Container orkestratie security: indentificeren van problemen en onderzoek naar de impact van security tools

Onderzoeksvoorstel Bachelorproef 2020-2021

Nick Heymans[1]

Samenvatting
In deze bachelorproef worden de moderne veiligheidsrisico's geanalyseerd die gepaard gaan met container virtualisatie en container orkestratie. Hierbij zal specifiek gekeken worden naar de grootste veiligheidsrisico's, welke effecten deze kunnen hebben op een productieomgeving en hoe deze vermeden kunnen worden. Tevens zal onderzocht worden welke 'security tools' (zoals 'Project Calico' en 'Kube-hunter') er bestaan en hoe deze ingezet kunnen worden bij het beveiligen van een container cluster. De laatste jaren is het gebruik van containers in de IT infrastructuur fors gestegen en dit zal zo blijven evolueren in de komende jaren. Aan alle technologieën zijn nu eenmaal veiligheidsrisico's verbonden, container orkestratie vormt hier geen uitzondering op de regel. In voorgaand onderzoek werd er reeds gefocust op de grootste veiligheidsrisico's desondanks is er zeer weinig ingegaan op de effecten bij het toepassen van 'best practices'. Met deze paper tracht ik het gebruik en de daaraan verbonden risico's van container virtualisatie en container orkestratie te onderzoeken. Daarnaast zal er ook gekeken worden naar hoe de verschillende 'security tools' kunnen helpen bij het beveiligen van containers. Ten slotte wordt er onderzocht hoe deze risico's vermeden of opgelost kunnen worden en welk effecten ze hebben op de relevante criteria. Dit laatste zal via een 'proof-of-concept' opstelling gebeuren.

Sleutelwoorden
Systeembeheer — Security — Containers — Container orkestratie

Co-promotor
Onbekend[2] (Bedrijfsnaam)

Contact: [1] nick.heymans@student.hogent.be; [2] onbekend@bedrijfsnaam.be;

Inhoudsopgave

1. Inleiding en State-of-the-art

1.1 Wat zijn containers?

Het uitrollen en schalen van applicaties wordt steeds vaker gedaan met behulp van containers. Tijdens de ontwikkeling van traditionele applicaties wordt de applicatie ontwikkeld in een specifiek testomgeving. Vervolgens wordt de applicatie overgezet naar de productieomgeving wat vaak voor problemen zorgt (bijvoorbeeld van een linux testomgeving naar een Windows productieomgeving). Een container is een pakket waar één enkele applicatie in zit, samen met alle nodige afhankelijkheden(Education, 2019). Dit zorgt ervoor dat deze gemakkelijk en snel van de ene omgeving naar de andere kan overgezet worden. De containers maken gebruik van een 'runtime engine', dit is een laag die verantwoordelijk is voor de communicatie tussen het operating system van de host machine en de containers zelf. De meeste gebruikte 'runtime engine' is de 'Docker Engine'[1]. Deze is al sinds 2013 de industriestandaard als het gaat over container software(McCarty, 2018). Naarmate het gebruik van containers steeg, steeg ook de nood naar op manier om deze vanuit één centrale locatie te beheren. Om aan deze vraag te voldoen werden container orkestratie tools, zoals Kubernetes [2], ontwikkeld. Deze tools helpen bij het opzetten, uitbreiden en verbinden van een grote hoeveelheid containers.

[1] https://docs.docker.com/engine/
[2] https://kubernetes.io/

1.2 Waarom container applicaties?

Container applicaties hebben enkele voordelen tegenover normale applicaties, ze draaien namelijk geïsoleerd van de rest van het systeem. Ze kunnen dus perfect werken zonder afhankelijk te zijn van andere containers. Dit garandeerd dat als er één container aangetast is, de rest zonder interruptie kan verderwerken. De containers delen wel verschillende resources van het host systeem, wat de deur opent voor veiligheidsinbreuken tussen containers.

1.3 Context voor dit onderzoek

Gartner (Pettey, 2019) voorspeld dat tegen 2022 maar liefst 75% van alle internationale organisaties gecontaineriseerde applicaties zullen gebruiken in hun productieomgeving. Dit zowel in lokale datacenters alsook in online cloud omgevingen. Uit een raport van Tripwire (2019) blijkt dat 94% van bevraagden bezorgd zijn over de veiligheid van hun containers. Uit hetzelfde raport blijkt ook dat 47% weet dat ze kwetsbare containers gebruiken in hun productieomgeving. Spijtig genoeg werd bij voorgaande onderzoeken, zoals StackRox (2020), het effect van 'security best practices en tools' op opzetsnelheid, benodigde resources en stabiliteit steeds onderbelicht.

1.4 Verloop van het onderzoek

In deze paper zal ik onderzoeken wat de belangrijkste bronnen van veiligheidsinbreuken zijn en hoe deze vermeden kunnen worden. Tegelijkertijd krijg ik via dit onderzoek de opportuniteit om er achter te komen of er vooral technische problemen of menselijke fouten aan de basis liggen van de veiligheidsrisico's. In de volgende paragraaf staat er beschreven hoe ik te werk zal gaan.

2. Methodologie

Voor dit onderzoek zullen er drie scenario's opgezet worden. Elk scenario zal verschillende keren worden uitgevoerd en voor elk criteria zal het genomen worden (eventueel reking houdende met uitschieters). Bij elke scenario zullen er verschillende 'security best practices en tools' gebruikt worden. Deze zullen getest worden op basis van de volgende criteria:

- Deployment snelheid
- Benodigde resources
- Stabiliteit

Voorbeelden van scenario's:

- S(0): Er wordt een container applicatie opgezet in een Kubernetes cluster zonder extra security configuratie.
- S(1): Er wordt een container applicatie opgezet in een Kubernetes cluster en enkele 'best practices' worden toegepast.
- S(2): Er wordt een container applicatie opgezet in een Kubernetes cluster waar er gebruik word gemaakt van enkele 'security tools' zoals 'Project Calico' en 'Kube-hunter'.

Door gebruik te maken van deze scenario's en criteria hopen we vast te stellen dat het toepassen van 'security best practices en tools' een positieve invloed heeft op het gebruik van containers en orkestratie tools.

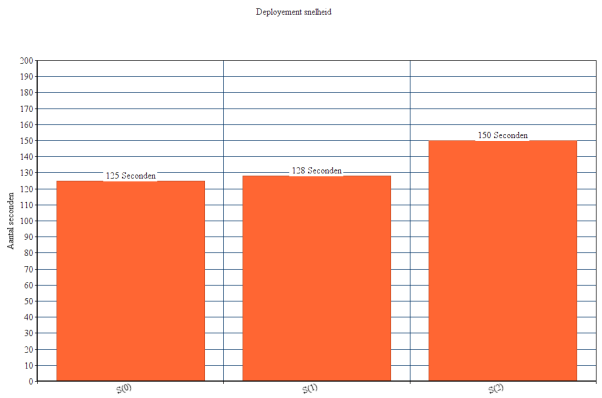
3. Verwachte resultaten

Op basis van de criteria wordt er verwacht dat Scenario 0 en 1 even snel op opgezet kunnen worden en evenveel resources gebruiken. Ze zullen beide kwetsbaarder zijn aangezien de 'best practices' vooral bestaan uit het correct gebruik van wachtwoorden en gebruiker privileges. Scenario 2 daarintegen zal iets meer tijd nodig hebben om opgezet te worden(zie Figuur1) en zal daarbij meer resources gebruiken(zie Figuur2). Dit zou te wijten zijn aan de gebruikte 'security tools' die extra tijd en resource nodig hebben.

4. Verwachte conclusies

Uit dit onderzoek willen we concluderen dat het toepassen van 'best practices' en het correct gebruik van security tools een positief effect teweeg brengt bij het gebruik van container orkestratie tools. We trachten daarnaast ook aan te duiden dat het omzeilen van security risico's een belangrijk aspect is bij het ontwikkelen van container applicaties. Tot slot kan er geconcludeerd worden dat het beveiligen van container clusters steeds belangrijker wordt. Daarnaast is het tevens van belang dat de persoon die een cluster opzet daarbij de onderliggende werkwijze goed kent en zich bewust is van de mogelijke valkuilen.

5. Bijlagen



Figuur 1. Verwachte opstart tijd

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

Figuur 2. Verwacht resource gebruik

Referenties

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

McCarty, S. (2018, februari 22). *A Practical Introduction to Container Terminology*. https://developers.redhat.com/blog/2018/02/22/container-terminology-practical-introduction/#h.6yt1ex5wfo3l

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/

StackRox. (2020, februari 19). *State of Container and Kubernetes Security* (onderzoeksrap.). StackRox. https://www.stackrox.com/kubernetes-adoption-security-and-market-share-for-containers/

Tripwire. (2019, januari 1). *Tripwire State of Container Security Report* (onderzoeksrap.). Tripwire. Verkregen 30 november 2020, van https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Tripwire-Dimensional-Research-State-of-Container-Security-Report.pdf