Updated on 12/17/2024

Sign up

KCSA® certification training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

Our preparation for the Kubernetes and Cloud Security Associate® (KCSA®) certification will give you all the keys you need to pass the exam. It will enable you to demonstrate your knowledge of cloud-native security issues.

The exam will review all the fundamental knowledge of Kubernetes and cloud-native security. The course will give you all the skills you need to secure a Kubernetes environment. The review focuses particularly on cloud providers, infrastructures and clusters. Containers and code will also be covered.

Our preparation will introduce you to everything you need to know to pass the exam. You'll learn all the strategies and best practices to validate your KCSA® certification. Our trainer will tailor the course to your needs, or if there are certain points that require special attention on your part.

The exam will run on version 1.31, which is the latest release of Kubernetes.

Objectives

- Be ready to take the KCSA® exam
- Get up and running with cloud-native security
- Get up to speed on Kubernetes security

Target audience

- **Devops**

- Network administrators

Prerequisites

- Kubernetes basics

MATERIALS REQUIRED

- A good Internet connection
- Kubernetes installed

Note: Ambient IT is not the owner of KCSA®, this certification belongs to The Linux Foundation®.

KCSA® certification training program

Overview of cloud-native security

- The 4 Cs
- Supplier and infrastructure security
- Controls and frameworks
- Insulation techniques
- Artifact Repository and image security
- Code and workload security

Component security in Kubernetes clusters

- API Server
- Controller Manager
- Scheduler
- Kubelet
- Container Runtime
- KubeProxy
- Pod
- Etcd
- Container Networking
- Client Security
- Storage

Kubernetes security fundamentals

- Pod Security Standards
- Pod Security Admissions

- Authentication and authorization
- Secrets
- Insulation and segmentation
- Audit and logging
- Network policy

Threats in Kubernetes

- Data flow and trust boundaries
- Persistence
- Denial of service (DoS)
- Malicious code and compromised applications in containers
- Network attacks
- Access to sensitive data
- Escalation of privileges

Platform security

- Supply Chain Safety
- Image Repository
- Observability
- Service Mesh
- ICP
- Connectivity
- Admission control

Compliance and safety framework

- Compliance Frameworks
- Threat modeling framework
- supply chain compliance
- Automation and tools

STRATEGY AND METHODS FOR PASSING THE MOCK EXAM

EXCHANGE ON SPECIFIC POINTS

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.