Security problemen in container orcherstratie tools indentificeren en vermijden

Onderzoeksvoorstel Bachelorproef 2020-2021

Nick Heymans[1]

Samenvatting
In deze bachelorproef worden de moderne beveiligingsrico's die gepaard gaan met container virtualisatie en container cluster orchestratie geanalyseerd en wordt er naar manieren gezocht om deze op te lossen of te vermijden. De laatste jaren is het gebruik van containers in de IT infrastructuur fors gestegen en dit zal zo blijven in de komende jaren. De kracht van container virtualisatie en container cluster orchestratie is dat het administrators en developers de mogelijkheid geeft om applicaties op een draagbare en snelle manier uit te rollen en te beheren op grote schaal. Maar zoals bij alle technologieën zijn hier enkelen veiligheidsrisico's aan verbonden. Tijdens het onderzoek zal het gebruik van container virtualisatie en container cluster orchestratie (en de daaraan verbonden risico's) onderzocht worden. In het tweede deel zal er, op basis van de bevindingen uit het eerste deel, onderzocht worden hoe deze risico's vermeden of opgelost kunnen worden. Als laatste zal er via een proof-of-concept opstelling gekeken worden wat voor effect deze oplossingen hebben op het uitrollen van een container cluster op vlak van snelheid en resource management.

Sleutelwoorden
Onderzoeksdomein. Security — Containerization — Container Orchestration

Co-promotor
?????????[2] (Bedrijfsnaam)

Contact: [1] nick.heymans@student.hogent.be; [2] piet.pieters@acme.be;

Inhoudsopgave

1. Introductie

Hier introduceer je werk. Je hoeft hier nog niet te technisch te gaan.

Je beschrijft zeker:

- de probleemstelling en context
- de motivatie en relevantie voor het onderzoek
- de doelstelling en onderzoeksvraag/-vragen

Het uirollen en schalen van applicaties word meer en meer gedaan met behulp van containers en container orcherstratie tools. Deze zorgen ervoor dat de ontwikkeling en het uitrollen van een applicatie vergemakkelijkt word. In traditionele Gartner (Pettey (2019)) voorspeld dat tegen 2022 maar liefst 75% van alle internatiale organisaties gecontaineriseerde applicaties zullen gebruiken in hun productieomgeving.

2. State-of-the-art

Hier beschrijf je de *state-of-the-art* rondom je gekozen onderzoeksdomein. Dit kan bijvoorbeeld een literatuurstudie zijn. Je mag de titel van deze sectie ook aanpassen (literatuurstudie, stand van zaken, enz.). Zijn er al gelijkaardige onderzoeken gevoerd? Wat concluderen ze? Wat is het verschil met jouw onderzoek? Wat is de relevantie met jouw onderzoek?

Verwijs bij elke introductie van een term of bewering over het domein naar de vakliteratuur, bijvoorbeeld (Kohgadai, 2020)! Denk zeker goed na welke werken je refereert en waarom.

Je mag gerust gebruik maken van subsecties in dit onderdeel.

3. Methodologie

Hier beschrijf je hoe je van plan bent het onderzoek te voeren [1] (Pettey, 2019). Welke onderzoekstechniek ga je toepassen om elk van je onderzoeksvragen te beantwoorden? Gebruik je hiervoor experimenten, vragenlijsten, simulaties? Je beschrijft ook al welke tools je denkt hiervoor te gebruiken of te ontwikkelen. Voor dit onderzoek zullen er enkele scenario's opgezet worden. Bij elke scenario zullen er verschillende security best practices en security tools gebruikt worden. Deze zullen getest worden op basis van

[1] "https://molecule.readthedocs.io"

de volgende criteria:

- Deployment snelheid
- Benodigde resources
- Stabiliteit

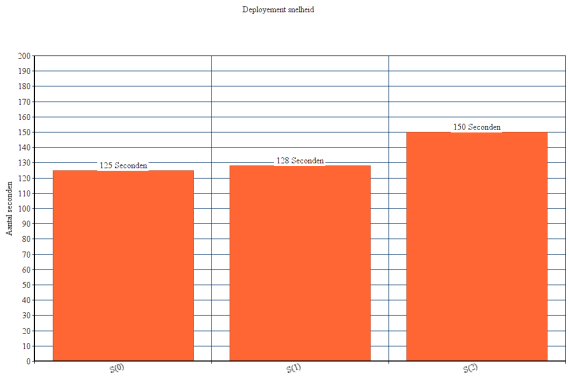
Voorbeelden van scenario's:

- S(0): Er word een container applicatie opgezet in een Kubernetes cluster zonder extra security configuratie.
- S(1): Er word een container applicatie opgezet in een Kubernetes cluster en enkele 'best practices' worden toegepast.
- S(2): Er word een container applicatie opgezet in een Kubernetes cluster waarin de grootste security risico's worden vermeden.

Door gebruik te maken van deze scenario's en criteria hopen we te kunnen aanwijzen dat het toepassen van security 'best practices' een positieve invloed heeft op het gebruik van containers en container orcherstratie tools.

4. Verwachte resultaten

Hier beschrijf je welke resultaten je verwacht. Als je metingen en simulaties uitvoert, kan je hier al mock-ups maken van de grafieken samen met de verwachte conclusies. Benoem zeker al je assen en de stukken van de grafiek die je gaat gebruiken. Dit zorgt ervoor dat je concreet weet hoe je je data gaat moeten structureren. Op basis van de criteria word er verwacht dat Scenario 0 en 1 even snel op gedeployed kunnen worden maar ze zullen wel beide kwetsbaar zijn aangezien de 'best practices' vooral bestaan uithet correct gebruik wachtwoorden en gebruiker privileges. Scenario 2 daarintegen zal iets meer tijd nodig hebben om te deployen en zal ook meer resources gebruiken. Dit zal vooral komen omdat het delen van resources tussen de containers een security risico is en dus tot een minimum zal moeten beperkt worden.(Education, 2019)



Figuur 1. Verwacht eindresultaat

Benodigde resources	CPU %	Memory %
S(0)	45%	30%
S(1)	46%	32%
S(2)	55%	45%

Figuur 2. Verwacht eindresultaat

5. Verwachte conclusies

Hier beschrijf je wat je verwacht uit je onderzoek, met de motivatie waarom. Het is **niet** erg indien uit je onderzoek andere resultaten en conclusies vloeien dan dat je hier beschrijft: het is dan juist interessant om te onderzoeken waarom jouw hypothesen niet overeenkomen met de resultaten.

Uit dit onderzoek verwachten verwachten we te kunnen concluderen dat het toepassen van 'best practices' en het correct gebruik van security tools een positief effect hebben het gebruik van container orcherstratie tools. We willen ook aanduiden dat het omzeilen van security risico's een belangrijk aspect is bij het developen van container applicaties. Tot slot is het mogelijk om de conclusie te trekken dat het beveiligen van container clusters steeds belangrijker word en het ook belangrijk is dat de persoon die een cluster opzet de onderliggende werkwijze goed kent en zich bewust is van de valkuilen.

Referenties

Education, I. C. (2019, mei 25). *Containerization*. IBM. https://www.ibm.com/cloud/learn/containerization#toc-what-is-co-r25Smlqq

Kohgadai, A. (2020, mei 15). *Kubernetes Security 101: Risks and 29 Best Practices*. https://www.stackrox.com/post/2020/05/kubernetes-security-101/

Pettey, C. (2019, april 23). *6 Best Practices for Creating a Container Platform Strategy*. https://www.gartner.com/smarterwithgartner/6-best-practices-for-creating-a-container-platform-strategy/