
Table of Contents

Preface.....	v
1. Introduction.....	1
Approaching Kubernetes security	2
Security principles	3
2. Securing The Cluster.....	7
API Server	7
Kubelet	9
Running etcd safely	11
Kubernetes Dashboard	12
Validating the Configuration	13
3. Authentication.....	15
Identity	15
Authentication Concepts	20
Authentication Strategies	21
Tooling And Good Practices	22
4. Authorization.....	25
Authorization Concepts	25
Authorization Modes	26
Access Control With RBAC	27
Tooling And Good Practices	32
5. Securing your Container Images.....	35
Scanning container images	36

Patching container images	36
CI/CD best practices	37
Image storage	38
Correct image versions	39
Image Trust and Supply Chain	40
Minimizing images to reduce the attack surface	41
6. Running Containers Securely.....	43
Say No To Root	43
Admission Control	44
Security Boundaries	45
Policies	48
7. Secrets Management.....	55
Applying the Principle of Least Privilege	55
Secret encryption	56
Kubernetes secret storage	56
Passing secrets into containerized code	58
Secret rotation and revocation	61
Secret access from within the container	62
Secret access as Kubelet	63
8. Advanced Topics.....	65
Monitoring, Alerting And Auditing	65
Host Security	66
Sandboxing and runtime protection	67
Multi-tenancy	68
Dynamic Admission Control	70
Network Protection	70
Static analysis of YAML	71
Avoiding Fork Bombs and other resource-based attacks	71
Avoiding crypto-currency mining	72
Kubernetes Security Updates	72