



Welcome to Cert007 - Your Ultimate IT Certification Partner



➤ Real Exam Questions

➤ Instant Access

➤ Free Updates

➤ Money-Back Guarantee

➤ Expert Support



Visit us at <https://www.cert007.com/> for more information

Exam : **KCSA**

Title : Kubernetes and Cloud
Native Security Associate
(KCSA)

Version : DEMO

1.Which standard approach to security is augmented by the 4C's of Cloud Native security?

- A. Zero Trust
- B. Least Privilege
- C. Defense-in-Depth
- D. Secure-by-Design

Answer: C

2.In a Kubernetes cluster, what are the security risks associated with using ConfigMaps for storing secrets?

- A. Storing secrets in ConfigMaps does not allow for fine-grained access control via RBAC.
- B. Storing secrets in ConfigMaps can expose sensitive information as they are stored in plaintext and can be accessed by unauthorized users.
- C. Using ConfigMaps for storing secrets might make applications incompatible with the Kubernetes cluster.
- D. ConfigMaps store sensitive information in etcd encoded in base64 format automatically, which does not ensure confidentiality of data.

Answer: B, D

3.What is the difference between gVisor and Firecracker?

- A. gVisor is a user-space kernel that provides isolation and security for containers. At the same time, Firecracker is a lightweight virtualization technology for creating and managing secure, multi-tenant container and function-as-a-service (FaaS) workloads.
- B. gVisor is a lightweight virtualization technology for creating and managing secure, multi-tenant container and function-as-a-service (FaaS) workloads. At the same time, Firecracker is a user-space kernel that provides isolation and security for containers.
- C. gVisor and Firecracker are both container runtimes that can be used interchangeably.
- D. gVisor and Firecracker are two names for the same technology, which provides isolation and security for containers.

Answer: A

4.You want to minimize security issues in running Kubernetes Pods.

Which of the following actions can help achieve this goal?

- A. Sharing sensitive data among Pods in the same cluster to improve collaboration.
- B. Running Pods with elevated privileges to maximize their capabilities.
- C. Implement Pod Security standards in the Pod's YAML configuration.
- D. Deploying Pods with randomly generated names to obfuscate their identities.

Answer: C

5.What was the name of the precursor to Pod Security Standards?

- A. Container Runtime Security
- B. Kubernetes Security Context
- C. Container Security Standards
- D. Pod Security Policy

Answer: D

