

Certified Kubernetes Security Specialist (CKS)

Harden Kubernetes clusters, secure the software supply chain and detect threats at runtime.

DURATION

3 days · 24 hours

LEVEL

Advanced

CURRICULUM

9 modules · 7 labs

DELIVERY

Live online, Onsite,
Corporate

Course overview

Running Kubernetes in production means defending it: locking down the API server, isolating workloads, controlling what images can run and spotting suspicious behaviour quickly. The CKS exam tests these skills hands-on, and this three-day course is built around practical hardening tasks in your own cluster.

Day one covers cluster setup and hardening: network policies, CIS benchmark checks, securing Ingress with TLS, protecting node metadata and binaries, restricting API access, tightening RBAC and service accounts, and keeping Kubernetes up to date.

Day two moves to system hardening and microservice isolation. You will reduce the host attack surface, use AppArmor and seccomp profiles, apply Pod Security Standards, manage Secrets securely, introduce sandboxed runtimes and examine pod-to-pod encryption options.

Day three is about the supply chain and runtime security: minimal base images, static analysis of manifests, image scanning, signing and admission policies, followed by audit logging, behavioural detection with Falco and investigating an incident. The day closes with timed mock tasks.

This course is aligned to the CKS exam curriculum published by The Linux Foundation and CNCF. The exam is performance-based and online proctored, and candidates must hold an active CKA certification before attempting it.

Highlights

- 24 hours of live, trainer-led sessions
- Hardening labs on your own multi-node cluster
- Pod Security, network policies and audit logging
- Image scanning, signing and admission control
- Runtime threat detection with Falco

What's included

- Dedicated multi-node lab cluster per learner
- CIS benchmark scanning and remediation
- AppArmor, seccomp and Pod Security Standards labs
- Image scanning, signing and admission policy
- Audit logging and Falco detection rules
- Mock tasks in the style of the exam
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- CKA holders responsible for production clusters
- Platform and DevSecOps engineers
- Cloud security engineers
- Site reliability engineers

Prerequisites

- An active CKA certification (required by the exam provider)
- Confident with kubectl and Linux administration
- Basic security concepts: TLS, least privilege

Detailed curriculum — 3 days, 24 hours, 9 modules, 7 hands-on labs

Day 1 Cluster Setup and Hardening

8 hours

1.1 Securing the cluster

- Network policies for default deny
- Ingress with TLS
- Verifying platform binaries
- CIS benchmark with kube-bench
- Protecting node metadata

LAB Run kube-bench and fix the findings · 50 min

1.2 API and access control

- Restricting API server access
- Service account hardening
- RBAC least privilege
- Disabling automounted tokens

LAB Lock down RBAC and service accounts · 40 min

1.3 Upgrades

- Keeping Kubernetes current
- Upgrade practice
- Deprecated APIs

Day 2 System Hardening and Microservice Isolation

8 hours

2.1 Host hardening

- Minimising host OS footprint
- IAM on the cloud provider
- Kernel hardening tools
- Reducing network exposure

LAB Apply AppArmor and seccomp profiles · 45 min

2.2 Workload isolation

- Pod Security Standards and admission
- OPA Gatekeeper policies
- Security contexts
- Sandboxed runtimes such as gVisor

LAB Enforce restricted Pod Security on a namespace · 40 min

2.3 Secrets and traffic

- Secret encryption at rest
- Pod-to-pod encryption and service mesh options
- External secret stores overview

LAB Encrypt Secrets at rest in etcd · 40 min

Day 3 Supply Chain, Runtime Security and Exam Readiness

8 hours

3.1 Supply chain security

- Minimal base images
- Image scanning with Trivy
- Allow-listing registries with admission policy
- Static analysis of manifests and Dockerfiles
- Image signing

LAB Scan, sign and gate images at admission · 55 min

3.2 Monitoring and runtime security

- Audit logging policies
- Immutable containers
- Behavioural detection with Falco
- Investigating an incident

LAB Detect and investigate suspicious activity with Falco · 50 min

3.3 Exam readiness

- Exam rules and environment
- Mock tasks with review
- Prioritising tasks

Skills and tools

Skills you will build

Kubernetes security

Network policies

CIS benchmarks

RBAC hardening

AppArmor

seccomp

Pod Security Standards

Secrets encryption

Supply chain security

Image scanning

Admission control

Audit logging

Falco

Tools used in class

kubecttl

kube-bench

Trivy

Falco

AppArmor

OPA Gatekeeper

gVisor

Cosign

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Certified Kubernetes Security Specialist (CKS)
Exam code	CKS
Duration	120 minutes
Format	Performance-based / lab
Delivery	Online proctored
Official page	https://training.linuxfoundation.org/certification/certified-kubernetes-security-specialist/

Exam skill areas covered

Cluster management
Cluster hardening
Cluster security
Container security
Network security
Service vulnerabilities

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Do I need CKA before CKS?

Yes. The exam provider requires an active CKA certification before you can sit the CKS exam.

What is the exam format?

It is performance-based and online proctored: you complete security tasks on live clusters within the time limit.

Which tools are covered?

We use widely adopted open-source tools such as kube-bench, Trivy, Falco, AppArmor and OPA Gatekeeper; check the current curriculum for the tools named by the exam.

Is this useful on managed Kubernetes?

Yes. Most workload, supply-chain and runtime controls apply directly to EKS, AKS and GKE.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/cks-certified-kubernetes-security-specialist · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Kubernetes, CKA, CKAD and CKS are trademarks of The Linux Foundation. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.