdeling.

TABEL 1.1: Planning

Week	Taak
1, 2	Skelet opzet scriptie, inleiding
3, 4	Theoretisch kader, afbakening
5, 6	Welke standaarden en best-practices voor het waarborgen van schaal- en onderhoudbaarheid zijn relevant voor de eisen van Developers.nl?
7, 8	Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?
9, 10	Wat voor verbeteringen ten aanzien van schaal- en onderhoudbaarheid kunnen worden toegepast op de huidige websites van Developers.nl?
11, 12	Hoe kunnen de gekozen verbeteringen ten aanzien van schaal- en onderhoudbaarheid geïmplementeerd worden?
13 – 17	Praktijk implementatie
18 – 20	Conclusie en deelvraag "Voldoen de verbeteringen aan de vereiste requirements?"

1.8 Leeswijzer

Vóór het "echte onderzoek" is eerst in het theoretisch kader (hoofdstuk in 2) een literatuuronderzoek uitgevoerd naar definities van de meest belangrijke begrippen: **Schaalbaarheid**, **onderhoudbaarheid**, en **infrastructuur**. Hierdoor is een concrete basis gelegd voor de opvolgende deelvragen.

In hoofdstuk 3 zijn de wensen en eisen van Developers.nl vastgelegd en requirements opgesteld. Daarna is in 4 onderzoek gedaan naar de mogelijke technieken, met de deelvraag: "Welke standaarden en best-practices voor het waarborgen van schaal- en onderhoudbaarheid zijn relevant voor de eisen van Developers.nl?". Hier zijn standaarden en best-practices besproken om te kunnen bewijzen dat de hoofdvraag daadwerkelijk beantwoord is.

In het volgende hoofdstuk (5) met deelvraag "Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?" zijn deze standaarden afgewogen tegen de huidige infrastructuur. Vervolgens wordt in hoofdstuk 6 onderzocht welke verbeteringen hier op toe te passen zijn, hierbij hoort de deelvraag "Wat voor verbeteringen ten aanzien van schaal- en onderhoudbaarheid kunnen worden toegepast op de huidige websites van Developers.nl?". In hoofdstuk 7 wordt de daadwerkelijke implementatie van deze verbeteringen besproken door verschillende opties met elkaar af te wegen. Hier wordt antwoord gegeven op de deelvraag "Wat voor verbeteringen ten aanzien van schaal- en onderhoudbaarheid kunnen worden toegepast op de huidige websites van Developers.nl?".

Hierna zijn de geïmplementeerde verbeteringen geëvalueerd in hoofdstuk 8, bijbehorende deelvraag "Voldoen de verbeteringen aan de vereiste requirements?". Nu alle deelvragen zijn beantwoord worden er in hoofdstuk 9 aanbevelingen

toegelicht voor toekomstige verbeteringen. Ten slotte wordt in hoofdstuk 10 antwoord gegeven op de hoofdvraag "Op welke wijze kan Developers.nl de architectuur van haar websites beter schaal- en onderhoudbaar maken?" door alle deelconclusies samen te binden tot één hoofdconclusie. In hoofdstuk 11 staat een zelfreflectie over het onderzoek.

1.9 Opdrachtgever

Deze scriptie is geschreven in opdracht van Developers.nl.

1.9.1 Core business

Developers.nl neemt software ontwikkelaars in dienst. De ontwikkelaars die worden aangenomen zullen voornamelijk gespecialiseerd zijn in PHP, Python, Java of front-end. Ze worden uitgezet naar een klant (een extern bedrijf) die naar een ontwikkelaar zoekt. Developers.nl kiest hier voor de beste ontwikkelaar voor de taak en zal deze inzetten bij een klant. De opdrachten van de ontwikkelaars zijn op locatie van de klant en duren voornamelijk langer dan een jaar, maar op uitzondering zijn er ook kortere opdrachten. Zodra de ontwikkelaar klaar is met zijn of haar taak zal Developers.nl zo snel mogelijk een nieuwe opdracht toewijzen [21]. Concreet zegt het positioneringsprofiel [22]: "Detachering van developers die software applicaties bouwen voor verschillende klanten."

1.9.2 Eigen omgeving

Tijdens de stageperiode neemt de stagiair een leidende rol aan in een team van 2 part-time studenten, een derdejaars-stagiair, en de tijdelijke hulpkrachten. Developers.nl heeft rond de 60 software ontwikkelaars. Deze zijn voornamelijk op een externe opdracht bij een klant. Elke vrijdag zullen 5 "kennisambassadeurs" op kantoor zijn. Dit zijn de meest senior ontwikkelaars per team. Deze zijn dan in staat om stagiairs en/of andere medewerkers persoonlijk te helpen. Hoewel ze maar één keer per week op kantoor aanwezig zijn, zijn ze altijd telefonisch bereikbaar of via Slack. Daarnaast kijken de kennisambassadeurs code van de interne systemen inhoudelijk na en geven hier feedback op.

De bedrijfsbegeleider voor deze stage is Maarten de Boer. Dit is de algemene directeur van Developers.nl en is in 2003 afgestudeerd aan de hogeschool Inholland met Strategic marketing. Aangezien Maarten zelf geen technische kennis heeft is er ook een technische begeleider aangewezen: Jelle van de Haterd. Jelle is senior developer, DevOps engineer en kennisambassadeur bij Developers.nl. Hij is in 2006 afgestudeerd op de Hogeschool Rotterdam met als opleiding Grafimediatechnologie [23].

Hoofdstuk 2

Theoretisch Kader

In dit hoofdstuk worden vier belangrijke begrippen uit de onderzoeksvraag behandeld. Er wordt een literatuuronderzoek gedaan naar de bestaande definities van schaalbaarheid, onderhoudbaarheid en architectuur met betrekking tot software. Hierna wordt het begrip afgebakend tot een concrete definitie waar het onderzoek op terug kan vallen.

2.1 Schaalbaarheid

M. D. Hill heeft in 1990 onderzoek gedaan naar een concrete definitie naar schaalbaarheid [24]. In zijn onderzoek concludeert hij het volgende:

> *I examined aspects of scalability, but did not find a useful, rigorous definition of it. Without such a definition, I assert that calling a system 'scalable' is about as useful as calling it 'modern'. I encourage the technical community to either rigorously define scalability or stop using it to describe systems.*

Na Hills conclusie zijn meerdere pogingen gedaan om schaalbaarheid te definiëren. zo zijn L. Duboc, D. S. Rosenblum en T. Wicks op deze conclusie ingegaan en hebben een poging gedaan om een framework te creëren voor karakterisering en analyse van software schaalbaarheid [25]. Dit framework is te complex voor de scope van dit onderzoek, maar zij definiëren schaalbaarheid als: "quality of software systems characterized by the causal impact that scaling aspects of the system environment and design have on certain measured system qualities as these aspects are varied over expected operational ranges".

In een onderzoek over de kenmerken van schaalbaarheid en de impact op prestatie heeft A. B. Bondy [26] schaalbaarheid verdeeld in een aantal verschillende aspecten, waaronder:

- **Structural scalability** (het vermogen van een systeem om uit te breiden in een gekozen dimensie zonder ingrijpende wijzigingen in de architectuur)
- **Load scalability** (het vermogen van een systeem om elegant te presteren naarmate het aangeboden verkeer toeneemt)
- **Space scalability** (het geheugenvereiste groeit niet naar "ondraaglijke niveaus" naarmate het aantal items toeneemt)
- **Space-time scalability** (het systeem blijft naar verwachtingen functioneren naarmate het aantal items dat het omvat toeneemt)

Bondy definieert schaalbaarheid als het vermogen van een systeem om een toenemend aantal elementen, objecten en werk gracieus te verwerken en / of vatbaar te zijn voor uitbreiding.

H. El-Rewini en M. Abd-El-Barr noemen in het boek Advanced computer architecture and parallel processing [27] ook een aantal "onconventionele" definities:

- **Size scalability** (Meet de maximale hoeveelheid processors dat een systeem kan accommoderen)
- **Application scalability** (de mogelijkheid om applicatiesoftware te draaien met verbeterde prestaties op een opgeschaalde versie van het systeem)
- **Generation scalability** (de mogelijkheid om op te schalen door het gebruik van de volgende generatie (snellere) componenten)
- **Heterogeneous scalability** (het vermogen van een systeem om op te schalen met behulp van hardware- en softwarecomponenten die door verschillende leveranciers zijn gemaakt)

C. B. Weinstock en J. B. Goodenough hebben een algemeen onderzoek uitgevoerd naar schaalbaarheid [28]. Zij noemen in hun conclusie dat er voornamelijk twee betekenissen van het woord schaalbaarheid zijn:

1. De mogelijkheid om met verhoogde werkdruk om te gaan (zonder extra resources aan een systeem toe te voegen).
2. De mogelijkheid om met verhoogde werkdruk om te gaan door herhaaldelijk een kosteneffectieve strategie toe te passen om de mogelijkheden van een systeem uit te breiden.

Het valt op dat een concrete definitie van schaalbaarheid alleen duidelijk te definiëren is wanneer het in meerdere verschillende soorten is opgesplitst. Daarom zal in dit onderzoek vanaf dit punt altijd worden gespecificeerd welke soort schaalbaarheid het betreft. In dit onderzoek wordt vooral de focus gelegd op de **structural scalability** en **load scalability** uit [26] omdat deze het meest relevant zijn met betrekking tot de probleemstelling, het beter afhandelen van piekmomenten in de hoeveelheid verkeer. Wel is er wat overlapping tussen deze twee definities, zodra een systeem aan structural scalability voldoet, is een deel van load scalability ook voldaan, aangezien het schalen in een dimensie er voor zorgt dat een systeem een grotere hoeveelheid verkeer aan kan. Het deel dat nog mist is functionele schaalbaarheid uit paragraaf 2.1.1. Application scalability uit [27] heeft veel ook overlapping met load scalability. Omdat load scalability iets generieker is en de twee definities van Weinstock en Goodenough [28] omvat wordt deze geprefereerd boven application scalability. De overgebleven definities zijn minder relevant voor dit onderzoek aangezien ze te maken hebben met hardware, of niet volledig toepasselijk zijn op de architectuur.

Schalen kan op twee verschillende manieren, namelijk horizontaal en verticaal. Horizontaal wilt zeggen dat er geschaald wordt door meerdere machines toe te voegen, terwijl verticaal schalen betekent dat er meer rekenkracht (als bijvoorbeeld een betere CPU of meer RAM) wordt toegevoegd aan een machine. Het gemak waarmee een horizontaal of verticaal kan schalen is **structural scalability**. Ook is bij het schaalbaar maken van systemen van belang dat het zo min mogelijk ten koste gaat van prestaties en niet meer kost dan nodig is.

2.1.1 (Niet-)functionele schaalbaarheid

Functionele schaalbaarheid is een term die in meerdere informele bronnen wordt gebruikt, maar nog nooit concreet gedefinieerd is in de literatuur. De informele bronnen gebruiken vaak een definitie in de richting van "De mogelijkheid om een systeem te verbeteren door nieuwe functionaliteit toe te voegen zonder bestaande activiteiten te verstoren". Het is echter niet duidelijk waar deze definitie vandaan komt, en is gelijkwaardig aan de definitie van **extensibility** [29], [30]. In dit onderzoek wordt een unieke definitie van functionele schaalbaarheid gedefinieerd: *In welke mate bestaande componenten moeten worden aangepast zodra een nieuwe functionele requirement wordt toegevoegd aan het systeem, en in hoeverre deze goed blijft functioneren naarmate de hoeveelheid gebruik van het systeem toeneemt.*

Omdat functionele schaalbaarheid concreet definieert over wat er precies 'extensible' moet zijn, en in zijn definitie de hoeveelheid gebruik meeneemt, is dit een meeromvattende term dan extensibility. Functionele schaalbaarheid is een *onderdeel* van onderhoudbaarheid (Wijzigbaarheid) en load scalability. Daarnaast past het de definitie van extensibility toe in de context van functionele requirements. Het onderscheidt zich door de complexiteitsgraad van algoritmes en hard-coded limieten mee te nemen in zijn definitie. Meer over de definitie van onderhoudbaarheid is te vinden in paragraaf 2.2.

Ook is het mogelijk om een definitie te creeëren voor **Niet-functionele schaalbaarheid**. Deze definitie is buiten de scope van het onderzoek maar luidt als volgt: "In hoeverre een niet-functionele requirement kan worden verbeterd zonder bestaande componenten te belemmeren, en in welke mate de kwaliteit van die requirement acceptabel blijft naarmate het gebruik van het systeem toeneemt." Om feedback te ontvangen van de gemaakte definities is een blog geschreven. Hier is ook meer informatie te vinden over niet-functionele schaalbaarheid en hoe deze twee definities tot stand zijn gekomen. [1] Feedback is te vinden in Bijlage C.3

2.2 Onderhoudbaarheid

P. Grubb en A. A. Takang definiëren in hun boek "Software Maintenance: Concepts And Practice" onderhoudbaarheid als "The discipline concerned with changes related to a software system after delivery" [31]. In 1993 heeft IEEE een "Standard Glossary of Software Engineering Terminology" opgesteld. Deze begrippenlijst definieert onderhoudbaarheid als "the ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment" [32]. Deze twee definities komen uiteindelijk op hetzelfde neer. Grubb en Takang noemen het in de context van een discipline, terwijl IEEE het als een kwaliteitseigenschap definieert. Ook specificeren Grubb en Takang het feit dat het alleen ná het opleveren gebeurt.

Grubb en Takang noemen ook een aantal redenen waarom software moet worden onderhouden:

- Ondersteuning van verplichte upgrades

[1] De blog is op de website van Developers.nl geplaatst:
https://developers.nl/blog/69/Defining-software-scalability-using-requirements

- Ondersteuning van verzoeken van gebruikers om verbeteringen toe te voegen
- Om toekomstige onderhoudswerkzaamheden te vergemakkelijken

K.K. Aggarwal et al. noemen in hun onderzoek een aantal factoren die van invloed zijn op onderhoudbaarheid van software [33]:

- Leesbaarheid van de broncode
- Kwaliteit van de documentatie
- Begrijpelijkheid van software

ISO 25010 [34] definieert onderhoudbaarheid als "The degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements" en verdeeld het in een vijftal kwaliteitseigenschappen.

- Modulariteit
- Herbruikbaarheid
- Analyseerbaarheid
- Wijzigbaarheid
- Testbaarheid

Omdat ISO 25010 [34] de meest recente definitie heeft en over het algemeen wordt beschouwd als een effectief framework om software-kwaliteit te waarborgen, word in dit onderzoek deze definitie gebruikt als uitgangspunt.

2.3 Architectuur

P. Kruchten noemt dat software-architectuur zich bezig houdt met het ontwerp en de implementatie van de structuur op hoog niveau [17]. Dit is echter een vrij vage definitie, het is niet duidelijk wat "hoog niveau" precies inhoudt.

S. T. Albin definieert software-architectuur als "De waarneembare eigenschappen van een softwaresysteem" [35]. Ook dit is een onduidelijke definitie, het is te algemeen.

L. Bass en P. Clements, definiëren de architectuur van software als het volgende [36]: "The architecture of a software-intensive system is the structure or structures of the system, which comprise software elements, the externally visible properties of those elements, and the relationships among them". Gerespecteerde boeken als [37], [38] nemen deze definitie als uitgangspunt. Ook noemen Bass en Clements vier verschillende aspecten die behoren bij software-architectuur:

- **Statische structuur** (interne design-time elementen zoals modules, classes, packages, services, of andere zelfstandige code-eenheden en hun opstelling.)
- **Dynamische structuur** (de runtime-elementen zoals informatie-flows, parallelle of opeenvolgende uitvoering van interne taken, of de invloed die ze hebben op data en hun interacties.)
- **Extern zichtbaar gedrag** (de functionele interacties tussen het systeem en zijn omgeving. Denk aan Informatie-flows in en uit het systeem, of API's.)

- **Kwaliteitseigenschappen** (externe zichtbare, niet-functionele eigenschappen van een systeem zoals prestaties, beveiliging of schaalbaarheid.)

ISO/IEC/IEEE 42010:2011 definieert software-architectuur als "Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution" [39]. The Open Group Architecture Framework (TOGAF) voegt nog een tweede definitie toe aan deze context [40]: "The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time". TOGAF is gebaseerd op een viertal architectuur-domeinen: business, data, applicatie en technische / infrastructuur architectuur. In dit onderzoek wordt alleen de technische / infrastructuur architectuur gebruikt. Dit domein omvat de IT infrastructuur, middleware, netwerken, communicaties en standaarden. Onder deze definitie passen ook de vier aspecten uit [36].

Hoofdstuk 3

Verwachtingen

Dit hoofdstuk gaat over de deelvraag "Wat zijn de wensen en eisen van Developers.nl met betrekking tot de schaal- en onderhoudbaarheid van haar huidige websites?". Om de verwachtingen duidelijk in kaart te brengen zijn discussies gevoerd met Jelle van de Haterd; stagebegeleider en kennisambassadeur DevOps. Notulen van deze discussie zijn te vinden in bijlage C.1. De requirements zijn gebaseerd op de huidige situatie van de website, in hoofdstuk 5 wordt hier nader op ingegaan.

3.1 Hoe ziet Developers.nl onderhoudbaarheid?

Om de workflow sneller te laten verlopen moeten zo veel mogelijk processen geautomatiseerd worden. Hieronder valt voornamelijk het automatiseren van de kwaliteitswaarborging. Het is belangrijk dat een nieuwe toevoeging of applicatie aan een aantal standaarden voldoet, zodat ontwikkelaars snel aan de slag kunnen. Jelle vind ten opzichte van daadwerkelijke code voornamelijk dat de infrastructuur aan verbetering toe is.

Developers.nl als product owner wil een nieuwe toevoeging of eventueel een volledig nieuwe applicatie kunnen bedenken en deze zo snel mogelijk geïmplementeerd zien. De workflow qua integratie en deployment moet verder geoptimaliseerd worden om Developers.nl deze snelheid te beloven.

3.2 Hoe ziet Developers.nl schaalbaarheid?

Developers.nl als product owner wil de voortgang van nieuwe toevoegingen of applicaties nauw kunnen volgen, zodat de kwaliteit hiervan op tijd gevalideerd kan worden. Dit heeft te maken met de agile werkmethodiek die Developers.nl gebruikt voor het ontwikkelen van haar interne applicaties.

Om de snelheid te verhogen waarop ontwikkelaars hun toevoegingen kunnen laten zien, ziet Developers.nl graag het concept van "Feature environments". Dit wil zeggen dat er per aangemaakte git branch gelijk gedeployed wordt naar een aparte omgeving, die dan te bekijken is door de product owner. Dit betekent dat er dus meerdere (verschillende) instanties van de applicatie naast elkaar moeten kunnen draaien. Daarnaast ziet Developers.nl graag de mogelijkheid om rekenkracht van de server te verdelen over deze instanties, waardoor er dus horizontaal geschaald

moet kunnen worden. Developers.nl prioriteert de feature environments boven het verdelen van de rekenkracht, omdat het implementeren van feature environments "twee vliegen in één klap" is. Dit zorgt namelijk voor onderhoudbaarheid én het betekent dat de oplossing schaalbaar is.

3.3 Waar wilt Developers.nl meer over te weten komen?

Developers.nl wil weten of de best-practices van de 12-Factor App toepasselijk zijn op de huidige infrastructuur. Ook wil Developers.nl meer te weten komen over verschillende standaarden die zij kunnen opvolgen om de kwaliteit van hun infrastructuur te waarborgen.

3.4 Wat zijn de concrete requirements waar de oplossing aan moet voldoen?

Om schaalbaarheid te realiseren moet de onderhoudbaarheid van de infrastructuur ook op een voldoende niveau zijn, hier moeten kwaliteitsstandaarden voor onderzocht worden. Daarnaast moet de oplossing zo generiek mogelijk zijn, en dus voor meerdere applicaties toe te passen zijn. Dit betekend dus ook dat de oplossing geschikt moet zijn voor applicaties met veel verkeer.

Om requirements op te stellen wordt gebruik gemaakt van de MoSCoW-methode. Deze afkorting staat voor: **M**ust haves, **S**hould haves, **C**ould haves, en **W**on't haves [41]. Deze methode helpt bij het opstellen van prioriteiten om zo te beslissen wat onder de scope van dit onderzoek valt.

Must haves

- De oplossing moet méér dan twee unieke instanties van de website naast elkaar kunnen draaien.
- De oplossing moet moet unieke instanties van de website automatisch kunnen aanmaken.
- De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen.
- Minimaal één monitoring tool voor het monitoren van performance.
- De oplossing moet voldoen aan één of meerdere kwaliteitsstandaarden.

Should haves

- De oplossing moet generiek genoeg zijn zodat meerdere applicaties er gebruik van kunnen maken.
- De oplossing moet de website horizontaal kunnen laten schalen bij een toe- of afnemende hoeveelheid verkeer. De efficiëntie moet 1:1 zijn. Bijvoorbeeld: Één extra instantie moet 50% van het verkeer opvangen.

Could haves

- De oplossing moet de website automatisch laten schalen.
- Er moet onderzoek gedaan worden naar cloud providers, en of dit een goede verbetering is.
- Er moet onderzoek gedaan worden naar serverless computing, en of dit een goede verbetering is.

Won't haves

- Een "boilerplate" voor het opzetten van nieuwe (schaal- en onderhoudbare) projecten.

3.5 Conclusie

Developers.nl wilt onderhoudbaarheid bereiken door kwaliteitsstandaarden af te dwingen. Ook wilt Developers.nl twee soorten schaalbaarheid. Eén in de vorm van het deployen van verschillende branches in aparte omgevingen, en één in de vorm van horizontaal schalen om meer verkeer aan te kunnen. Deze twee soorten kunnen niet gerealiseerd worden zonder de onderhoudbaarheid te waarborgen. Er zijn vijf must-have requirements:

- De oplossing moet méér dan twee unieke instanties van de website naast elkaar kunnen draaien.
- De oplossing moet moet unieke instanties van de website automatisch kunnen aanmaken.
- De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen.
- Minimaal één monitoring tool voor het monitoren van performance.
- De oplossing moet voldoen aan één of meerdere kwaliteitsstandaarden.

Hoofdstuk 4

Technieken

Dit hoofdstuk gaat over de deelvraag "Welke standaarden en best-practices voor het waarborgen van schaal- en onderhoudbaarheid zijn relevant voor de eisen van Developers.nl?". Developers.nl wil als "Must-have" requirement kwaliteitsstandaarden zien waarmee te bewijzen is dat de oplossing schaal- en onderhoudbaar is. Hierdoor zijn twee methodieken nodig, één voor schaalbaarheid, en één voor onderhoudbaarheid. Ook is Developers.nl benieuwd naar de 12-Factor App en hoe relevant deze methodiek kan zijn voor de interne systemen. De kwaliteitsstandaarden hebben betrekking tot software-architectuur.

4.1 ISO 25010

ISO normen zijn wereldwijde standaarden, daarom is dit een ideale manier om kwaliteit te waarborgen. ISO-norm 25010 [34] is de opvolger van ISO-9126 en beschrijft software kwaliteitskenmerken in acht categorieën. Een categorie hiervan is onderhoudbaarheid. Elke categorie heeft een aantal subcategorieën, bij onderhoudbaarheid zijn dat [1]:

Modulariteit: De mate waarin een systeem of computerprogramma opgebouwd is in losstaande componenten zodat wijzigingen van een component minimale impact hebben op andere componenten.

Herbruikbaarheid: De mate waarin een bestaand onderdeel gebruikt kan worden in meer dan één systeem of bij het bouwen van een nieuw onderdeel.

Analyseerbaarheid: De mate waarin het mogelijk is om effectief en efficiënt de impact, van een geplande verandering van één of meer onderdelen, op een product of systeem te beoordelen, om afwijkingen en/of foutoorzaken van een product vast te stellen of om onderdelen te identificeren die gewijzigd moeten worden.

Wijzigbaarheid: De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden zonder fouten of kwaliteitsvermindering tot gevolg.

Testbaarheid: De mate waarin effectief en efficiënt testcriteria vastgesteld kunnen worden voor een systeem, product of component en waarin tests uitgevoerd kunnen worden om vast te stellen of aan die criteria is voldaan.

Om de applicatie "onderhoudbaar" te noemen moeten alle subcategorieën voldoende worden vervuld. Er moet een analyse worden uitgevoerd per subcategorie over eventuele tekortkomingen.

[1] Vertaling van ISO-norm uit wikipedia: https://nl.wikipedia.org/wiki/ISO_25010

4.2 Van Twelve naar Fifteen-Factor App

A. Wiggins [15] heeft een methodologie opgezet om moderne, schaalbare en onderhoudbare web-applicaties te bouwen. De methodologie past goed bij de probleemstelling, het minimaliseren van de kosten en tijd die het kost om nieuwe ontwikkelaars aan het project te laten werken en de gemakkelijkheid van het schalen. Daarnaast wilde Developers.nl graag weten of de 12-Factor app relevant kan zijn voor de huidige infrastructuur. Ook zorgt het voor structural scalability, draagbaarheid tussen uitvoeringsomgevingen, de mogelijkheid om te deployen op moderne cloud platformen en een minimale divergentie tussen development en productie waardoor CD gemakkelijk wordt om te implementeren.

De methodologie heeft 12 factoren (best-practices) die voor deze eigenschappen zorgen. Deze methodologie wordt regelmatig aangeraden door professionals en wordt veel gebruikt. Kritiek op de 12-Factor App gaat voornamelijk over het feit dat het gelimiteerd is tot Heroku [42]. Vijf jaar nadat Wiggins de 12-Factor App heeft opgesteld is K. Hoffman aan de slag gegaan met een boek genaamd "Beyond the 12-Factor App" [43]. Dit boek heeft als doel om de 12 factoren concreter te definiëren en voegt daarnaast nog 3 extra factoren toe om applicaties in de cloud "niet alleen te laten functioneren maar ook te laten gedijen". Hierdoor is de methodologie ook niet meer persé gericht op Heroku. Deze factoren zijn telemetry, security, en het concept "API first". Eigenlijk is een betere benaming voor deze methodologie dus de "Fifteen-Factor App". In bijlage B.1 is een gevolg samen met een uitleg bij elke factor geplaatst. Zodra een factor te maken heeft met onderhoudbaarheid is een subcategorie van ISO 25010 onderhoudbaarheid aan gekoppeld. Alle 15 factoren zullen worden meegenomen bij het behandelen van de deelvragen.

4.3 Schaalbaarheids-controle

In het onderzoek van Weinstock en Goodenough [28] noemen zij dat het niet echt mogelijk is om te testen of een systeem schaalbaar is. Wel zijn er methoden om de schaalbaarheid te waarborgen:

- Onderzoek de "performance curves" en karakteriseer deze met een Big O notatie. Hoe veranderen deze curves bij het aanpassen van een schaalstrategie?
- Identificeer mechanismen om knelpunten aan het licht te brengen of waar aannames van het schaalbaarheids- ontwerp beginnen te worden geschonden. Deze knelpunten hebben vooral te maken met de eerste betekenis van Weinstock en Goodenough. Er moet gecontroleerd worden op de toenemende administratieve werkdruk, de "hard-coded" limieten op capaciteit, de user-interface en de complexiteitsgraad van algoritmen. De schaalbaarheids-aannames gaan over het onderzoeken hoe de uitbreiding van een systeem nieuwe problemen kan onthullen. Zodra een systeem zich uitbreidt is er een grotere kans op errors in de systeemconfiguratie, "zeldzame" errors komen vaker voor, is het belangrijk dat een probleem in het systeem gelokaliseerd blijft, en kan het een stuk complexer en lastiger worden om het systeem te begrijpen.
- Voer een SWOT analyse uit op de schaalbaarheids-strategie.

- **S**trengths (de soorten groei waar de strategie voor ontworpen is)
- **W**eaknesses (de soorten groei waar de strategie niet voor ontworpen is)
- **O**pportunities (mogelijke veranderingen in werklast of technologie die de strategie goed zou kunnen benutten)
- **T**hreats (mogelijke veranderingen in de werklast of technologie die de strategie in twijfel zouden kunnen trekken)

Door het karakteriseren van de performance curves met een Big O notatie wordt voornamelijk de load scalability gewaarborgd. Het identificeren van de knelpunten en aannames samen met het uitvoeren van een SWOT analyse zorgt voor het waarborgen van de functionele schaalbaarheid.

4.4 Overige

Er zijn meer standaarden en best-practices dan hierboven genoemd. Deze worden niet gebruikt in dit onderzoek in verband met verscheidene redenen maar zijn wel noemenswaardig.

4.4.1 Schaalbaarheid

L. Duboc, D.S. Rosenblum en T.Wicks hebben een framework opgezet voor karakterisering en analyse van software schaalbaarheid [25]. Dit framework is te complex voor de scope van dit onderzoek, maar is wel gebruikt in paragraaf 2.1 om de definitie van schaalbaarheid op te stellen.

Verder heeft Azure [44] een zogenaamde “scalability checklist” gemaakt. Deze checklist kan gebruikt worden om een applicatie vanaf het oogpunt van schaalbaarheid te beoordelen. Om de rode lijn in het onderzoek te behouden wordt deze checklist niet gebruikt voor het oordelen van de huidige situatie. Wel kan de checklist gebruikt worden om uiteindelijk te beoordelen of de website klaar is om te schalen.

4.4.2 Onderhoudbaarheid

Een bekende manier om onderhoudbaarheid te meten is de zogenaamde Maintainability Index (MI). Hier is echter veel kritiek op [45]–[48]. Enerzijds is het een duidelijk cijfer om een indicatie te geven van de onderhoudbaarheid. Anderzijds is het uiteindelijk niet duidelijk welke aspecten precies voor het eindresultaat hebben gezorgd of welke acties er genomen moeten worden om de indicatie te verbeteren. Een andere methode om onderhoudbaarheid te meten is het model van I. Heitlager, T. Kuipers en J. Visser [48]. Dit model gebruikt echter een verouderd ISO standaard, namelijk ISO 9126 – de voorganger van ISO 25010 – en is dus niet relevant meer.

[49] noemt 10 richtlijnen voor het schrijven van onderhoudbare code en vervolgens een manier om onderhoudbaarheid te meten op basis van ISO 25010. Dit boek is voornamelijk gericht op code, en niet op de algemene infrastructuur. Vandaar dat dit boek niet relevant is voor het onderzoek.

4.5 Conclusie

De 12-Factor App is een methodologie die twaalf best-practices samenvoegt om moderne, schaal- en onderhoudbare web-applicaties te bouwen. Het boek “Beyond the 12-factor app” [43] is hierop verder gegaan door nog een drietal factoren toe te voegen. Door een applicatie te evalueren op deze vijftien factoren, samen met de definitie van ISO-25010 [34] is te beoordelen of deze schaal- en onderhoudbaar is. Om de schaalbaarheid van een systeem te waarborgen zijn de methoden van Weinstock en Goodenough [28] een geschikte manier.

Hoofdstuk 5

Huidige situatie

Dit hoofdstuk gaat over de deelvraag “Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?”.

5.1 Huidige Architectuur

In dit onderzoek wordt voornamelijk gefocussed op de website. Dit is de applicatie die het meest frequent gebruikt wordt, en dus de meeste aandacht verdiend. De huidige website is een combinatie van een PHP plus Symfony back-end API met Content Management Systeem (CMS), samen met een React plus Next.js front-end. De infrastructuur is momenteel gebouwd op Docker(-compose) + Ansible. Bitbucket pipeline wordt gebruikt voor het Continuous Integration / Deployment.

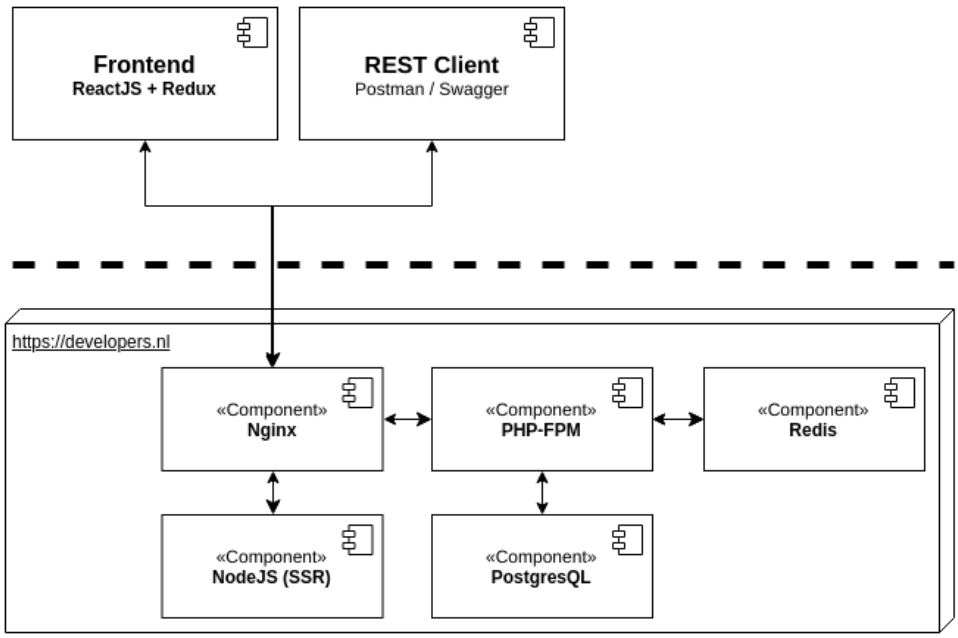
In figuur 5.1 staat een component diagram van de huidige website-structuur. De front- en back-end structuur bevat 5 Docker containers:

- **PHP-FPM** (back-end)
- **Nginx** (front- en back-end)
- **Redis** (back-end)
- **NodeJS** (front-end)
- **PostgreSQL** (back-end)

PHP-FPM is een FastCGI Process Manager, deze Container serveert de Symfony “FosREST” API en het Content Management Systeem. De NodeJS container serveert een statische Next.js React applicatie en maakt gebruik van Server Side Rendering. Er zit een Nginx reverse proxy in die kiest om een request naar de back-end of de front-end te laten gaan. Redis is een Key-Value Database die gebruikt wordt voor het cachen, en een PostgreSQL container als database. De Bitbucket Pipeline gebruikt Ansible om op de servers de geüpdatete containers te pullen en te starten.

Voor zowel de front- als back-end is één monitoring tool genaamd “Sentry” geïmplementeerd. Sentry creëert een duidelijk overzicht voor alle errors die opkomen in productie.

Ook heeft Developers.nl een “Employee Management Systeem” (EMS) gebouwd. Deze heeft een soortgelijke structuur als de website. Het EMS bevat zeer veel gevoelige informatie en het is dus van hoog belang dat dit goed beveiligd is.



FIGUUR 5.1: Infrastructuur website front- en back-end [50]

5.2 Metingen

Nu de infrastructuur in kaart is gebracht luidt de vraag; hoe schaalbaar is deze infrastructuur eigenlijk? Om dit te beantwoorden worden de verschillende definities van schaalbaarheid individueel behandeld.

5.2.1 Structural scalability

Definitie: Het vermogen van een systeem om uit te breiden in een gekozen dimensie zonder ingrijpende wijzigingen in de architectuur. Bij structural scalability horen factor 2 **(API First)** en 5 **(Configuration, credentials, and code)** van de 15-factor app.

API First

De website van Developers.nl is momenteel in 2 delen gesplitst: de React Front-end en de PHP API als back-end. Deze worden apart ontwikkeld, waardoor dus het principe altijd wordt toegepast. Daarnaast heeft het EMS geen API, en is dus out-of-scope voor deze factor.

Configuration

Een test om te bewijzen dat alle configuratie correct uit de code is verwerkt, is of de applicatie op elk gewenst moment open-source kan worden gemaakt zonder geclassificeerde informatie vrij te geven.

Voor de website wordt er gebruik gemaakt van docker-secrets en ansible-vault. Deze combinatie zorgt ervoor dat er nooit wachtwoorden, API sleutels en dergelijke plain-text in versiebeheer komt te staan. Deze secrets worden uiteindelijk in de containers als environment variabelen opgeslagen en uitgelezen door Symfony. In het EMS is deze techniek nog niet gebruikt en staan credentials wél plaintext in de repository.

Om aan factor 5 te voldoen moet de configuratiefiles niet per specifieke omgeving (productie, test, staging) gegroepeerd worden maar moeten juist individueel per deployment geregeld worden. Dit gebeurt in zowel het EMS als de website, de bitbucket pipeline heeft zijn eigen specifieke environment variabelen om te gebruiken en de variabelen in de docker containers worden meegegeven in de algemene docker-compose file die in elke deployment hetzelfde zal zijn.

5.2.2 Load scalability

Definitie: Het vermogen van een systeem om elegant te presteren naarmate het aangeboden verkeer toeneemt. Bij load scalability horen factor 12 **(stateless processes)**, 13 **(concurrency)** en 7 **(disposability)** van de 15-factor app methodologie.

Stateless processes

Factor 12 vereist dat de applicatie als één of meerdere "stateless processes" moet uitgevoerd worden. Bij de PHP containers worden geüploade bestanden weggeschreven naar een volume, dit zorgt ervoor dat de container niet volledig stateless meer is. Ook zijn databases in docker containers geplaatst, dit is een stateful process aangezien het van belang is dat niet alle data verloren gaat zodra de container stopt.

Concurrency

Voor factor 13 is het van belang dat een applicatie horizontaal uit te schalen is. Zolang de applicatie aan factor 7 **(Disposability)** en 12 **(Stateless processes)** voldoet, zit deze factor goed [43]. Er is alleen nog geen manier geïmplementeerd om daadwerkelijk meerdere Docker containers naast elkaar te draaien of te managen.

Disposability

Voor factor 7 moet een applicatie opstarttijd minimaliseren. Zodra de docker images de initiële buildtime voorbij zijn kan de applicatie snel uit en aan worden gezet.

Ook vereist factor 7 dat processen netjes worden afgesloten zodra ze een `SIGTERM` ontvangen. Zodra een docker container met `docker stop <container>` gestopt wordt zal er een SIGTERM worden gestuurd naar de draaiende processen. De vier containers met processen zijn PostgreSQL, PHP-FPM, Nginx en Redis. Deze sluiten allemaal netjes af, de outputs zijn te zien in Bijlage A.3.

Ook moeten de processen bestendig zijn tegen "sudden death". Om dit te simuleren kan `docker kill <container>` gebruikt worden om een `SIGKILL` te sturen naar de hoofdprocessen. In bijlage A.4 is te zien dat alle containers na een `docker kill` zonder problemen weer kunnen opstarten.

5.2.3 Weinstock & Goodenough controle

Om de functionele schaalbaarheid te waarborgen zullen de 3 methoden van Weinstock en Goodenough [28] uitgevoerd worden. Performance curves zullen worden gevisualiseerd, knelpunten zullen worden uitgelicht en een SWOT analyse op de schaalbaarheid zal worden uitgevoerd.

Om de performance curves te visualiseren zal een load-test worden uitgevoerd. Er zijn hier meerdere tools voor vergeleken, waaronder:

- https://loader.io/
- https://gatling.io/
- https://k6.io/
- http://tsung.erlang-projects.org/

De gratis versie van loader.io is niet genoeg voor de wensen van de test, voor gatling.io is Ruby kennis nodig, en voor Tsung worden de tests in XML geschreven wat het lastig maakt om de load op te schalen. Uiteindelijk is gekozen voor K6 omdat zo goed als elke ontwikkelaar genoeg Javascript kennis heeft om deze tool te gebruiken. Ook heeft k6 een eenvoudige manier om de hoeveelheid Virtual Users (VU) geleidelijk te verhogen. Om de uitkomsten te visualiseren is InfluxDB samen met Grafana gebruikt.

In bijlage A.1 is de implementatie hiervan te vinden, in bijlage A.2 de resultaten. In verband met de implementaties tegen DDoS-aanvallen zijn 43% van de requests geblokkeerd. De VUs lopen op van 20 naar 120. Op 12:02:28 is te zien dat de minimum waarde van de request duration spontaan daalt. Het is mogelijk dat TransIP hier iets mee te maken heeft, maar het is apart dat de maximum waardes niet dalen. De echte reden van de daling is vooralsnog onduidelijk. Ook is te zien dat de request duration geen significante stijging heeft naarmate de hoeveelheid VUs oplopen. Dit kan te maken hebben met het feit dat de server te krachtig is om te vertragen. Hier is uit op te maken dat het opschalen van de website wellicht niet veel effect gaat hebben.

Één limiterende factor bij het schalen van de website is de hoeveelheid opslag. Voornamelijk omdat het CMS dubbel functioneert als "file-server". Daarnaast bevat de content van de website een grote hoeveelheid foto's en video's, waardoor het opslaggebruik snel kan oplopen. Door het commando `$ df -h` is te zien dat 27G – oftewel 57% – van de totale 49G wordt gebruikt:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        49G   27G   21G  57% /
```

Bij nader onderzoek is te zien dat de directory die gebruikt wordt voor statische bestanden (waar ook de geüploade bestanden in zitten) maar `278M` in beslag

neemt, dus er is nog veel ruimte (21G) voor uitbreiding in dit aspect en zal voor een redelijk lange tijd geen probleem vormen:

```
root@developers:/etc/developers.nl# du -shc ./static/
278M        ./static/
```

Omdat 27G nogal veel leek voor wat er op de server draait is er onderzoek uitgevoerd naar de oorzaak. Het blijkt dat er veel ongebruikte oude Docker volumes en images op de server staan. Na een `$ docker system prune --volumes` en een `$ docker image prune -a` is er 14G vrijgemaakt:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        49G   13G   34G  28% /
```

Qua functionele schaalbaarheid is dit dus een verbeterpunt. Oude volumes, maar voornamelijk images moeten automatisch worden opgeschoond.

Een andere factor zou kunnen zijn dat de rate-limits van externe API's wordt bereikt. De twee externe API's die nu worden gebruikt zijn `meetup.com` voor de TechNights en `bullhorn.com` voor de vacatures. Voor Bullhorn heeft Developers.nl de "Enterprise Edition", dit betekend dat Developers.nl 50 API sessies tegelijk kan hebben, en maximaal 2.000.000 calls per dag heeft. Aangezien de website niet dichtbij deze getallen komt, en hoogstwaarschijnlijk op lange termijn niet gaat halen, zit dit goed. Toch worden de responses gecached in Redis waardoor de calls nog minder zullen zijn. Voor de API van Meetup zijn er maximaal 200 requests per uur en maximaal 200 results per request. Ook dit verkeer heeft de website voorlopig nog niet, maar om toch zeker te zijn dat dit niet wordt bereikt worden ook deze responses in Redis opgeslagen. De cachemethode is generiek genoeg opgezet waardoor het voor toekomstige API's ook kan worden toegepast.

Om de schaalbaarheid nog verder te analyseren is een SWOT analyse uitgevoerd op basis van de aanbeveling van Weinstock en Goodenough.

Strengths

- Stateless processes
- Concurrency
- Disposability

Weaknesses

- De hoeveelheid opslag
- Piekmomenten in de hoeveelheid verkeer
- Nog geen manier van automatisch schalen geïmplementeerd

Opportunities

- Het daadwerkelijk schalen door middel van container orchestration

Threats

- De hoeveelheid onderhoud die een nieuwe schaalstrategie met zich mee brengt.

5.2.4 Onderhoudbaarheid

De definitie van onderhoudbaarheid waarvan wordt uitgegaan in dit onderzoek luidt als volgt: "The degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements". Om de onderhoudbaarheid van de huidige infrastructuur te analyseren worden de vijf subcategorieën van ISO-25010 [34]; Modulariteit, Herbruikbaarheid, Analyseerbaarheid, Wijzigbaarheid en Testbaarheid individueel behandeld.

Modulariteit

De mate waarin een systeem of computerprogramma opgebouwd is in losstaande componenten zodat wijzigingen van een component minimale impact heeft op andere componenten.

De website van Developers.nl is opgebouwd in twee applicaties, de Node & React front-end samen met de PHP & Symfony back-end. Een wijziging in één van de API endpoints van de back-end zou kunnen betekenen dat de front-end breekt. Om dit te voorkomen is een versioning systeem [1] geïmplementeerd waardoor er zonder problemen individueel de front-of back-end gedeployed kan worden.

Voor de 15-Factor App geldt Factor 1 **(One codebase, one application)**, 3 **(Dependency management)** en 8 **(Backing services)**. Factor 1 vereist dat er per applicatie één enkele codebase is. De huidige situatie is dat er één repository is voor de back-end van de website, één voor de front-end van de website, en één voor het EMS. De regel wordt gebroken omdat het opbouwen van de infrastructuur met Ansible op elke repository voorkomt. Om aan Factor 3 te voldoen wordt Composer gebruikt voor het managen van de dependencies. Daarnaast worden waardes als de database host of het Redis adres in environment variabelen opgeslagen, waardoor factor 8 wordt voldaan. Om dit te implementeren worden backing services gedefinieerd als een handle, deze ziet er voor de database als volgt uit:

```
postgresql://username:password@developers.nl/database
```

[1] Voor de API wordt FOSRestBundle gebruikt, deze heeft een eigen implementatie van versioning, zie: https://symfony.com/doc/master/bundles/FOSRestBundle/versioning.html

Herbruikbaarheid

De mate waarin een bestaand onderdeel gebruikt kan worden in meer dan één systeem of bij het bouwen van een nieuw onderdeel.

Hoewel de Docker containers en Ansible infrastructuur generiek zijn opgesteld zijn er toch specifieke aanpassingen voor de website en voor het EMS. Dit betekent dat de PHP Docker image van de website niet precies gelijk is aan de PHP Docker image voor het EMS. Ook is de door-Ansible-opgebouwde infrastructuur nog niet herbruikbaar voor meerdere projecten, aangezien het in dezelfde codebase zit als de applicatie.

Analyseerbaarheid

De mate waarin het mogelijk is om effectief en efficiënt de impact, van een geplande verandering van één of meer onderdelen, op een product of systeem te beoordelen, om afwijkingen en/of foutoorzaken van een product vast te stellen of om onderdelen te identificeren die gewijzigd moeten worden.

Voor de 15-Factor App geldt Factor 6 **(Logs)**, 10 **(Administrative processes)** en 14 **(Telemetry)**. Voor factor 6 is het belangrijk dat alle relevante logs naar de `stdout` worden gestuurd, dit gebeurt voor alle containers. Hierdoor zijn de logs gemakkelijk te bereiken via `$ docker logs <container>` . Voor factor 10 moeten alle "administrative processes" als individuele processen gedraaid worden. Deze processen als bijvoorbeeld database migrations zijn een simpel commando. In het geval van database migrations is dit `$ bin/console doctrine:migrations:migrate` [2]. Deze commando's worden meegenomen bij het bouwen van de Docker image waardoor het automatisch wordt uitgevoerd, maar wél als een apart proces. Factor 14 vertelt dat de applicatie voldoende gemonitord moet worden. Er zijn voor zowel het EMS als de website geen monitoring tools in gebruik voor performance. Wel is Sentry geïmplementeerd, een monitoring tool die gericht is op errors.

Wijzigbaarheid

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden zonder fouten of kwaliteitsvermindering tot gevolg.

Voor de 15-Factor app geldt Factor 4 **(Design, build, release and run)**, 9 **(Environment parity)** en 11 **(Port binding)**. Factor 4 is volledig van kracht, allereerst is de design fase het beslissen wat voor features er in de volgende release komen. De build stage is het bouwen van de Docker images om die klaar te maken voor de volgende fase – release – waar de Docker images in de environment worden geplaatst en uiteindelijk voor de laatste fase gerund worden. Factor 9 vereist dat verschillende environments als development, test en productie zo gelijk mogelijk aan elkaar zijn. Docker maakt dit een stuk gemakkelijker, en is geïmplementeerd in zowel het EMS als de website. De verschillen tussen environments zijn minimaal.

[2] Dit is onderdeel van de DoctrineMigrationsBundle, zie:
https://symfony.com/doc/master/bundles/DoctrineMigrationsBundle/index.html
voor meer informatie.

Factor 11 vereist dat applicaties services via port binding exporteren. Voor PHP is dit niet de best ondersteunde manier van werken [51]–[53], aangezien PHP ontworpen is om een webserver te gebruiken. Er is wel een library voor beschikbaar genaamd ReactPHP, maar dit is redelijk onbekend en heeft dus als gevolg niet voldoende ondersteuning om PHP-FPM samen met Nginx weg te concurreren. Hierdoor zou het gebruik van port binding met PHP de onderhoudbaarheid juist verlagen.

Testbaarheid

De mate waarin effectief en efficiënt testcriteria vastgesteld kunnen worden voor een systeem, product of component en waarin tests uitgevoerd kunnen worden om vast te stellen of aan die criteria is voldaan.

Er is een implementatie om test-coverage te visualiseren, maar er is niks in de ontwikkelstraat dat ervoor zorgt dat de coverage minimaal hetzelfde blijft.

5.3 Conclusie

Om de deelvraag "Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?" te beantwoorden zijn door dit onderzoek meerdere punten van verbetering gevonden. Een verbeterpunt in de schaalbaarheid is de hoeveelheid opslag van de server. Deze kan snel vol raken door ongebruikte Docker volumes en images die ontstaan bij een deployment.

Ook wordt factor 1 **(One codebase, one application)** van de 15-Factor App niet volledig opgevolgd. De infrastructuur wordt op meerdere plekken opgebouwd en zou netter staan in een aparte codebase. De applicaties voldoen aan factor 13 (Concurrency) maar er wordt nog geen gebruik van gemaakt.

Factor 11 **(Port binding)** is voor PHP geen goed idee aangezien PHP juist ontworpen is om een webserver ervoor te hebben, dit verslechtert dus juist de onderhoudbaarheid. Er zijn voor zowel het EMS als de website geen monitoring tools in gebruik voor performance, dat betekend dat factor 14 **(Telemetry)** beter kan. Er is geen concrete manier om tests uit te voeren of aan testcriteria is voldaan. Hierdoor is de Testbaarheid van de systemen minimaal.

Hoofdstuk 6

Verbeteringen

Dit hoofdstuk gaat over de deelvraag "Wat voor verbeteringen ten aanzien van schaal- en onderhoudbaarheid kunnen worden toegepast op de huidige websites van Developers.nl?". Gebaseerd op de conclusie uit hoofdstuk 5 en de requirements van Developers.nl zijn verschillende technieken onderzocht om de gevonden verbeterpunten te verbeteren. Daarna zijn deze gevonden technieken op prioriteit geordend door middel van de requirements.

6.1 Feature-environments

Met feature-environments is het mogelijk om een staging-omgeving te creëren voor elke individuele feature branch. Dit betekent dat de product owners en developers elke feature afzonderlijk van andere features kunnen testen, om deze daarna naar productie te deployen. Deze manier van werken kan het ontwikkelproces erg versnellen, waardoor de onderhoudbaarheid verbeterd wordt. Ook betekenen feature-environments dat de applicatie schaalbaar moet zijn, dit heeft te maken met het feit dat de applicatie meerdere instanties van zichzelf moet kunnen draaien. Oftewel; horizontaal moet kunnen schalen. De feature-environment workflow is niet erg conventioneel of populair, aannemelijk omdat het niet gemakkelijk is om te implementeren. De meest relevante informatie voor dit onderzoek is een blog van Christian Lüdemann [54], hoewel de implementatie niet past bij de huidige situatie van Developers.nl. Uit onderzoek over verschillende technieken zijn de volgende opties gekomen:

- Een Kubernetes cluster met individuele namespaces voor elke environment.
- Tools als `https://platform.sh/` of `https://continuouspipe.io/` .
- Een dynamische reverse proxy die requests naar verschillende docker netwerken stuurt.
- Een dynamische reverse proxy die requests naar verschillende aparte VM's stuurt die gemanaged worden met Proxmox, of een cloud provider.

Een kubernetes cluster net namespaces valt af, dit heeft te maken met het onderhoudswerk van een cluster. Meer hierover is te lezen in paragraaf 6.4. Ook Docker Swarm is geen optie, Swarm heeft geen equivalent van kubernetes namespaces en er kunnen niet meerdere nodes op één machine staan. Tools als Platform.sh of Continuouspipe.io hebben een geïntegreerde oplossing voor feature

environments, maar voegen veel overhead toe. Bovendien kost Platform.sh geld, waar Developers.nl het niet voor over heeft.

Er zijn twee opties voor het maken van feature environments met een reverse proxy. Het gebruik maken van aparte VM's versus het aanmaken van docker netwerken. Het zusterbedrijf van Developers.nl – gemvision – maakt gebruik van Proxmox om hun Virtual Machines te beheren. Hoewel Proxmox een goede tool is om de VM's te beheren, is het echt gebaseerd op enterprise settings. Dit maakt het lastiger voor andere ontwikkelaars om goed gebruik te maken van deze tool. Aangezien Docker netwerken al geïntegreerd zijn in Docker voegt deze oplossing veel minder overhead toe. Dit is dus de beste optie. Er zijn verschillende reverse proxies. Relevante voor dit project zijn:

- Traefik
- jwilder/Nginx-Proxy
- HAProxy

Elke reverse proxy heeft zijn voor- en nadelen. De Website en het EMS maken al gebruik van Nginx als FastCGI webserver voor PHP-FPM. Daarom is nginx-proxy een interessante optie[1]. Nginx-proxy is een abstractielaag boven Nginx die gebruik maakt van de Docker socket om op die manier requests naar de juiste plek te sturen. Het nadeel is dat Nginx hier niet expliciet voor bedoeld is, waardoor een aantal tekortkomingen aanwezig zijn, zoals ondersteuning voor Docker Swarm[2]. Traefik werkt goed samen met Docker (swarm), aangezien Traefik ingebouwde service-discovery heeft voor docker containers en Let's Encrypt. Bovendien heeft Traefik een minder steile learning curve door de aanwezige documentatie. Het nadeel is dat het meer overhead creëert doordat het een compleet aparte en nieuwe tool is die moet worden toegevoegd. Dit nadeel is ook aanwezig bij HAProxy. HAProxy is snel en capabel voor load balancing, maar is complex om op te zetten zodra het op feature environments toekomt, omdat er geen ingebouwde service-discovery aanwezig is.

In het geval van Developers.nl is Traefik de beste optie, omdat het de minste complexiteit bevat en goed samen met Docker en Docker Swarm werkt. Een nadeel van de service-discovery oplossingen is dat de Docker Socket moet worden geëxposeerd. Dit is een groot beveiligingslek[3]. Zodra een hacker met kwaadaardige intenties Traefik weet te kapen betekent dat dat de hacker root toegang heeft op de host machine. Een oplossing hiervoor is het exposen van de Docker Socket door het Transmission Control Protocol (TCP) en deze te beveiligen door middel van Transport Layer Security (TLS).

In bijlage C.2 zijn Slack conversaties met Jelle te vinden die te maken hebben met de feature environments, en over het beveiligen van de Docker socket.

6.2 Één generieke infrastructuur

One codebase, One application is Factor 1 van de 15-Factor App en zorgt voor herbruikbaarheid van ISO 25010. De huidige infrastructuur van de Website en het

[1] https://github.com/jwilder/nginx-proxy
[2] https://github.com/jwilder/nginx-proxy/issues/927
[3] https://github.com/containous/traefik/issues/4174

EMS wordt opgebouwd met Ansible. "Ansible is a radically simple IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs" [5]. Kort gezegd is Ansible een Configuration Management (CM) tool.

Zoals de structuur nu is opgebouwd word er voor elke applicatie een apart stuk IaC geschreven. Om modulariteit en herbruikbaarheid van ISO 25010 [34] te verbeteren is het mogelijk om één centrale, algemene infrastructuur repository te maken waar installaties (stukken code dus) als Docker of databases en user-management kunnen worden hergebruikt voor meerdere applicaties.

Andere IaC tools als Chef of Puppet, kunnen ook voor dit doeleinde worden gebruikt, maar aangezien Ansible al gebruikt wordt is het niet efficiënt om dit om te herschrijven naar iets anders. Het is mogelijk om nog een hoger level van abstractie toe te voegen door een IaC tool als Terraform te gebruiken om een machine in te richten.

6.3 Policy-as-Code

Developers.nl heeft in haar website al een aantal manieren om kwaliteit van code te waarborgen. Automatische unit, integration, functional en end-to-end tests. Er mist een manier om de infrastructuur te waarborgen op kwaliteit. Dit is een verplichtte requirement: "De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen". Door policies zijn er duidelijke standaarden waaraan moet worden voldaan. Policies kunnen in meerdere vormen voorkomen [55], waaronder:

- **Compliance Policies.** Deze policies verzekeren dat nieuwe toevoegingen voldoen aan standaarden als bijvoorbeeld AVG of SOC.
- **Security Policies.** Deze policies verdedigen de integriteit van de infrastructuur door bijvoorbeeld te verzekeren dat bepaalde poorten niet open staan.
- **Operational Excellence.** Deze policies voorkomen uitval of verslechtering van geleverde services, bijvoorbeeld door nieuwe configuratie te valideren.

Vóór Policy-as-Code (PaC) werden deze policies opgeschreven door iemand en handmatig gecontroleerd. De – nog vrij nieuwe – techniek PaC richt zich op het automatiseren van dit proces door policies te kunnen definiëren in de vorm van code.

De techniek zorgt ervoor dat configuratie getest kan worden op kwaliteit. Daarnaast komt het voordeel dat de policies opgeslagen kunnen worden in versiebeheer. Hierdoor kunnen de policies ook worden hergebruikt. Dit sluit goed aan met de huidige Infrastructure-as-Code (IaC) oplossing die Developers.nl gebruikt voor het inrichten van haar servers.

Het automatiseren van deze kwaliteitscontroles verhoogt de onderhoudbaarheid aanzienlijk. Als we uitgaan van de ISO-25010 definitie van onderhoudbaarheid [34] zorgt het omzetten van een handmatige naar een geautomatiseerde controle voor betere **analyseerbaarheid** op veranderingen van de systemen, omdat afwijkingen en/of fouten gemakkelijker worden vastgesteld. Daarnaast zijn policies in

principe testcriteria, waardoor als gevolg ook de **testbaarheid** van de systemen stijgt bij het implementeren van policies as code. Ook zorgen policies voor **wijzigbaarheid**, aangezien het systeem gewijzigd kan worden zonder fouten of kwaliteitsverminderingen als gevolg omdat het simpelweg niet geïmplementeerd mag worden zodra een wijziging niet aan een policy voldoet. Bovendien zijn security policies handig voor het beschermen van de gevoelige data die het EMS bevat.

Er zijn twee technieken om PaC te implementeren. HashiCorps "Sentinel" en "Open Policy Agent" (OPA). In verband met de reden dat Sentinel closed-source is, is OPA de betere keuze. Dit past beter bij de bedrijfscultuur, slogan en budgetwensen van Developers.nl. Ook is Sentinel alleen toepasbaar op hashiCorp producten, waardoor de techniek een stuk beperkter is.

6.4 Container Orchestration

Om gebruik te maken van Factor 13 **(Concurrency)** moet de applicatie horizontaal en verticaal kunnen schalen. Dit heeft ook te maken met de should-requirement "De oplossing moet de website horizontaal kunnen laten schalen bij een toe- of afnemende hoeveelheid". Omdat de systemen bij Developers.nl op Docker containers draaien moet er een manier zijn om deze te beheren. "Container orchestration" platforms helpen bij het automatiseren van alle aspecten behorend bij het beheren van containers. Dit doen zij door meerdere containers als één entiteit te beschouwen – voor doeleinden van beschikbaarheid, schaalbaarheid, netwerken en de initiële containerimplementatie [56].

Er zijn twee technieken voor container orchestration leidend in de context van Docker, namelijk Docker Swarm of Kubernetes (K8s). Over het algemeen is Swarm een stuk gemakkelijker en minder complex dan K8s. Dit zou betekenen dat als er rekening word gehouden met onderhoudbaarheid, swarm de beste keuze is om te gebruiken. Maar om de grootste hoeveelheid controle over de containers te hebben is K8s de juiste tool. Ook wordt K8s beter ondersteund door cloud providers doordat AWS, GCP, en Azure een speciale service bieden om K8s toe te passen. Dit heeft te maken met het feit dat de community van K8s ook een stuk groter is vergeleken met Swarm. Het is wel mogelijk om Swarm te gebruiken met de cloud services maar het er is geen out-of-the-box service zoals er bij K8s wel is.

Als er gekeken wordt naar de wensen van Developers.nl en de scope van dit onderzoek is Swarm de meest passende keuze. De meeste prioriteit qua schalen gaat niet specifiek naar het automatiseren en managen van hoge hoeveelheden verkeer maar naar het draaien van meerderen omgevingen naast elkaar, om zo verschillende features apart te deployen of A/B te testen.

6.5 Opschonen Docker images

De Docker images moeten automatisch worden opgeschoond om de functionele schaalbaarheid te verbeteren. Dit is mogelijk om periodiek uit te voeren met een `systemd` timer of een `cron job` , maar omdat Developers.nl al gebruik maakt

van Ansible in hun websites kan het gemakkelijk geïmplementeerd worden met een Ansible taak die bij elke deployment gebruik maakt van de `docker_prune` module.

6.6 Logging & Monitoring

Logging en monitoring is een verplichtte requirement vanuit Developers.nl. Uit onderzoek in hoofdstuk 5 blijkt dat Telemetry, Factor 14 van de 15-Factor app nog aan verbetering toe is. [43] noemt drie verschillende categorieën van data om te monitoren in een applicatie:

- Application performance monitoring (APM)
- Domain-specific telemetry
- Health and system logs

Om de juiste keuze van monitoring tool te maken is het belangrijk om te specificeren wat Developers.nl graag gemonitord ziet worden. Na een overleg met Jelle is besloten om te beginnen met APM als de hoeveelheid CPU/geheugen dat wordt gebruikt. Om dit te realiseren kan een tool als Prometheus samen met Grafana worden gebuikt, waardoor het erg simpel is om in de toekomst de hoeveelheid en soort data dat wordt gemonitord uit te breiden.

6.7 Codecov

Om de testbaarheid te verbeteren moet een tool worden gebruikt om de testcoverage van nieuwe toevoegingen te waarborgen. De meest prominente tool hiervoor is codecov. Het zorgt voor een duidelijk overzicht van de coverage tools en kan direct bij pull-requests nakijken of de nieuwe features wel voldoende zijn getest.

6.8 Prioriteiten

Om te beslissen welke verbeteringen geïmplementeerd worden voor dit onderzoek worden ze op prioriteit geordend door middel van ze onder de requirements te verdelen.

Must-requirements:

- De oplossing moet méér dan twee unieke instanties van de website naast elkaar kunnen draaien.
  - Feature Environments
- De oplossing moet moet unieke instanties van de website automatisch kunnen aanmaken.
  - Feature Environments
- De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen.

  - Policy-as-code
  - Codecov
- Minimaal één monitoring tool voor het monitoren van performance.
  - Logging & Monitoring
- De oplossing moet voldoen aan één of meerdere kwaliteitsstandaarden.
  - Opschonen Docker images
  - Logging & monitoring

Should-requirements:

- De oplossing moet generiek genoeg zijn zodat meerdere applicaties er gebruik van kunnen maken.
  - Generieke infrastructuur
- De oplossing moet de website horizontaal kunnen laten schalen bij een toe- of afnemende hoeveelheid verkeer. De efficiëntie moet 1:1 zijn. Bijvoorbeeld: Één extra instantie moet 50% van het verkeer opvangen.
  - Container orchestration

Hier is de volgende prioriteitvolgorde uit op te maken:

1. Feature Environments
2. Logging & Monitoring
3. PaC – Codecov – Opschonen Docker images
4. Generieke infrastructuur – Container orchestration

6.9 Conclusie

Om de kenmerken modulariteit en herbruikbaarheid van ISO 25010 te verbeteren kan er een centrale infrastructuur IaC repository gemaakt worden met Ansible. Om de kenmerken analyseerbaarheid, testbaarheid en wijzigbaarheid te verbeteren kunnen policies worden afgedwongen door middel van PaC. Om de testbaarheid te waarborgen kan een tool als Codecov worden gebruikt. Om onderhoudbaarheid te verbeteren en schaalbaarheid te bewijzen is het concept van feature-environments erg geschikt. Developers.nl ziet dit concept graag in de praktijk, dit heeft dan ook de hoogste prioriteit als uitkomst van dit onderzoek.

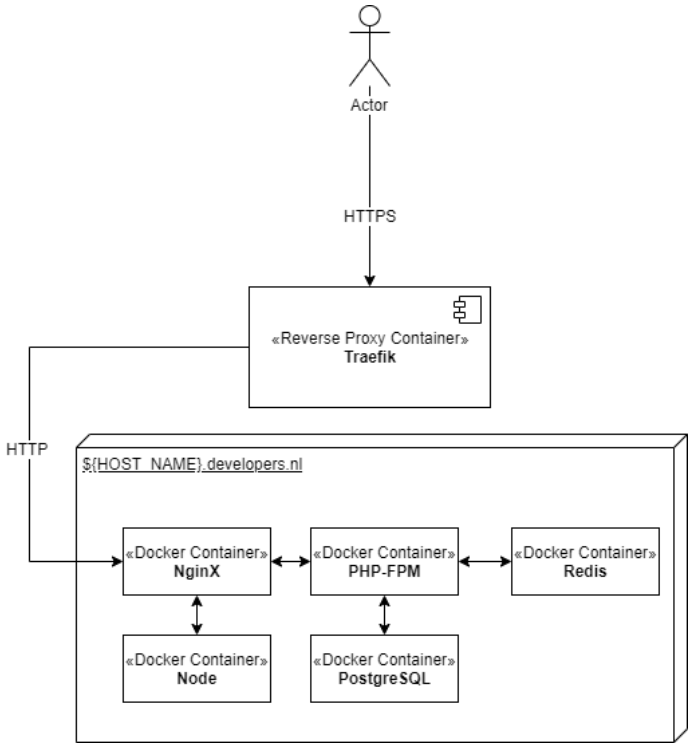
Hoofdstuk 7

Implementatie

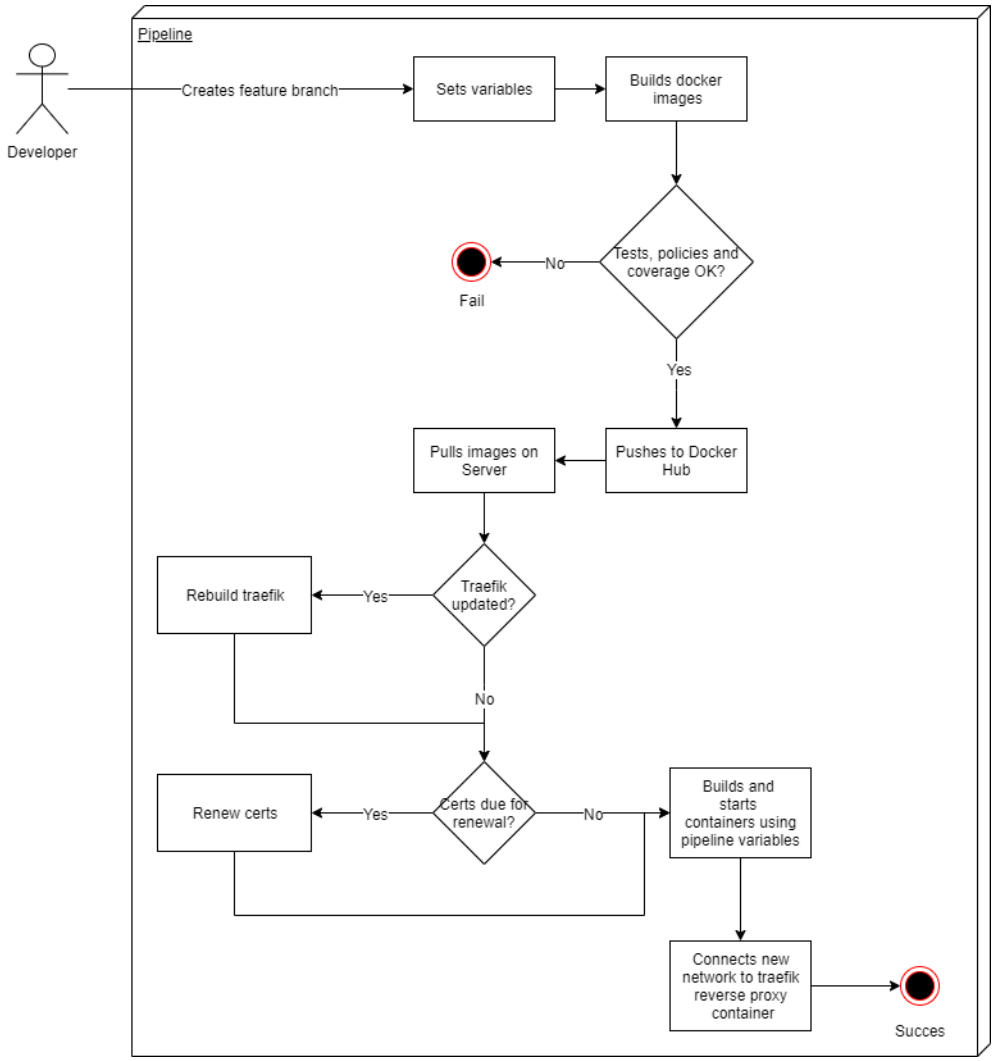
Dit hoofdstuk gaat over de deelvraag “Hoe kunnen de gekozen verbeteringen ten aanzien van schaal- en onderhoudbaarheid geïmplementeerd worden?”. In dit hoofdstuk staat de bijbehorende gedachtegang met referenties naar de code en ontwerpen in bijlage A.

7.1 Feature-environments

Alle code en ontwerpen zijn te vinden in bijlage A.6. Om te helpen met de ontwikkelfase en documentatie zijn allereerst twee diagrammen ontworpen. Een component diagram voor de Docker containers samen met de reverse proxy (figuur 7.1). Dit is een bijgewerkte versie van figuur 5.1. Daarnaast is een activity diagram ontworpen om de deployment workflow te visualiseren (figuur 7.2).



FIGUUR 7.1: Nieuwe infrastructuur met Traefik reverse proxy



FIGUUR 7.2: Activity Diagram voor de pipeline

Hierna is de Docker opstelling gemaakt voor Traefik. De bestaande drie Docker-compose bestanden zijn aangepast door de Nginx service labels te geven die zorgen voor de service-discovery van Traefik. Vervolgens zijn basis, productie, en development docker-compose bestanden aangemaakt voor Traefik. Het afhandelen van SSL in development gebeurt niet meer via Nginx maar via Traefik, daarom is de development_ssl service hier naar verplaatst. Deze service is tevens ook aangepast om wildcard certificaten te genereren, en niet meer afhankelijk te zijn van een image uit een derde partij. Hierdoor is ook de Nginx configuratie aangepast om de afhandeling van SSL niet meer te ondersteunen. Ook is een configuratiebestand voor traefik toegevoegd voor de TLS instellingen. Om de development omgeving te ondersteunen is de Makefile bijgewerkt en een script gemaakt om de omgeving op te zetten. Dit script gebruikt de development Docker-compose bestanden om de containers te draaien en verbind vervolgens Nginx met Traefik.

Traefik runt standaard als root, dit is geen best-practice voor het gebruiken van Docker Containers [57]. Daarom is een Dockerfile toegevoegd die verder bouwt op de Traefik image. Deze dockerfile maakt een user en group aan om deze vervolgens te gebruiken om het proces mee te runnen. Deze user en group komen overeen

met users op de host machine, waardoor deze rechten heeft tot de Docker client certificaten.

Vervolgens is er een Ansible role ontwikkeld om de Docker Daemon te beveiligen via TLS[1]. Om te helpen bij de ontwikkeling is eerst een Vagrantfile toegevoegd om met Virtualbox lokaal de Ansible role te kunnen testen. Deze role genereert een Certificate Authority (CA), server, en client keys door middel van OpenSSL. Ook zorgt deze role er voor dat de Docker Daemon correct is ingesteld om deze certificaten te kunnen gebruiken, en dat de permissions van alle bestanden juist zijn ingesteld. De `daemon.json` wordt gevuld met variabelen uit Ansible door middel van een Jinja2 template. Er wordt gebruik gemaakt van Ansible-Vault om de passphrase van de certificaten veilig op te slaan.

Om de implementatie te deployen naar productie zijn de bestaande Ansible roles aangepast om gebruik te maken van de Traefik proxy en beveiligde Docker Daemon. In de `frontend-images` role is de Dockerfile toegevoegd met de relevante build arguments. De frontend role haalt de environment variabelen uit de Bitbucket Pipeline en parsed deze om zo de correcte subdomein, Fully Qualified Domain Name (FQDN), en network name te registreren. Deze worden gebruikt als variabelen in de docker-compose bestanden om zo de correcte subdomeinen aan te maken. Vervolgens worden de containers gebuild en Nginx aan de Traefik en PHP-FPM containers verbonden. Zodra de naam van de git branch geen "Feature/WEB-" bevat wordt er geen aparte feature-environment gebruikt voor de deployment.

De Bitbucket Pipeline is aangepast om Traefik te updaten bij een deployment of bootstrap.

7.2 Codecov

Code voor het implementeren is te zien in bijlage A.5. De README is bijgewerkt, Bitbucket en codecoverage environment variabelen moesten worden doorgegeven door build arguments. Het builden van de Docker images gebeurt met Ansible. In de php7-fpm dockerfile zijn de build args omgezet naar environment variablen, een aantal apk packages toegevoegd en is het codecov script toegevoegd. Er is een script geschreven om pcov te installeren zodat dit kan hergebruikt worden zowel in de 'develop.sh' entrypoint als in de test-stage van de dockerfile.

Om BitBucket een betere ondersteuning te geven met codecov is hier ook een Pull-Request naar codecov-bash gemaakt. Deze is te zien op:
`https://github.com/codecov/codecov-bash/pull/225` . De maintainers van codecov waren tevreden met deze verbeteringen en hebben de Pull-Request geaccepteerd en gemerged.

[1]https://github.com/ansible/role-secure-docker-daemon is gebruikt voor inspiratie, maar omdat dit project erg verouderd is, is besloten om een verbeterde versie te ontwikkelen.

7.3 Opschonen Docker images

In het bestand `developers.nl/ansible/group_vars/all.yml` is een variabele geplaatst om de images te filteren, images die ouder zijn dan 4 uur worden verwijderd.

```
image_delete_until_time: 4h
```

In `developers.nl/ansible/deploy.yml` is een ansible taak geplaatst die gebruik maakt van de `docker_prune` module, om zo alle dangling images te verwijderen.

```
- name: "Clean up images older than {{ image_delete_until_time }}"
  docker_prune:
    images: yes
    images_filters:
      dangling: false
      until: "{{ image_delete_until_time }}"
  register: prune_result
```

7.4 Policy as Code

Implementatie van Open Policy Agent staat in Bijlage A.8. Er zijn verschillende locaties waar policies afgedwongen kunnen worden; build-time en run-time. Build-time policies kunnen bijvoorbeeld pipelines laten failen zodra er Docker images gebouwd worden met incorrecte poorten of met niet-toegestane users. Run-time policies kunnen draaiende containers evalueren of users managen. Voor deze eerste opzet wordt gekeken naar de user die een Docker commando uitvoert. Dit mogen alleen `runuser` , `developer` of `root` zijn.

Voor het evalueren van build-time policies wordt gebuik gemaakt van de `openpolicyagent/opa` Docker image die het `eval` commando gebruikt. Deze container wordt gebuild in de Ansible role die alle Docker images voor de website build. Dit gebeurt door middel van de Ansible `docker_container` module. Deze task faalt zodra de text `"allow": true` niet in de container stdout voorkomt. Voor deze eerste opzet is een policy aangemaakt die evalueert of 1 gelijk is aan 2. Als dat zo is, faalt de pipeline.

De run-time policy is geplaatst in de Ansible `secure-daemon` role. Meer over deze role is te vinden in paragraaf 7.1. Deze role configureert de Docker Daemon van verschillende users door een `config.json` te plaatsen in de home directory van de toegestane users. De JSON wordt gevuld met variabelen uit Ansible, door middel van een Jinja2 template. Deze configuratie stuurt een HttpHeader mee met uitgevoerde Docker commando's die OPA vertelt wie de uitvoerende user is. OPA evalueert hierna of deze user rechten heeft om dit commando uit te voeren door middel van de `openpolicyagent/opa-docker-authz` Docker plugin. Om Traefik toegang te geven tot Docker is ook toestemming gegeven aan requests die via TLS gaan, en de subject common name `client` hebben.

7.5 Logging & Monitoring

Bij de implementatie van Prometheus blijkt dat er twee dingen moeten gebeuren voordat Prometheus correct kan werken in productie.

1. De Docker Daemon moet in "experimental" mode draaien
2. Docker moet in Swarm mode draaien

Docker raad het volgende aan [58]: "Experimental features must not be used in production environments". Verder draait de website (nog) niet in Swarm mode. Door deze is het verstandig om te wachten met de implementatie van Prometheus. Wel is Grafana geïmplementeerd door gebruik te maken van de Grafana Docker image en labels toe te voegen waardoor Traefik weet waar de request heen moet. Traefik maakt een subdomein aan op `grafana.<root_server_name>` . De implementatie staat in bijlage A.7.

7.6 Conclusie

er zijn vijf technieken geïmplementeerd: Feature-environments, Codecov, Opschonen van Docker images, Open Policy Agent, en Grafana.

Codecov is in de back-end van de website geïmplementeerd om coverage te visualiseren op Pull-Requests, het genereren hiervan gebeurt in de `php7-fpm` Dockerfile in een test-buildstage.

Docker images worden opgeschoond door middel van de Ansible `docker_prune` module. Deze ruimt images ouder dan 4 uur op bij elke deployment.

De implementatie van Feature-environments heeft de basis gelegd voor een aantal opvolgende implementaties. Het heeft de infrastructuur, pipeline, en workflow veranderd door Traefik – een reverse proxy – te implementeren die er voor zorgt dat meerdere individuele omgevingen naast elkaar kunnen draaien, die te bereiken zijn door subdomeinen. Ook beveiligt het de Docker Socket door het met TLS te encrypten.

De implementatie van Policy-as-Code gaat verder op de beveiliging van de Docker Socket in en gebruikt Open Policy Agent om de users van docker commando's te limiteren. Ook staat er een opzet voor het evalueren van build-time policies.

Verder wordt Traefik gebruikt om Grafana – een monitoring dashboard – te exposen op een subdomein.

Hoofdstuk 8

Requirements

Dit hoofdstuk gaat over de deelvraag "Voldoen de verbeteringen aan de vereiste requirements?". De must-requirements worden per paragraaf behandeld om zo individueel te beoordelen of de implementaties adequaat zijn.

8.1 Unieke instanties van de website naast elkaar

De opstelling van de reverse proxy door middel van Traefik maakt het mogelijk om requests te verdelen over docker containers in aparte netwerken. Omdat deze containers in aparte netwerken zitten is het mogelijk om oneindig veel unieke instanties van de website naast elkaar te draaien. Deze requirement is behaald.

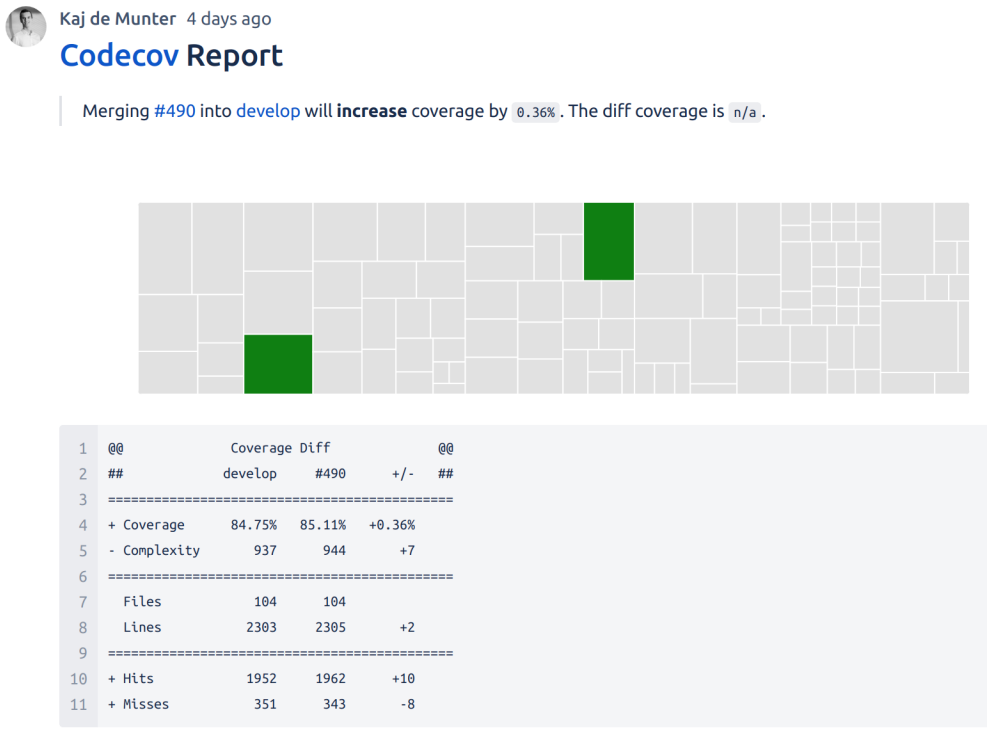
8.2 Unieke instanties van de website automatisch kunnen aanmaken

Door de Bitbucket-Pipeline en de ansible roles voor het beveiligen van de Docker Daemon, en het Deployen van de applicatie worden deze unieke instanties automatisch gedeployed naar een server. Deze instanties zijn dan bereikbaar via `<subdomein>.developers.nl` of `<subdomein>.test.developers.nl`.

De enige tekortkoming is dat de instanties van de website nog niet automatisch worden verwijderd zodra een branch gemerged wordt. Deze requirement is tot op zekere hoogte behaald, maar er is nog ruimte voor verbetering.

8.3 Kwaliteitswaarborging

Om kwaliteit van code te waarborgen is Codecov geïmplementeerd. Codecov zorgt ervoor dat er niet gemerged kan worden via een Pull Request zodra de code coverage van de tests niet voldoende is. Zie figuur 8.1.



Kaj de Munter 4 days ago

Codecov Report

Merging #490 into develop will **increase** coverage by `0.36%`. The diff coverage is `n/a`.

```
@@             Coverage Diff             @@
##            develop     #490      +/-   ##
==========================================
+ Coverage      84.75%   85.11%   +0.36%
- Complexity       937      944       +7
==========================================
  Files            104      104
  Lines           2303     2305       +2
==========================================
+ Hits            1952     1962      +10
+ Misses           351      343       -8
```

FIGUUR 8.1: Codecov bot reactie op een Pull-Request

Verder is er veel rekening gehouden met de beveiliging van de oplossing. Traefik draait niet als root in de container en de Docker Socket is beveiligd via TLS. Verder is OPA geïmplementeerd om beveiliging te waarborgen door middel van het limiteren van users die Docker commando's kunnen gebruiken. Ook is er een opzet gemaakt dat policies build-time kan evalueren zodat kwaliteit afgedwongen kan worden vóórdat het wordt gedeployed. Deze requirement is behaald.

8.4 Monitoren van performance

De implementatie van Grafana betekent dat er data uit allerlei verschillende databases gevisualiseerd kan worden. In dit onderzoek is als eerst besloten dat Prometheus een goede tool is om metrics te verzamelen. Uiteindelijk is geconcludeerd dat dit geen goede optie is. Daarom is de optie van monitoring vrijgesteld, maar er wordt nog niks daadwerkelijk gemonitord. Deze requirement is niet volledig behaald, daarom is er een aanbeveling gemaakt.

8.5 Kwaliteitsstandaarden

Door het monitoren van performance is de factor Telementry van de 15-Factor App verbeterd. De factor One Codebase, One application is niet verbeterd tijdens dit onderzoek, maar door middel van een generieke ansible infrastructuur kan deze verbeterd worden. Testbaarheid van ISO 25010 is verbeterd door het toevoegen van Codecov.

Schalen in de context van horizontaal schalen is ook niet geïmplementeerd, maar door Feature-environments is wel bewezen dat de website schaalbaar is. Ook is advies uitgebracht over de methode van schalen door middel van de container orchestration tool Docker Swarm.

8.6 Conclusie

Must-requirements:

- De oplossing moet méér dan twee unieke instanties van de website naast elkaar kunnen draaien.
  - Behaald.
- De oplossing moet moet unieke instanties van de website automatisch kunnen aanmaken.
  - Behaald tot op zekere hoogte, de instanties kunnen nog niet automatisch worden verwijderd. Hier is een aanbeveling over gemaakt.
- De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen.
  - Behaald. Er is een aanbeveling gemaakt om hier verder op in te gaan.
- Minimaal één monitoring tool voor het monitoren van performance.
  - Niet volledig behaald. Grafana is geïmplementeerd om data te visualiseren, maar er is nog geen data.
- De oplossing moet voldoen aan één of meerdere kwaliteitsstandaarden.
  - Behaald, maar er zijn nog verbeteringen. Hier is een aanbeveling over gemaakt.

Over de Should, Could en Won't requirements zijn aanbevelingen gemaakt in hoofdstuk 9.

Hoofdstuk 9

Aanbevelingen

9.1 Cloud service providers

Momenteel worden de applicaties binnen Developers.nl gehost op een simpele, traditionele server van TransIP. Een overweging om te maken is of dit niet beter naar een cloud service provider kan worden verplaatst, aangezien dit mogelijk de onderhoudbaarheidslast verminderd. L. Wang *et al.* [59] definiëren cloud computing als "A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way". Volgens [60] zijn er drie verschillende categorieën van Cloud computing:

- Infrastructure as a Service (IaaS): Een virtueel aangeboden infrastructuur van rekenkracht en/of geheugen [61].
- Platform as a Service (PaaS): Een aangeboden platform voor ondersteuning van deployment, ontwikkelen en testen van applicaties [62].
- Software as a Service (SaaS): Een aangeboden (web)applicatie dat direct gebruikt kan worden [61].

Om te overwegen of een cloud provider bij de wensen van Developers.nl past worden de voor-en nadelen op een rijtje gezet:

Voordelen Cloud

De kosten van cloud hosting zijn flexibel, er wordt alleen betaalt voor wat er daadwerkelijk gebruikt wordt, zolang er maar verstandig gebruik van wordt gemaakt. Dit betekend dat het mogelijk erg kostenefficiënt kan zijn voor Developers.nl aangezien er tijdens de maandelijkse "Tech Nights" piekmomenten zijn op de website, en er heel weinig verkeer is op het EMS. Een ander voordeel is dat er bijna een ongelimiteerde hoeveelheid opslagruimte beschikbaar is. Aangezien het CMS van de website dubbel functioneert als "file-server" en er veel foto's worden geüpload is het fijn dat er geen rekening hoeft worden gehouden met de hoeveelheid opslag. Bovendien worden software updates automatisch uitgevoerd, software als K8s kunnen al inbegrepen zijn bij de infrastructuur en het maakt schalen gemakkelijker. Aangezien cloud providers meer middelen voor beveiliging hebben wordt de veiligheid ook een stuk verbeterd.

Voordelen traditioneel

Ook al is cloud hosting meer kostenefficiënt is het toch mogelijk dat een web host goedkoper uitkomt. Zolang er maar geen hoge piekmomenten zijn in het verkeer. Dit is dus niet van toepassing op Developers.nl aangezien de "Tech Nights" of andere evenementen voor piekmomenten zorgen.

Nadelen cloud

Cloud providers hebben de mogelijkheid voor technische problemen buiten de controle van klanten, waardoor het mogelijk is dat er downtime ontstaat. Ook kan het duurder uitpakken zodra er niet goed word omgegaan met de schaalstrategie of benodigde rekenkracht.

Nadelen traditioneel

De mogelijkheid bestaat dat er meer kosten worden gemaakt dan nodig is. Ook is shared-hosting een risico omdat zodra een andere klant veel rekenkracht opeist de kans ontstaat dat de prestaties dalen.

Aanbeveling

Er zijn veel verschillende cloud providers, waarvan de grootste Amazon Web Services (AWS), Microsoft Azure en Google Cloud Platform (GCP) zijn. Er moet onderzoek worden uitgevoerd over de kosten van het overstappen. Het is verstandig om samen met een migratie naar een cloud provider ook zaken mee te nemen als e-mail beheer in het bedrijf, of de inbegrepen software pakketen als Microsoft Office of Google Drive.

9.2 Serverless computing

Serverless computing is een "application defined as a set of event-triggered functions that execute without requiring the user to explicitly manage servers" [9].

In verband met de lage hoeveelheid verkeer op het EMS is "serverless computing" een goede oplossing om kosten te besparen.

9.3 Container Orchestration

Container Orchestration met Docker Swarm zou het mogelijk maken om de website op te schalen. Er is bewezen dat de website schaalbaar is, dus er zijn geen implicaties voorzien bij het implementeren. Wel moet er rekening gehouden worden met Traefik, en de integratie hiervan met Docker Swarm.

9.4 Één generieke infrastructuur

Het maken van een enkele ansible infrastructuur zou het concept "one codebase, one application" van de 15-factor app verbeteren. Ook zou dit onderhoudbaarheid verbeteren omdat nieuwe applicaties gelijk een infrastructuur op hoog niveau tot beschikking hebben.

9.5 Policies

Er moet onderzoek gedaan worden naar build- en run-time policies. Met Open Policy Agent is veel meer mogelijk dan wat er in dit onderzoek is geïmplementeerd. Bijvoorbeeld policies die kijken of een container niet als de `root` user draait of die evalueren of er geen onveilige poorten worden geopend.

Hoofdstuk 10

Conclusie

10.1 Verwachtingen

Developers.nl wilt onderhoudbaarheid bereiken door kwaliteitsstandaarden af te dwingen. Ook wilt Developers.nl twee soorten schaalbaarheid. Eén in de vorm van het deployen van verschillende branches in aparte omgevingen, en één in de vorm van horizontaal schalen om meer verkeer aan te kunnen. Deze twee soorten kunnen niet gerealiseerd worden zonder de onderhoudbaarheid te waarborgen. Er zijn vijf must-have requirements:

- De oplossing moet méér dan twee unieke instanties van de website naast elkaar kunnen draaien.
- De oplossing moet moet unieke instanties van de website automatisch kunnen aanmaken.
- De oplossing moet een methode bevatten om kwaliteit van nieuwe toevoegingen aan de infrastructuur automatisch te waarborgen.
- Minimaal één monitoring tool voor het monitoren van performance.
- De oplossing moet voldoen aan één of meerdere kwaliteitsstandaarden.

10.2 Technieken

De 12-Factor App is een methodologie die twaalf best-practices samenvoegt om moderne, schaal- en onderhoudbare web-applicaties te bouwen. Het boek “Beyond the 12-factor app” [43] is hierop verder gegaan door nog een drietal factoren toe te voegen. Door een applicatie te evalueren op deze vijftien factoren, samen met de definitie van ISO-25010 [34] is te beoordelen of deze schaal- en onderhoudbaar is. Om de schaalbaarheid van een systeem te waarborgen zijn de methoden van Weinstock en Goodenough [28] een geschikte manier.

10.3 Huidige situatie

Om de deelvraag “Hoe onderhoud- en schaalbaar zijn de huidige websites van Developers.nl met betrekking tot de relevante kwaliteitsstandaarden?” te beantwoorden zijn door dit onderzoek meerdere punten van verbetering gevonden.

Een verbeterpunt in de schaalbaarheid is de hoeveelheid opslag van de server. Deze kan snel vol raken door ongebruikte Docker volumes en images die ontstaan bij een deployment.

Ook wordt factor 1 **(One codebase, one application)** van de 15-Factor App niet volledig opgevolgd. De infrastructuur wordt op meerdere plekken opgebouwd en zou netter staan in een aparte codebase. De applicaties voldoen aan factor 13 (Concurrency) maar er wordt nog geen gebruik van gemaakt.

Factor 11 **(Port binding)** is voor PHP geen goed idee aangezien PHP juist ontworpen is om een webserver ervoor te hebben, dit verslechtert dus juist de onderhoudbaarheid. Er zijn voor zowel het EMS als de website geen monitoring tools in gebruik voor performance, dat betekend dat factor 14 **(Telemetry)** beter kan. Er is geen concrete manier om tests uit te voeren of aan testcriteria is voldaan. Hierdoor is de Testbaarheid van de systemen minimaal.

10.4 Verbeteringen

Om de kenmerken modulariteit en herbruikbaarheid van ISO 25010 te verbeteren kan er een centrale infrastructuur IaC repository gemaakt worden met Ansible. Om de kenmerken analyseerbaarheid, testbaarheid en wijzigbaarheid te verbeteren kunnen policies worden afgedwongen door middel van PaC. Om de testbaarheid te waarborgen kan een tool als Codecov worden gebruikt. Om onderhoudbaarheid te verbeteren en schaalbaarheid te bewijzen is het concept van feature-environments erg geschikt. Developers.nl ziet dit concept graag in de praktijk, dit heeft dan ook de hoogste prioriteit als uitkomst van dit onderzoek.

10.5 Implementatie

10.6 Requirements

Hoofdstuk 11

Reflectie

11.1 Literatuuronderzoek

Het theoretisch kader heeft geholpen bij het definiëren van schaalbaarheid, onderhoudbaarheid en architectuur. De meest nuttige definities waren schaal- en onderhoudbaarheid, de definitie van architectuur is niet vaak voorgekomen in het onderzoek. Ik merkte dat schaalbaarheid erg lastig was om te definiëren, omdat er erg veel verschillende interpretaties van waren. Daarom heb ik een poging gedaan om een concretere definitie te creëren, het inbrengen van een nieuwe definitie (functionele, en niet-functionele schaalbaarheid) lijkt mij een succes. Er is aardig wat discussie over ontstaan, en ik ben van mening dat ik mijn steentje heb bijgedragen bij het creëren van een algemene definitie van schaalbaarheid.

Ik heb iets te veel literatuuronderzoek gedaan, waardoor de uiteindelijke onderzoeksresultaten daar onder geleden hebben. Als ik hier iets minder op had gefocust was het opgeleverde Proof-of-Concept wellicht iets uitgebreider. Ook was de definitie van schaalbaarheid in de ogen van Developers.nl anders dan wat uit het literatuuronderzoek is gekomen. Wel heeft het theoretisch kader een daadwerkelijk stevige basis gelegd voor de rest van het onderzoek, het heeft voor een betere begripsvorming gezorgd waardoor ik helderder kon uitleggen waar het over ging. Verder was het combineren van de definities samen met de 15-Factor App erg nuttig.

11.2 Uitvoering

Ik had eerder moeten beginnen met het maken van concrete requirements. Dit had geholpen bij het onderzoek doordat het duidelijkere richtlijnen creëert. Onderzoek naar de technieken is goed verlopen, hierdoor kon de huidige situatie goed worden geëvalueerd en uiteindelijk kon er door middel van deze technieken worden gevalideerd of de situatie verbeterd is. Ik heb veel verbeteringen gevonden die mogelijk zijn om te implementeren.

Niet al deze verbeteringen zijn geïmplementeerd tijdens het onderzoek, in verband met tijdstekort. Ik had iets te veel hooi op mijn vork genomen waardoor veel verbeteringen alleen bleven bij een aanbeveling. De implementatie heeft iets langer geduurd dan verwacht, maar ik ben trots op het feit dat het toch gelukt is. Het was geen makkelijke opdracht aangezien de methode van feature-environments niet frequent wordt gebruikt door anderen, en Policy-as-Code een vrij nieuwe techniek is met weinig documentatie. Dit heeft er voor gezorgd dat ik veel geleerd heb.

11.3 Uitkomsten

Over het algemeen ben ik van mening dat dit onderzoek zeker de hoofdvraag adequaat heeft beantwoord. Er zijn veel punten van verbetering gevonden en er kan goed mee verder worden gewerkt in de toekomst. De implementatie van feature-environments had ik niet voor ogen toen ik aan het onderzoek begon, dit heeft mij aangenaam verrast.

Literatuurlijst

[1] P. S. S. GmbH. (2019). Proxmox - powerful open-source server solutions, [Online]. Available: https://www.proxmox.com/.

[2] AVINetworks. (2019). Service discovery definition, [Online]. Available: https://avinetworks.com/glossary/service-discovery/.

[3] The Linux Foundation. (2019). Production-grade container orchestration, [Online]. Available: https://kubernetes.io.

[4] Docker Inc. (2019). Enterprise container platform for high-velocity innovation, [Online]. Available: https://docker.com.

[5] Red Hat inc. (2019). How ansible works, [Online]. Available: https://www.ansible.com/overview/how-ansible-works.

[6] Amber Ankerholz. (Apr. 2016). 8 container orchestration tools to know, [Online]. Available: https://www.linux.com/news/8-open-source-container-orchestration-tools-know/.

[7] Nginx Inc. (2019). Nginx | high performance load balancer, webserver, and reverse proxy, [Online]. Available: https://nginx.com.

[8] HashiCorp Inc. (2019). Vagrant by hashicorp: Development environments made easy, [Online]. Available: https://vagrantup.com.

[9] A. Pérez, G. Moltó, M. Caballer, and A. Calatrava, "Serverless computing for container-based architectures", Feb. 2018. DOI: https://doi.org/10.1016/j.future.2018.01.022.

[10] A. M. Andreas Wittig, "Amazon web services in action", 2016. [Online]. Available: https://s3-ap-southeast-1.amazonaws.com/tv-prod/documents%2Fnull-Amazon+Web+Services+in+Action.pdf.

[11] Chef. (2019). Chef, [Online]. Available: https://chef.io.

[12] Puppet. (2019). Unparalleled infrastructure automation and delivery, [Online]. Available: https://puppet.com.

[13] HashiCorp. (2019). Introduction to terraform, [Online]. Available: https://www.terraform.io/intro/index.html.

[14] T. G. Peter Mell, "The nist definition of cloud computing", p. 1, Oct. 2011. DOI: https://doi.org/10.6028/NIST.SP.800-145. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[15] A. Wiggins, "The twelve-factor app", 2017. [Online]. Available: https://12factor.net.

[16] D. D. Gereld Weber, *Trends in Enterprise Application Architecture*. Feb. 2006, vol. 4437.

[17] P. Kruchten, "Architectural blueprints—the "4+1" view model of software architecture", pp. 42–50, Nov. 1995.

[18] Red Hat, Inc. (Dec. 2019). Templating (jinja2), [Online]. Available: https://docs.ansible.com/ansible/latest/user_guide/playbooks_templating.html.

[19] (Dec. 2019). Ansible vault, [Online]. Available: https://docs.ansible.com/ansible/latest/user_guide/vault.html.

[20] D. A. Wheeler, "Why open source software/free software (oss/fs)? look at the numbers", Nov. 2004. [Online]. Available: http://www.robotcub.org/index.php/robotcub/content/download/290/1049/file/Why%20Open%20Source%20Software.pdf.
[21] K. de Munter, "Stageplan en oriëntatie developers.nl", 2017.
[22] Developers.nl, "Positioneringsprofiel developers.nl", 2018.
[23] K. de Munter, "Afstudeervoorstel", 2019.
[24] M. D. Hill, "What is scalability?", vol. 18, pp. 18–21, 4 Dec. 1990. [Online]. Available: https://dl.acm.org/citation.cfm?id=121975.
[25] T. W. Leticia Duboc David S. Rosenblum, "A framework for modelling and analysis of software systems scalability", May 2006. [Online]. Available: http://discovery.ucl.ac.uk/4990/1/4990.pdf.
[26] A. B. Bondi, "Characteristics of scalability and their impact on performance", Sep. 2000. [Online]. Available: https://www.win.tue.nl/~johanl/educ/2II45/2010/Lit/Scalability-bondi%202000.pdf.
[27] M. A.-E.-B. Hesham El-Rewini, *Advanced computer architecture and parallel processing*. 2005.
[28] J. B. G. Charles B. Weinstock, "On system scalability", 2006. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7887.
[29] Magento. (2019). Extensibility and modularity, [Online]. Available: https://devdocs.magento.com/guides/v2.3/architecture/extensibility.html.
[30] A. L. Niklas Johansson, "Designing for extensibility: An action research study of maximizing extensibility by means of design principles", Jun. 2009. [Online]. Available: http://hdl.handle.net/2077/20561.
[31] A. A. T. Penny Grubb, *Software Maintenance: Concepts And Practice (Second Edition)*. River Edge, N.J.: World Scientific, 2003, vol. 2.
[32] IEEE, "Standard glossary of software engineering terminology", IEEE 610.12, 1990.
[33] J. K. C. Krishan K. Aggarwal Yogesh Singh, "An integrated measure of software maintainability", 2002. DOI: https://doi.org/10.1109/RAMS.2002.981648.
[34] ISO, "Software product quality", International Organization for Standardization, Geneva, CH, ISO 25010, 2011.
[35] S. T. Albin, *The art of software architecture: design methods and techniques*. Wiley Publishing, Inc., Indianapolis, Indiana, Mar. 2003, vol. 9, ISBN: 9780471468295.
[36] P. C. Len Bass, *Software Architecture in Practice*. Pearson Education (US), Sep. 2012, ISBN: 9780321815736.
[37] E. W. Nick Rozanski, *Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives*. Nov. 2011, ISBN: 9780132906074.
[38] R. K. Humberto Cervantes, *Designing Software Architectures: A Practical Approach*. Addison-Wesley Professional, 2016, ISBN: 9780134390789.
[39] IEEE, "Standard glossary of software engineering terminology", ISO/IEC/IEEE std. 42010, 2011.
[40] a. s. o. T. O. G. TOGAF® Standard Version 9.2, "Core concepts", 2018. [Online]. Available: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap02.html.
[41] H. van Vliet, *Software Engineering: Principles and Practice*. May 1993, vol. 3, p. 63, ISBN: 978-0470031469.
[42] B. Horowitz, "Mra, part 5: Adapting the twelve-factor app for microservices", *Nginx, Inc.*, Jul. 2016.

[43] K. Hoffman, *Beyond the Twelve-Factor App – Exploring the DNA of Highly Scalable, Resilient Cloud Applications*. O'Reilly Media, Inc., Apr. 2016, ISBN: 9781491944011.

[44] Microsoft Azure. (Oct. 2018). Scalability checklist, [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/checklist/scalability.

[45] O. T. Berna Seref, "Software code maintainability: A literature review", vol. 7, 3 May 2016. [Online]. Available: http://aircconline.com/ijsea/V7N3/7316ijsea05.pdf.

[46] R. Niedermayr, "Why we don't use the software maintainability index", Mar. 2016. [Online]. Available: https://www.cqse.eu/en/blog/maintainability-index.

[47] A. van Deursen, "Think twice before using the "maintainability index"", Aug. 2014. [Online]. Available: https://avandeursen.com/2014/08/29/think-twice-before-using-the-maintainability-index/.

[48] J. V. Ilja Heitlager Tobias Kuipers, "A practical model for measuring maintainability", 2007. [Online]. Available: https://www.softwareimprovementgroup.com/wp-content/uploads/2016/10/APracticalModelForMeasuringMaintainability.pdf.

[49] J. Visser, *Building Maintainable Software: Ten Guidelines for Future-Proof Code*. O'Reilly Media Inc., 2016, ISBN: 9781491953525.

[50] Developers.nl. (2019). Documentatie interne systemen developers.nl.

[51] C. McMahon, "The 12 factor php app", Nov. 2014. [Online]. Available: http://slashnode.com/the-12-factor-php-app-part-2/.

[52] V. Tardia, "The 12 factors of php", Oct. 2016. [Online]. Available: https://vito.tardia.me/blog/the-12-factors-of-php.

[53] B. Holt, "The twelve-factor app applied to php", Nov. 2011. [Online]. Available: https://www.bradley-holt.com/2011/11/the-twelve-factor-app-applied-to-php/.

[54] C. Lüdemann, "Feature environments in all environments – a guide to faster delivery", Nov. 2018. [Online]. Available: https://christianlydemann.com/feature-branches-in-all-environments-a-guide-to-test-once-and-deploy/.

[55] A. DadGar, "Why policy as code?", *HashiCorp, Inc.*, Jan. 2018. [Online]. Available: https://www.hashicorp.com/blog/why-policy-as-code/.

[56] A. Khan, "Key characteristics of a container orchestration platform to enable a modern application", vol. 4, pp. 42–48, 5 Dec. 2017. DOI: 10.1109/MCC.2017.4250933.

[57] Docker Inc. (2019). Dockerfile best practices, [Online]. Available: https://docs.docker.com/develop/develop-images/dockerfile_best-practices/.

[58] Docker Inc. (2019). Docker experimental features, [Online]. Available: https://github.com/docker/docker-ce/blob/master/components/cli/experimental/README.md.

[59] L. Wang, G. von Laszewski, M. Kunze, and J. Tao, "Cloud computing: A perspective study", pp. 1–11, 2010. DOI: https://doi.org/10.1007/s00354-008-0081-5.

[60] D. Chappell, "A short introduction to cloud platforms – an enterprise-oriented view", Aug. 2008.

[61] A. Apostu, F. C. Puican, G. Ularu, G. Suciu, and G. Todoran, "Study on advantages and disadvantages of cloud computing – the advantages of telemetry applications in the cloud", 2013.

[62] J. F. S. William Y. Chang Hosame Abu-Amara, *Transforming Enterprise Cloud Services*. 2010, ISBN: 9789048198450.

Bijlage A

Implementatie en resultaten

A.1 Docker-compose opstelling voor k6, InfluxDB & Grafana

Om de loadtest met k6, influxDB en grafana op te stellen heeft Loadimpact een docker-compose opstelling gemaakt. Na wat onderzoek is het opgevallen dat deze opstelling erg verouderd is. Daarom is ervoor gekozen om een eigen opstelling te maken:

```
version: '3.4'

networks:
  k6:
  grafana:

services:
  influxdb:
    image: influxdb:1.5.4
    networks:
    - k6
    - grafana
    ports:
      - "8086:8086"
    environment:
      - INFLUXDB_DB=k6

  grafana:
    image: grafana/grafana:6.4.1
    networks:
      - grafana
    ports:
      - "3000:3000"
    environment:
      - GF_AUTH_ANONYMOUS_ORG_ROLE=Admin
      - GF_AUTH_ANONYMOUS_ENABLED=true
      - GF_AUTH_BASIC_ENABLED=false
    volumes:
      - ./grafana/datasource.yml:/etc/grafana/provisioning/datasources
        ↪ /datasource.yml
```

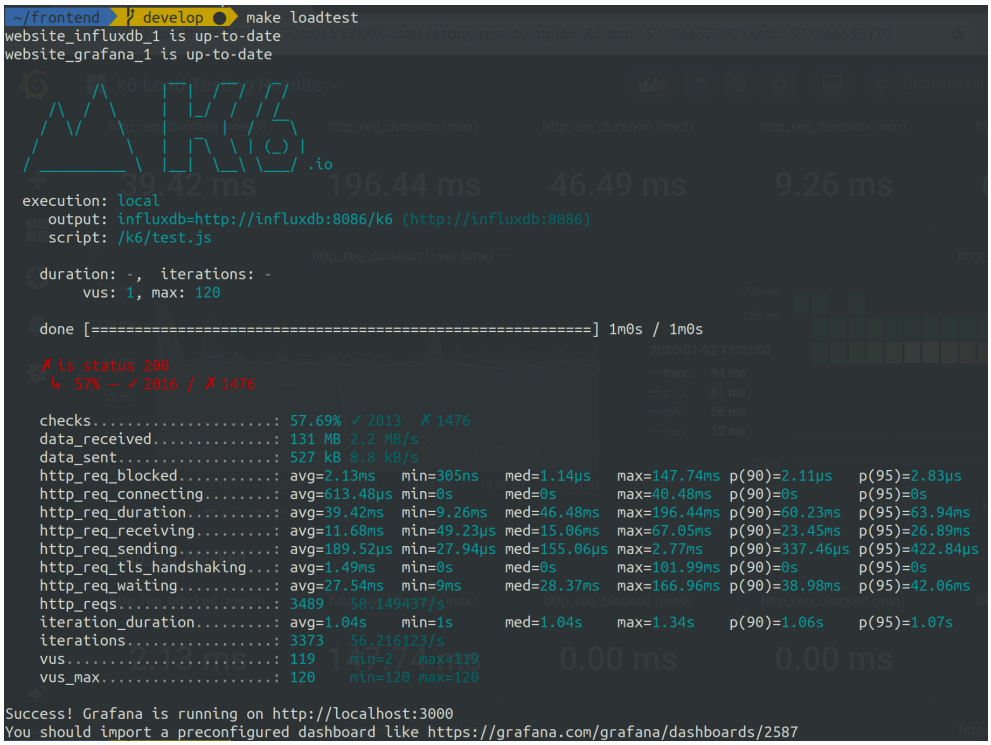
```
30
31    k6:
32      image: loadimpact/k6:0.25.1
33      networks:
34        - k6
35      ports:
36        - "6565:6565"
37      environment:
38        - K6_OUT=influxdb=http://influxdb:8086/k6
39      volumes:
40        - ../k6:/k6
```

Hiervoor is een Pull-Request gemaakt naar loadimpact/k6 om dit te verbeteren. `https://github.com/loadimpact/k6/pull/1183` samen met de issue `https://github.com/loadimpact/k6/issues/1182` . Hierin is te lezen wat precies de veranderingen waren. De maintainers van k6 waren blij met de verandering en hebben deze geaccepteerd en gemerged naar master. De loadtest is geschreven in javascript met de volgende code:

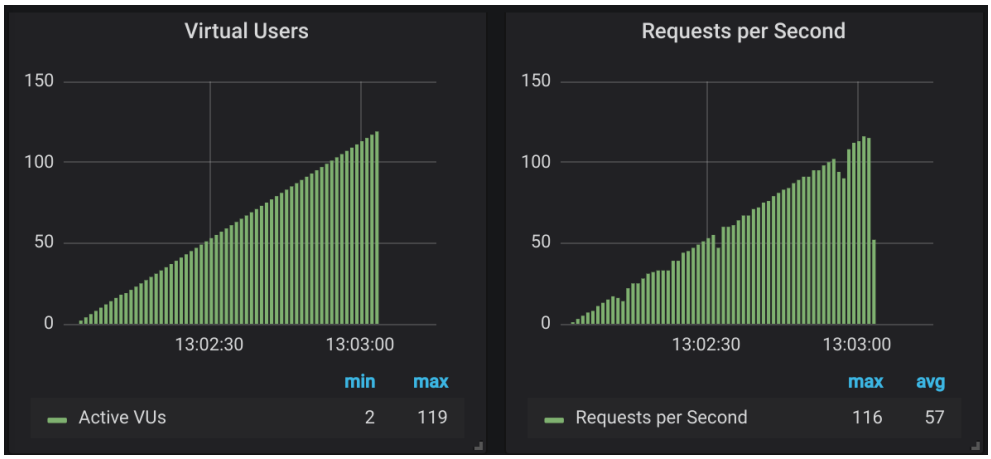
```
1  import http from "k6/http";
2  import { sleep, check } from "k6";
3
4  export let options = {
5    stages: [
6      { duration: "10s", target: 20 },
7      { duration: "10s", target: 40 },
8      { duration: "10s", target: 60 },
9      { duration: "10s", target: 80 },
10     { duration: "10s", target: 100 },
11     { duration: "10s", target: 120 },
12   ]
13 };
14
15 export default function() {
16   check(http.get("https://test.developers.nl/"), {
17     "is status 200": (r) => r.status === 200
18   });
19   sleep(1);
20 };
```

A.2 k6 load test resultaten

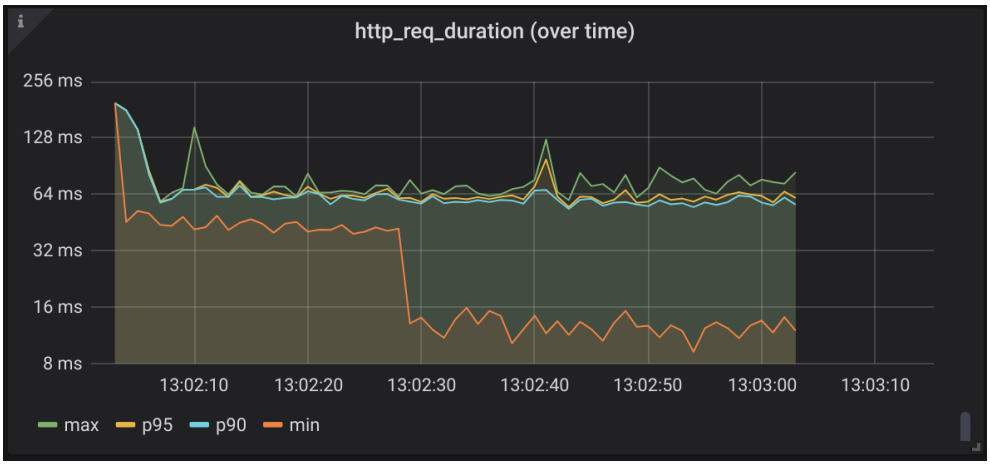
In figuur A.1 is de CLI output van de loadtest te vinden. In figuur A.2 zijn de oplopende hoeveelheid VUs uitgebeeld in Grafana, en in figuur A.3 is in Grafana te zien hoe lang de requests duren.



FIGUUR A.1: k6 loadtest CLI resultaten



FIGUUR A.2: k6 loadtest hoeveelheid VUs en requests



FIGUUR A.3: k6 loadtest resultaten

A.3 Docker container exits

PostgreSQL

```
LOG: received smart shutdown request
LOG: background worker "logical replication launcher" (PID 43) exited
 ↪  with exit code 1
LOG: shutting down
LOG: database system is shut down
```

PHP-FPM

```
NOTICE: Terminating ...
NOTICE: exiting, bye-bye!
```

Redis

```
1:signal-handler (1570781278) Received SIGTERM scheduling shutdown...
# User requested shutdown...
* Saving the final RDB snapshot before exiting.
* DB saved on disk
* Removing the pid file.
# Redis is now ready to exit, bye bye...
```

Nginx

```
[notice] 1#1: signal 15 (SIGTERM) received from 56, exiting
[notice] 48#48: exiting
[notice] 47#47: exiting
[notice] 47#47: exit
[notice] 1#1: signal 14 (SIGALRM) received
[notice] 1#1: signal 17 (SIGCHLD) received from 48
[notice] 1#1: cache manager process 48 exited with code 0
[notice] 1#1: worker process 47 exited with code 0
[notice] 1#1: exit
```

A.4 Docker container kill & restarts

```
$ docker ps -q
d0829783af18
f72e9967771b
01dd48ff5a59
fab794731d47
ca510c065d11
3ee85578efb5

$ docker kill $(docker ps -q)

$ docker ps
d0829783af18
f72e9967771b
01dd48ff5a59
fab794731d47
ca510c065d11
3ee85578efb5

$ docker ps -q

$ docker start $(docker ps -aq)
d0829783af18
f72e9967771b
01dd48ff5a59
fab794731d47
d68d7ab9809c
ca510c065d11
3ee85578efb5
e1866ab6c1af

$ docker ps -q
d0829783af18
```

```
f72e9967771b
01dd48ff5a59
fab794731d47
ca510c065d11
3ee85578efb5
```

A.5 Codecov implementatie

README.MD:

```
## Tests

We enforce that code coverage stays acceptable using codecov:

[![codecov](https://codecov.io/bb/developers_nl/developers.nl/branch/master/graph/badge.svg?token=DzAv79t9Gd)](https://codecov.io/bb/developers_nl/developers.nl)
```

Het builden van de Docker images met Ansible, inclusief de build arguments nodig voor codecov:

```
docker_images:
  - dockerfile: docker/php7-fpm/Dockerfile
  path: ../
  name: developersnl/website-php-fpm
  buildargs:
    GROUP_ID: 9000
    USER_ID: 9000
    BITBUCKET_BRANCH: "{{ lookup('env','BITBUCKET_BRANCH') }}"
    BITBUCKET_COMMIT: "{{ lookup('env', 'BITBUCKET_COMMIT') }}"
    BITBUCKET_BUILD_NUMBER: "{{ lookup('env','BITBUCKET_BUILD_NUMBER') }}"
    BITBUCKET_REPO_OWNER: "{{ lookup('env','BITBUCKET_REPO_OWNER') }}"
    BITBUCKET_REPO_SLUG: "{{ lookup('env','BITBUCKET_REPO_SLUG') }}"
    BITBUCKET_PR_ID: "{{ lookup('env','BITBUCKET_PR_ID') }}"
    CODECOV_TOKEN: "{{ lookup('env','CODECOV_TOKEN') }}"
    CI: "{{ lookup('env','CI') }}"
```

In de php7-fpm dockerfile zijn de build args omgezet naar environment variablen, een aantal apk packages toegevoegd en is het codecov script toegevoegd:

```
FROM application AS test

ENV SYMFONY_PHPUNIT_VERSION 8.0.0

ARG BITBUCKET_BRANCH
```

```
ARG BITBUCKET_BUILD_NUMBER
ARG BITBUCKET_REPO_OWNER
ARG BITBUCKET_REPO_SLUG
ARG BITBUCKET_PR_ID
ARG CODECOV_TOKEN
ARG CI
ARG BITBUCKET_COMMIT

ENV BITBUCKET_BRANCH=$BITBUCKET_BRANCH
ENV BITBUCKET_BUILD_NUMBER=$BITBUCKET_BUILD_NUMBER
ENV BITBUCKET_REPO_OWNER=$BITBUCKET_REPO_OWNER
ENV BITBUCKET_REPO_SLUG=$BITBUCKET_REPO_SLUG
ENV BITBUCKET_PR_ID=$BITBUCKET_PR_ID
ENV CODECOV_TOKEN=$CODECOV_TOKEN
ENV CI=$CI

# TODO: Cange VCS_COMMIT_ID to BITBUCKET_COMMIT when
 ↪  https://github.com/codecov/codecov-bash/pull/225 is deployed
ENV VCS_COMMIT_ID=$BITBUCKET_COMMIT

COPY --from=composer:1.9.0 /usr/bin/composer /usr/bin/composer

RUN apk add \
    php7-pdo_sqlite \
    php7-sqlite3 \
    php7-phar \
    php7-pear \
    php7-dev \
    redis \
    curl \
    bash \
    git \
    mercurial \
    findutils \
    g++ \
    make \
 && . /bin/pcov.sh \
 && redis-server --daemonize yes --requirepass test \
 && composer install -d /app/src --optimize-autoloader
  ↪  --no-interaction --no-suggest --no-scripts \
 && chmod u+x,g+x /app/src/bin/phpunit \
 && /app/src/bin/phpunit --configuration /app/src/phpunit.xml
  ↪  --coverage-clover=coverage.xml \
 && curl -s https://codecov.io/bash | bash -s - -X coveragepy
```

pcov script:

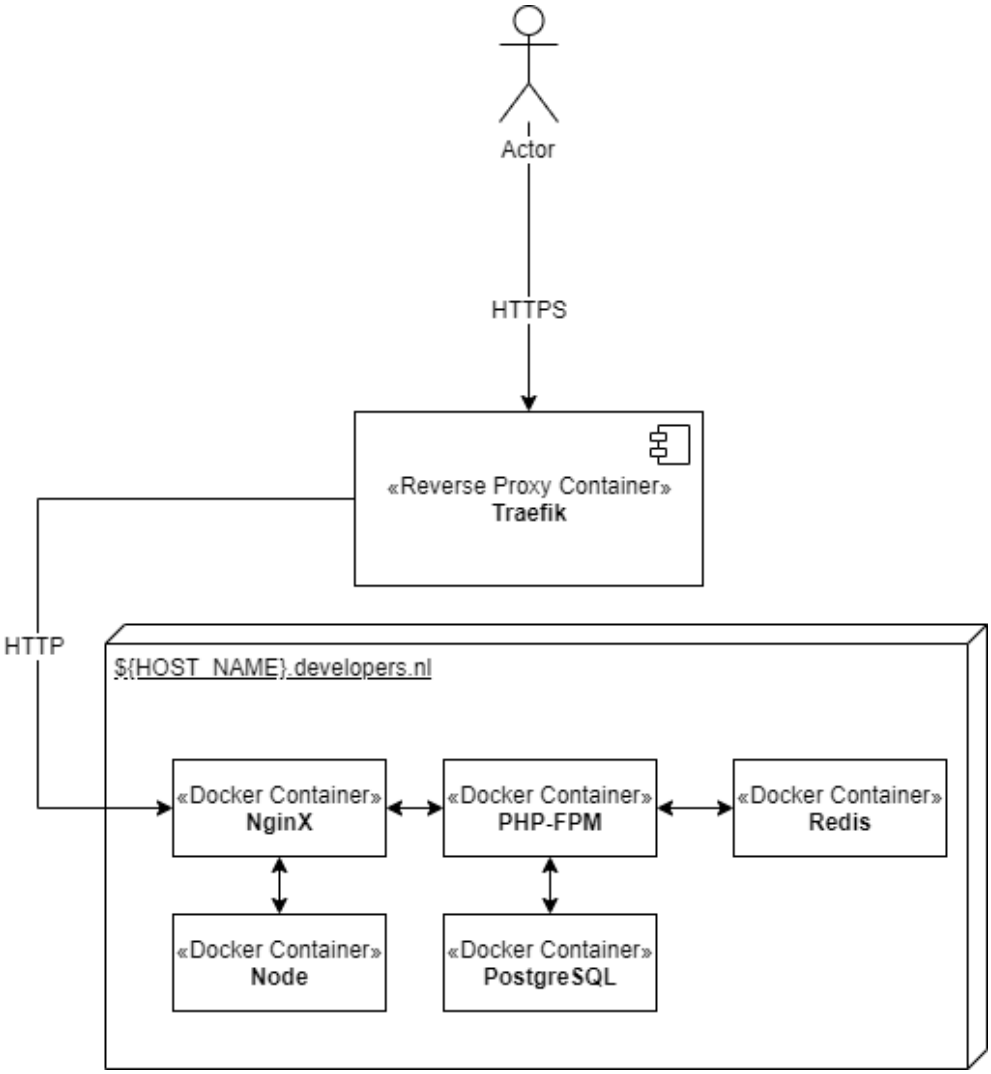
```
#!/bin/sh

```

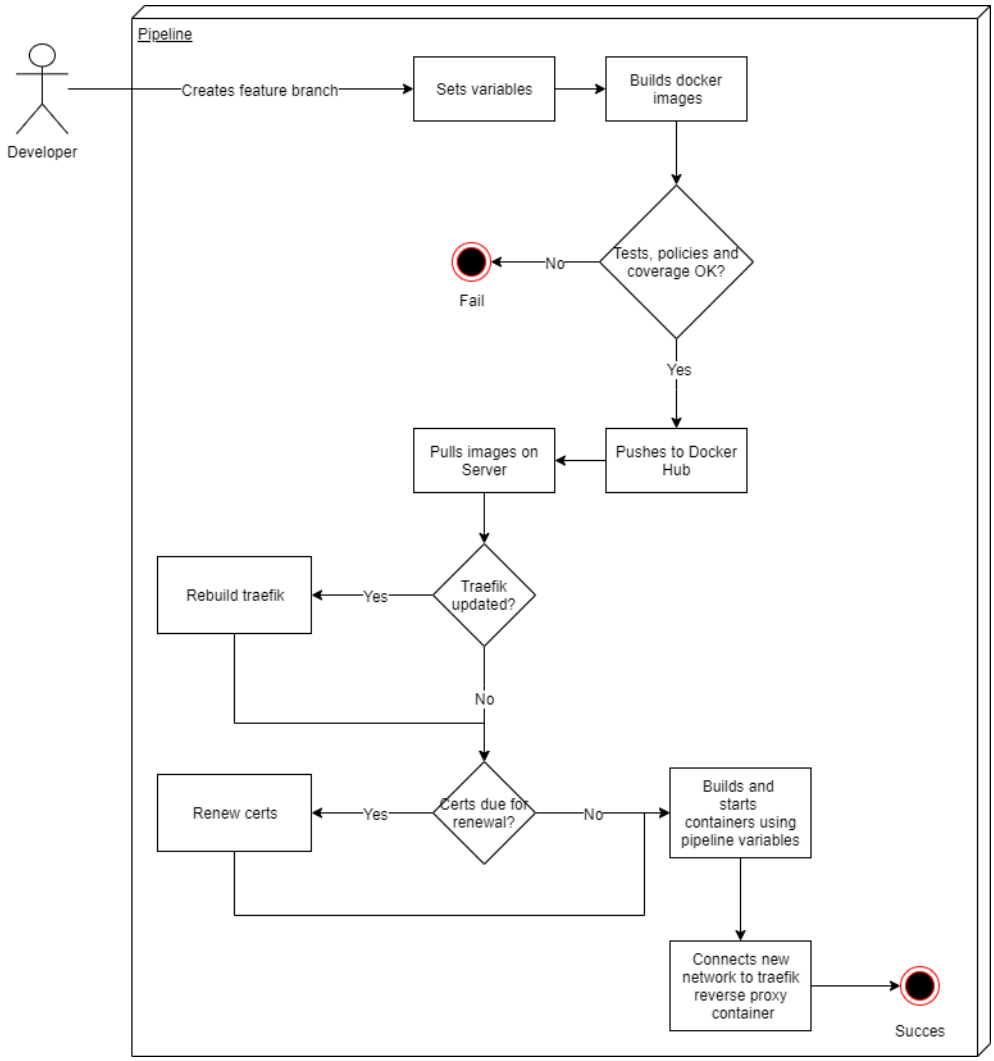
```
# Add PHP Coverage ini configuration
echo "- Enabling pcov"
cat <<-EOF > /etc/php7/conf.d/pcov.ini
extension=pcov
pcov.enable=1
EOF

echo "- Installing pcov"
if ! pecl list | grep pcov >/dev/null 2>&1;
then
    pecl install pcov ||
    {
        echo "Could not pecl install pcov" >&2;
        exit 1;
    }
fi
```

A.6 Feature-environments implementatie



FIGUUR A.4: Nieuwe infrastructuur met Traefik reverse proxy



FIGUUR A.5: Activity Diagram voor de pipeline

docker/docker-compose.yml

```
version: "3.4"

networks:
  nginx:
    driver: bridge

services:
  node:
    networks:
      - nginx
    environment:
      - NODE_ENV=production
      - BACKEND_URL=http://nginx:3000
    restart: always
    expose:
      - 3000
```

```
17
18    nginx:
19      restart: always
20      networks:
21        - nginx
22      environment:
23        - server_name=${server_name}
24      labels:
25        - traefik.enable=true
26        - traefik.docker.network=${net_name}_nginx
27        - traefik.http.routers.${net_name}_nginx.rule=
          ↪  Host(`${server_name}`) || Host(`werkenbij.${server_name}`)
28        - traefik.http.routers.${net_name}_nginx.entrypoints=http
29        - traefik.http.routers.${net_name}_nginx.middlewares=
          ↪  nginx-https-redirect
30        - traefik.http.middlewares.nginx-https-redirect.redirectscheme.
          ↪  scheme=https
31        - traefik.http.middlewares.nginx-https-redirect.redirectscheme.
          ↪  permanent=true
32        - traefik.http.routers.${net_name}_nginx-secure.rule=
          ↪  Host(`${server_name}`) || Host(`werkenbij.${server_name}`)
33        - traefik.http.routers.${net_name}_nginx-secure.entrypoints=
          ↪  https
34        - traefik.http.routers.${net_name}_nginx-secure.tls=true
35        - traefik.http.routers.${net_name}_nginx-secure.tls.options=
          ↪  myTLSOptions@file
36      expose:
37        - 8080
```

docker/docker-compose.dev.yml

```
1   version: "3.4"
2
3   volumes:
4       development_ssl: ~
5
6   services:
7     node:
8       user: "1000"
9       image: node:10.16.0-alpine
10      volumes:
11        - ../htdocs:/app:delegated
12      environment:
13        - NODE_ENV=development
14      working_dir: /app
15      command: ['/bin/sh', '-c', 'npm install --from-lock-file
        ↪  --no-optional --no-save && npm run dev']
16
17    nginx:
```

```
    build:
      context: ./nginx
      dockerfile: Dockerfile
    volumes:
      - development_ssl:/etc/letsencrypt/live/localhost
      - ./nginx/etc/nginx/temp/nginx.conf:/etc/nginx/temp/nginx.conf
      - ./nginx/etc/nginx/temp/conf.d:/etc/nginx/temp/conf.d
      - ../htdocs/static:/srv/html/static
    environment:
      - server_name=localhost
      - error_page=onderhoud.dev.html
      - php_backend_address=149.210.228.97:443
      - pass_type=proxy_pass https://phpbackend
      - cache_max_time=1s
      - hsts_max_time=0
      - cache_max_age=1
      - node_backend_address=node:3000
```

docker/docker-compose.prod.yml

```
version: "3.4"

volumes:
  logs: ~
  app_root: ~

services:
  node:
    image: "developersnl/node:${node_tag}"
    environment:
      - server_name=${server_name}

  nginx:
    image: "developersnl/nginx:${nginx_tag}"
    environment:
      - error_page=onderhoud.html
      - php_backend_address=php-fpm:9000
      - pass_type=fastcgi_pass phpbackend
      - php_app_location=/app/src/public
      - cache_max_time=4m
      - hsts_max_time=31536000
      - cache_max_age=31536000
      - node_backend_address=node:3000
    volumes:
      - /etc/developers.nl/static:/srv/html/static
      - logs:/var/log/nginx
```

docker/docker-compose.proxy.yml

```yaml
version: "3.4"

volumes:
  development_ssl: ~

services:
  traefik:
    labels:
      - traefik.enable=true
      - traefik.http.routers.traefik.entrypoints=http
      - traefik.http.routers.traefik.rule=Host
        ↪ (`traefik.${root_server_name}`)
      - traefik.http.routers.traefik.middlewares=
        ↪ traefik-https-redirect
      - traefik.http.middlewares.traefik-https-redirect.
        ↪ redirectscheme.scheme=https
      - traefik.http.routers.traefik-secure.entrypoints=https
      - traefik.http.routers.traefik-secure.rule=
        ↪ Host(`traefik.${root_server_name}`)
      - traefik.http.routers.traefik-secure.middlewares=traefik-auth
      - traefik.http.routers.traefik-secure.tls=true
      - traefik.http.routers.traefik-secure.tls.options=
        ↪ myTLSOptions@file
      - traefik.http.routers.traefik-secure.service=api@internal
    environment:
      - TRAEFIK_PROVIDERS_DOCKER_EXPOSEDBYDEFAULT=false
      - TRAEFIK_PROVIDERS_FILE_FILENAME=/dynamic_conf.toml
      - TRAEFIK_API_INSECURE=false
```

docker/docker-compose.proxy.prod.yml

```yaml
version: "3.4"

volumes:
  development_ssl: ~

services:
  traefik:
    image: developersnl/traefik:${traefik_tag}
    user: runuser
    ports:
      - 80:8080
      - 443:8443
    volumes:
      - /etc/traefik/dynamic_conf.toml:/dynamic_conf.toml
      - /etc/letsencrypt/live/${root_server_name}/fullchain.pem:/ssl/
        ↪ fullchain.pem
      - /etc/letsencrypt/live/${root_server_name}/privkey.pem:/ssl/
        ↪ privkey.pem
```

```
      - /home/runuser/.docker:/ssl/docker # TODO: runuser as variable
    labels:
      - traefik.http.middlewares.traefik-auth.basicauth.users=
        ↪ administrator:$$2y$$05$$WFGxILOwRePTQdqxrR8aoObKpf.
        ↪ ikMvpGv2ZLdEbRO13rmhuQo4xu
    environment:
      - TRAEFIK_ENTRYPOINTS_HTTP_ADDRESS=:8080
      - TRAEFIK_ENTRYPOINTS_HTTPS_ADDRESS=:8443
      - TRAEFIK_PROVIDERS_DOCKER_TLS_CAOPTIONAL=false
      - TRAEFIK_PROVIDERS_DOCKER_TLS_CA=/ssl/docker/ca.pem
      - TRAEFIK_PROVIDERS_DOCKER_TLS_CERT=/ssl/docker/cert.pem
      - TRAEFIK_PROVIDERS_DOCKER_TLS_KEY=/ssl/docker/key.pem
      - TRAEFIK_PROVIDERS_DOCKER_ENDPOINT=tcp://172.17.0.1:2376 # TODO
        ↪ BIP var
```

docker/docker-compose.proxy.dev.yml

```
version: "3.4"

volumes:
  development_ssl: ~

services:
  traefik:
    image: traefik:2.1
    ports:
      - 80:80
      - 443:443
    volumes:
      - ./traefik/dynamic_conf.toml/:/dynamic_conf.toml
      - /var/run/docker.sock:/var/run/docker.sock:ro
      - development_ssl:/ssl
    labels:
      - traefik.http.middlewares.traefik-auth.basicauth.users=test
        ↪ :$$apr1$$H6uskkkW$$IgXLP6ewTrSuBkTrqE8wj/ #test:test
    environment:
      - TRAEFIK_ENTRYPOINTS_HTTP_ADDRESS=:80
      - TRAEFIK_ENTRYPOINTS_HTTPS_ADDRESS=:443
      - TRAEFIK_LOG_LEVEL=debug
      - TRAEFIK_PROVIDERS_DOCKER_ENDPOINT=unix:///var/run/docker.sock

  ssl:
    build:
      context: ssl-dev
    volumes:
      - development_ssl:/ssl
```

Makefile

```
SHELL := /bin/bash

MAKEFLAGS := --silent --no-print-directory

.DEFAULT_GOAL := help

.PHONY: help node.shell node.logs

export secrets_dir :=$(CURDIR)/../.devnl-backend-vault/
export root_server_name=localhost
export server_name=localhost
export net_name=localhost

help:
	@echo "Please use 'make <target>' where <target> is one of"
	@awk 'BEGIN {FS = ":.*?## "} /^[a-zA-Z0-9\._-]+:.*?## / {printf "\033[36m%-30s\033[0m %s\n", $$1, $$2}' $(MAKEFILE_LIST)

### Development commands ###

up: ## Up containers in development mode
	. ./docker/up.sh

down: ## Down containers in development mode
	docker-compose -f docker/docker-compose.yml -f docker/docker-compose.dev.yml -p ${server_name} down
	docker-compose -f docker/docker-compose.proxy.yml -f docker/docker-compose.proxy.dev.yml -p proxy down

restart: ## Restart containers in development mode
	docker-compose -f docker/docker-compose.yml -f docker/docker-compose.dev.yml -p ${server_name} restart
	docker-compose -f docker/docker-compose.proxy.yml -f docker/docker-compose.proxy.dev.yml -p proxy down

build: ## Build containers
	docker-compose -f docker/docker-compose.yml -f docker/docker-compose.dev.yml -p ${server_name} build
	docker-compose -f docker/docker-compose.proxy.yml -f docker/docker-compose.proxy.dev.yml -p proxy down

loadtest: ## Start influxdb + grafana on localhost:3000 and run a k6 load test
	docker-compose -f docker/docker-compose.k6.yml -p website up -d influxdb grafana
	docker-compose -f docker/docker-compose.k6.yml -p website run --rm k6 run /k6/test.js
```

```
40          @echo Success! Grafana is running on http://localhost:3000
41          @echo You should import a preconfigured dashboard like
             ↪  "https://grafana.com/grafana/dashboards/2587"
42
43  secrets.edit: ## Edit the vault file to remove or add secrets
44          ansible-vault edit ansible/shared_vars/vault.yml
             ↪  --vault-password-file=../.vault-password
45
46  ansible.lint: ## Run Ansible Lint
47          docker run \
48                  --rm \
49                  --workdir=/ansible \
50                  -v $(CURDIR)/ansible:/ansible \
51                  -it survivorbat/ansible:v0.3 \
52                  ansible-lint /ansible/site.yml
53
54  #stack:
55  #         POSTGRES_PORT=5432 \
56  #         docker stack deploy -c docker/docker-compose.swarm.yml
     ↪  --with-registry-auth website
57
58  ### Node commands ###
59
60  node.shell: ## Enter the shell of the node container
61          docker-compose -f docker/docker-compose.yml -f
             ↪  docker/docker-compose.dev.yml -p ${server_name} run --rm
             ↪  node sh
62
63  node.logs: ## See logs of the node container
64          docker-compose -f docker/docker-compose.yml -f
             ↪  docker/docker-compose.dev.yml -p ${server_name} logs -f
             ↪  node
65
66  node.tests: ## Run tests in the node container
67          docker-compose -f docker/docker-compose.yml -f
             ↪  docker/docker-compose.dev.yml -p ${server_name} run --rm
             ↪  node npm run test /app
68
69  storybook.run: ## Run storybook on port 6006
70          docker run --rm -u node --name ${net_name}_storybook_1 -v
             ↪  ${CURDIR}/htdocs:/app --workdir=/app -p 6006:6006
             ↪  node:10.16.0-alpine npm run storybook
71          @echo Success! Storybook is now running over at
             ↪  http://localhost:6006
72
73  ### e2e commands ###
74
75  # TODO: Make sure this does not run as root (setting the user makes it
     ↪  crash)
76  cypress.run: ## Run Cypress frontend tests locally against running
     ↪  containers
```

```
77          docker run --rm \
78          --network ${server_name}_nginx \
79          --name ${server_name}_cypress_1 \
80          -e CYPRESS_baseUrl=https://nginx:8443 \
81          -v $(CURDIR)/e2e:/e2e \
82          --workdir=/e2e \
83          cypress/included:3.2.0 cypress run --spec
            ↪  "cypress/integration/frontend/**/*"
84
85  cypress.run.be: # Run Cypress backend test on the testserver (make
    ↪  sure you set the correct admin credentials in the command and to
    ↪  NOT commit them)
86          docker run --rm \
87          --network ${server_name}_nginx \
88          --name ${server_name}_cypress_1 \
89          -e CYPRESS_baseUrl="https://test.developers.nl" \
90          -e CYPRESS_admin_username="" \
91          -e CYPRESS_admin_password="" \
92          -v $(CURDIR)/e2e:/e2e \
93          --workdir=/e2e \
94          cypress/included:3.2.0 cypress run --spec
            ↪  "cypress/integration/backend/**/*"
```

docker/up.sh

```
1   #!/bin/bash
2
3   docker-compose -f docker/docker-compose.yml -f
    ↪  docker/docker-compose.dev.yml -p ${server_name} up -d
4   docker-compose -f docker/docker-compose.proxy.yml -f
    ↪  docker/docker-compose.proxy.dev.yml -p proxy up -d ssl traefik
5
6   networks=$(docker network inspect -f '{{range
    ↪  .Containers}}{{.Name}}{{end}}' ${net_name}_nginx)
7
8   if [[ $networks != *"proxy_traefik"* ]]; then
9     echo "Connecting ${net_name}_nginx to proxy_traefik_1..."
10    docker network connect ${net_name}_nginx proxy_traefik_1
11  fi
```

docker/traefik/Dockerfile

```
1   FROM traefik:2.1
2
3   ARG USER_ID
4   ARG GROUP_ID
5
6   RUN addgroup -g ${GROUP_ID} rungroup \
7    && adduser -u ${USER_ID} -S -G rungroup runuser \
```

```
 && mkdir -p /ssl/docker \
 && chown -R ${USER_ID}:${GROUP_ID} /ssl
```

docker/traefik/dynamic_conf.toml

```
[tls]
  [[tls.certificates]]
    certFile = "/ssl/fullchain.pem"
    keyFile = "/ssl/privkey.pem"

[tls.options]
  [tls.options.default]
    minVersion = "VersionTLS12"

  [tls.options.myTLSOptions]
    minVersion = "VersionTLS13"
    cipherSuites = [
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305",
        "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305"
    ]
```

Vagrantfile

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

VAGRANTFILE_API_VERSION = "2"

Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
  config.vm.box = "ubuntu/bionic64"
  config.vm.network :private_network, ip: "192.168.33.39"
  config.ssh.insert_key = false

  config.vm.hostname = "docker.test"
  config.vm.provider :virtualbox do |v|
    v.name = "docker.test"
    v.memory = 1024
    v.cpus = 2
    v.customize ["modifyvm", :id, "--natdnshostresolver1", "on"]
    v.customize ["modifyvm", :id, "--ioapic", "on"]
  end

  # Enable provisioning with Ansible.
  config.vm.provision "ansible" do |ansible|
    ansible.compatibility_mode = "2.0"
```

```
    ansible.extra_vars = {
        node_tag: "website-latest",
        nginx_tag: "website-latest",
        add_latest_tag: "false"
    }
    ansible.galaxy_role_file = "./ansible/requirements.yml"
    ansible.playbook = "./ansible/site.yml"
    ansible.vault_password_file = "../.vault-password"
  end
end
```

secure-daemon/defaults/main.yml

```
---
system_tmp: /tmp
country: NL
state: Zuid Holland
locality: Rotterdam
organization: Developers.nl
host: 127.0.0.1
email: info@developers.nl
common_name: "{{ host }}"
passphrase: "{{ docker_cert_passphrase }}"
subject_alt_name: DNS:localhost,IP:172.17.0.1,IP:127.0.0.1
ca_cipher: aes256

server_cert_path: /etc/docker
client_cert_path: "/home/{{ default_user }}/.docker"
temp_path: "{{ system_tmp }}/ansible-secure-deamon"
csr_form_file: "{{ temp_path }}/csr_form.txt"
extfile: "{{ temp_path }}/extfile.cnf"
```

secure-daemon/tasks/generate_client_certs.yml

```
- name: Generate OpenSSL private key with default values (4096 bits,
 ↪  RSA)
  openssl_privatekey:
    path: "{{ server_cert_path }}/key.pem"

- name: Generate an OpenSSL Certificate Signing Request
  openssl_csr:
    path: "{{ server_cert_path }}/client.csr"
    privatekey_path: "{{ server_cert_path }}/key.pem"
    common_name: client
    extended_key_usage:
      - clientAuth

- name: Generate OpenSSL certificate signed with your own CA
 ↪  certificate
```

```
14    openssl_certificate:
15      path: "{{ server_cert_path }}/cert.pem"
16      csr_path: "{{ server_cert_path }}/client.csr"
17      ownca_path: "{{ server_cert_path }}/ca.pem"
18      ownca_privatekey_path: "{{ server_cert_path }}/ca-key.pem"
19      ownca_privatekey_passphrase: "{{ passphrase }}"
20      provider: ownca
21
22  - name: Ensure {{ client_cert_path }}
23    file:
24      state: directory
25      path: "{{ client_cert_path }}"
26      owner: "{{ default_user }}"
27      group: "{{ default_group }}"
28
29
30  - name: Copy client certs
31    copy:
32      remote_src: yes
33      src: "{{ server_cert_path }}/{{ item }}"
34      dest: "{{ client_cert_path }}/."
35      owner: "{{ default_user }}"
36      group: "{{ default_group }}"
37    loop:
38      - ca.pem
39      - cert.pem
40      - key.pem
41
42  - name: Ensure file permissions for keys
43    file:
44      path: "{{ client_cert_path }}/key.pem"
45      mode: 0400
46
47  - name: Ensure file permissions for certificates
48    file:
49      path: "{{ client_cert_path }}/{{ item }}"
50      mode: 0444
51    loop:
52      - ca.pem
53      - cert.pem
```

secure-daemon/tasks/generate_server_certs.yml

```
1   - name: Generate OpenSSL private key with default values (4096 bits,
    ↪  RSA)
2     openssl_privatekey:
3       path: "{{ server_cert_path }}/server-key.pem"
4
5   - name: Generate OpenSSL Certificate Signing Request
```

```
  openssl_csr:
    path: "{{ server_cert_path }}/server.csr"
    privatekey_path: "{{ server_cert_path }}/server-key.pem"
    subject:
      commonName: "{{ common_name }}"
    subject_alt_name: "{{ subject_alt_name }}"

- name: Generate OpenSSL certificate signed with your own CA
  ↪ certificate
  openssl_certificate:
    path: "{{ server_cert_path}}/server-cert.pem"
    csr_path: "{{ server_cert_path }}/server.csr"
    ownca_path: "{{ server_cert_path }}/ca.pem"
    ownca_privatekey_path: "{{ server_cert_path }}/ca-key.pem"
    ownca_privatekey_passphrase: "{{ passphrase }}"
    provider: ownca

- name: "Ensure the server cert path {{ server_cert_path }}"
  file:
    state: directory
    path: "{{ server_cert_path }}"

- name: Ensure file permissions for keys
  file:
    path: "{{ server_cert_path }}/server-key.pem"
    mode: 0400

- name: Ensure file permissions for certificates
  file:
    path: "{{ server_cert_path }}/{{ item }}"
    mode: 0444
  loop:
    - ca.pem
    - server-cert.pem
```

secure-daemon/tasks/main.yml

```
---
- name: Create docker directory
  file:
    state: directory
    path: /etc/docker
    owner: "{{ default_user }}"
    group: "{{ default_group }}"
    mode: '600'

- name: Deploy Docker daemon.json
  template:
    src: etc/docker/daemon.json.j2
```

```
13      dest: /etc/docker/daemon.json
14      owner: "{{ default_user }}"
15      group: "{{ default_group }}"
16      mode: '600'
17
18  - name: Create a tempdir
19    file:
20      state: directory
21      path: "{{ temp_path }}"
22
23  - name: Generate OpenSSL private key with default values (4096 bits,
    ↪  RSA) and passphrase
24    openssl_privatekey:
25      path: "{{ server_cert_path }}/ca-key.pem"
26      cipher: "{{ ca_cipher }}"
27      passphrase: "{{ passphrase }}"
28
29  - name: Ensure ca-key.pem permissions
30    file:
31      path: "{{ server_cert_path }}/ca-key.pem"
32      mode: 0400
33
34  - name: Generate ca certificate
35    command: "openssl req -new -x509 -days 365 -key {{ server_cert_path
      ↪  }}/ca-key.pem -sha256 -out {{ server_cert_path }}/ca.pem -passin
      ↪  pass:{{ passphrase }} -subj '/C={{ country }}/ST={{ state
      ↪  }}>/L={{ locality }}/O={{ organization }}/CN={{ common_name }}'"
36
37  - name: Ensure CA certificate permissions
38    file:
39      path: "{{ server_cert_path }}/ca.pem"
40      mode: 0444
41
42  - name: Create/Renew server certs
43    include: generate_server_certs.yml
44
45  - name: Create/Renew client certs
46    include: generate_client_certs.yml
47
48  - name: Ensure docker.service.d directory
49    file:
50      state: directory
51      path: /etc/systemd/system/docker.service.d
52      owner: "{{ default_user }}"
53      group: "{{ default_group }}"
54      mode: '644'
55
56  - name: Override docker service
57    template:
58      src: etc/systemd/system/docker.service.d/override.conf.j2
```

```
    dest: /etc/systemd/system/docker.service.d/override.conf
    owner: "{{ default_user }}"
    group: "{{ default_group }}"
    mode: '644'

- name: Restart daemon
  command: "systemctl daemon-reload"

- name: Restart docker
  command: "systemctl restart docker"
```

secure-daemon/templates/etc/docker/daemon.json.j2

```
{
  "tlsverify": true,
  "tlscacert": "{{ server_cert_path }}/ca.pem",
  "tlscert": "{{ server_cert_path }}/server-cert.pem",
  "tlskey": "{{ server_cert_path }}/server-key.pem",
  "hosts": ["0.0.0.0:2376", "fd://"]
}
```

secure-daemon/templates/etc/systemd/system/docker.service.d/override.conf.j2

```
[Service]
  ExecStart=
  ExecStart=/usr/bin/dockerd
  ↪ --containerd=/run/containerd/containerd.sock
```

ansible/group_vars/all.yml

```
default_groups:
  # First group is the default group
  - name: rungroup
    gid: 9000
  - name: developer
    gid: 50000

default_users:
  # First user is the default user
  - name: runuser
    uid: 9000
    system: yes
    group: 'rungroup'
  - name: developer
    uid: 50000
    group: 'developer'
    password: "{{ developer_password }}"
```

```
    authorized_key: "{{ developer_authorized_keys }}"

default_sudo_groups:
  - developer

default_user: "{{ default_users[0].name }}"
default_group: "{{ default_groups[0].name }}"

pip_install_packages:
  - name: setuptools
  - name: pyopenssl
    version: 16.2.0
  - name: certbot-dns-transip
  - name: docker
  - name: docker-compose
  - name: cryptography
    version: 2.1
docker_install_compose: yes
```

ansible/roles/frontend-images/defaults/main.yml

```
docker_images:
  - dockerfile: docker/node/Dockerfile
    path: ../
    name: developersnl/node
    tag: "{{ node_tag }}"
    buildargs:
      node_version: 10.16.0
  - dockerfile: Dockerfile
    path: ../docker/nginx
    name: developersnl/nginx
    tag: "{{ nginx_tag }}"
  - dockerfile: Dockerfile
    path: ../docker/traefik
    name: developersnl/traefik
    tag: "{{ traefik_tag }}"
    buildargs:
      USER_ID: 9000
      GROUP_ID: 9000

add_latest_tag: yes
publish_images: no
docker_username: ""
docker_password: ""
docker_email: ""
```

ansible/roles/frontend/defaults/main.yml

```yaml
---
local_base_dir: ../../../..
project_dir: /srv/app/frontend
project_dir_files:
  - "{{ local_base_dir }}/docker/docker-compose.yml"
  - "{{ local_base_dir }}/docker/docker-compose.prod.yml"
  - "{{ local_base_dir }}/docker/docker-compose.proxy.yml"
  - "{{ local_base_dir }}/docker/docker-compose.proxy.prod.yml"

nginx_host_config_directory: /etc/developers.nl/nginx
nginx_config_files:
  - { src: "{{ local_base_dir }}/docker/nginx/nginx.conf", dest: "{{ nginx_host_config_directory }}" }
  - { src: "{{ local_base_dir }}/docker/nginx/conf.d", dest: "{{ nginx_host_config_directory }}" }

traefik_host_config_directory: /etc/traefik
traefik_config_files:
  - { src: "{{ local_base_dir }}/docker/traefik/dynamic_conf.toml", dest: "{{ traefik_host_config_directory }}/dynamic_conf.toml" }

nginx_host_letsencrypt_email: sentry@developers.nl
nginx_host_letsencrypt_post_hook: 'docker restart $(docker ps -q --filter="name=traefik")'
nginx_host_static_directory: /etc/developers.nl/
local_static_directory: "{{ local_base_dir }}/htdocs/static"

env: test

static_root_files:
  - { src: 'etc/developers.nl/static/robots.txt', dest: 'robots.txt' }
  - { src: 'etc/developers.nl/static/sitemap.xml', dest: 'sitemap.xml' }

image_delete_until_time: 4h
```

ansible/roles/frontend/tasks/application.yml

```yaml
---
- name: "Ensure Docker login"
  docker_login:
    username: "{{ docker_username }}"
    email: "{{ docker_email }}"
    password: "{{ docker_password }}"

- name: "Clean {{ project_dir }}"
  file:
    state: absent
    path: "{{ project_dir }}"
```

```
12
13 - name: "Ensure {{ project_dir }}"
14   file:
15     state: directory
16     path: "{{ project_dir }}"
17     owner: "{{ default_user }}"
18     group: "{{ default_group }}"
19     recurse: yes
20
21 - name: "Ensure files in {{ project_dir }}"
22   copy:
23     src: "{{ item }}"
24     dest: "{{ project_dir }}/"
25     owner: "{{ default_user }}"
26     group: "{{ default_group }}"
27   loop: "{{ project_dir_files }}"
28
29 - name: "Ensure static files in {{ nginx_host_static_directory }}"
30   copy:
31     src: "{{ local_static_directory }}"
32     dest: "{{ nginx_host_static_directory }}"
33     owner: "{{ default_user }}"
34     group: "{{ default_group }}"
35
36 - name: "Ensure static root files in {{ nginx_host_static_directory
   ↪  }}"
37   template:
38     src: "{{ item.src }}"
39     dest: "{{ nginx_host_static_directory }}/static/{{ item.dest }}"
40     owner: "{{ default_user }}"
41     group: "{{ default_group }}"
42   loop: "{{ static_root_files }}"
43
44 - name: "Ensure {{ traefik_host_config_directory }}"
45   file:
46     state: directory
47     path: "{{ traefik_host_config_directory }}"
48     owner: "{{ default_user }}"
49     group: "{{ default_group }}"
50     recurse: yes
51
52 - name: "Ensure traefik files in {{ traefik_host_config_directory }}"
53   copy:
54     src: "{{ item.src }}"
55     dest: "{{ item.dest }}"
56     owner: "{{ default_user }}"
57     group: "{{ default_group }}"
58   loop: "{{ traefik_config_files }}"
59
60 - name: "Get BITBUCKET_BRANCH"
```

```
61    set_fact:
62      branch: "{{ lookup('env','BITBUCKET_BRANCH') }}"
63
64  # Subdomain retrieved from bitbucket branch name. For example
    ↪  `WEB-123`
65  - name: "Set subdomain"
66    shell: echo {{ branch }} | grep -o 'WEB-[0-9]\+'
67    when: "'feature/WEB-' in branch"
68    register: subdomain
69
70  # server_name will be the FQDN. For example: `WEB-123.developers.nl`.
71  - name: "Set server name"
72    set_fact:
73      server_name: "{{ inventory_hostname if subdomain.stdout is
        ↪  undefined else subdomain.stdout + '.' + inventory_hostname}}"
74
75  # Net name is a stripped and cased-down server_name. For example:
    ↪  `web-123developersnl`
76  - name: "Get Net name"
77    shell: echo {{ server_name }} | tr -dc '[:alnum:]_-' | tr
      ↪  '[:upper:]' '[:lower:]'
78    register: net_name
79
80  - name: "Ensure stop old docker containers"
81    docker_container:
82      name: "{{ item }}"
83      state: stopped
84    loop:
85      - website_node_1
86      - website_nginx_1
87
88  - name: "Ensure Docker restart project {{ server_name }}"
89    environment:
90      node_tag: "{{ node_tag }}"
91      nginx_tag: "{{ nginx_tag }}"
92      server_name: "{{ server_name }}"
93      net_name: "{{ net_name.stdout }}"
94    docker_compose:
95      state: present
96      restarted: yes
97      project_name: "{{ server_name }}"
98      project_src: "{{ project_dir }}"
99      files:
100       - "docker-compose.yml"
101       - "docker-compose.prod.yml"
102
103 - name: "Ensure Docker restart proxy"
104   environment:
105     traefik_tag: "{{ traefik_tag }}"
106     root_server_name: "{{ inventory_hostname }}"
```

```
    server_name: "{{ server_name }}"
    net_name: "{{ net_name.stdout }}"
  docker_compose:
    state: present
    restarted: yes
    project_name: "proxy"
    project_src: "{{ project_dir }}"
    files:
      - "docker-compose.proxy.yml"
      - "docker-compose.proxy.prod.yml"
  when: bootstrap_proxy | bool

- name: "Connect {{ net_name.stdout }}_nginx to traefik"
  docker_network:
    name: "{{ net_name.stdout }}_nginx"
    connected:
      - proxy_traefik_1
    appends: yes

# There is option for network aliases in docker_network so we have to
 ↪  use shell
- name: "Connect {{ net_name.stdout }}_nginx to PHP-FPM"
  shell: "docker network connect --alias php-fpm {{ net_name.stdout
   ↪  }}_nginx websitebackend_php-fpm_1"
  ignore_errors: yes

- name: "Clean up images older than {{ image_delete_until_time }}"
  docker_prune:
    images: yes
    images_filters:
      dangling: false
      until: "{{ image_delete_until_time }}"
  register: prune_result

- debug:
    var: prune_result
```

ansible/roles/frontend/tasks/letsencrypt.yml

```
---
- name: "Ensure transip.ini"
  template:
    src: etc/letsencrypt/transip.ini.j2
    dest: /etc/letsencrypt/transip.ini
    owner: root
    group: root
    mode: '600'

- name: "Ensure TransIP key"
```

```
11    copy:
12      content: "{{ transip_key }}"
13      dest: "/root/transip.key"
14      owner: root
15      group: root
16      mode: '600'
17
18  - name: "Run certbot challenge"
19    command: "certbot certonly
20          --agree-tos
21          -m {{ nginx_host_letsencrypt_email }}
22          -d {{ inventory_hostname }}
23          -d *.{{ inventory_hostname }}
24          -a certbot-dns-transip:dns-transip
25          --certbot-dns-transip:dns-transip-credentials
            ↪  /etc/letsencrypt/transip.ini
26          --certbot-dns-transip:dns-transip-propagation-seconds 240
27          --expand
28          -n"
29
30  - name: "Ensure certbot-renewal.timer templates"
31    template:
32      src: "{{ item }}"
33      dest: "/etc/systemd/system/"
34      owner: root
35      group: root
36      mode: '644'
37    loop:
38      - etc/systemd/system/certbot-renewal.service
39      - etc/systemd/system/certbot-renewal.timer
40
41  - name: "Start and enable service certbot-renewal.timer"
42    service:
43      name: "certbot-renewal.timer"
44      state: started
45      enabled: yes
46
47  - name: "Ensure dhparam.pem"
48    openssl_dhparam:
49      path: "/etc/letsencrypt/live/{{ inventory_hostname }}/dhparam.pem"
50      owner: "{{ default_user }}"
51      group: "{{ default_group }}"
52      size: 2048
53
54  - name: "Ensure letsencrypt directory permissions"
55    file:
56      state: directory
57      path: /etc/letsencrypt/live
58      recurse: yes
59      owner: "{{ default_user }}"
```

```
60      group: "{{ default_group }}"
```

ansible/site.yml

```
1   ---
2   - name: Ensure common
3     hosts: all
4     become: yes
5     tags: server_install
6     gather_facts: no
7     vars_files:
8       - shared_vars/vault.yml
9     pre_tasks:
10      - name: "Ensure python"
11        raw: test -e /usr/bin/python || (apt -y update && apt install -y
            ↪  python-minimal)
12        register: output
13        changed_when: (output.stdout | length) > 0
14    roles:
15      - common
16
17  - name: Ensure secure TLS docker socket
18    hosts: all
19    become: yes
20    gather_facts: true
21    vars_files:
22      - shared_vars/vault.yml
23    roles:
24      - { tags: server_install, role: geerlingguy.pip }
25      - { tags: server_install, role: geerlingguy.docker }
26      - { tags: server_install, role: secure-daemon }
27
28  # Ensure built images for the pipeline
29  - name: Ensure frontend images
30    hosts: localhost
31    connection: local
32    vars_files:
33      - shared_vars/vault.yml
34    roles:
35      - { tags: build_images,publish_images, role: frontend-images }
36
37  # Ensure frontend host
38  - name: Ensure Frontend
39    hosts: frontend
40    become: yes
41    vars_files:
42      - shared_vars/vault.yml
43    roles:
```

```
    - { tags: server_install, role: geerlingguy.certbot }
    - { tags: server_deploy, server_install, role: frontend }
```

docker/nginx/etc/nginx/temp/conf.d/0004_developers.nl.conf

```
server {
    listen 8080;

    server_name ${server_name} nginx;

    rewrite ^/(?!(?!admin).)*/$ /$1 permanent;
    port_in_redirect off;

    root /srv/html/static;

    location ~ ^/(api|admin|login|logout) {
        try_files $uri $uri/ @php;

        limit_req zone=req_limit_per_ip burst=90 nodelay;
        limit_conn conn_limit_per_ip 40;
    }

    location /werkenbij {
        return 301 https://werkenbij.${server_name};
    }

    location /sleutel {
            default_type "text/html";
            alias /srv/html/static/sleutel.html;
        }

    location ~ ^/(uploads|css|bundles|img) {
        try_files $uri $uri/ @php;

        add_header Cache-Control
        ↪ "public,max-age=${cache_max_age},immutable" always;

        limit_req zone=req_limit_per_ip burst=130 nodelay;
        limit_conn conn_limit_per_ip 45;
    }

    location /service-worker.js {
        add_header Cache-Control no-cache;
        expires 0;

        proxy_pass http://nodebackend;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $http_host;
```

```
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_hide_header X-Powered-By;

        limit_req zone=req_limit_per_ip burst=40 nodelay;
        limit_conn conn_limit_per_ip 15;
    }

    location @php {
        ${pass_type};

        # PHP
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME ${php_app_location}/index.php;

        # External proxy
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_hide_header X-Powered-By;

        add_header Access-Control-Allow-Origin *;
        add_header 'Access-Control-Allow-Methods' 'GET, HEAD, OPTIONS,
        ↪  POST';

        limit_req zone=req_limit_per_ip burst=30 nodelay;
        limit_conn conn_limit_per_ip 15;
    }

    location @node {
        proxy_pass http://nodebackend;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_hide_header X-Powered-By;
        proxy_cache DEVELOPERSNL_node;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $http_host;
        proxy_set_header X-Forwarded-Proto $scheme;

        limit_req zone=req_limit_per_ip burst=30 nodelay;
        limit_conn conn_limit_per_ip 15;
    }

    location / {
        try_files $uri $backendpool;
    }

    location ~ ^/_next/static/*. {
        proxy_pass http://nodebackend;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

```
93          proxy_set_header Host $http_host;
94          proxy_set_header X-Forwarded-Proto $scheme;
95          proxy_hide_header X-Powered-By;
96          proxy_hide_header Cache-Control;
97
98          add_header Cache-Control
            ↪ "public,max-age=${cache_max_age},immutable" always;
99
100         limit_req zone=req_limit_per_ip burst=80 nodelay;
101         limit_conn conn_limit_per_ip 50;
102     }
103
104     error_page 500 502 503 504 /${error_page};
105     location /onderhoud {
106        root /srv/html/static;
107        internal;
108     }
109 }
```

docker/nginx/etc/nginx/temp/conf.d/0004_werkenbij.developers.nl.conf

```
1  server {
2      listen 8080;
3
4      server_name werkenbij.${server_name};
5
6      rewrite ^/werkenbij/(.*)/$ /$1 permanent;
7      port_in_redirect off;
8
9      root /srv/html/static;
10
11     location / {
12         try_files $uri /werkenbij$request_uri;
13     }
14
15     location ~ ^/(uploads|css|bundles|img) {
16         try_files $uri $uri/ @backend;
17
18         add_header Cache-Control
           ↪ "public,max-age=${cache_max_age},immutable" always;
19
20         limit_req zone=req_limit_per_ip burst=130 nodelay;
21         limit_conn conn_limit_per_ip 45;
22     }
23
24     location @backend {
25         ${pass_type};
26
27         # External proxy
```

```
28          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
29          proxy_set_header X-Forwarded-Proto $scheme;
30          proxy_set_header Host $http_host;
31          proxy_set_header X-Real-IP $remote_addr;
32
33          limit_req zone=req_limit_per_ip burst=30 nodelay;
34          limit_conn conn_limit_per_ip 15;
35      }
36
37      location /robots.txt {
38          alias /srv/html/static/block/robots.txt;
39      }
40
41      location /werkenbij {
42          proxy_pass http://nodebackend;
43          proxy_set_header X-Real-IP $remote_addr;
44          proxy_hide_header X-Powered-By;
45          proxy_cache DEVELOPERSNL_node;
46          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
47          proxy_set_header Host $http_host;
48          proxy_set_header X-Forwarded-Proto $scheme;
49
50          limit_req zone=req_limit_per_ip burst=30 nodelay;
51          limit_conn conn_limit_per_ip 15;
52
53          internal;
54      }
55
56      location ~ ^/(_next|static) {
57          proxy_pass http://nodebackend;
58          proxy_set_header X-Real-IP $remote_addr;
59          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
60          proxy_set_header Host $http_host;
61          proxy_set_header X-Forwarded-Proto $scheme;
62          proxy_hide_header X-Powered-By;
63          proxy_hide_header Cache-Control;
64
65          add_header Cache-Control
            ↪ "public,max-age=${cache_max_age},immutable" always;
66
67          limit_req zone=req_limit_per_ip burst=40 nodelay;
68          limit_conn conn_limit_per_ip 15;
69      }
70
71      error_page 500 502 503 504 /${error_page};
72      location /onderhoud {
73         root /srv/html/static;
74         internal;
75      }
76  }
```

docker/ssl-dev/Dockerfile

```
# Docker image to generate SSL certificates for a root domain and a wildcard subdomain in your development environment
FROM alpine:latest

RUN apk update --no-cache \
 && apk add --no-cache openssl bash

WORKDIR /ssl

RUN ["/bin/bash", "-c", "openssl req \
                         -x509 \
                         -nodes \
                         -newkey \
                         rsa:4096 \
                         -keyout /ssl/privkey.pem \
                         -out /ssl/fullchain.crt \
                         -days 9999 \
                         -subj '/C=NL/ST=Zuid Holland/L=Rotterdam/O=Developers.nl/OU=Development/CN=*.localhost/emailAddress=info@developers.nl' \
                         -extensions san \
                         -config <( \
                           echo '[req]'; \
                           echo 'distinguished_name=req'; \
                           echo '[san]'; \
                           echo 'subjectAltName=DNS:localhost') \
                         && openssl x509 -in /ssl/fullchain.crt -out /ssl/fullchain.pem -outform PEM"]

ENTRYPOINT ["openssl"]
```

Bitbucket-Pipelines.yml

```
pipelines:
  default:
    - step:
        name: 'Build'
        image: survivorbat/ansible:v0.3
        caches:
          - docker
        script:
          - 'echo -e $VAULT_PASSWORD > ../.vault-password'
          - 'ansible-galaxy install -r ansible/requirements.yml'
          - 'ansible-playbook
            -e node_tag=website-latest
            -e nginx_tag=website-latest
            -e traefik_tag=website-latest
            -i ansible/inventories/local.yml
```

```
            --vault-password-file=../.vault-password
            -e add_latest_tag=false
            --tags=build_images ansible/site.yml'

  custom:
    e2e@test.developers.nl:
      - step:
          name: 'E2E @test.developers.nl'
          image: cypress/included:3.2.0
          caches:
            - node
          artifacts:
            - e2e/cypress/screenshots/**/*
          script:
            - 'cd e2e && CYPRESS_baseUrl=https://test.developers.nl
              ↪ cypress run'
    e2e@developers.nl:
      - step:
          name: 'E2E @developers.nl'
          image: cypress/included:3.2.0
          caches:
            - node
          artifacts:
            - e2e/cypress/screenshots/**/*
          script:
            - 'cd e2e && CYPRESS_baseUrl=https://developers.nl cypress
              ↪ run'
    deploy@test.developers.nl:
      - step:
          name: 'Deploy @test.developers.nl'
          deployment: test
          image: survivorbat/ansible:v0.3
          caches:
            - docker
          script:
            - 'echo -e $VAULT_PASSWORD > ../.vault-password'
            - 'ansible-galaxy install -r ansible/requirements.yml'
            - 'ansible-playbook
              -e node_tag=test-website-$BITBUCKET_BUILD_NUMBER
              -e nginx_tag=test-website-$BITBUCKET_BUILD_NUMBER
              -e traefik_tag=test-website-$BITBUCKET_BUILD_NUBER
              -e publish_images=true
              -e bootstrap_proxy=false
              --vault-password-file=../.vault-password
              -i ansible/inventories/test.yml
              --skip-tags server_install
              ansible/site.yml'
      - step:
          name: 'E2E @test.developers.nl'
          image: cypress/included:3.2.0
```

```
64          caches:
65            - node
66          artifacts:
67            - e2e/cypress/screenshots/**/*
68          script:
69            - 'cd e2e && CYPRESS_baseUrl=https://test.developers.nl
               ↪  cypress run'
70    deploy@developers.nl:
71      - step:
72          name: 'Deploy @developers.nl'
73          deployment: production
74          image: survivorbat/ansible:v0.3
75          caches:
76            - docker
77          script:
78            - 'echo -e $VAULT_PASSWORD > ../.vault-password'
79            - 'ansible-galaxy install -r ansible/requirements.yml'
80            - 'ansible-playbook
81              -e node_tag=website-$BITBUCKET_BUILD_NUMBER
82              -e nginx_tag=website-$BITBUCKET_BUILD_NUMBER
83              -e traefik_tag=website-$BITBUCKET_BUILD_NUMBER
84              -e publish_images=true
85              -e bootstrap_proxy=false
86              --vault-password-file=../.vault-password
87              -i ansible/inventories/production.yml
88              --skip-tags server_install
89              ansible/site.yml'
90      - step:
91          name: 'E2E @developers.nl'
92          image: cypress/included:3.2.0
93          caches:
94            - node
95          artifacts:
96            - e2e/cypress/screenshots/**/*
97          script:
98            - 'cd e2e && CYPRESS_baseUrl=https://developers.nl cypress
               ↪  run'
99    bootstrap@test.developers.nl:
100     - step:
101         name: 'Bootstrap @test.developers.nl'
102         deployment: test
103         image: survivorbat/ansible:v0.3
104         caches:
105           - docker
106         script:
107           - 'echo -e $VAULT_PASSWORD > ../.vault-password'
108           - 'ansible-galaxy install -r ansible/requirements.yml'
109           - 'ansible-playbook
110             -e node_tag=test-website-$BITBUCKET_BUILD_NUMBER
111             -e nginx_tag=test-website-$BITBUCKET_BUILD_NUMBER
```

```
112               -e traefik_tag=test-website-$BITBUCKET_BUILD_NUMBER
113               -e publish_images=true
114               -e bootstrap_proxy=true
115               --vault-password-file=../.vault-password
116               -i ansible/inventories/test.yml
117               ansible/site.yml'
118     bootstrap@developers.nl:
119       - step:
120           name: 'Bootstrap @developers.nl'
121           deployment: production
122           image: survivorbat/ansible:v0.3
123           caches:
124             - docker
125           script:
126             - 'echo -e $VAULT_PASSWORD > ../.vault-password'
127             - 'ansible-galaxy install -r ansible/requirements.yml'
128             - 'ansible-playbook
129                -e node_tag=website-$BITBUCKET_BUILD_NUMBER
130                -e nginx_tag=website-$BITBUCKET_BUILD_NUMBER
131                -e traefik_tag=website-$BITBUCKET_BUILD_NUMBER
132                -e publish_images=true
133                -e bootstrap_proxy=true
134                --vault-password-file=../.vault-password
135                -i ansible/inventories/production.yml
136                ansible/site.yml'
137 options:
138   docker: true
139
140 definitions:
141   services:
142     docker:
143       memory: 3072
```

A.7 Grafana implementatie

docker/docker-compose.proxy.prod.yml

```
1   grafana:
2     image: "grafana/grafana:6.4.1"
3     networks:
4       - grafana
5     expose:
6       - 5000
7     environment:
8       - GF_AUTH_BASIC_ENABLED=true
9     labels:
10      - traefik.enable=true
11      - traefik.docker.network=proxy_grafana
```

```
      - traefik.http.routers.proxy_grafana.rule=
      ↪ Host(`grafana.${root_server_name}`)
      - traefik.http.routers.proxy_grafana.entrypoints=http
      - traefik.http.routers.proxy_grafana.middlewares=
      ↪ grafana-https-redirect
      - traefik.http.middlewares.grafana-https-redirect.
      ↪ redirectscheme.scheme=https
      - traefik.http.middlewares.grafana-https-redirect.
      ↪ redirectscheme.permanent=true
      - traefik.http.routers.proxy_grafana-secure.rule=
      ↪ Host(`grafana.${root_server_name}`)
      - traefik.http.routers.proxy_grafana-secure.entrypoints=https
      - traefik.http.routers.proxy_grafana-secure.tls=true
      - traefik.http.routers.proxy_grafana-secure.tls.options=
      ↪ myTLSOptions@file
```

A.8 Open Policy Agent implementatie

frontend-images/tasks/evaluate_policies.yml

```
- name: Ensure policy directory
  file:
    path: "{{ clone_dir }}/policies"
    state: directory
    owner: root
    group: root

- name: Ensure policies
  template:
    src: policies/containers.rego.j2
    dest: "{{ clone_dir }}/policies/containers.rego"
    owner: root
    group: root

- name: Run Open Policy Agent
  docker_container:
    detach: false
    name: OPA
    state: started
    image: openpolicyagent/opa:0.16.0
    command: "eval --format=pretty -d /policies 'data.containers'"
    volumes:
      - "{{ clone_dir }}/policies:/policies"
    cleanup: yes
  register: opa_container
  failed_when: "'\"allow\": true' not in
  ↪ opa_container.ansible_facts.docker_container.Output"
```

frontend-images/tasks/main.yml

```yaml
---
- import_tasks: "build.yml"
- import_tasks: "publish.yml"
- import_tasks: "evaluate_policies.yml"
- import_tasks: "publish.yml"
```

frontend-images/templates/policies/containers.rego.j2

```
package containers

allow {
    not deny
}

deny {
    poc
}

poc {
    1 == 2
}
```

secure-daemon/tasks/evaluate_policies.yml

```yaml
- name: Ensure policy directory
  file:
    path: "/etc/docker/policies"
    recurse: yes
    state: directory
    owner: "{{ default_user }}"
    group: "{{ default_group }}"

- name: Ensure policies
  template:
    src: etc/docker/policies/authz.rego.j2
    dest: /etc/docker/policies/authz.rego
    owner: "{{ default_user }}"
    group: "{{ default_group }}"

- name: Ensure .docker directories
  file:
    path: "{{ item }}/.docker"
    state: directory
  loop:
    - "/home/{{ default_user }}"
    - "/home/{{ default_users[1].name }}"
    - "/root"
```

```
24
25 - name: Ensure docker http headers
26   template:
27     src: config.json.j2
28     dest: "/home/{{ item }}/.docker/config.json"
29   vars:
30     user: "{{ item }}"
31   loop:
32     - "{{ default_user }}"
33     - "{{ default_users[1].name }}"
34
35 - name: Ensure root docker http headers
36   template:
37     src: config.json.j2
38     dest: "/root/.docker/config.json"
39   vars:
40     user: "root"
41
42 - name: Install OPA plugin
43   command: 'docker plugin install --grant-all-permissions
   ↪  openpolicyagent/opa-docker-authz-v2:0.4 opa-args="-policy-file
   ↪  /opa/policies/authz.rego"'
```

secure-daemon/templates/config.json.j2

```
1 {
2   "HttpHeaders": {
3     "Authz-User": "{{ user }}"
4   }
5 }
```

secure-daemon/templates/etc/docker/daemon.json.j2

```
1 {
2   "tlsverify": true,
3   "tlscacert": "{{ server_cert_path }}/ca.pem",
4   "tlscert": "{{ server_cert_path }}/server-cert.pem",
5   "tlskey": "{{ server_cert_path }}/server-key.pem",
6   "hosts": ["0.0.0.0:2376", "fd://"],
7   "authorization-plugins": ["openpolicyagent/opa-docker-authz-v2:0.4"]
8 }
```

secure-daemon/templates/etc/docker/policies/authz.rego.j2

```
1 package docker.authz
2
3 default allow = false
4
```

```
allow = true {
    input.Headers["Authz-User"] == "{{ default_user }}"
}

allow = true {
    input.Headers["Authz-User"] == "{{ default_users[1].name }}"
}

allow = true {
    input.Headers["Authz-User"] == "root"
}

# Needed for Traefik to communicate through TLS.
allow = true {
    input.User == "client"
}
```

bitbucket-pipelines.yml

```
pipelines:
  default:
    - step:
        name: 'Build'
        image: survivorbat/ansible:v0.3
        caches:
          - docker
        script:
          - 'echo -e $VAULT_PASSWORD > ../.vault-password'
          - 'ansible-galaxy install -r ansible/requirements.yml'
          - 'ansible-playbook
            -e node_tag=website-latest
            -e nginx_tag=website-latest
            -e traefik_tag=website-latest
            -e clone_dir=$BITBUCKET_CLONE_DIR
            -i ansible/inventories/local.yml
            --vault-password-file=../.vault-password
            -e add_latest_tag=false
            --tags=build_images ansible/site.yml'

  custom:
    e2e@test.developers.nl:
      - step:
          name: 'E2E @test.developers.nl'
          image: cypress/included:3.2.0
          caches:
            - node
          artifacts:
            - e2e/cypress/screenshots/**/*
          script:
```

```
            - 'cd e2e && CYPRESS_baseUrl=https://test.developers.nl
              ↪ cypress run'
    e2e@developers.nl:
      - step:
          name: 'E2E @developers.nl'
          image: cypress/included:3.2.0
          caches:
            - node
          artifacts:
            - e2e/cypress/screenshots/**/*
          script:
            - 'cd e2e && CYPRESS_baseUrl=https://developers.nl cypress
              ↪ run'
    deploy@test.developers.nl:
      - step:
          name: 'Deploy @test.developers.nl'
          deployment: test
          image: survivorbat/ansible:v0.3
          caches:
            - docker
          script:
            - 'echo -e $VAULT_PASSWORD > ../.vault-password'
            - 'ansible-galaxy install -r ansible/requirements.yml'
            - 'ansible-playbook
              -e node_tag=test-website-$BITBUCKET_BUILD_NUMBER
              -e nginx_tag=test-website-$BITBUCKET_BUILD_NUMBER
              -e traefik_tag=test-website-$BITBUCKET_BUILD_NUBER
              -e publish_images=true
              -e clone_dir=$BITBUCKET_CLONE_DIR
              -e bootstrap_proxy=false
              --vault-password-file=../.vault-password
              -i ansible/inventories/test.yml
              --skip-tags server_install
              ansible/site.yml'
      - step:
          name: 'E2E @test.developers.nl'
          image: cypress/included:3.2.0
          caches:
            - node
          artifacts:
            - e2e/cypress/screenshots/**/*
          script:
            - 'cd e2e && CYPRESS_baseUrl=https://test.developers.nl
              ↪ cypress run'
    deploy@developers.nl:
      - step:
          name: 'Deploy @developers.nl'
          deployment: production
          image: survivorbat/ansible:v0.3
          caches:
```

```
78            - docker
79          script:
80            - 'echo -e $VAULT_PASSWORD > ../.vault-password'
81            - 'ansible-galaxy install -r ansible/requirements.yml'
82            - 'ansible-playbook
83              -e node_tag=website-$BITBUCKET_BUILD_NUMBER
84              -e nginx_tag=website-$BITBUCKET_BUILD_NUMBER
85              -e traefik_tag=website-$BITBUCKET_BUILD_NUMBER
86              -e publish_images=true
87              -e clone_dir=$BITBUCKET_CLONE_DIR
88              -e bootstrap_proxy=false
89              --vault-password-file=../.vault-password
90              -i ansible/inventories/production.yml
91              --skip-tags server_install
92              ansible/site.yml'
93      - step:
94          name: 'E2E @developers.nl'
95          image: cypress/included:3.2.0
96          caches:
97            - node
98          artifacts:
99            - e2e/cypress/screenshots/**/*
100         script:
101           - 'cd e2e && CYPRESS_baseUrl=https://developers.nl cypress
              ↪ run'
102   bootstrap@test.developers.nl:
103     - step:
104         name: 'Bootstrap @test.developers.nl'
105         deployment: test
106         image: survivorbat/ansible:v0.3
107         caches:
108           - docker
109         script:
110           - 'echo -e $VAULT_PASSWORD > ../.vault-password'
111           - 'ansible-galaxy install -r ansible/requirements.yml'
112           - 'ansible-playbook
113             -e node_tag=test-website-$BITBUCKET_BUILD_NUMBER
114             -e nginx_tag=test-website-$BITBUCKET_BUILD_NUMBER
115             -e traefik_tag=test-website-$BITBUCKET_BUILD_NUMBER
116             -e publish_images=true
117             -e clone_dir=$BITBUCKET_CLONE_DIR
118             -e bootstrap_proxy=true
119             --vault-password-file=../.vault-password
120             -i ansible/inventories/test.yml
121             ansible/site.yml'
122   bootstrap@developers.nl:
123     - step:
124         name: 'Bootstrap @developers.nl'
125         deployment: production
126         image: survivorbat/ansible:v0.3
```

```
127           caches:
128             - docker
129           script:
130             - 'echo -e $VAULT_PASSWORD > ../.vault-password'
131             - 'ansible-galaxy install -r ansible/requirements.yml'
132             - 'ansible-playbook
133                 -e node_tag=website-$BITBUCKET_BUILD_NUMBER
134                 -e nginx_tag=website-$BITBUCKET_BUILD_NUMBER
135                 -e traefik_tag=website-$BITBUCKET_BUILD_NUMBER
136                 -e publish_images=true
137                 -e clone_dir=$BITBUCKET_CLONE_DIR
138                 -e bootstrap_proxy=true
139                 --vault-password-file=../.vault-password
140                 -i ansible/inventories/production.yml
141                 ansible/site.yml'
142 options:
143   docker: true
144
145 definitions:
146   services:
147     docker:
148       memory: 3072
```

Bijlage B

Tabellen

B.1 Beyond the 12-factor app

In deze tabel worden de 15 factoren behandeld.

Factor	Naam	Gevolg	Waarom?
1	One codebase, one application	Onderhoudbaarheid (Modulariteit)	Een applicatie is een losstaand component waardoor wijzigingen minimale impact hebben op andere componenten.
2	API first	Structural scalability	Door de API op de eerste rang te zetten van het development proces wordt de mogelijkheid gecreëerd om met elkaars contracten te communiceren zonder interne ontwikkelingsprocessen te verstoren. Zo kunnen veel nieuwe services gemakkelijker worden toegevoegd.
3	Dependency management	Onderhoudbaarheid (modulariteit)	Gemakkelijk opzetten van project voor nieuwe ontwikkelaars.
4	Design, build, release, and run	Onderhoudbaarheid (wijzigbaarheid)	Door duidelijke stadia te definiëren worden wijzigingen aan de applicatie sneller in productie geplaatst.
5	Configuration, credentials, and code	Structural scalability	Environment variabelen zijn niet in omgevingen maar per deployment opgezet, zo maakt de hoeveelheid omgevingen niet uit.

6	Logs	Onderhoudbaarheid (analyseerbaarheid)	Door logs naar de `stdout` te sturen is het gemakkelijker om specifieke fouten te vinden, overzicht te creëren en actief meldingen te versturen naar ontwikkelaars.
7	Disposability	Load scalability	Door processen gemakkelijk te laten stoppen en starten gaat het schalen een stuk sneller.
8	Backing services	Onderhoudbaarheid (modulariteit)	Door backing services als "attached resources" te behandelen maakt het niet uit welke techniek er wordt gebruikt en zijn deze dus los gekoppeld.
9	Environment parity	Onderhoudbaarheid (wijzigbaarheid)	Er kan een stuk vaker gedeployed worden naar een specifieke omgeving, doordat alle omgevingen zo goed als gelijk aan elkaar zijn.
10	Administrative processes	Onderhoudbaarheid (analyseerbaarheid)	Door commands in versiebeheer op te slaan is er een duidelijk overzicht en een geschiedenis van alle "one-off processes" die gebeuren.
11	Port binding	Onderhoudbaarheid (wijzigbaarheid)	Door HTTP als een service te beschouwen ontstaat er meer controle over lagere levels van de infrastructuur (HTTP & TCP).
12	Stateless processes	Load scalability	Mede door de shared-nothing architectuur kan het systeem gemakkelijker schalen.
13	Concurrency	Load scalability	Door het horizontaal of verticaal schalen kan de applicatie een groeiende hoeveelheid verkeer beter aan.
14	Telemetry	Onderhoudbaarheid (Analyseerbaarheid)	Door gegevens van de applicatie in productie goed te kunnen monitoren is op te maken hoe de applicatie zich gedraagt. Zodra er iets fout is kan er meteen op worden gereageerd.

15	Authentication and authorization	Security	Een cloud-native applicatie moet veilig zijn, aangezien de code over meerdere data centers wordt getransporteerd en door veel verschillende cliënten wordt benaderd.

Bijlage C

Gesprekken

C.1 Requirements

Dit zijn de gemaakte aantekeningen tijdens discussies over de requirements met Jelle:

- schaalbaarheid: meerdere omgevingen (feature branches)
- Merge train -> automatische merges en deploys
- Pulumi
- Generieke boilerplate voor een CI/CD Pipeline
- segregation of duties
- docker swarm voor performance curves te laten zien
- Advies over deployment targets
- testbaarheid -> static code analysis -> integratie tests ->
- Hoeveelheid coverage -> pipeline
- Probleemstelling & requirements
- Functional scalability
- Wat te monitoren?
- Product owner validatie & automatisch testen apart
- Validaties zo veel mogelijk automatisch (policies, segregation of duties)
- Kwaliteit waarborgen -> concreter
- Functional scalability -> Extensibility
- Extensibility functioneel? niet functioneel? Vragen stellen feedback online!
- Monitoring: Metrics als ruimte -> cpu -> memory uiteindelijk verkeer, etc. promethius
- terraform (firewalls, netwerken) voor alles tot aan de VM en ansible om de vm af te configureren
- TransIP Terraform API
- Nexpertise Terraform

C.2 Feature environments

Slack conversatie met Jelle:

```
Hey ik heb denk ik iets gevonden wat mij wel een leuke oplossing
lijkt:
https://github.com/jwilder/nginx-proxy
Het luistert naar je docker run commands om daaruit environment
variabelen te halen; waaronder VIRTUAL_HOST , waardoor het dus iets
als VIRTUAL_HOST=${BITBUCKET_BRANCH}.${HOSTNAME} kan worden. Wat vind
jij hiervan? Een mogelijke oplossing? Of tenminste een deel
hiervan.... zodat er niet een volledige abstractielaag op zit
```

Reactie van Jelle:

```
Zou idd een oplossing zijn, kijk anders ook ffe naar traefik.io
```

Conversatie over het beveiligen van de Docker Socket:

```
Kaj:
Oke dit lijkt mij wel een probleem:
https://github.com/containous/traefik/issues/4174
Zowel de nginx-proxy als traefik hebben dit.. is dit:
https://github.com/Tecnativa/docker-socket-proxy écht de beste
oplossing hiervoor, of heb jij toevallig nog een geniale ingeving?

Jelle:
Zou ik me even in moeten verdiepen, met de oplossing die ik met nginx
aan het rommelen was gebruikte ik docker labels en docker inspect

Kaj:
Hmm oke oke
Misschien is dat ook wel een goeie, want nginx moet er toch inblijven
aangezien traefik geen fastCGI support heeft

Jelle:
Ja maar das dan achter traefik als load balancer zegmaar

Kaj:
Oh.. dus dan heb je traefik statisch geconfigureerd?

Jelle:
Bekijk de docker-compose file:
https://medium.com/@luiscoutinh/reverse-proxy-com-docker-traefik-nginx-
php-mysql-mosquitto-phpmyadmin-basic-34c95b690f5c

Kaj:
Ja precies, dat is ongeveer hoe het wordt aangeraden. Maar ook die
oplossing exposed de docker socket
```

```
Jelle:
ja idd dat is een probleem, iig voor productie
Expose the Docker socket over TCP, instead of the default Unix socket
file

Kaj:
Dat is eigenlijk het enige waar ik tegenaan loop, want een oplossing
met traefik lijkt mij bijna precies wat ik zoek

Jelle:
dat kan wel, via certificaten beveiligen:
https://docs.traefik.io/providers/docker/#docker-api-access
```

C.3 (niet-)functionele schaalbaarheid

Na het promoten van de geschreven blog[1] is dit de meest populaire blog van Developers.nl in 2019 geworden. Dit heeft het volgende feedbackpuntje opgeleverd: "Scalability is a two way thing, so adding and removing should be in the definition (and thought lines)". Waar ik het volledig mee eens ben, en zal verbeteren in de toekomst. Ook is er een leuke discussie uit gekomen. Marlon Etheredge, MSc vroeg:

```
Hi Kaj,

Mijn vraag behoeft enige introductie.

Ik ben werkzaam in een deelgebied van de
informatica/software-engineering waarbij performantie zeer belangrijk
is, computer graphics. Onze implementaties dienen zo snel als mogelijk
antwoorden te geven op soms complexe berekeningen, doorgaans in
(minder dan) millisecondes.

Schaalbaarheid in mijn context staat dan ook voor twee dingen; ten
eerste gaat het om het niet schenden van tijdsgrenzen waar wij mee te
maken hebben (e.g. één frame dient in 1/50 seconde klaar te zijn)
onafhankelijk van de hoeveelheid data die verwerkt moet worden. Ten
tweede staat schaalbaarheid voor implementaties die rekbaar zijn op
basis van veranderende eisen die aan een systeem worden gesteld.

In deze context gaat het dan niet zo zeer om een veranderend systeem,
waarbij bijvoorbeeld functionaliteit wordt toegevoegd
("... must be modified as soon ..." in je eerste definitie), of het
systeem verbeterd wordt ("... is able to be improved ..." in je tweede
definitie), maar eerder om een kwaliteitskenmerk van een systeem in
ogenschouw nemend welke eisen mogelijk in de toekomst aan dit systeem
gesteld zullen worden en de hoeveelheid energie die het zal kosten om
het systeem te laten aansluiten op deze eisen. In die zin denk ik
overigens ook dat dit een interessant onderwerp is, aangezien het
ontwerpen van dergelijke systemen fundamenteel is aan de informatica.
```

[1] https://developers.nl/blog/69/Defining-software-scalability-using-requirements

```
Mijn concrete vraag aan jou is als volgt; je schrijft:

"Instead of adding more of the same requirement, non-functional
requirements like security or usability are always able to be
improved. Therefore, scaling a non-functional requirement is the same
as improving it. Setting clear requirements helps proving your
solution is scalable non-functionally."

Is verandering (bijvoorbeeld in de vorm van verbetering) noodzakelijk
voor schaalbaarheid, of is het mogelijk schaalbaarheid te toetsen los
van verandering?
```

Mijn antwoord:

```
Schaalbaarheid in jouw context sluit goed aan op mijn twee definities:
Je noemt "het niet schenden van tijdsgrenzen ... onafhankelijk van de
hoeveelheid data"; in dit geval zijn de berekeningen een functionele
requirement, en deze moeten voldoende blijven functioneren naarmate
het hoeveelheid gebruik toe neemt. In deze context gaat het
functioneren dus over het niet schenden van tijdsgrenzen, en de
hoeveelheid gebruik over de hoeveelheid data.

De tweede definitie die je noemt (schaalbaarheid voor implementaties
die rekbaar zijn op basis van veranderende eisen) omvat in dit geval
zowel functionele als niet functionele schaalbaarheid. In mijn
definities heb ik het vooral over opschalen, dit is nog een
verbeterpunt. Het concept van "veranderende eisen" vind ik een mooie.

Om antwoord te geven op je vraag: Schaalbaarheid is een
kwaliteitskenmerk, het daadwerkelijk schalen is een uitoefening van
dit kenmerk. Dus, ja, het is mogelijk om schaalbaarheid te toetsen los
van daadwerkelijke verandering. Een kwaliteitsanalyse op kenmerken als
complexiteit van algoritmes bijvoorbeeld. In de context van
functionele schaalbaarheid is dit "to what extent it continues to
function properly as the amount of use of the system increases", en
van niet-functionele schaalbaarheid "to what extent the quality of
that requirement remains acceptable as the use of the system
increases".

Ik hoop dat ik hiermee je vraag voldoende heb beantwoord, zo niet hoor
ik het graag uiteraard.
```

Marlon was tevreden met dit antwoord:

```
Duidelijk, dank voor je antwoord, erg interessant.
```