Updated on 12/17/2024

Sign up

CKS Certification Training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

Did you attend our Kubernetes training for administrators, and would you like to obtain the CKS certification? You don't want to fail the exam? For 2 days, we'll prepare you for the assessment so that you have every chance of becoming a certified Kubernetes security specialist.

CKS (Certified Kubernetes Security Specialist) is a recognized certification that lets you show your staff that you have the skills needed to ensure the security of your Kubernetes applications. Namely, the protection of applications in containers and platforms during construction, deployment and execution on Kubernetes.

The exam is divided into 6 parts: Setting up the cluster, Protecting the cluster, Protecting the system, Reducing the vulnerability of microservices, Protecting the supply chain and Monitoring, logging and runtime security. We'll go into these 6 concepts in depth on the preparation day, so that you can pass your assessment.

Objectives

- Know how to use Kubernetes in the most secure way while ensuring the scalability of your infrastructure.
- Be ready to pass the CKS exam

Target audience

Developers, Architects, Systems administrators, DevOps

Prerequisites

- Good knowledge of using Kubernetes for administration or have taken our advanced Kubernetes training course
- Basic knowledge of a Unix system and how containers work
- CKA certification

TECHNICAL PREREQUISITES

- SSH client and virtual machines at your disposal
- Docker installed
- Unrestricted Internet access
- PC with administrator access (WSL if Windows)

CKS exam preparation program

Detailed Kubernetes architecture

- ApiServer
- Etcd
- Kube Scheduler
- Kube Controller Manager
- Kubelet
- Kube-proxy

Networking in Kubernetes

- Ingress and TLS security
- Advanced NetworkPolicy
- Pod to Pod mTLS

Hardening Clusters

- Service Account
- RBAC
- Principle of least privilege
- Hardening of Kubernetes components (kubelet, controlplane, dashboard)
- Updating Kubernetes with kubeadm
- CIS benchmark

Hardening System

- AppArmor and AppArmor
- Kernel modules
- Reduced attack surface (network, system)

Hardening workloads

- SecurityContext
- Container Runtime
- Secrets
- OPA Gatekeeper
- Security Policy

Securing the supply chain

- Image signature
- Image scanning
- Registry Docker
- Hardening Dockerfile
- SAST on Dockerfile and Kubernetes manifests
- Admission Controller

Monitoring and Logging

- AuditPolicy
- Falco
- Runtime security

Strategies and methods for success

- Shortcuts and aliases
- Advanced use of kubectl
- Navigating between clusters and namespaces

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.