



HoGent

Faculteit Bedrijf en Organisatie

Docker for Windows

Stephan Heirbaut

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Steven Vermeulen
Co-promotor:
Gert Schepens

Instelling: —

Academiejaar: 2017-2018

Tweede examenperiode

Faculteit Bedrijf en Organisatie

Docker for Windows

Stephan Heirbaut

Scriptie voorgedragen tot het bekomen van de graad van
professionele bachelor in de toegepaste informatica

Promotor:
Steven Vermeulen
Co-promotor:
Gert Schepens

Instelling: —

Academiejaar: 2017-2018

Tweede examenperiode

Samenvatting

Docker for Windows Server 2016 is uit beta gekomen op 22 februari 2017. Maar, ondanks het feit dat dit platform nu al een ruime tijd beschikbaar is, heeft het nog steeds geen tractie gevonden bij DevOps-teams. Dit ondanks het feit dat dit een krachtige tool kan zijn voor organisaties die ook Microsoft Certified Partners willen zijn. In een notendop, er zal dus gekeken worden of Docker for Windows Server 2016 een goed alternatief is voor het draaien van Docker in een Linux omgeving. Om dit op een methodologische manier uit te testen zal er vertrokken worden van een standaard Windows Server 2016 en CentOS 7.4 installatie waarop Docker geïnstalleerd zal worden. Waarna beide omgevingen getest zullen worden door middel van prestatie- en beveiligingstesten, om zo een vergelijking te maken van beide omgevingen. Daarbovenop zal ook de documentatie voor beide platformen bekeken worden op vlak van compleetheid.

De verwachting is dat het verschil tussen beide systemen minimaal zal zijn, maar dat de prestaties van de CentOS server beter zullen zijn. De documentatie voor CentOS zal ook meer compleet zijn, maar dat zowel Windows als Docker een grote inhaalbeweging aan het maken zijn.

Verdere vragen die men hierna nog zou kunnen stellen zijn:

- Hoe goed scoren beide op vlak van user-friendliness?
- Hoe goed ondersteunen beide Cloud platforms?
- Hoe stabiel draaien beide omgevingen?

Voorwoord

Deze bachelorproef voert een vergelijkende studie uit tussen Docker for Windows en Docker for Linux. Specifiek wordt er gebruik gemaakt van een Windows Server 2016 met GUI, waarop Docker for Windows wordt geïnstalleerd. Deze Linux omgeving bestaat uit een CentOS 7.4 waarop Docker for Linux wordt geïnstalleerd. Op beide platformen worden daarna twee containers uitgerold: de eerste container is een Microsoft SQL server en de tweede container bevat een .NET webapplicatie.

Als eerste werd de documentatie vergeleken tussen beide omgevingen op vlak van volledigheid en gebruiksgemak. Vervolgens werden beide systemen getest op de benodigde tijd voor het uitvoeren van een volledige installatie en de installatie van de containers. Voor de installatie van beide systemen wordt er gebruik gemaakt van Vagrant. Zodanig dat de installatie van het besturingssysteem, de benodigde applicaties en de containers zoveel mogelijk geautomatiseerd kon worden. Dit maakte het mogelijk om op een methodologische manier de prestaties te testen van beide systemen. Vervolgens werd er een vergelijkende studie uitgevoerd tussen de veiligheid van de CentOS-omgeving en de Windows-omgeving. Van Linux is geweten dat de veiligheid er goed is, als men alle functionaliteit ervan gebruikt. De vraag was dus: welke mogelijkheden heeft Windows om die te evenaren? Ten slotte volgt er op het einde een conclusie welk systeem het best past binnen DevOps teams en hoe men het best met beide om gaat.

De reden waarom ik dit onderwerp koos zijn meervoudig: als eerste vind ik de Container-technologie uitermate fascinerend en ga ik hier zeker verder mee spelen na mijn bachelorproef. Daarnaast was ik aangenaam verrast dat Docker ging samenwerken met Microsoft om hun technologie beschikbaar te stellen voor het Windows OS. Dit past natuurlijk wel in het manifesto van Microsoft CEO Satya Nadella om het bedrijf een nieuwe richting te doen inslaan. Ten slotte leek me dit een uitermate geschikt onderwerp voor een bachelorproef.

Er zijn al verschillende Blog posts en artikels verschenen hierover. Maar, de meeste raken alleen maar de oppervlakte van de zaak of erger: leveren geen concrete cijfers, maar alleen buikgevoel gedreven meningen.

De bachelorproef uitwerken ging vrij vlot. Buiten een paar problemen met de webapplicatie en het automatiseren van de Windows-omgeving zat dit wel snor. Het schrijven was een beetje moeilijker, aangezien er geen linguïst verloren is gegaan aan mij. Ondanks het moeilijke schrijven was het wel een aangename ervaring. Ik had nog niet eerder een werk van dit kaliber mogen opleveren en hoewel het zwaar werken was, ik ben wel tevreden van het werk dat ik geleverd heb.

Ten slotte zou ik nog graag enkele mensen bedanken:

Als eerste zou ik mijn promotor Steven Vermeulen willen bedanken. Hij heeft me vooral op literair vlak een stevige duw kunnen geven in de goede richting met zijn feedback.

Daarnaast zou ik ook graag mijn co-promotor willen bedanken: Gert Schepens. Zelfs tijdens drukke momenten heeft hij tijd kunnen vrijmaken voor mij en mijn bachelorproef.

Vervolgens wil ik ook even mijn vriendin in de bloemetjes zetten. Ze heeft mij meerdere malen geholpen bij het verbeteren van mijn teksten, wanneer ik wel wist wat ik wou schrijven. Maar, niet hoe.

Ten slotte wou ik ook Bert Van Vreckem bedanken voor zijn hulp bij dit onderwerp. Zonder zijn hulp zou de webapplicatie misschien nog steeds niet werken. Via hem ben ik ook op het idee gekomen om dit onderwerp te behandelen.

Stephan Heirbaut 25 mei 2018, Lokeren

Inhoudsopgave

1	Inleiding	11
1.1	Stand van zaken	11
1.1.1	DevOps	11
1.1.2	Docker	13
1.1.3	Linux Containers	17
1.1.4	Hyper-V	17
1.1.5	Windows Job objects	19
1.1.6	Silos	19
1.1.7	Virtual Box	19
1.1.8	Vagrant	20
1.1.9	PowerShell	21
1.1.10	Bash	21
1.1.11	Software testing	22

1.2	Probleemstelling en Onderzoeksvragen	23
1.3	Opzet van deze bachelorproef	24
2	Methodologie	25
2.1	Literatuurstudie	25
2.2	Bekijken van documentatie	25
2.3	Opzetten van de servers	25
2.4	Uitvoeren van de verschillende tests	26
2.5	Vergelijkende studie uitvoeren	26
3	Documentatie	27
3.1	Requirements	27
3.2	Installatie	28
3.3	Container tot stand brengen	28
3.4	Automatisatie	28
3.5	Conclusie	29
4	Opstelling	31
4.1	Windows Server 2016	31
4.1.1	Vagrant	31
4.1.2	PowerShell	34
4.2	CentOS 7.4	37
4.2.1	Vagrant	37
4.2.2	Bash	38

5	Performantie test	43
5.1	CentOS 7.4	44
5.1.1	Performantie installatie	44
5.1.2	Performantie containers	45
5.2	Windows Server 2016	46
5.2.1	Performantie installatie	46
5.2.2	Performantie applicatie	48
5.3	Conclusie	49
6	Security test	51
6.1	CentOS	52
6.1.1	Linux containers	52
6.1.2	SELinux	52
6.1.3	Firewalld	53
6.1.4	Seccomp	53
6.2	Windows	54
6.3	Hyper-V containers	54
6.4	Integrity levels	54
6.5	Windows Defender	55
6.5.1	ACL	55
6.6	Conclusie	55
7	Conclusie	57
	Bibliografie	58

1. Inleiding

Voor 22 februari 2017 kon men enkel Docker installeren op Linux-besturingssystemen. Ondernemingen zonder Linux-kennis die wilden evolueren naar DevOps werden op die manier gedwongen om iemand in dienst te nemen die deze kennis wel had, ofwel om zelf een spoedcursus te volgen. Echter met de komst van Windows 10 en Windows Server 2016, en de daarmee gepaard gaande groei van PowerShell en Hyper-V, is Docker nu ook toegankelijk voor organisaties die meer Windows-gezind willen zijn.

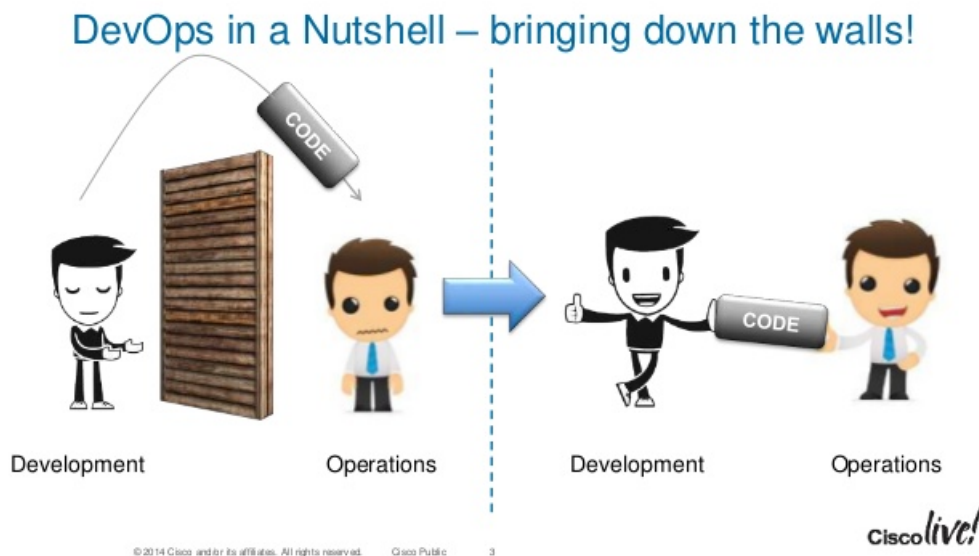
Het zou namelijk een vergissing zijn om Docker zomaar te negeren als men de DevOps-richting wil uitgaan. Het biedt immers verschillende tools aan voor zowel developers als system administrators. Bijvoorbeeld: Containers as a Service (CaaS) en role-based access control voor Operations (system administrators), en een zelfbedieningsmanier van werken voor Developers waarbij ze services kunnen opvragen wanneer ze die nodig hebben. Momenteel wordt Docker gebruikt in 44 procent van de ondernemingen die van plan zijn om de DevOps-richting uit te gaan.

1.1 Stand van zaken

1.1.1 DevOps

DevOps is een samenstelling van de woorden 'Development' en 'Operations': ontwikkeling en beheer. Voorheen werkten deze IT-groeperingen strikt gescheiden, waardoor je ofwel bij de ene groep zat ofwel bij de andere. Dit zorgde ervoor dat, als men een applicatie wou maken, de developers deze dan eerst ontwikkelden, waarna de systeembeheerders de applicatie uitrolden. Als de systeembeheerders hierna nog problemen hadden met het

Figuur 1.1: Links ziet men hoe de communicatie in klassieke ontwikkelomgevingen gebeurt, rechts in DevOps teams

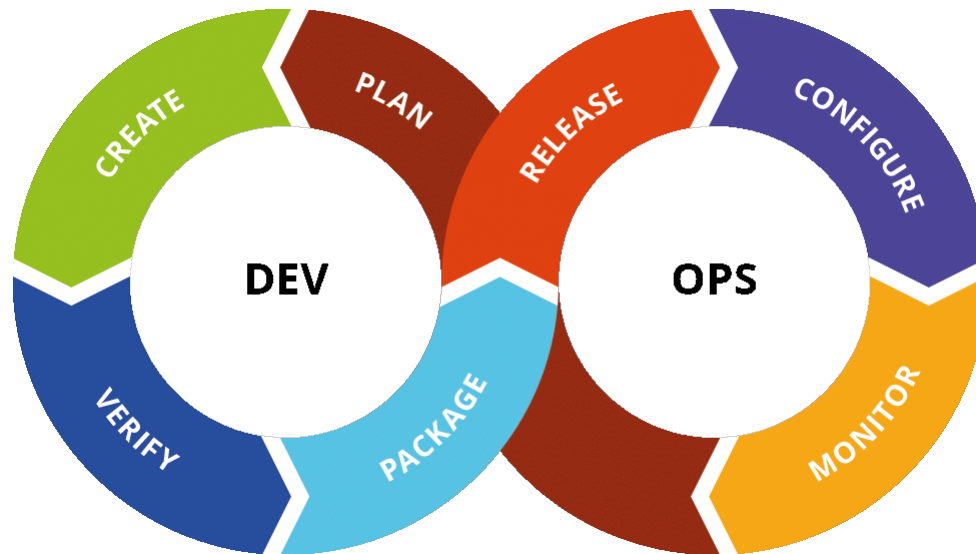


uitrollen, verliep de communicatie veelal stroef. De applicatie werkte immers op de computers van de developers, dus waarom zou dat niet het geval zijn bij de systeembeheerders? Echter, aangezien beide groeperingen onvoldoende kennis hadden over elkaars werkveld, was er veel onbegrip.

Als éénduidige definitie voor DevOps gebruikt met het acroniem 'CALMS'.

- Culture (Cultuur)
- Automatisation (Automatisatie)
- Learning (Leren, voorheen Lean)
- Measure (Metten)
- Sharing (Delen)

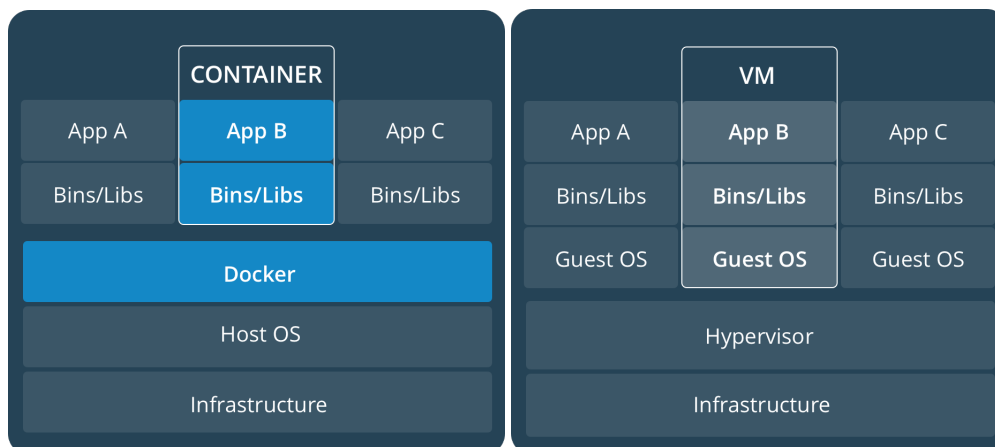
Bij DevOps worden deze groepen gedwongen om samen te werken in één team, zodat het geheel groter wordt dan de som. In praktijk vertaalt dit zich naar een cultuur die gestimuleerd dient te worden, waarin het automatiseren van zoveel mogelijk zaken centraal staat met een focus op continue ontwikkeling en oplevering (cfr. CI/CD). Hierbij is het leren, delen van informatie, en communicatie in het algemeen, heel belangrijk. Er worden verschillende manieren voorzien om informatie te verzamelen uit de applicatie, door methodes te implementeren die men gebruikt om een doorzichtiger systeem te creëren. Het is dus eerder een groep van concepten en ideeën die uitgegroeid zijn tot een beweging die snel tractie aan het winnen is.



1.1.2 Docker

De beste manier om de verschillen in werking te beschrijven tussen fysieke servers, virtuele machines (VM's) en containers, is door ernaar te kijken zoals een woning. Fysieke servers en virtuele machines zijn zoals huizen. Ze werken volledig onafhankelijk en voorzien zelf in al hun noden qua infrastructuur. Een fysieke server wordt bovendien volledig onafhankelijk opgebouwd vanaf nul. Een virtuele machine echter wordt naast een bestaand host besturingssysteem gedraaid, waarbij het een bepaalde hoeveelheid infrastructuur opeist. Een virtuele machine is dus eigenlijk een computer in een computer. Beide systemen hebben hetzelfde grote nadeel, namelijk dat er veel meer infrastructuur nodig is en dat deze niet optimaal wordt gebruikt. Containers zijn eerder te vergelijken met appartementen, namelijk dat de infrastructuur wordt opgedeeld. Alle middelen van de host-machine waar de Docker Daemon op geïnstalleerd wordt, worden verdeeld onder de verschillende containers. Elke container vraagt hierbij alleen de nodige grondstoffen om te voldoen aan de noden van zijn bewoner, net zoals bij een appartement. Containers lijken op het eerste zicht erg op virtuele machines, maar het is belangrijk om te onthouden dat de onderliggende architectuur sterk verschilt tussen beide.

Doordat een Container alleen de benodigde infrastructuur opeist die hij nodig heeft, bouwt die een lichter en onafhankelijk uitvoerbaar softwarepakket op, dat consistentie kan garanderen omdat het telkens dezelfde achterliggende Docker Images en Daemon gebruikt. Een van de meest voorkomende problemen bij het uitrollen van een applicatie is het verschil tussen de test- en productieomgeving, en de hiermee gepaarde infrastructuurlast.



Docker is een tool om deze Containers te bouwen. Hiermee kan men het uitrollen van applicaties sneller en makkelijker maken, doordat het de applicatie en al haar benodigdheden eerst in één geautomatiseerd pakket verzamelt. Dit pakket noemt een image. De uitgerolde versie van een image noemt men een Container en deze zal los van het host besturingssysteem werken.

Om een Container op te bouwen van begin tot einde maakt men gebruik van de Docker Client. Via de Client kan men communiceren met de Docker Daemon. De Docker Daemon is een proces dat op de achtergrond draait tot het aangeroepen wordt door de gebruiker via de syntaxis van Docker. De Docker Daemon is uiteindelijk degene die de Docker commando's interpreteert en uitvoert, zoals het bouwen, draaien en onderhouden van containers.

Bij het bouwen van een container via Docker zijn er 23 werkmethodes te onderscheiden, namelijk een standaard-, minimalistische- of geautomatiseerde methode. De minimalistische methode wordt gebruikt bij installaties die geen customisation vereisen, bijvoorbeeld een SQL-server. De standaardmethode wordt gebruikt bij alle andere installaties, bijvoorbeeld een CentOS-server. De standaardmethode bestaat uit 4 stappen die hieronder meer uitgebreid besproken worden. Bij de minimalistische methode worden enkel de eerste en de laatste stap uitgevoerd.

- docker pull

De eerste stap is docker pull. Hiermee kan men een Docker Image ophalen van de Docker Hub. Deze images zijn momentopnames van bijvoorbeeld containers of besturingssystemen. Deze kunnen, afhankelijk van de gebruiker, uitgebreid worden via een Dockerfile. Het is met deze parent image dat men een container kan bouwen.

- Dockerfile

De tweede stap is Dockerfile, waarin men aan de hand van de syntaxis een gepersonaliseerde Docker Image kan definiëren. Men kan aangeven vanaf welke image men wil beginnen via het 'FROM'-commando. Men hoeft hier echter niet per se een parent image mee te geven, bijvoorbeeld via 'FROM scratch'. Vervolgens kan men environment varia-

bles meegeven via 'ENV', 'ADD' of 'EXPOSE'. Daarnaast kan men via 'RUN' ook orders meegeven om specifieke commando's uit te voeren die de container zou herkennen zoals Bash of PowerShell. Ten slotte kan men via 'ENTRYPOINT' aangeven of de container uitvoerbaar moet zijn of niet.

- docker build

De derde stap is docker build, waarmee men opnieuw de Docker Daemon aanspreekt. Op die manier kan die de syntax interpreteren en een gepersonaliseerde container bouwen.

- docker run <options> <image>

Ten slotte is er docker run, waarmee men het bevel geeft aan de Docker Daemon om de image uit te rollen tot een container. Hoe de image zich uitrolt, hangt af van de bevelen in het commando en van de image die gebruikt wordt.

Bij de geautomatiseerde methode maakt men ook gebruik van de 4 hierboven beschreven stappen. Maar, voegt men een extra component toe in de vorm van docker-compose.yml. In dit bestand kan men meerdere services beschrijven waarvan Docker containers moet maken. Daarnaast dient dit bestand geplaatst te worden in dezelfde folder als het 'dockerfile'-bestand. Ten slotte, zullen alle services die hierin beschreven staan in orde gebracht worden door het 'docker-compose up'-commando uit te voeren.

Docker-compose is daarom vooral handig wanneer men meerdere services wil in orde brengen die afhankelijk zijn van elkaar, zoals een webapplicatie en de bijhorende SQL-server. Hieronder ziet u een voorbeeld van een docker-compose.yml-bestand.

```
backend: image: redis:3 restart: always
```

```
frontend: build: commander links: - backend:redis ports: - 8081:8081 environment: - VAR1=value restart: always
```

Docker voorziet ook commando's om de Docker Images en Boxes te beheren. De voorname staan hieronder beschreven.

Commando	Uitleg
docker images	toont alle Docker Images beschikbaar op dit systeem
docker ps	toont alle draaiende containers
docker inspect <container>	toont de specificaties van een specifieke container
docker logs <container>	toont alle logs voor een specifieke container
docker start <container>	start een specifieke container op
docker stop <container>	stopt een specifieke container
docker rm <container>	verwijdert containers

Doordat elk deel van een applicatie in een 'appartementje' zit, is het maken van continue ontwikkeling en oplevering voor de applicatie heel gemakkelijk. Men moet immers alleen die specifieke Container updaten/graden. Hierdoor is het de perfecte technologie om te dienen als test- en productieomgeving. Daarnaast versoepelt het ook de communicatie

binnen het DevOps-team, doordat iedereen continu in dezelfde omgeving werkt. Er zijn immers geen grote veranderingen nodig bij de verschillende stappen binnen de leveringsketen, omdat men in staat is om verschillende frameworks te draaien op één platform. Containers zijn namelijk vrij agnostisch zijn op vlak van programmeertaal of platform. Ten slotte kunnen Containers ook makkelijk van host-besturingssysteem verplaatst worden. Al deze kenmerken van Docker Containers vergemakkelijken het werk van DevOps-teams aanzienlijk.

Door al deze redenen blijft Docker ook jaar na jaar groeien. Tijdens de recentste DockerCon heeft de CEO van Docker dit ook aangetoond met volgend cijfermateriaal:

- Meer dan 14 miljoen Docker hosts
- More dan 900.000 applicaties die draaien op Docker
- Een verhoging van 40 procent in het toepassen ervan in 1 jaar

Docker heeft deze groei ook verdiend door constant in contact te blijven met zijn gebruikers. In het verleden kregen ze immers de klacht dat ze te snel of te traag updates toevoegden aan het systeem. Om dit te remediëren hebben ze naast Docker Community Edition, waarmee alles is begonnen, nu ook Docker Enterprise Edition ontworpen. Daarbovenop is er een verschuiving naar time-based updates. Hierbij kan men kiezen tussen een maandelijks update, maar zonder garantie op stabiliteit van de runtime (Edge), ofwel voor een viermaandelijks update voor gebruikers die meer stabiliteit prefereren, zowel op vlak van onderhoud als van beheer (Stable). Daarbovenop heeft de Enterprise Edition ook een meer uitgebreide ondersteuning met verschillende gradaties.

Docker CE

Zoals eerder aangehaald is Docker Community Edition het originele platform waarmee Docker begonnen is. Het is ideaal voor kleinere teams of onafhankelijke developers die willen experimenteren met Container-technologie. Deze technologie is beschikbaar voor zowel Linux als Mac, waardoor het perfect is als kleine en snelle installatie waarmee men direct aan de slag kan gaan. Ten slotte, biedt het ook ondersteuning voor het uitrollen naar Cloud-omgevingen, zoals Amazone Web Services of Azure.

Docker EE

Docker Enterprise Edition is het volledige pakket voor zij die op een professionele manier met een Containers-as-a-Service-platform willen werken. Docker EE is een geïntegreerd en getest platform voor Linux- of Windows Enterprise en Cloud-providers, met door Docker gecertificeerde componenten en ondersteuning. In het bijzonder is het voor datacenters een handig dashboard waar men de zogenaamde multi-architecture orchestration, secure software supply chain en infrastructure independence aangeboden krijgt. Vooral aan dat laatste heeft Docker extra veel aandacht besteed., met kenmerken zoals trusted delivery.

Docker for Windows

Daarnaast heeft Docker ook een versie ontwikkeld specifiek gericht voor Developers die gebruik willen maken van Windows als ontwikkel platform. Docker for Windows maakt gebruik van dezelfde Daemon en Client als Docker for Linux. Maar, met een paar verschillen zoals: Docker for Windows maakt gebruik van de Windows-native Hyper-V Virtualisatie. Wat betekent dat de gebruiker een Windows 8+ Pro edition of een Windows Server 2008+ nodig heeft. Aangezien alleen deze versies van Windows Hyper-V hebben. Daarnaast is de enige manier om Docker CE for Windows te installeren door gebruik te maken van een GUI installatie. Men kan gebruik maken van PowerShell commando's zoals Invoke-WebRequest. Maar, er is geen native PowerShell commando voor het installeren van Docker for Windows. Docker EE for Windows kan dan weer wel via de commandline geïnstalleerd worden. Ten slotte, wordt docker-compose ook automatisch geïnstalleerd als men Docker CE for Windows installeert. Het maakt deel uit van het totaal pakket. Dit in tegenstelling tot Docker EE for Windows, waarbij docker-compose wél nog apart geïnstalleerd moet worden.



1.1.3 Linux Containers

Docker CE for Linux maakt gebruik van de technologie achter Linux Container voor het maken van zijn Docker Containers.

Linux containers hebben hun eigen netwerk resources, geheugen geïsoleerde CPU, geheugen en I/O block. Maar, ze gebruiken wel dezelfde kernel als het host besturingssysteem. Hierdoor kunnen ze lichte en gestroomlijnde containers bouwen. Cgroups en Namespaces maakt dit mogelijk.

Cgroups

Namespaces

1.1.4 Hyper-V

Hyper-V is één van de technologie die gekozen werd om de twee servers, CentOS en Windows Server 2016, op te laten draaien. Dit is het Microsoft-platform voor het virtualiseren van hardware. Het maakt gebruik van hypervisor-gebaseerde virtualisatie technologie om

de interactie tussen de virtuele machine en de hardware te voorzien. Hierdoor is men in staat om een andere computer te laten werken bovenop het host-besturingssysteem. De voornaamste componenten en hun functies van dit platform zijn:

- Windows Hypercall

Hypercall voorziet communicatie met de Hypervisor.

- Windows hypervisor

Dit is een softwarelaag wiens primaire verantwoordelijkheid is om geïsoleerde execution environments te voorzien. Deze execution environments noemen partitions. Hypervisor is gelegen tussen de hardware en één of meer besturingssystemen, zodat het hardwaregebruik kan optimaliseren voor al de partitions.

- Hyper-V Virtual Machine Management Service

VMMS is verantwoordelijk voor het beheren van de staat van alle virtuele machines in zogenaamde child partitions.

- Virtual Machine Bus

Dit channel-based communicatiemechanisme voorziet de communicatie tussen verschillende partitions op systemen met meer dan één virtual partition.

- Virtualization Service Provider

VSP bevindt zich in de root partition en voorziet synthetische ondersteuning aan child partitions over de VMBus.

- Virtual Infrastructure Driver

De VID voorziet partition-, processor- en memory services.

Daarnaast bevat Hyper-V ook nog andere low level componenten, zoals:

- APIC - Advanced Programmable Interrupt Controller
- IC - Integration component
- MSR - Memory Service Routine
- VMWP - Virtual Machine Worker Process
- VSC - Virtualization Service Client
- WinHv - Windows Hypervisor Interface Library
- WMI - Virtual Machine Management Service

Tenslotte heeft Hyper-V ook enkele tools voor het beheren van en verbinden met zijn virtuele machines. Deze kunnen geïnstalleerd worden op zowel computers waar Hyper-V op staat, als op externe computers. Deze zijn meer specifiek:

- Hyper-V Manager

- Hyper-V module for Windows PowerShell
- Virtual Machine Connection
- Windows PowerShell Direct

Om deze servers te verbinden met het internet wordt ook gebruik gemaakt van de Hyper-V Virtual Switch. Deze laag 2 Ethernet netwerkswitch voorziet programmeer- en uitbreidbare mogelijkheden om het beheren van virtuele en fysieke netwerken te vergemakkelijken. Het voorziet veiligheid, isolatie en service levels om de nodige veiligheid af te dwingen.

Hyper-V is een type 1 Hypervisor. Dit betekent dat het opstarten van een virtuele machine als volgt gaat:

- Eerst wordt de fysieke machine opgestart.
- Vervolgens wordt de controle van het boot systeem van de fysieke machine overgedragen aan Hyper-V, bijvoorbeeld BIOS of EUFI.
- Daarna start Hyper-V het management operating system.
- Ten slotte maakt Hyper-V partitions aan voor de virtuele machines, afhankelijk van de boot- of gebruikersinstructies.

Daarnaast draait een type 1 Hypervisor ook direct op de hardware. Daarom worden ze ook wel 'native', 'bare metal' of 'embedded' Hypervisors genoemd.

1.1.5 Windows Job objects

=cgroups process grouping en resource controls

1.1.6 Silos

= namespaces isolation execution environment voor file system, geistry en object namespaces.

1.1.7 Virtual Box

Virtual Box is de tweede Hypervisor die ondersteund wordt in deze bachelorproef. Deze wordt ontwikkeld door Oracle Corporation, maar is wel een type 2 Hypervisor. Type 2 Hypervisors gedragen zich meer als een gewone software applicatie en worden daarom 'host' Hypervisors genoemd. Ze maken een abstractie van de verbinding met de hardware en moeten hiervoor requests sturen naar het host OS, net zoals gewone applicaties.

De opstartvolgorde is hierdoor ook anders:

- Eerst wordt de fysieke machine gestart.
- Vervolgens wordt de controle van het boot systeem van de fysieke machine overgedragen aan Virtual Box, bijvoorbeeld BIOS of EUFI.
- Daarna start een gebruiker de Virtual Box applicatie op.

- Ten slotte zal de gebruiker kiezen welke virtuele machines worden opgestart, waarbij Virtual Box de benodigde hosting processes aanmaakt.

Ten slotte bestaat Virtual Box uit een soortgelijke lijst van componenten, waarbij er toch kleine wijzigingen zijn omdat het een type 2 is.

- IPRT (a portable runtime library)
- Virtual Machine Monitor
- Execution Manager
- Recompiled Execution Monitor
- Trap Manager
- Hardware Acceleration Manager
- Guest Interface Manager
- Pluggable Device Manager
- Page Manager
- Patch Manager
- Time Manager
- Configuration Manager
- Saved State Manager
- Virtual USB
- Debug Facility

1.1.8 Vagrant

Vagrant is een tool voor het bouwen en onderhouden van virtuele machines. Het maakt gebruik van een enkele workflow voor het automatiseren van ontwikkelomgevingen. Doordat het zo makkelijk te gebruiken is, verlaagt het de installatietijd en verhoogt het de productiviteit. Dit is waarom het een geliefde tool is binnen DevOps-teams.

Vagrant werkt aan de hand van een configuratiebestand dat uitgelezen moet worden. Dit configuratiebestand dat Vagrant nodig heeft, heet een 'Vagrantfile'. Hierin wordt alles gedefinieerd dat nodig is, meer bepaald: welke box, scripts en andere bestanden er nog nodig zijn voor de installatie.

Een 'Vagrant Box' is een verpakte base image die een clone is van een virtuele machine. Een base image is het minimum van een besturingssysteem waarop er nog verschillende andere functies gebouwd kunnen worden, zoals bijvoorbeeld een GUI. Via deze box wordt een besturingssysteem en bijbehorende software geïnstalleerd. Deze boxes worden opgehaald door middel van 'config.vm.box = boxnaam'. Als de box nog niet eerder gebruikt werd, wordt deze eerst gedownload vanop Vagrant Cloud, waarna de box wordt opgeslagen zodat deze steeds beschikbaar is voor later gebruik.

Als de box goed is, maar er moet nog verdere installatie of configuratie van de software gebeuren, kan men deze ook meegeven met het 'provision'-gedeelte. Met provisioning voegt men verdere configuratiemogelijkheden toe, zoals het uitvoeren van scripts, het uploaden van bestanden of folders tijdens de installatie, of het specificeren van een net-

werkadres. Door provisioning kan men ook makkelijk wijzigingen aanbrengen aan het systeem tijdens de run-time. Er wordt ook gebruik gemaakt van een eigen syntax die aangeleerd dient te worden. Deze bestaat uit 'vagrant' en de functie die uitgevoerd dient te worden, bijvoorbeeld: met 'vagrant up' wordt geprobeerd om het systeem online te brengen. De configuratie van de 'Vagrantfile' heeft ook zijn eigen syntax, bestaande uit het woord 'config' en de functie bepalend wat ermee moet gebeuren.

Vagrant ondersteunt bovendien verschillende platformen om zijn installatie op uit te voeren, gaande van VirtualBox en Hyper-V tot Docker en AWS. Het grote aantal beschikbare platformen om op te releasen is ook een sterkte van Vagrant.

Daarbovenop zijn er mogelijkheden om de functionaliteit van Vagrant zelf uit te breiden door gebruik te maken van plug-ins die geschreven worden door andere gebruikers, of door gebruik te maken van andere Configuration Management tools, zoals Ansible. Plug-ins worden meestal geschreven in de programmeertaal Ruby. Voor de gebruikte Windows Server-opstelling in deze bachelorproef is deze functionaliteit heel handig, omdat de Windows Server herstart dient te worden na de installatie van Docker. Hiervoor kan een plug-in gebruikt worden.

Om al deze redenen werd geopteerd om gebruik te maken van deze technologie. Er zijn gelijkaardige zero-touch installatiemogelijkheden, zoals Chef, Puppet of Terraform. Echter geen van hen biedt hetzelfde gebruiksgemak of dezelfde mogelijkheden.

1.1.9 PowerShell

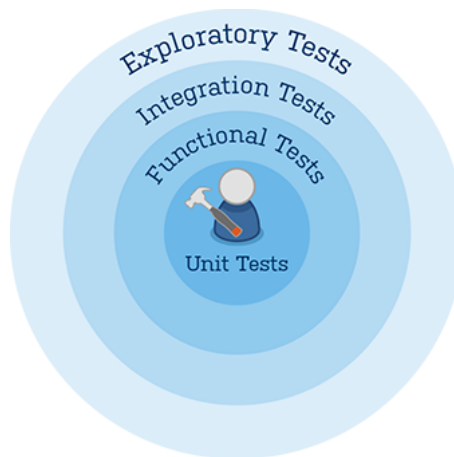
De configuratie van de Windows Server gebeurt grotendeels aan de hand van deze command-line interface. Deze CLI, die bovendien gebruik maakt van het .NET framework om objecten terug te geven, is namelijk speciaal ontwikkeld voor system administrators. Een groot voordeel hierbij is dat objecten veel makkelijker te verwerken zijn, in tegenstelling tot andere CLI's die vaak tekst gebruiken voor het uitvoeren van commando's. Daarnaast is de structuur van de command-lets (cmdlet) simpel en makkelijk aan te leren. De commando's bestaan namelijk altijd uit dezelfde samenstelling, bestaande uit 'werkwoord'-'te behandelen onderwerp', bijvoorbeeld: Get-Service.

1.1.10 Bash

Als tegenpool is er Bash voor Linux besturingssystemen. Deze CLI dateert al van 1989, met als volledige naam 'Bourne Again shell'. In essentie werkt Bash op dezelfde wijze als PowerShell. Net zoals PowerShell herkent Bash namelijk een aantal woorden, waardoor men ermee kan communiceren en het acties kan laten uitvoeren. Het grote verschil ligt in de uitvoering: Bash heeft namelijk enkel tekst als in- en uitvoer, wat het verwerken van opdrachten kan bemoeilijken. Echter, omdat Bash reeds geruime tijd bestaat, kan deze Unix shell wel genieten van een enorme gebruiks- en ondersteuningsbasis. Bash is namelijk de werkmethode bij uitstek voor Linux administrators.

1.1.11 Software testing

Bij software testing ligt de focus op kwaliteit in alle delen van de organisatie. Dit is belangrijk omdat het ontwikkelingsteam verantwoordelijk is voor de kwaliteit. QA-teams kunnen op tijd aan de alarmbel trekken, maar de verantwoordelijkheid van kwaliteit ligt nog steeds bij het ontwikkelingsproces. Daarom eist software testing dat iedereen, inclusief de gebruiker, betrokken is bij het ontwikkelingsproces. Software testing heeft een methodologische manier ontwikkeld om de kwaliteit te waarborgen, waarbij men laag per laag en stap per stap gaat kijken of het systeem voldoet aan de vereisten.



Verder zegt REF over software testing dat het een empirische en technische manier is om software of services te testen, doordat men op een objectieve manier kijkt naar de kwaliteit van een software of service. Dit is de voornaamste reden waarom voor deze methode gekozen is in deze bachelorproef. Daarnaast sluit het heel goed aan bij de principes van het DevOps manifeste.

Meer specifiek wordt er gebruik gemaakt worden van performantie- en veiligheidstesten.

Performantietesten zijn testen waarbij men gaat kijken hoe het systeem presteert wanneer het een bepaalde werkdruk moet verwerken, met de focus op snelheid, schaalbaarheid en stabiliteit.

Bij veiligheidstesten wordt er gekeken naar alle verschillende veiligheidsmaatregelen, en in hoeverre ze in staat zijn om de zwaktes van het systeem te beschermen.



1.2 Probleemstelling en Onderzoeksvragen

Het grootste probleem bij Docker is dat het op zich nog een relatief jonge technologie is, die bovendien een eigen syntaxis heeft. Daarnaast is er een andere denk- en werkwijze vereist om Docker te beheersen. Doorheen de tijd zijn Linux administrators reeds vertrouwd geraakt met deze technologie, maar voor Windows administrators is deze werkomgeving nog gloednieuw.

De onderzoeksvragen die uit deze probleemstelling voortvloeien zijn de volgende:

- Hoe vlot kan men een Docker-opstelling maken op een Windows-besturingssysteem tegenover een Linux-besturingssysteem?
- Hoe is het gesteld met de documentatie voor Docker for Windows tegenover de bestaande documentatie voor Linux?
- Hoe groot is de snelheidswinst bij Linux tegenover Windows?
- Hoe goed is de technologie geïntegreerd met Hyper-V en met het Windows besturingssysteem in het algemeen?
- Hoe is het gesteld met de veiligheid? Hoe pakt men deze aan vanuit een Windows administrator perspectief?

Op al deze vragen kon tot op heden geen afdoend antwoord worden gegeven. Men heeft in het verleden wel al Docker for Windows uitgetest en vergeleken met Linux, maar nooit op een concrete en methodische manier. Vaak benaderde men deze technologie ook vanuit een bestaande mening, en niet vanuit een neutraal perspectief.

Dit onderzoek zal vooral een grote meerwaarde zijn voor DevOps-teams die op zoek zijn naar Windows-oplossingen voor hun problemen in verband met automatisatie en continue oplevering.

1.3 Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:

In Hoofdstuk 2 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.

In Hoofdstuk 3 wordt de documentatie van beide platformen besproken. Er wordt gekeken naar volledigheid, interne en externe bronnen, en hoeveel ondersteuning er is vanuit de hoofdorganisatie.

In Hoofdstuk 4 worden beide opstellingen bekeken en besproken, meer specifiek hoe het is om beide op te bouwen, en hoe het zit met gelijkenissen en verschillen.

In Hoofdstuk 5 wordt gekeken naar het resultaat van de werklading dat beide systeem te verduren hebben gekregen en hoe ze beide gepresteerd hebben.

In Hoofdstuk 6 worden de beschikbare veiligheidsmaatregelen voor Docker besproken binnen beide systemen en hoe effectief deze zijn.

In Hoofdstuk 7 wordt ten slotte een conclusie gevormd en wordt er een antwoord geformuleerd op de onderzoeksvragen. Hierbij wordt ook een aanzet gegeven naar mogelijk toekomstig onderzoek binnen dit domein.

2. Methodologie

In dit hoofdstuk wordt uitgelegd hoe er te werk is gegaan. Elke titel stelt een grote fase voor in deze bachelorproef. Er wordt kort toegelicht welke stappen er ondernemen zijn in deze fasen en vooral waarom.

2.1 Literatuurstudie

Het startpunt van deze bachelorproef was een literatuurstudie over Docker for Windows, waarvan het resultaat zichtbaar is in de inleiding. Specifiek werd opgezocht hoe Docker werkt en welke requirements nodig zijn om het succesvol te installeren op een Windows Server 2016 en CentOS 7.4.

2.2 Bekijken van documentatie

Vervolgens werd de verzamelde documentatie voor beide omgevingen bekeken en beoordeeld op volledigheid. Aan de hand hiervan werd een conclusie getrokken.

2.3 Opzetten van de servers

Hierna werd een Windows Server 2016 en CentOS 7.4 gemaakt met op beide Docker geïnstalleerd, door middel van Vagrant en PowerShell voor Windows Server, en Bash voor CentOS. Op deze twee omgevingen werden uiteindelijk ook de software tests uitgevoerd.

Deze omgevingen werden daarna geüpload op GitHub zodat de code vrij beschikbaar was voor iedereen.

2.4 Uitvoeren van de verschillende tests

Nadat het opstellen van beide omgevingen was afgerond en de systemen volledig automatisch vanaf nul naar draaiend konden worden gebracht aan de hand van een werkende applicatie, werden op beide 3 manieren van software testing uitgevoerd:

- Performance testing
- Security testing

Deze manieren werden verschillende malen uitgevoerd, zodat het populatiegemiddelde groot genoeg was om een kleinere invloed te ondervinden van outliers.

2.5 Vergelijkende studie uitvoeren

Ten slotte werden alle resultaten van de testresultaten verzameld en verwerkt, om het gemiddelde, de variantie en de standaardafwijking te verkrijgen. Deze waarden werden nadien gebruikt om een grafische weergave te creëren van de resultaten.

3. Documentatie

Docker is al enkele jaren beschikbaar voor Linux en in die tijdspanne hebben de verschillende gebruikers van het systeem al gretig onderzocht hoe ze deze nieuwe technologie het beste kunnen gebruiken. Echter, nog belangrijker is dat de gebruikers ook documenteren wat ze doen en hoe ze bepaalde resultaten behalen, bijvoorbeeld via blogs of issues op GitHub. Hierdoor wordt er niet alleen een indrukwekkende hoeveelheid documentatie gecreëerd over het Docker systeem, maar verlaagt ook in de instapdrempel voor nieuwe gebruikers. Tezamen met de officiële documentatie die Docker zelf voorziet, kan men vorm geven aan een reeks van best practices om optimaal gebruik te maken van Docker. In dit hoofdstuk wordt er gekeken in hoeverre Microsoft, Docker en hun gebruikers al in staat zijn om de literaire kloof te dichten in vergelijking met Linux.

3.1 Requirements

Er is weinig info te vinden over de vereisten die nodig zijn om Docker met succes te installeren en uit te voeren.

Voor CentOS komt dit neer op drie lijnen tekst die eisen dat men gebruik maakt van een maintained version, dat 'centos-extras' repository enabled is en dat men gebruik maakt van de 'overlay2' storage driver.

Windows is op dit vlak een klein beetje beter. Het heeft een hele pagina speciaal toegewijd aan de installatie van Docker, waarin één hoofdstuk beschrijft wat er specifiek nodig is om Docker te installeren: Hyper-V enabled, virtualisatie in de BIOS aanzetten, 64bit Windows 10 Pro, Enterprise en Education of Windows Server 2016 en een beschrijving van hoe de container zou werken met andere gebruikers en parallel instances.

3.2 Installatie

Docker installeren is ook heel verschillend op beide systemen, wat op zich niet zo verbazend is gezien het verleden van beide apparaten.

Voor CentOS focust men puur op de command-line interface. Dit is ook logisch, aangezien er bij de basisinstallatie van CentOS geen GUI inbegrepen is. Daarom gaat Docker er meteen van uit dat men gebruik zal maken van Bash, wat een CLI is. De gids die Docker hiervoor aanbiedt is ook vrij compleet. Men vertrekt zelfs vanuit het idee dat de gebruiker al een oudere versie kan hebben staan, met als gevolg dat het ook Bash-commando's installeert die eerst de oude versie verwijderen en vervolgens vanaf nul alle nodige stappen ondernemen.

Ook hierin verschilde Windows sterk. Docker gaat er bij het Windows-platform van uit dat men gebruik wil maken van de GUI en biedt bijkomend de mogelijkheid om de installatie via PowerShell te laten gebeuren, wat ook een CLI is. Normaal gesproken zou het een bonus moeten zijn dat er twee verschillende benaderingsmethodes zijn, maar in dit geval is het eerder een nadeel omdat de focus op de GUI ligt. Dit is een minpunt omdat de meeste gebruikers zich liever focussen op automatisatie, wat bij de GUI geen optie is. Verder is dit ook een rare keuze, aangezien PowerShell een moderne en flexibele taal is omdat het met objecten werkt. Dit zou het beheren van de Docker-applicatie moeten vergemakkelijken, wat niet het geval is.

3.3 Container tot stand brengen

De installatie van een container vereist bij de beide platformen grotendeels dezelfde logica, namelijk via Docker-commando's. Het enige verschil is het aanmaken, invullen en uitlezen van de Dockerfile.

Zoals eerder aangehaald maakt CentOS gebruik van Bash om Docker te installeren. Deze trend zet zich ook voort bij het aanmaken van de Dockerfile. De in- en uitvoer van Bash is tekstgebaseerd, wat uitstekend past bij de vereiste voor het succesvol uitvoeren van een Dockerfile, zijnde Docker-commando's.

Voor Windows maakt Docker gebruik van PowerShell om de Dockerfile aan te maken. Zodoende kan men in de CLI-omgeving blijven en daarin verder werken nadat het bestand is aangemaakt. Zoals eerder aangehaald maakt PowerShell gebruik van objecten, C# om precies te zijn. Om een tekstbestand aan te maken, zoals een Dockerfile, is dit geen probleem, maar het is wel spijtig dat Docker hier niet beter gebruik van maakt.

3.4 Automatisatie

Rekening houdend met de doelgroep van deze bachelorproef is automatisatie zeker geen punt dat genegeerd mag worden. Automatisatie is immers één van de pijlers van DevOps.

CentOS heeft hierbij een streepje voor. Aangezien Docker meteen vertrekt vanuit Bash, dient men alleen deze commando's nog in een script te steken met de extensie `.sh` of `.bash` en dit vervolgens aan te roepen.

Ook hier is het weer wat moeilijker voor Windows. Een groot struikelblok is namelijk dat de nadruk minder op automatisatie ligt en meer op GUI, waardoor automatiseren moeilijker gaat. Echter, het grootste struikelblok is dat het Windows-platform een heropstart vereist na de installatie van Docker. Via plug-ins en scripting kan men hier nog rond werken, maar het maakt de automatisatie toch weer wat moeilijker.

3.5 Conclusie

De voornaamste informatiebron, zowel voor Docker for Windows als voor CentOS, is de documentatie op de officiële websites van Docker, RedHat en Microsoft. Docker en Microsoft doen hun best om de literaire kloof te sluiten, in tegenstelling tot CentOS. Zowel Docker als Microsoft proberen hierbij gretig gebruik te maken van hun communities om artikels te publiceren die door gebruikers worden geschreven of aangepast. Op deze manier hopen ze om het platform te promoten, zodat toekomstige gebruikers in staat zijn om hun eigen Docker-omgeving op te starten.

Ondanks deze inhaalbeweging gaat de meeste documentatie er nog steeds van uit dat men Docker wil draaien op Linux. Aangezien Docker voor Linux al beschikbaar is sinds 13 maart 2013 en pas recent voor Windows (22 februari 2017) is dit ook geen verrassing.

Het voordeel hiervan is wel dat de documentatie voor Docker for Windows vaker up-to-date is, omdat deze pas recent geschreven is en dan nog vaak door mensen die doorheen de jaren meegegroeid zijn met de technologie. Hoewel Container-technologie al lang bestaat, is het gebruik ervan tot recent vrij onbestaand geweest. Hierdoor heeft Docker for Windows de eerste moeilijke jaren van het uitzoeken naar een gepaste werkwijze vermeden.

Ten slotte is er wel één groot voordeel betreffende de documentatie voor Docker for Linux, namelijk troubleshooting. Doordat er al meer mee geëxperimenteerd is, zijn er al oplossingen gevonden voor verschillende problemen. Dit is van onschatbare waarde voor de CentOS-opstelling en is tegelijkertijd een hekelpunt voor de Windows-opstelling.

4. Opstelling

De set-up van beide machines wordt geautomatiseerd door middel van Hyper-V, Vagrant en scripts. Hiermee kan men garanderen dat, telkens er gewerkt wordt aan de machines, deze op dezelfde manier worden geïnstalleerd en aangepast. Een uitdaging hierbij is het vinden van gepaste Vagrant Boxes voor beide platformen, want hoewel CentOS wel een officiële Vagrant Image voorziet op Vagrant Cloud, wat de opslagplek is van alle publieke images, doet Microsoft dit niet. Hierdoor wordt men gedwongen om gebruik te maken van onofficiële bronnen. Ten slotte is het belangrijk dat de middelen en de werklading van beide machines evenredig zijn waar mogelijk. Natuurlijk zijn er subtiele verschillen, maar deze worden maximaal weggewerkt indien mogelijk.

4.1 Windows Server 2016

4.1.1 Vagrant

Voor de Windows-opstelling wordt er gekozen om de 'w16s'-image te gebruiken van de gebruiker 'gusztavvargadr'. Deze Vagrant Image bevat een Windows Server 2016 Standard 1607 (14393.2155). Verder bevat deze image ook al Chocolatey, wat maakt dat er alleen nog maar gekeken moet worden of Chocolatey up to date is.

Chocolatey is namelijk een community-driven packet manager voor Windows, zoals APT er bijvoorbeeld een is voor Debian. Met een packet manager kan men het installeren en beheren van applicaties automatiseren. Hiermee kan men de installatie vereenvoudigen.

Vervolgens wordt er ingesteld dat deze Vagrant Box 4GB RAM en 2 cores krijgt bij het uitrollen, zodat de installatie van Docker en uiteindelijk de containers vlot en snel kan

verlopen. Daarnaast stelt men ook een naam in voor de VM, evenals een host-naam. Dit maakt het makkelijker om de VM later aan te spreken.

```

1  # -*- mode: ruby -*-
2
3  # vi: set ft=ruby :
4
5  VAGRANTFILE_API_VERSION = "2"
6
7  ENV['VAGRANT_DEFAULT_PROVIDER'] = 'virtualbox'
8
9  ▾ Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
10
11     config.vm.network "private_network", ip: "192.168.56.16"
12
13     # full version WS2016
14     config.vm.box = "gusztavvargadr/w16s"
15
16     # alternative:
17     # config.vm.box = "mwrock/Windows2016"
18
19     config.vm.network "public_network", bridge: "Intel(R) Dual Band Wireless-AC 3160"
20
21     # configuration for virtualbox
22  ▾ config.vm.provider "virtualbox" do |v|
23         v.name = "DockerForWinVM"
24         v.memory = 4096
25         v.cpus = 2
26     end
27
28     # configuration for hyperv
29  ▾ config.vm.provider "hyperv" do |v|
30         v.vmname = "DockerForWinVM"
31         v.memory = 4096
32         v.cpus = 2
33     end
34
35     config.vm.boot_timeout = 420
36
37     config.vm.hostname = "DockerForWinVM"
38
39     config.vm.provision :shell, path: "Provisioning/Chocolatey.ps1"
40
41     config.vm.provision :shell, path: "Provisioning/Docker-P1.ps1"
42

```

Uitzonderlijk voor de Windows Server wordt er ook gebruik gemaakt van een plug-in voor Vagrant, namelijk, de 'Vagrant Reload'-plug-in van Aidan Nagorcka-Smith. Hiermee kan men het 'Vagrant Reload'-commando uitvoeren tijdens het uitrollen van de Vagrant Image naar een Box. Dit is een belangrijke voorwaarde, want de Windows Server dient heropgestart te worden naar de installatie van Docker.

Daarnaast dient er ook gebruik gemaakt te worden van een klein .BAT-script om docker-compose te installeren via pip.

```
42
43     # reload plugin for restart during provision
44     # download from aidanns/vagrant-reload with 'vagrant plugin install vagrant-reload'
45     config.vm.provision :reload
46
47     config.vm.provision :shell, path: "Provisioning/Docker-P2.ps1"
48
49     config.vm.provision :shell, path: "Provisioning/docker-compose.bat"
50
51     # config.vm.provision :shell, path: "Provisioning/Restart-Network.ps1"
52
53     # Verschil in connectiestring = User ID != User
54     config.vm.provision "file", source: "../VoorbeeldProjectWindows", destination: "~/VoorbeeldProject"
55
56     # config.vm.provision "file", source: "D:/Documenten/School/HoGent/StageEnBachelorproef/bachelorproef,
57
58     config.vm.provision :shell, path: "Provisioning/images.ps1"
59
60     config.vm.provision :shell, path: "Provisioning/applicaties.ps1"
61
62 end
63
```

Ten slotte wordt er ook gebruik gemaakt van een reeks provision-commando's om het systeem te voorzien van de nodige scripts en een voorbeeld-project. Het voorbeeld-project bevat een .NET-webapplicatie, die de onderstaande startpagina zou moeten tonen:

```

1  #!/usr/bin/bash
2  # abort on nonzero exitstatus
3  set -o errexit
4  # abort on unbound variable
5  set -o nounset
6  # don't mask errors in piped commands
7  set -o pipefail
8
9  # Going to the directory which contains the .csproj-file
10 cd /home/vagrant/VoorbeeldProject/DienstenCheques
11
12 # cd /home/vagrant/09solSportsStore-master/SportsStore
13
14 # Creates dockerfile
15 echo "Creating dockerfile"
16 cat > Dockerfile << EOF
17 FROM microsoft/dotnet:2.0.5-sdk-2.1.4
18
19 RUN mkdir -p /app
20
21 WORKDIR /app
22
23 COPY . /app
24
25 RUN dotnet restore
26
27 RUN dotnet build
28
29 EXPOSE 5000/tcp
30
31 ENV ASPNETCORE_URLS http://*:5000
32
33 ENTRYPOINT ["dotnet", "run"]
34 EOF
35
36 # Creates docker-compose.yml
37 echo "Creating docker-compose.yml"
38 cat > docker-compose.yml << EOF
39 version: "3"
40
41 services:
42   web:
43     build: .
44     ports:
45       - "8080:5000"
46     depends_on:
47       - db
48   db:
49     image: "microsoft/mssql-server-linux"
50     environment:
51       SA_PASSWORD: "Vagrant123"
52       ACCEPT_EULA: "Y"
53 EOF
54
55 # Building image
56 echo "Building docker image"
57 docker-compose build
58
59 # Running container
60 echo "Building container"

```

4.1.2 PowerShell

De 6 scripts die voorzien worden, configureren elk een component dat nodig is om de omgeving af te werken.

- Chocolatey

In dit script wordt er gekeken of Chocolatey al geïnstalleerd is. Zoja, wordt er gecontroleerd of Chocolatey reeds up to date is, en anders installeert het de packet manager.

```
# Controlen en aanpassen Execution-Policy Windows PowerShell naar BYPASS
$CurrentPolicy = get-ExecutionPolicy

Write-Host "#CURRENT POLICY IS $CurrentPolicy#"

if($CurrentPolicy -ne "Bypass")
{
    Write-Host "SETTING CURRENT POLICY TO Bypass"
    Set-ExecutionPolicy Bypass
}

# Installeren Chocolatey
Write-Host "#INSTALLING CHOCOLATEY#"
iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
choco upgrade chocolatey
Write-Host "#CHOCOLATEY INSTALLED#"

# Chocolatey globale uitvoerrechten geven
Write-Host "#SET CHOCOLATEY EXECUTIONRIGHTS#"
chocolatey feature enable -n=allowGlobalConfirmation
Write-Host "#EXECUTIONRIGHTS SET#"
```

- Docker #1

Hierna wordt het eerste deel van de Docker installatiescripts uitgevoerd. Dit installeert Docker en geeft daarna een melding dat er een reboot aan komt.

Nadat Docker geïnstalleerd is, vereist het systeem namelijk dat het opnieuw wordt opgestart. Deze plug-in is de makkelijkst gevonden manier, zonder in te grijpen in het automatisatie-proces.

```
# Controlen en aanpassen Execution-Policy Windows PowerShell naar BYPASS
$CurrentPolicy = get-ExecutionPolicy

Write-Host "#CURRENT POLICY IS $CurrentPolicy #"

if($CurrentPolicy -ne "Bypass")
{
    Write-Host "SETTING CURRENT POLICY TO Bypass"
    Set-ExecutionPolicy Bypass
}

# Installeren Docker
Write-Host "#INSTALLING DOCKER#"
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
Install-Package -Name docker -ProviderName DockerMsftProvider -Force
Write-Host "#DOCKER INSTALLED#"

Write-Host "#REBOOTING#"
```

- Docker #2

Vervolgens wordt Posh-Docker geïnstalleerd. Deze tool voorziet de installatie van Python en Pip door gebruik te maken van Chocolatey. Daarnaast wordt er in dit script ook getest of Docker correct is geïnstalleerd en worden de firewall-rules ingesteld.

```

net start com.docker.service

# Installeren Pip
Write-Host "#INSTALLING PYTHON/PIP#"
choco install -y python2
setx PATH "$env:path;C:\tools\python2;C:\tools\python2\Scripts" -m
$env:path += ";C:\tools\python2;C:\tools\python2\Scripts"
choco install pip

# Testen installatie
Write-Host "#RUN TEST CONTAINER#"
docker container run hello-world:nanoserver

# Toevoegen poorten voor Docker
Write-Host "#ADDING FIREWALL RULES#"
netsh advfirewall firewall add rule name=mssqlin dir=in action=allow protocol=TCP localport=1433
netsh advfirewall firewall add rule name=mssqlout dir=out action=allow protocol=TCP localport=1433

netsh advfirewall firewall add rule name=dockerappin dir=in action=allow protocol=TCP localport=8080
netsh advfirewall firewall add rule name=dockerappout dir=out action=allow protocol=TCP localport=8080

netsh advfirewall firewall add rule name=httplin dir=in action=allow protocol=TCP localport=80
netsh advfirewall firewall add rule name=httput dir=out action=allow protocol=TCP localport=80

netsh advfirewall firewall add rule name="docker engine" dir=in action=allow protocol=TCP localport=2375

```

- docker-compose.bat

Hierna wordt het docker-compose.bat-script uitgevoerd. Dit script maakt gebruik van Pip om docker-compose te installeren.

```

echo '#INSTALLING DOCKER-COMPOSE#'
pip install docker-compose

```

- Images

Vervolgens wordt het Images.ps1-script uitgevoerd. Dit script is verantwoordelijk voor het installeren van de container waarin de databank wordt gehost die de applicatie nodig heeft. Dit gebeurt aan de hand van een Microsoft SQL server Docker Image die van het internet wordt gehaald en waar vervolgens een container mee wordt gebouwd.

```

Write-Host "#DOWNLOADING IMAGES#"
# download mssql image
docker pull microsoft/mssql-server-windows-developer

# download dotnet image
docker pull microsoft/dotnet:2.0.5-sdk-2.1.4
Write-Host "#IMAGES DOWNLOADED#"

```

- Application

Ten slotte haalt het laatste script die specifieke .NET-sdk Docker Image op die nodig is om de container te bouwen die de webapplicatie vereist. Daarna maakt het script de Dockerfile aan en vult deze op met de vereiste tekst om de container te bouwen, alsook de commando's om daarna de Docker Image en Container te bouwen.

```
# Naar directory gaan waarin het .csproj-bestand zit
sl ../../Users/vagrant/VoorbeeldProject/DienstenCheques

# Aanmaken app-folder, dockerfile en docker-compose.yml
Write-Host "#CREATING APP, DOCKERFILE EN DOCKER-COMPOSE.YML#"
New-Item "dockerfile" -Force
New-Item "docker-compose.yml" -Force
New-Item "app" -ItemType Directory -Force

# Opvullen dockerfile
Write-Host "#FILLING DOCKERFILE#"
$DockerCommands = 'FROM microsoft/dotnet:2.0.5-sdk-2.1.4'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'WORKDIR /app'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'COPY . /app'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'RUN ["dotnet", "restore"]'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'RUN ["dotnet", "build"]'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'EXPOSE 5000/tcp'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'ENV ASPNETCORE_URLS http://*:5000'
$DockerCommands | Add-Content "Dockerfile"
$DockerCommands = 'ENTRYPOINT ["dotnet", "run"]'
$DockerCommands | Add-Content "Dockerfile"
```

```
# Opvullen docker-compose.yml
# indentatie belangrijk!
Write-Host "#FILLING DOCKER-COMPOSE.YML#"
$ComposeCommand = 'version: "3"'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = 'services:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '  web:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    build: .'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    ports:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '      - "8080:5000"'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    depends_on:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '      - db'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '  db:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    image: "microsoft/mssql-server-windows-developer"'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    environment:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '      SA_PASSWORD: "Vagrant123"'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '      ACCEPT_EULA: "Y"'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = 'networks:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '  default:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    external:'
$ComposeCommand | Add-Content "docker-compose.yml"
$ComposeCommand = '    name: nat'
$ComposeCommand | Add-Content "docker-compose.yml"

# Bouwt de image
Write-Host "#BUILDING IMAGE#"
docker-compose build

# Bouwt de container
Write-Host "#BUILDING CONTAINER#"
docker-compose up -d
```

4.2 CentOS 7.4

4.2.1 Vagrant

Om de CentOS-server te installeren wordt er gebruik gemaakt van de officiële Vagrant Image die beschikbaar wordt gesteld door de organisatie achter CentOS, namelijk Red Hat Enterprise Linux (RHEL). Deze voorziet alleen een basis installatie van een CentOS

7.4 server, maar voorziet wel de mogelijkheid om uitgerold te worden op alle populaire platformen.

```

1  # -*- mode: ruby -*-
2
3  # vi: set ft=ruby :
4
5  VAGRANTFILE_API_VERSION = "2"
6  # Staat standaard op virtualbox maar kan op hyperv gezet worden
7  # ALS JE HYPERV GEBRUIKT MOET JE config.vm.network IN COMMENTAAR ZETTEN
8  ENV['VAGRANT_DEFAULT_PROVIDER'] = 'virtualbox'
9
10 Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
11
12     # IP Adres toevoegen aan virtuele machine
13     # IN COMMENTAAR ZETTEN ALS JE HYPERV GEBRUIKT, NOG NIET ONDERSTEUND DOOR VAGRANT BIJ HYPERV
14     config.vm.network "private_network", ip: "192.168.56.15"
15
16     config.vm.box = "centos/7"
17

```

Ook hier krijgt het systeem 4GB RAM en 2 cores, zodat er op een eerlijke manier naar de prestaties van beide systemen kan worden gekeken. Verder krijgt het systeem ook een hostname en VMName.

```

20  config.vm.provider "virtualbox" do |v|
21     v.name = "CentOS Docker"
22     v.memory = 4096
23     v.cpus = 2
24  end
25
26  # configuration for hyperv
27  config.vm.provider "hyperv" do |v|
28     v.vminame = "DockerForWinVM"
29     v.memory = 4096
30     v.cpus = 2
31  end
32
33  config.vm.hostname = "CentOS Docker"
34
35  config.vm.provision :shell, path: "scripts/prereq.sh"
36
37  config.vm.provision :shell, path: "scripts/images.sh"
38
39  config.vm.provision "file", source: "D:/Documenten/School/HoGent/StageEnBachelorproef/bachelorproef/BachelorproefDocker/CentOSDocker/VoorbeeldProject/09solSportsST
40
41  # config.vm.provision "file", source: "D:/Documenten/School/HoGent/StageEnBachelorproef/bachelorproef/BachelorproefDocker/CentOSDocker/09solSportsST
42
43  config.vm.provision :shell, path: "scripts/applicaties.sh"
44  end
45

```

Ten slotte worden er 3 scripts voorzien bij het provision-gedeelte, zodat alle benodigde componenten kunnen worden geïnstalleerd. Hieronder behoort onder andere een script om dezelfde webapplicatie te voorzien als voor Windows.

4.2.2 Bash

- prereq

In dit gedeelte van het script worden alle functionaliteiten voorzien die nodig zijn voordat men kan beginnen aan het uitrollen van de applicatie, waaronder de installatie van Docker,

docker-compose, Epel-Release, Git, Nano en anderen. Daarnaast worden ook regels toegevoegd aan de firewall, zodat de container beschikbaar is nadat deze volledig is opgesteld.

```

1  #!/usr/bin/bash
2
3  # Provisioning script
4
5  # Settings for Bash
6  # abort on nonzero exitstatus
7  set -o errexit
8  # abort on unbound variable
9  set -o nounset
10 # don't mask errors in piped commands
11 set -o pipefail
12
13 # The name of the user that is going to manage the Docker service
14 readonly docker_admin=vagrant
15
16 # Install utilities
17 echo "Installing utilities"
18
19 yum -y install epel-release \
20             git \
21             nano \
22             patch
23
24 yum -y install python-pip
25
26 # Install Docker CE
27 echo "Installing Docker"
28
29 # Docker requires yum-utils and yum-config-manager
30 yum install -y yum-utils \
31             device-mapper-persistent-data \
32             lvm2
33
34 yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
35
36 # Installing Docker CE stable
37 yum install -y docker-ce
38
39 # Optional: Docker CE edge and test repository
40 # yum-config-manager --enable docker-ce-edge
41 # yum-config-manager --enable docker-ce-test
42

```

```

43 # Set Dockeradmin
44 echo "Adding user vagrant to group docker"
45 usermod -aG docker ${docker_admin}
46
47 # Service management
48 echo "Enabling services"
49 systemctl start docker.service
50 systemctl start firewalld.service
51
52 echo "Starting services"
53 systemctl enable docker.service
54 systemctl enable firewalld.service
55
56 # Test docker
57 echo "Testing Docker installation"
58
59 docker run hello-world
60
61 # Add ports to firewall
62 echo "Configuring firewall"
63 firewall-cmd --add-port=8080/tcp --permanent
64 firewall-cmd --add-port=80/tcp --permanent
65 firewall-cmd --add-port=5000/tcp --permanent
66 firewall-cmd --add-port=1433/tcp --permanent
67 firewall-cmd --reload
68
69 # Restarting Docker service due to firewall
70 echo "Restarting docker.service"
71 systemctl restart docker.service
72
73 # Install Docker-Compose
74 # sudo curl -L https://github.com/docker/compose/releases/download/1.21.0/docker-compose
75
76 # chmod +x /usr/local/bin/docker-compose
77 echo "Installing docker-compose"
78 pip install docker-compose
79
80 echo "Testing Docker-compose"
81 docker-compose --version

```

- images

Bij het volgende script worden alle Docker Images van Docker Hub gehaald, wat de officiële online repository van Docker is waar alle beschikbare Docker Images op staan.

```
1 #!/usr/bin/bash
2 # abort on nonzero exitstatus
3 set -o errexit
4 # abort on unbound variable
5 set -o nounset
6 # don't mask errors in piped commands
7 set -o pipefail
8
9 # Required images
10 echo "Pulling images"
11
12 # MSSQL image
13 docker pull microsoft/mssql-server-linux
14
15 # .NET image
16 docker pull microsoft/dotnet:2.0.5-sdk-2.1.4
```

- applicaties

Ten slotte worden in het laatste script de benodigde databank en applicatie omhoog gebracht aan de hand van een dockerfile, docker run- en docker build-commando's. De dockerfile- en dockercompose.yml-bestand worden opgevuld met een 'EOF' identifier. Hierdoor blijft Bash de invoer pipen in de dockerfile tot hij 'EOF' tegenkomt, waarna hij stopt zonder 'EOF' mee te nemen.

```
1  #!/usr/bin/bash
2  # abort on nonzero exitstatus
3  set -o errexit
4  # abort on unbound variable
5  set -o nounset
6  # don't mask errors in piped commands
7  set -o pipefail
8
9  # Going to the directory which contains the .csproj-file
10 cd /home/vagrant/VoorbeeldProject/DienstenCheques
11
12 # cd /home/vagrant/09solSportsStore-master/SportsStore
13
14 # Creates dockerfile
15 echo "Creating dockerfile"
16 cat > Dockerfile << EOF
17 FROM microsoft/dotnet:2.0.5-sdk-2.1.4
18
19 RUN mkdir -p /app
20
21 WORKDIR /app
22
23 COPY . /app
24
25 RUN dotnet restore
26
27 RUN dotnet build
28
29 EXPOSE 5000/tcp
30
31 ENV ASPNETCORE_URLS http://*:5000
32
33 ENTRYPOINT ["dotnet", "run"]
34 EOF
35
36 # Creates docker-compose.yml
37 echo "Creating docker-compose.yml"
38 cat > docker-compose.yml << EOF
39 version: "3"
40
41 services:
42   web:
43     build: .
44     ports:
45       - "8080:5000"
46     depends_on:
47       - db
48   db:
49     image: "microsoft/mssql-server-linux"
50     environment:
51       SA_PASSWORD: "Vagrant123"
52       ACCEPT_EULA: "Y"
53 EOF
54
55 # Building image
56 echo "Building docker image"
57 docker-compose build
58
59 # Running container
60 echo "Building container"
```


5. Performantie test

In dit hoofdstuk worden de resultaten besproken van de uitgevoerde performantietests.

De performantie van beide systemen werden op twee manieren getest: Eerst werd de benodigde tijd gemeten voor het uitvoeren van het 'vagrant up'-commando. 'vagrant up' installeerde en configureerde het besturingssysteem, de applicaties en de containers vanaf nul.

Vervolgens werd de benodigde tijd gemeten bij het uitvoeren van het 'vagrant provision'-commando. Hierbij waren het besturingssysteem en de applicaties al geïnstalleerd en geconfigureerd, en moesten alleen de containers nog tot stand gebracht worden. Om de internetsnelheid als factor te schrappen, waren de Docker Images ook al gedownload.

Daarnaast werd 'time' als prefix aan het commando toegevoegd. Hierdoor werd er op het einde van de commando's de tijd getoond die nodig was voor het uitvoeren.

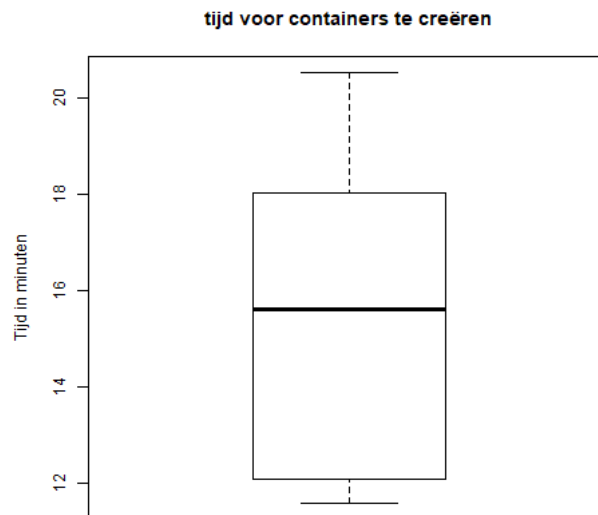
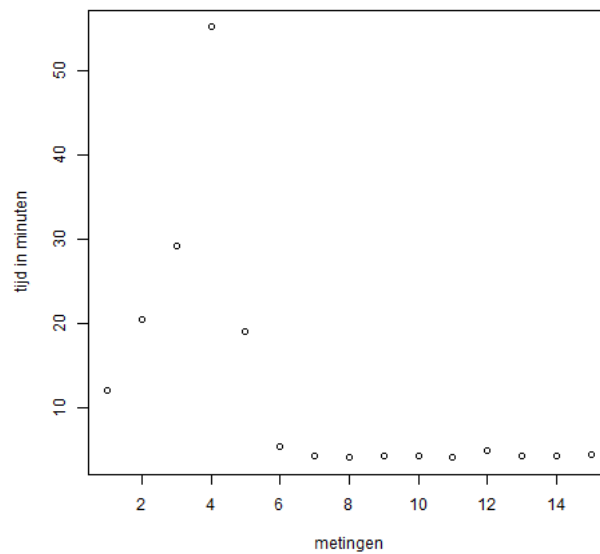
Vervolgens werden beide commando's vijftien keer uitgevoerd op beide opstellingen. Hierdoor werd de invloed van outliers vermindert. Outliers zijn observatiepunten die ver van andere punten verwijderd liggen.

Ten slotte werden deze resultaten genoteerd in een tabel in Rstudio. Zodanig dat deze resultaten konden worden gebruikt om het gemiddelde, de variantie en standaarddeviatie te berekenen. Alsook voor het genereren van een scatterplot en boxplot.

5.1 CentOS 7.4

5.1.1 Performantie installatie

Hieronder kan men de eerste resultaten zien van het 'time vagrant up'-commando voor de CentOS-opstelling.



$$\mu = 12.06457$$

$$\sigma^2 = 203.7204$$

$$\sigma = 14.27307$$

De gemiddelde benodigde tijd voor het commando bij de CentOS-opstelling was laag en vrijwel stabiel, met maar een paar outliers. De reden voor deze outliers kwam omdat deze metingen genomen waren in een omgeving met een slechtere internetverbinding.

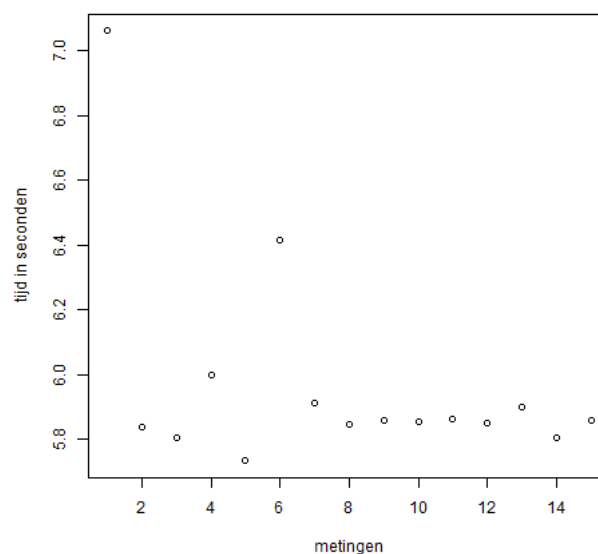
Dit was dus de grootste bottleneck voor deze opstelling. De impact hiervan op de installatie was in dit geval groot, zoals te zien valt aan de hoge variatie en standaarddeviatie.

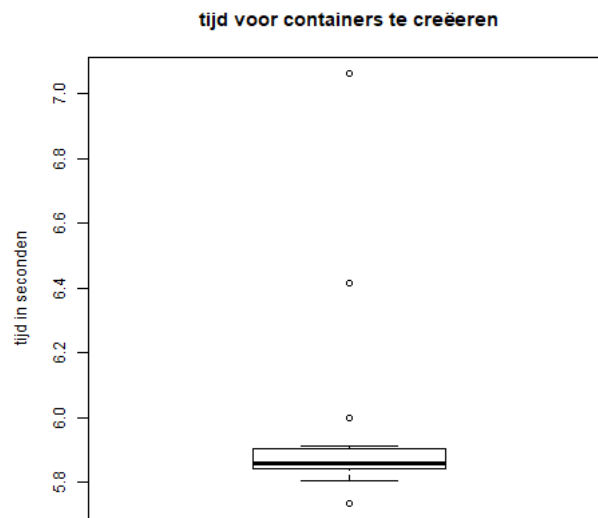
Maar, in het algemeen valt was de performantie van de CentOS-opstelling goed te noemen.

5.1.2 Performantie containers

Vervolgens kan men hier de resultaten zien voor elke keer dat het 'time vagrant provision'-commando werd uitgevoerd op de CentOS-opstelling. Deze keer uitgedrukt in seconden.

Bij deze resultaten moest het Operating System niet meer geïnstalleerd worden en ook de Docker Image moeten niet meer gedownload worden. Er werd alleen gekeken hoelang de Docker Daemon nodig had om de orders te interpreteren en de container tot staand te brengen.





$$\mu = 5.972333$$

$$\sigma^2 = 0.1150491$$

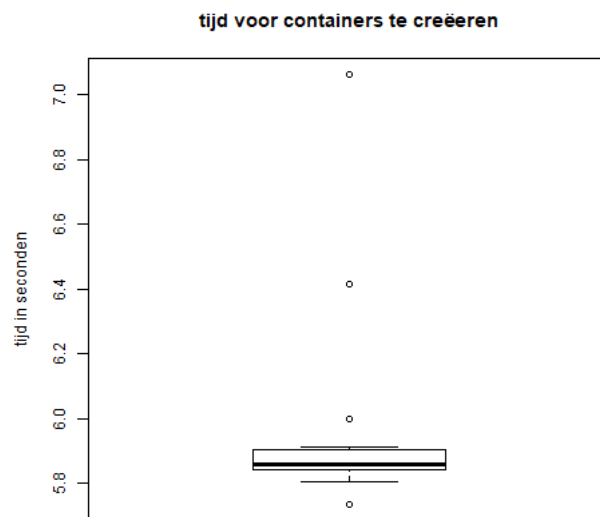
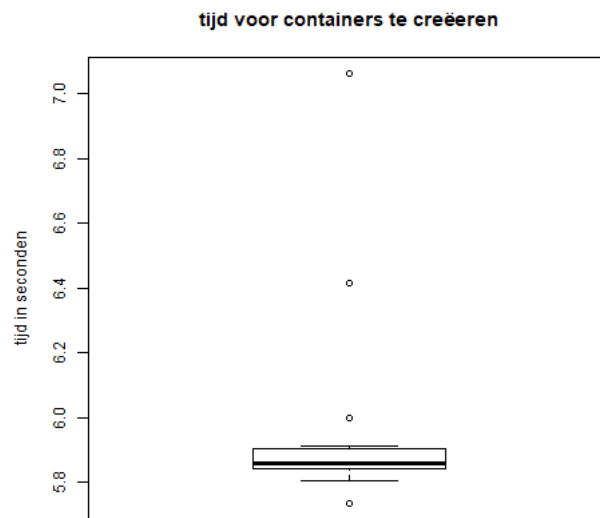
$$\sigma = 0.3391889$$

De installatie van alleen de container ging vlot, met een stabielere gemiddelde tijd, en een kleinere variantie en standaarddeviatie. Dit kwam doordat de applicaties en Docker Images niet meer gedownload diende te worden. Hierdoor lagen de tijden veel lager en was er geen invloed meer van de bottleneck.

5.2 Windows Server 2016

5.2.1 Performantie installatie

Vervolgens kan men ook de resultaten zien van 'time vagrant up' voor de Windows-opstelling.



$$\mu = 5.972333$$

$$\sigma^2 = 0.1150491$$

$$\sigma = 0.3391889$$

De installatie van de Windows opstelling duurde gemiddeld 10 keer langer dan de CentOS-opstelling. De gemiddelde tijd voor een volledige installatie was immers 45 minuten. De variantie en standaarddeviatie lagen ook . Hier waren verschillende redenen voor:

- Installatie Windows OS

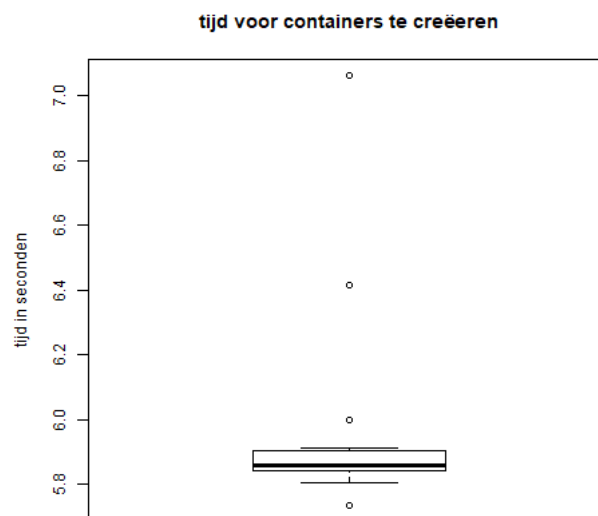
Om te beginnen duurde de installatie van het besturingssysteem langer omdat er een GUI gebruikt werd. Als Windows Server Core werd gebruikt zou de performantie al sterk verbeteren. Maar, dan kon men geen Docker CE for Windows installeren. Windows Server Nano was helaas ook geen optie, omdat deze helemaal niet ondersteund werd door Docker for Windows, zelfs niet voor Docker EE. Ten slotte hoefde CentOS ook niet heropgestart te worden na de installatie van Docker.

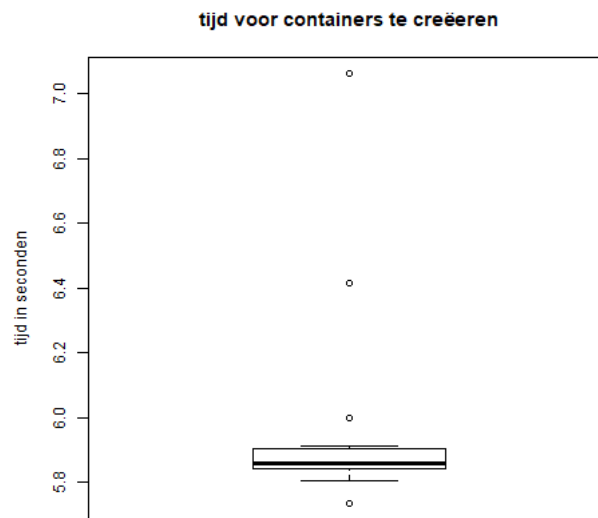
- Microsoft SQL server container

De MSSQL server container voor Windows was meer dan 10 keer zo groot als de Linux variant, 6GBs tegenover 479MBs. Hierdoor was de installatie een groot deel van zijn tijd bezig met het downloaden van deze Docker Image.

5.2.2 Performantie applicatie

Ten slotte kan men hieronder ook de resultaten zien van 'time vagrant provision' voor de Windows-opstelling van alleen de benodigde tijd om de containers te installeren.





$$\mu = 5.972333$$

$$\sigma^2 = 0.1150491$$

$$\sigma = 0.3391889$$

Hier waren de resultaten al iets meer gelijk aan de CentOS-opstelling. Doordat de Windows-opstelling nu niet meer tijd verloor met het installeren van een GUI, heropstarten of downloaden van grotere Docker Images.

5.3 Conclusie

6. Security test

Dit hoofdstuk vergelijkt de verschillende manieren waarop beide besturingssystemen, Linux en Window, in staat zijn om hun systemen te beschermen. Deze security review vergelijkt welke industrie standaarden beide systemen kunnen implementeren om hun systemen te harden tegen aanvallen.

Zoals eerder gezegd is een container automatisch veiliger dan een klassieke VM, doordat er een laag van isolatie ligt tussen de container en het besturingssysteem waarop het draait. Maar, als men toch via de container toegang zou kunnen verkrijgen tot het host systeem wat dan? Elk systeem is immers maar even sterk als zijn zwakste schakel. Dit werd ook bevestigd voor Solomon Hykes, CTO van Docker op DockerCon 2017 in Austin, USA op vlak van Linux beveiliging. Hij zei: "We denken dat Docker niet de verantwoordelijkheid is om Linux subsystemen te beveiligen. Sterker nog, we denken niet dat deze verantwoordelijkheid bij één bedrijf in het bijzonder moeten liggen. Linux is té groot and té belangrijk. Dus, daarom is het zó belangrijk dat veiligheid vanuit de community komt. En de community is goed bezig. Iedereen werkt samen, en niet elk in zijn donker hoekje".

Het is daarom dat deze security review zal vertrekken vanuit de populairste veiligheidsopaties voor het harden van een CentOS machine, en deze vergelijkt met equivalente opties voor Windows.

6.1 CentOS

6.1.1 Linux containers

Als eerste werd er gekeken naar hoe Linux containers tot staan gebracht worden en hoe sterk het isolatie niveau ervan is.

Zoals in de inleiding verteld hebben Linux containers hun eigen netwerk resources, geheugen geïsoleerde CPU, geheugen en I/O block. Maar, maken ze wel gebruik van dezelfde kernel als het host besturingssysteem. Dit zorgt ervoor dat containers licht en gestroomlijnd kunnen zijn containers. Maar, hierin zitten er sterktes en zwaktes.

Om te beginnen is het veel moeilijker om diepe toegang te krijgen tot de hoogste mogelijke privileges bij een container. Dit is een direct gevolg van de isolatie die er is tussen de container en zijn host. Maar, als dit wel lukt is er een reëel probleem. De Linux Container deelt immers de kernel met zijn host systeem. Waardoor system calls een groot probleem is. Door een geminimaliseerde OS te gebruiken kan men dit probleem verlagen, maar niet verhelpen.

Daarnaast is er wel het voordeel dat Root-toegang tot de container niet automatisch betekent dat je Root-toegang hebt op het host systeem. Maar, dan moet je wel oppassen met privileged containers. Deze worden wel standaard gebonden aan het host uid 0. Waardoor deze containers niet root-safe zijn, en ook niet root-safe kunnen gemaakt worden. Daarom maakt men best gebruik van Mandatory Access Control, zoals SELinux of AppArmor, seccomp filters en het laten vallen van namespaces.

Vervolgens is er het probleem dat heeft Cgroups standaard geen limiet. Waardoor men makkelijk een Denial of Service-attack kan uitvoeren op een CentOS-systeem. Dit risico kan verlaagt worden door memory, cpu and pods aand te passen in de configuratie van lxc.cgroup.

Ten slotte zijn aanvallers vaak vrij teleurgesteld als men in een container geraken. Want, best practise zegt: Geen data in containers. Waardoor de grootste reden om te aanvallen niet veel zal opleveren. Kijk immers maar naar de ransomware attacks die steeds populairder aan het worden zijn. Deze hebben als doen om data 'gevangen' te nemen tot het losgeld ervoor betaald is.

6.1.2 SELinux

SELinux of Security-Enhanced Linux gebruikt Linux Security Modules (LSM) om een Linux systeem te harden tegen aanvallen. De verschillende modules kunnen worden aan of uit gezet via een reeks van boolean. Daarnaast kan men ook handgemaakte waardes toevoegen aan deze lijst om ze te blokkeren of door te laten.

SELinux bestaat uit onderwerpen zoals users of applicatie processen, objecten zoals bestanden en folders, en een set van regels. Deze regels bepalen wat er een onderwerp mag

doen met een object.

Voor Docker bestaat er ook een SELModule. Deze module moet eerst enabled worden via 'semodule -v -e docker'. Daarna dient Docker herstart te worden met de volgende waarde: `--selinux-enabled`. Deze waarde dient geplaatst te worden in `docker.service` configuratiebestand. Ten slotte dient men Docker herop te starten, waarna Docker altijd met SELinux enabled zal opstarten.

De invloed van deze module is veelvoudig, de belangrijkste hiervan zijn: Beperken tot welke folders Docker toegang heeft, de 'privileged' Docker processen krijgen niet dezelfde privileges als andere privileged processen en via het 'docker run'-commando kan men de kernel mogelijkheden beperken door er '`--cap-drop=`' aan toe te voegen.

Van alle tools die beschikbaar zijn om een Linux server te beveiligen is SELinux veruit de krachtigste. Maar, SELinux heeft wel een prijs te betalen voor al deze functionaliteit. De gebruikersvriendelijkheid ervan kun je op zijn minst 'moeilijk' noemen.

Ondanks loont het om vaardig te worden in deze module.

6.1.3 Firewalld

Daarnaast kan men op CentOS Firewalld configureren om bepaalde poorten te openen of blokkeren. Want, in essentie gebruikt Firewalld gewoon IpTables met een XML-overlay. Wat het gebruik ervan veel vergemakkelijkt heeft.

Hiermee kan men dan de verschillende zones en poorten instellen die men wilt blokkeren of doorlaten. Maar, men kan ook gekende services toevoegen aan Firewalld. Waarbij deze automatisch de standaard poorten ervoor open of toe zet. Standaard is de zone 'public' en worden de meeste poorten geblokkeerd.

6.1.4 Seccomp

Ten slotte kan men ook Secure Computing gebruiken (Seccomp) gebruiken. Hiermee kan men de system calls beperken dat een process kan maken. Hierdoor kan het systeem beschermt tegen hackers, wanneer ze system calls willen maken die niet eerder gedeclareerd zijn.

Hoewel Seccomp in het verleden stroef was om te gebruiken, is het gebruik (Libseccomp) ervan sterk gegroeid. Door onder andere het toe voegen van BPF (Berkeley Packet Filters). BPF werd in het verleden gebruikt om netwerk pakketten te filteren, maar door het potentieel ervan groeide de potentiële toepassingen ervoor ook.

Seccomp zijn voordelen liggen vooral in het blokkeren van system calls vanuit de containers naar het host systeem als deze niet van toepassingen zijn. Daardoor kunnen aanvallen vanuit de container end-points tegen gehouden worden.

6.2 Windows

6.3 Hyper-V containers

Hyper-V Containers, zoals ze gebruikt word door Docker for Windows, verschilt op één belangrijke manieren van Linux Containers. Namelijk, Hyper-V containers gebruiken de base image om een VM aan te maken, door deze in de Hyper-V partition wrapper te steken. Waarna er in deze VM een Windows container wordt aangemaakt om de applicatie in te steken. Hierdoor is er een extra isolatielaag tussen de container en de kernel, namelijk de Hypervisor van de VM. Dit verhelpt veel van de problemen die de Linux Containers hebben op vlak van kwetsbaarheden.

Maar, hier staat er wel een kost tegenover: dit zorgt er namelijk voor dat de Hyper-V containers in het algemeen groter zullen zijn dan Linux Containers en meer tijd zullen nodig hebben om opgezet te worden. Maar, doordat Hyper-V een type 1 Hypervisor is en dus rechtstreeks op de hardware draait, is de last niet al te groot.

Ten slotte bestaat er ook het gevaar dat de VM crasht wanneer men in de container zit, en men niet meer uit de container boundaries kan geraken.

6.4 Integrity levels

Windows Integrity Levels (WIC) is het Windows equivalent van SELinux. Deze functie zat reeds al ingebouwd in Windows Vista. Waar het als doel had om objecten te beschermen, zoals: bestanden, printers en pipes. WIC werkt door de betrouwbaarheid van alle objecten en de interactie hiermee een waarde te geven, een level of trustworthiness. Als men een actie wilt uitvoeren op dit object, zal men het niveau op zijn minst moeten evenaren. WIC heeft een grotere prioriteit dan normale permissies.

Er zijn in totaal zes niveaus die WIC kan geven aan objecten. Van hoog naar laag zijn dit: untrusted (anonieme processen), low (interactie met het internet), meduim (meest objecten, onder andere de shell), high (Administrators), system (system) of installer (speciaal voor .EXE's).

Hoewel deze functie praktisch onopgemerkt is gegaan. Heeft dit de veiligheid van Windows wel sterk verbeterd. Want, hiervoor had Windows geen manier om aan Mandatory Access Control te doen.

Helaas is er wel nog werk aan de winkel. Er is bijvoorbeeld een gebrek aan management of configuratie tool voor administrators en het systeem is ook niet feilloos. Zoals er in Vyacheslav Rusakov wordt aangetoond.

6.5 Windows Defender

Windows Defender is begonnen als een anti-spyware systeem, waarnaast men nog andere anti-virus functies moest installeren zoals Microsoft Security Essentials om een complete verdediging te hebben. Maar, sinds Windows 8 heeft het ook definitief deze rol overgenomen.

Qua performantie krijgt Windows Defender gemengde reviews. Vooral de firewall van Windows Defender kan een last vormen op de CPU. Daardoor is de meest gezochte term voor Windows Defender hoe je het uitschakelt. Vaak is men beter af om een extra third-party systeem te gebruiken voor firewall. Zoals een PFSense of een WatchGuard.

6.5.1 ACL

Het Windows equivalent voor Seccomp is Windows Access Control Lists.

De ACL bestaat uit een lijst van Access Control Entries (ACE's). Waarbij elke ACE een trustee aanduidt en bepaald welke Access Rights deze heeft.

Helaas wordt het niet aangeraden om rechtstreeks met de inhoud van een ACL te werken. Er zijn functies en modules om deze te wijzigen, maar ook hier kan de administrator geen rechtstreekse invloed hebben op het systeem.

6.6 Conclusie

Linux heeft een meer hands-on aanpak voor zijn systemen te beveiligen, waarbij de administrator van het Linux-systeem veel zelf kan en moet bepalen. Maar, dit betekent wel dat de veiligheid van een Linux-opstelling even goed is als de kennis van zijn administrator. Wat ofwel ijzersterk is of gatenkaas. Windows daarentegen neemt veel controle van de administrator weg, en doet het voor hem. Dit betekent dat er een basisniveau is qua veiligheid. Maar, dat dit niveau ver onder het niveau van een Linux-opstelling kan liggen, als de administrator ervan weet wat hij hoort te doen.

7. Conclusie

De onderzoeksvraag voor deze bachelorproef was: hoe goed presteert Docker for Windows op vlak van performantie en veiligheid tegenover Docker for Linux? Hiervoor werden er twee systemen opgesteld. Waarbij de eerste opstelling een Windows Server 2016 met Docker for Windows is. De tweede opstelling bevatte een CentOS 7.4 met Docker for Linux. Vervolgens werd de performantie van beide systemen vergeleken door te kijken hoe lang beide nodig hadden om een volledige installatie uit te voeren en hoeveel tijd voor alleen hun containers. Ten slotte werd de beveiliging van beide systemen onder de loop genomen. Waarbij er vertrokken werd uit de veiligheidsmaatregelen die men kan nemen met CentOS en of Windows hier een equivalent voor had.

Welk systeem de betere performantie had was duidelijk. Bij de volledige installatie had Windows tot wel 10 keer meer tijd nodig om alles geïnstalleerd te krijgen. Dit komt onder andere doordat Docker for Windows een GUI nodig heeft om te installeren. Daarnaast zijn de containers en base images groter dan die voor Linux. Dit zijn twee hekelpunten die zeker nog weggewerkt moeten worden door Docker en Microsoft. Zeker als men Docker for Windows ook verkocht wilt krijgen aan DevOps teams.

Aan de andere kant, deze grafische interface maakt Docker wel veel toegankelijker voor beginnende developers die op een Windows OS werken. Deze hebben immers geen nood aan een volledig geautomatiseerde omgeving. Maar, hechten veel meer waarde aan een toegankelijke applicatie. Daarnaast zijn deze developers niet meer verplicht om een Linux VM te draaien op hun systeem. Ten slotte, zullen deze beginnende developers ook niet evenveel containers draaien als een professionele onderneming. Waardoor de grote ervan minder belangrijk is.

Mijn conclusie voor performantie is dat Docker for Linux meer geschikt zal zijn voor

bedrijven die op een professionele manier willen omgaan met container-technologie. Maar, dat Docker for Windows meer geschikt is voor beginnende developers. Zeker als men al werkt op een Windows systeem.

Op vlak van veiligheid ligt de bal een beetje meer in het midden. Linux heeft enkele sterke voordelen, zoals SELinux, Firewalld en Seccomp. Maar, dit vereist wel enige kennis. Dus, is de beveiliging van Linux voor een groot deel afhankelijk van de kennis van zijn administrator. Daartegenover is de beveiliging van Windows veel meer basic. Maar, is er wel een minimum aan veiligheid doordat Microsoft bepaalde beslissingen uit de handen van zijn administrators neemt en deze instelt voor hem. Dit is zowel een voor- als nadeel. Want ook Microsoft is niet feilloos. Maar, Hyper-V Containers zijn dan wel weer een pak veiliger dan de Linux Containers. Doordat ze een extra niveau van isolatie hebben.

De resultaten van dit onderzoek zijn min of meer binnen de lijnen van het verwachte. Alleen de performantie kun je vrij schokkend noemen. Als Docker en Microsoft Docker for Windows even competitief willen maken als Docker for Linux is er nog werk aan de winkel. Op vlak van veiligheid zijn beide systemen equivalent aan elkaar. Waar vooral de kennis van de administrator een grote rol speelt.

Verdere onderzoeksvragen die uit deze bachelorproef oprijzen zijn:

- Hoe goed integreert Docker for Linux met het Windows besturingssysteem?
- Kun je de installatie van Docker for Windows beter automatiseren door PowerShell modules aan te maken?
- Zijn er manieren om de grootte van de Hyper-V containers te verkleinen?

Lijst van figuren

1.1 Links ziet men hoe de communicatie in klassieke ontwikkelomgevingen gebeurt, rechts in DevOps teams	12
---	----

Lijst van tabellen