#1 Cloud and VM Certification Guide

Linux Foundation CKS

LINUX FOUNDATION KUBERNETES SECURITY SPECIALIST CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

CKS

Certified Kubernetes Security Specialist (CKS)

20-25 Questions Exam – 67% Cut Score – Duration of 120 minutes

www.VMExam.com

Table of Contents

Know Your CKS Certification Well:

The CKS is best suitable for candidates who want to gain knowledge in the Linux Foundation Cloud & Containers. Before you start your CKS preparation you may struggle to get all the crucial Kubernetes Security Specialist materials like CKS syllabus, sample questions, study guide.

But don't worry the CKS PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CKS syllabus?
- How many questions are there in the CKS exam?
- Which Practice test would help me to pass the CKS exam at the first attempt?

Passing the CKS exam makes you Certified Kubernetes Security Specialist (CKS). Having the Kubernetes Security Specialist certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Linux Foundation CKS Kubernetes Security Specialist Certification Details:

Exam Name	Certified Kubernetes Security Specialist
Exam Code	CKS
Exam Price	$445 USD
Duration	120 minutes
Number of Questions	20-25
Passing Score	67%
Recommended Training / Books	**Kubernetes Security Essentials (LFS260)**
Schedule Exam	**The Linux Foundation Training & Certification**
Sample Questions	**Linux Foundation CKS Sample Questions**
Recommended Practice	**Certified Kubernetes Security Specialist (CKS) Practice Test**

CKS Syllabus:

Section	Objectives	Weight
Cluster Setup	- Use Network security policies to restrict cluster level access - Use CIS benchmark to review the security configuration of Kubernetes components (etcd, kubelet, kubedns, kubeapi) - Properly set up Ingress with TLS - Protect node metadata and endpoints - Verify platform binaries before deploying	**15%**
Cluster Hardening	- Use Role Based Access Controls to minimize exposure - Exercise caution in using service accounts e.g. disable defaults, minimize permissions on newly created ones - Restrict access to Kubernetes API - Upgrade Kubernetes to avoid vulnerabilities	**15%**
System Hardening	- Minimize host OS footprint (reduce attack surface) - Using least-privilege identity and access management - Minimize external access to the network - Appropriately use kernel hardening tools such as AppArmor, seccomp	**10%**
Minimize Microservice Vulnerabilities	- Use appropriate pod security standards - Manage Kubernetes secrets - Understand and implement isolation techniques (multi-tenancy, sandboxed containers, etc.) - Implement Pod-to-Pod encryption using Cilium	**20%**
Supply Chain Security	- Minimize base image footprint - Understand your supply chain (e.g. SBOM, CI/CD, artifact repositories) - Secure your supply chain (permitted registries, sign and validate artifacts, etc.) - Perform static analysis of user workloads and container images (e.g. Kubesec, KubeLinter)	**20%**

Section	Objectives	Weight
Monitoring, Logging and Runtime Security	- Perform behavioral analytics to detect malicious activities - Detect threats within physical infrastructure, apps, networks, data, users and workloads - Investigate and identify phases of attack and bad actors within the environment - Ensure immutability of containers at runtime - Use Kubernetes audit logs to monitor access	**20%**

Linux Foundation CKS Sample Questions:

Question: 1

What is the recommended frequency for scanning container images for known vulnerabilities?

a) Never, as container images are inherently secure and free from vulnerabilities
b) Once at the initial build stage and not necessary afterwards
c) Only when significant updates or changes are made to the container images
d) Regularly and consistently, including during the build and deployment process

Answer: d

Question: 2

How can you leverage audit logs to monitor access effectively?

a) By disabling all logging processes for increased performance
b) By recording and analyzing all access attempts, actions, and events for auditing and security analysis
c) By granting unrestricted access to all audit logs for simplified management
d) By encrypting all audit logs to ensure confidentiality

Answer: b

Question: 3

Why is it important to exercise caution when using service accounts in Kubernetes?

a) Service accounts increase the attack surface of the cluster.
b) Service accounts can bypass RBAC policies and gain excessive privileges.
c) Service accounts consume excessive system resources.
d) Service accounts introduce compatibility issues with other Kubernetes components.

Answer: a

Question: 4

How can behavioral analytics help detect threats within physical infrastructure, apps, networks, data, users, and workloads?

a) By analyzing patterns and anomalies in behavior to identify potential security risks
b) By disabling all network communication within the environment for increased security
c) By granting full administrative privileges to all users and workloads
d) By encrypting all data at rest and in transit for improved confidentiality

Answer: a

Question: 5

Which security measure can help protect the host OS from malware and unauthorized code execution?

a) Enabling automatic software updates
b) Implementing regular vulnerability scans
c) Using anti-malware software
d) Applying strict file and process access controls

Answer: d

Question: 6

How do container runtime sandboxes contribute to the security of multi-tenant environments?

a) By enforcing strict resource limits for each container
b) By isolating and preventing container escape or privilege escalation
c) By encrypting all container-to-container communication
d) By optimizing container networking for improved performance

Answer: b

Question: 7

What is the importance of ensuring the immutability of containers at runtime?

a) To simplify troubleshooting and debugging tasks
b) To optimize resource allocation within the environment
c) To enable seamless communication between containers
d) To prevent unauthorized modifications or tampering of container contents

Answer: d

Question: 8

Which tool can be used to assess Kubernetes cluster security against the CIS benchmark?

a) Kubelet
b) Prometheus
c) Kube-bench
d) Fluentd

Answer: c

Question: 9

Why is it recommended to minimize the use of GUI elements in a Kubernetes cluster?

a) GUI elements consume excessive system resources
b) GUI elements are prone to security vulnerabilities
c) GUI elements hinder cluster performance
d) GUI elements are not supported in Kubernetes

Answer: b

Question: 10

What is the role of Role-Based Access Control (RBAC) in securing a Kubernetes cluster?

a) It provides secure communication between nodes in the cluster.
b) It encrypts all network traffic within the cluster.
c) It restricts access to the Kubernetes API based on user roles and permissions.
d) It ensures high availability of the cluster by load balancing the API requests.

Answer: c

Study Guide to Crack Linux Foundation Kubernetes Security Specialist CKS Exam:

- Getting details of the CKS syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CKS exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Linux Foundation provided training for CKS exam could be of much help. If there is specific training for the exam, you can discover it from the link above.

- Read from the CKS sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CKS practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CKS Certification

Make VMExam.com your best friend during your Certified Kubernetes Security Specialist exam preparation. We provide authentic practice tests for the CKS exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CKS exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don’t bother if you don’t get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CKS exam.

Start Online practice of CKS Exam by visiting URL

https://www.vmexam.com/linux-foundation/cks-certified-kubernetes-security-specialist