Document Generated: 11/25/2026

Learning Style: Virtual Classroom

Technology: Linux Foundation

Difficulty: Intermediate

Course Duration: 4 Days

Linux Foundation Certified Kubernetes Security Fundamentals



About this course:

Kubernetes has become the standard platform for running containerized applications, and that makes it a prime target. A single misconfiguration in a cluster, a vulnerable container image, or an overly permissive access policy can expose an entire environment. Securing Kubernetes takes a deliberate approach that starts before a cluster is built and continues long after workloads are running.

This course gives you the knowledge and skills to maintain security in dynamic, multi-project environments and to address the security concerns of cloud production environments. You'll start with a cloud security overview, then work through security across the full container supply chain, from preparing and installing a cluster through deployment and ongoing operations.

Course Objectives:

- Understand core cloud security concepts and the Kubernetes threat landscape
- Prepare for and install a Kubernetes cluster with security in mind from the start
- Harden cluster components and keep Kubernetes up to date
- Secure the kube-apiserver and control access with authentication, authorization, and RBAC
- Implement network policies to restrict traffic between pods and namespaces
- Apply Pod Security Admission and other controls to secure workloads
- Minimize vulnerabilities in microservices and container images
- Secure the container supply chain, from image build through deployment
- Monitor and log security events, and detect and respond to suspicious activity in a cluster
- Find and use ongoing sources of security and vulnerability information
- Build the skills tested on the Certified Kubernetes Security Specialist (CKS) exam

Audience:

- Kubernetes administrators who hold the Certified Kubernetes Administrator (CKA) certification

- Cloud security engineers and architects
- DevOps and DevSecOps engineers
- Platform and site reliability engineers (SREs)
- System administrators responsible for containerized environments
- IT professionals responsible for securing cloud production environments
- Anyone preparing for the Certified Kubernetes Security Specialist (CKS) exam

Prerequisites:

To get the most out of this course, you should have:

- A good understanding of Linux, including command-line use and system administration (equivalent to Linux System Administration (LFS307) or Linux for System Engineers (LFS311))
- Solid hands-on experience administering Kubernetes clusters, at the level of the Certified Kubernetes Administrator (CKA) certification
- Familiarity with containers and container images

Course Outline:

Introduction

- Linux Foundation
- Linux Foundation Training
- Linux Foundation Certifications
- Linux Foundation Digital Badges
- Laboratory Exercises, Solutions and Resources
- Things Change in Linux and Open Source Projects
- ELearning Course: LFS260
- Platform Details

Cloud Security Overview

- Multiple Projects

- What is Security?
- Assessment
- Prevention
- Detection
- Reaction
- Classes of Attackers
- Types of Attacks
- Attack Surfaces
- Hardware and Firmware Considerations
- Security Agencies
- Manage External Access
- Labs

Preparing to Install

- Image Supply Chain
- Runtime Sandbox
- Verify Platform Binaries
- Minimize Access to GUI
- Policy Based Control
- Labs

Installing the Cluster

- Update Kubernetes
- Tools to Harden the Kernel
- Kernel Hardening Examples
- Mitigating Kernel Vulnerabilities
- Labs

Securing the kubeapiserver

- Restrict Access to API
- Enable Kubeapiserver Auditing
- Configuring RBAC
- Pod Security Policies
- Minimize IAM Roles
- Protecting etcd
- CIS Benchmark
- Using Service Accounts
- Labs

Networking

- Firewalling Basics
- Network Plugins
- Mitigate Brute Force Login Attempts
- Ingress Objects
- Pod to Pod Encryption
- Restrict Cluster Level Access

- Labs

Workload Considerations

- Minimize Base Image
- Static Analysis of Workloads
- Runtime Analysis of Workloads
- Container Immutability
- Mandatory Access Control
- SELinux
- AppArmor
- Generate AppArmor Profiles
- Labs

Issue Detection

- Understanding Phases of Attack
- Preparation
- Understanding an Attack Progression
- During an Incident
- Handling Incident Aftermath
- Intrusion Detection Systems
- Threat Detection
- Behavioral Analytics
- Labs

Domain Reviews

- Preparing for the Exam
- Labs

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges