Document Generated: 11/20/2026

Learning Style: Online Instructor-Led

Technology: Linux Foundation

Difficulty: Beginner

Course Duration: 4 Days

Linux Foundation Certified Kubernetes Administrator (CKA)



About This Course:

Kubernetes is the standard platform for running containerized applications, and organizations need administrators who can keep their clusters stable, secure, and running. The Certified Kubernetes Administrator (CKA) is the most widely recognized way to show you have those skills. The Linux Foundation and the Cloud Native Computing Foundation (CNCF), the organization behind the Kubernetes

project, created it together.

Course Objectives:

- Troubleshoot clusters, nodes, and cluster components
- Monitor cluster and application resource usage, and manage and evaluate container logs
- Troubleshoot services and networking issues
- Manage role-based access control (RBAC)
- Prepare infrastructure for a Kubernetes cluster, then create and manage clusters with kubeadm through their full lifecycle
- Set up and configure a highly available control plane
- Use Helm and Kustomize to install cluster components
- Understand extension interfaces (CNI, CSI, CRI), custom resource definitions (CRDs), and operators
- Understand Pod-to-Pod connectivity, and define and enforce Network Policies
- Use ClusterIP, NodePort, and LoadBalancer services, the Gateway API, Ingress, and CoreDNS
- Manage deployments, rolling updates, and rollbacks, and configure applications with ConfigMaps and Secrets
- Configure workload autoscaling, Pod admission, and scheduling
- Set up storage classes, dynamic volume provisioning, persistent volumes (PVs), and persistent volume claims (PVCs)

Audience:

- Kubernetes and cluster administrators
- Cloud and infrastructure engineers
- DevOps engineers

Prerequisites:

- Strong Linux command-line skills
- Working knowledge of containers and container images
- Hands-on experience deploying and administering Kubernetes clusters

Course Outline:

Module 1: Cloud Security Overview

- Cloud native security concepts
- The 4C’s of cloud native security
- Threat modeling for Kubernetes
- Security tools and resources

Module 2: Preparing to Install

- Verifying platform binaries
- CIS benchmarks and kube-bench
- Minimizing the host operating system footprint

Module 3: Installing the Cluster

- Installing a cluster securely
- Limiting access to nodes
- Restricting access to cluster components

Module 4: Securing the kube-apiserver

- Authentication
- Authorization and role-based access control (RBAC)
- Admission controllers
- Service accounts
- Audit logging

Module 5: Networking

- Network policies
- Securing ingress with TLS
- Restricting access to metadata and cloud APIs
- Service mesh and mTLS overview

Module 6: Workload Considerations

- Security contexts
- Pod Security Standards and admission
- AppArmor and seccomp

- Managing Kubernetes Secrets
- Runtime sandboxes
- Supply chain security: image scanning, signing, and allowed registries

Module 7: Issue Detection

- Detecting threats at runtime
- Behavioral analytics with Falco
- Investigating with audit logs
- Ensuring container immutability

Module 8: CKS Exam Domain Review

- CKS exam domains and format