

No. 111

CYBERSECURITY

Kubernetes and Container Security

Securing images, clusters and workloads from build to runtime

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 111

Kubernetes and Container Security

Securing images, clusters and workloads from build to runtime

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Kubernetes and Container Security

Securing images, clusters and workloads from build to runtime

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Kubernetes is a registered trademark of The Linux Foundation. Docker and other product names are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Containers in brief 5
2 Kubernetes architecture 6
3 The 4Cs 8
4 Threats to Kubernetes 9
5 Lessons from incidents 10
6 The container lifecycle 11
7 Frameworks and benchmarks 12
8 The tool landscape 13

PART II · IMAGES AND SUPPLY CHAIN

9 Secure images 15
10 Dockerfile practices 16
11 Scanning images 17
12 Signing and provenance 19
13 Registries 20
14 SBOMs for containers 21

PART III · THE CLUSTER

15 Securing API access 23
16 Authentication 24
17 RBAC 25
18 Pod Security Standards 26
19 Admission control 27
20 Workload hardening 28
21 Network policies 29
22 Secrets 30
23 Nodes 31

FREE SAMPLE · ojayo.com

24 Service mesh and mutual TLS 32

PART IV · OPERATIONS

25 Runtime detection 34
26 Logging and audit 36
27 Incident response 37
28 Managed Kubernetes 38
29 AI workloads on Kubernetes 39
30 Multi-tenancy 40
31 GitOps 41
32 Common mistakes 42
33 A worked example 43
34 A hardening plan 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Containers package applications with everything they need to run, and **Kubernetes** runs those containers at scale across clusters of machines. Together they have become the standard way to run modern applications: the CNCF's survey published in January 2026 found that 82% of container users run Kubernetes in production.

That success makes Kubernetes a target. Exposed clusters, vulnerable images, over-privileged workloads and stolen credentials have all led to breaches and crypto-mining infections. This book explains container and Kubernetes security for beginners, following an application from build to runtime.

What this book covers

- Container and Kubernetes basics, and the threats they face.
- Building, scanning and signing secure images.
- Securing the cluster: API access, RBAC, Pod Security Standards and admission control.
- Workload hardening, network policies and secrets.
- Runtime detection, logging, incident response and managed Kubernetes.

Who this book is for

- **Developers and DevOps engineers** who build and deploy containers.
- **Platform engineers** running Kubernetes.
- **Security beginners** moving into cloud native security.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–8): containers, Kubernetes architecture, the 4Cs, threats, real incidents, the container lifecycle, frameworks, and the tool landscape.
- **Part II — Images and supply chain** (Chapters 9–14): secure images, Dockerfile practices, scanning, signing and provenance, registries, and SBOMs.
- **Part III — The cluster** (Chapters 15–24): API server access, authentication, RBAC, Pod Security Standards, admission control, workload hardening, network policies, secrets, nodes, and service mesh.
- **Part IV — Operations** (Chapters 25–34): runtime detection, logging and audit, incident response, managed Kubernetes, AI workloads, multi-tenancy, GitOps, common mistakes, a worked example, and a hardening plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in a real cluster.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on examples and screens

YAML examples are illustrative and were checked for valid syntax; adapt them to your environment. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain containers and Kubernetes, the layers of security, the threats and the frameworks that guide defence.

FREE SAMPLE · ojayo.com

CHAPTER 1

Containers in brief

Containers package applications consistently.

What a container is

A **container** is a lightweight, isolated process running from an **image**: a package containing an application and its dependencies. Containers share the host's operating system kernel, unlike virtual machines.

Why isolation matters

Containers are isolated using Linux features such as namespaces and control groups, but the isolation is weaker than between virtual machines. A container running with too many privileges can affect the host and other containers.

Images are layers

Images are built in layers, often starting from a public **base image**. Every package in those layers can carry vulnerabilities.

> **KEY IDEA**
> A container is only as secure as its image and the privileges it runs with.

FREE SAMPLE · ojayo.com

CHAPTER 2

Kubernetes architecture

Kubernetes orchestrates containers at scale.

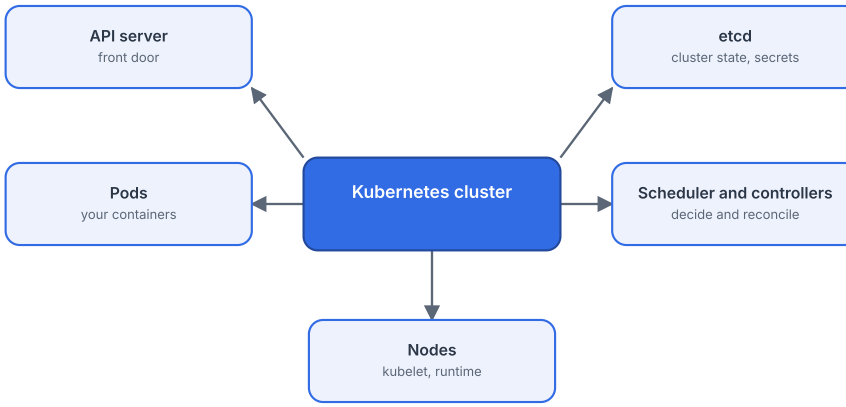


Figure 2.1 Main parts of a Kubernetes cluster

Control plane

The **API server** is the front door for every action. **etcd** stores the cluster's state, including secrets. Controllers and the scheduler keep the cluster in its desired state.

Nodes

Worker **nodes** run the **kubelet**, which manages pods, and a container runtime such as containerd.

FREE SAMPLE · ojayo.com

Pods and namespaces

A **pod** is one or more containers deployed together. **Namespaces** group resources and are a key unit for access control and policy.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security (you are rea…

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Kubernetes and Container Security

Enjoyed it? The full book has 52 pages and 34 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.