

# Kubernetes inter-pod container isolation

Aarni Halinen

## School of Science

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 1.6.2023

## Thesis supervisor:

Prof. Mario Di Francesco

## Thesis advisors:

M.Sc. (Tech.) José Luis Martin

Navarro

M.Sc. (Tech.) Jacopo Bufalino

Author: Aarni Halinen		
Title: Kubernetes inter-pod container isolation		
Date: 1.6.2023	Language: English	Number of pages: 5+8
Department of Computer Science		
Professorship: Computer Science		
Supervisor: Prof. Mario Di Francesco		
Advisors: M.Sc. (Tech.) José Luis Martin Navarro, M.Sc. (Tech.) Jacopo Bufalino		
<p>Your abstract in English. Try to keep the abstract short; approximately 100 words should be enough. The abstract explains your research topic, the methods you have used, and the results you obtained. Your abstract in English. Try to keep the abstract short; approximately 100 words should be enough. The abstract explains your research topic, the methods you have used, and the results you obtained. Your abstract in English. Try to keep the abstract short; approximately 100 words should be enough. The abstract explains your research topic, the methods you have used, and the results you obtained. Your abstract in English. Try to keep the abstract short; approximately 100 words should be enough. The abstract explains your research topic, the methods you have used, and the results you obtained.</p>		
Keywords: Kubernetes, Container, Docker, Security		

## Preface

I want to thank Professor Pirjo Professori and my instructor Olli Ohjaaja for their good and poor guidance.

Otaniemi, 16.1.2015

Eddie E. A. Engineer

# Contents

<b>Abstract</b>	<b>ii</b>
<b>Preface</b>	<b>iii</b>
<b>Contents</b>	<b>iv</b>
<b>Symbols and abbreviations</b>	<b>v</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Background</b>	<b>2</b>
2.1 Microservices? . . . . .	2
2.2 Containerization and Docker . . . . .	2
2.2.1 Docker components . . . . .	2
2.2.2 Linux control groups and namespaces . . . . .	2
2.2.3 Linux capabilities, privileged containers, Container breakout . . . . .	2
2.3 Kubernetes system components . . . . .	2
2.3.1 apiserver . . . . .	2
2.3.2 etcd . . . . .	2
2.3.3 scheduler . . . . .	2
2.3.4 controller-manager . . . . .	2
2.4 Kubernetes resources . . . . .	2
2.4.1 Namespaces . . . . .	2
2.4.2 Pods . . . . .	2
2.4.3 Network policies . . . . .	2
2.4.4 Admission control . . . . .	2
2.5 Principle of least privilege, Zero trust... . . . .	2
<b>3 Research material and methods</b>	<b>3</b>
<b>4 Results</b>	<b>4</b>
<b>5 Summary</b>	<b>5</b>
<b>References</b>	<b>6</b>
<b>A Esimerkki liitteestä</b>	<b>7</b>

# Symbols and abbreviations

## Symbols

- ↑ electron spin direction up
- ↓ electron spin direction down

## Operators

- $\nabla \times \mathbf{A}$  curl of vector in  $\mathbf{A}$

## Abbreviations

- K8s Kubernetes
- STRIDE an object-oriented analog circuit simulator and design tool

# 1 Introduction

Tämän tekstin lähteenä oleva tiedosto on opinnäytteen pohja, jota voi käyttää kandidaatintyössä, diplomityössä ja lisensiaatintyössä. Tekstin lähteenä oleva tiedosto on kirjoitettu L<sup>A</sup>T<sub>E</sub>X-tiedoston rakenteen opiskelemista ajatellen. Tiedoston kommentit sisältävät tietoa, joka on hyödyllistä opinnäytettä kirjoitettaessa.

Johdanto selvittää samat asiat kuin tiivistelmä, mutta laiveammin. Johdannossa kerrotaan yleensä seuraavat asiat

- Tutkimuksen taustaa ja tutkimusaiheen yleisluonteinen esittely
- Tutkimuksen tavoitteet
- Pääkysymys ja osaongelmat
- Tutkimuksen rajaus ja keskeiset käsitteet.

Lyhyiden opinnäytteiden johdannot ovat yleensä liian pitkiä, joten johdannon paisuttamista on vältettävä. Diplomityöhön sopii johdanto, joka on 2–4 sivua. Kandidaatintyön johdannon on oltava diplomityön johdantoa lyhyempi. Sopivasti tiivistetty johdanto ei kaipaa alaotsikoita.

## **2 Background**

### **2.1 Microservices?**

### **2.2 Containerization and Docker**

#### **2.2.1 Docker components**

#### **2.2.2 Linux control groups and namespaces**

#### **2.2.3 Linux capabilities, privileged containers, Container breakout**

[1]

1. Privileged container
2. CAP\_SYS\_ADMIN, mounting /proc and chroot
3. CAP\_SYS\_PTRACE, shellcode injection to running program, nc 172.17.0.1 on port running shell
4. Mounted docker socket, creating privileged containers

### **2.3 Kubernetes system components**

#### **2.3.1 apiserver**

#### **2.3.2 etcd**

#### **2.3.3 scheduler**

#### **2.3.4 controller-manager**

### **2.4 Kubernetes resources**

#### **2.4.1 Namespaces**

#### **2.4.2 Pods**

#### **2.4.3 Network policies**

#### **2.4.4 Admission control**

### **2.5 Principle of least privilege, Zero trust...**

### **3 Research material and methods**

Tässä osassa kuvataan käytetty tutkimusaineisto ja tutkimuksen metodologiset valinnat, sekä kerrotaan tutkimuksen toteutustapa ja käytetyt menetelmät.



## 4 Results

Tässä osassa esitetään tulokset ja vastataan tutkielman alussa esitettyihin tutkimuskysymyksiin. Tieteellisen kirjoitelman arvo mitataan tässä osassa esitettyjen tulosten perusteella.

Tutkimustuloksien merkitystä on aina syytä arvioida ja tarkastella kriittisesti. Joskus tarkastelu voi olla tässä osassa, mutta se voidaan myös jättää viimeiseen osaan, jolloin viimeisen osan nimeksi tulee »Tarkastelu». Tutkimustulosten merkitystä voi arvioida myös »Johtopäätökset»-otsikon alla viimeisessä osassa.

Tässä osassa on syytä myös arvioida tutkimustulosten luotettavuutta. Jos tutkimustulosten merkitystä arvioidaan »Tarkastelu»-osassa, voi luotettavuuden arviointi olla myös siellä.

## 5 Summary

Opinnäytteen tekijä vastaa siitä, että opinnäyte on tässä dokumentissa ja opinnäytteen tekemistä käsittelevillä luennoilla sekä harjoituksissa annettujen ohjeiden mukainen muotoseikoiltaan, rakenteeltaan ja ulkoasultaan.

## References

- [1] Thanh Bui. “Analysis of docker security”. In: *arXiv preprint arXiv:1501.02967* (2015).

## A Esimerkki liitteestä

Liitteet eivät ole opinnäytteen kannalta välttämättömiä ja opinnäytteen tekijän on kirjoittamaan ryhtyessään hyvä ajatella pärjäävänsä ilman liitteitä. Kokemattomat kirjoittajat, jotka ovat huolissaan tekstiosan pituudesta, paisuttavat turhan helposti liitteitä pitääkseen tekstiosan pituuden annetuissa rajoissa. Tällä tavalla ei synny hyvää opinnäytettä.