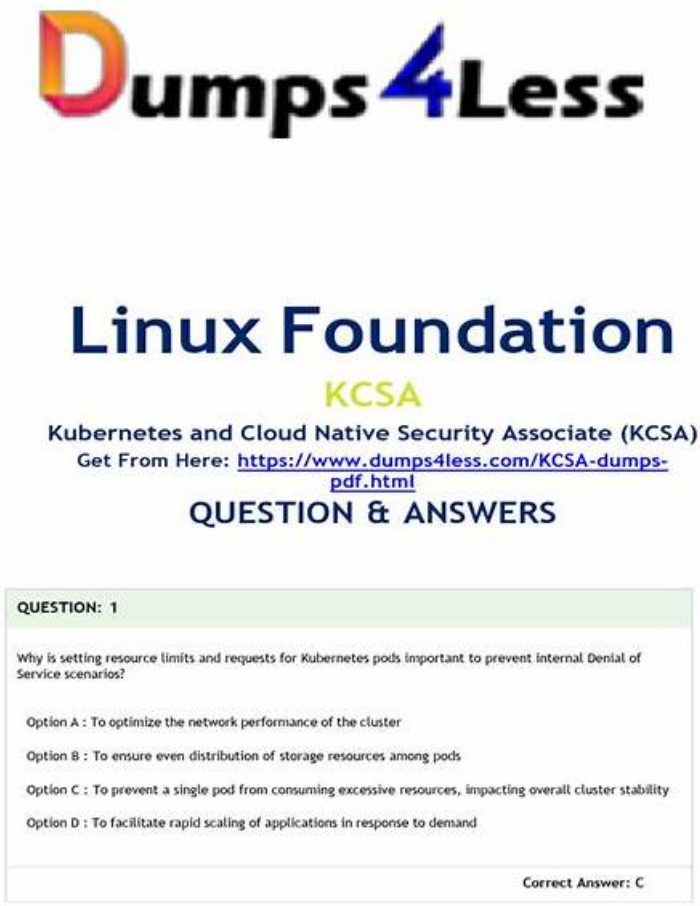
Linux Foundation Offers Valid and Real Linux Foundation KCSA Exam Questions



The content of our KCSA practice braindumps is chosen so carefully that all the questions for the exam are contained. And our KCSA study materials have three formats which help you to read, test and study anytime, anywhere. They are the versions of the PDF, Software and APP online. This means with our KCSA training guide, you can prepare for exams efficiently. If you desire a KCSAcertification, our products are your best choice.

Linux Foundation KCSA Exam Syllabus Topics:

Topic	Details
Topic 1	• Platform Security: This section of the exam measures the skills of a Cloud Security Architect and encompasses broader platform-wide security concerns. This includes securing the software supply chain from image development to deployment, implementing observability and service meshes, managing Public Key Infrastructure (PKI), controlling network connectivity, and using admission controllers to enforce security policies.
Topic 2	• Overview of Cloud Native Security: This section of the exam measures the skills of a Cloud Security Architect and covers the foundational security principles of cloud-native environments. It includes an understanding of the 4Cs security model, the shared responsibility model for cloud infrastructure, common security controls and compliance frameworks, and techniques for isolating resources and securing artifacts like container images and application code.

Topic 3	• Compliance and Security Frameworks: This section of the exam measures the skills of a Compliance Officer and focuses on applying formal structures to ensure security and meet regulatory demands. It covers working with industry-standard compliance and threat modeling frameworks, understanding supply chain security requirements, and utilizing automation tools to maintain and prove an organization's security posture.

>> KCSA Valid Test Pass4sure <<

Providing You 100% Pass-Rate KCSA Valid Test Pass4sure with 100% Passing Guarantee

Getting tired of humdrum life, you may want to get some successful feeling or try something different instead. We all know that is of important to pass the KCSA exam and get the KCSA certification for someone who wants to find a good job in internet area, and it is not a simple thing to prepare for exam. So you are in the right place now. The KCSA practice materials are a great beginning to prepare your exam. Actually, just think of our Linux Foundation practice materials as the best way to pass the exam is myopic. They can not only achieve this, but ingeniously help you remember more content at the same time.

Linux Foundation Kubernetes and Cloud Native Security Associate Sample Questions (Q55-Q60):

NEW QUESTION # 55
Which of the following is a control for Supply Chain Risk Management according to NIST 800-53 Rev. 5?

- A. Supply Chain Risk Management Plan
- B. Access Control
- C. Incident Response
- D. System and Communications Protection

Answer: A

Explanation:
* NIST SP 800-53 Rev. 5 introduces a dedicated family of controls calledSupply Chain Risk Management (SR).
* Within SR,SR-2 (Supply Chain Risk Management Plan)is a specific control.
* Exact extract from NIST 800-53 Rev. 5:
* "The organization develops and implements a supply chain risk management plan for the system, system component, or system service."
* While Access Control, System and Communications Protection, and Incident Response are control families, the correctsupply chain-specific controlis theSupply Chain Risk Management Plan (SR-2).
References:
NIST SP 800-53 Rev. 5 -Security and Privacy Controls for Information Systems and Organizations:
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NEW QUESTION # 56
What is the difference between gVisor and Firecracker?

- A. 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.
- B. 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.
- 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: B

Explanation:
* gVisor:
* Google-developed, implemented as auser-space kernelthat intercepts and emulates syscalls made by containers.
* Providesstrong isolationwithout requiring a full VM.
* Official docs: "gVisor is a user-space kernel, written in Go, that implements a substantial portion of the Linux system call interface."
* Source: https://gvisor.dev/docs/
* Firecracker:
* AWS-developed,lightweight virtualization technologybuilt on KVM, used in AWS Lambda and Fargate.
* Optimized for running secure, multi-tenant microVMs (MicroVMs) for containers and FaaS.
* Official docs: "Firecracker is an open-source virtualization technology that is purpose-built for creating and managing secure, multi-tenant container and function-based services."
* Source: https://firecracker-microvm.github.io/
* Key difference:gVisor # syscall interception in userspace kernel (container isolation). Firecracker # lightweight virtualization with microVMs (multi-tenant security).
* Therefore, optionAis correct.
References:
gVisor Docs: https://gvisor.dev/docs/
Firecracker Docs: https://firecracker-microvm.github.io/

NEW QUESTION # 57
Which security knowledge-base focuses specifically onoffensive tools, techniques, and procedures?

- A. NIST Cybersecurity Framework
- B. OWASP Top 10
- C. MITRE ATT&CK
- D. CIS Controls

Answer: C

Explanation:
* MITRE ATT&CKis a globally recognizedknowledge base of adversary tactics, techniques, and procedures (TTPs). It is focused on describingoffensive behaviorsattackers use.
* Incorrect options:
* (B)OWASP Top 10highlights common application vulnerabilities, not attacker techniques.
* (C)CIS Controlsare defensive best practices, not offensive tools.
* (D)NIST Cybersecurity Frameworkprovides a risk-based defensive framework, not adversary TTPs.
References:
MITRE ATT&CK Framework
CNCF Security Whitepaper - Threat intelligence section: references MITRE ATT&CK for describing attacker behavior.

NEW QUESTION # 58
Which of the following statements best describes the role of the Scheduler in Kubernetes?

- A. The Scheduler is responsible for monitoring and managing the health of the Kubernetes cluster.
- B. The Scheduler is responsible for assigning Pods to nodes based on resource availability and other constraints.
- C. The Scheduler is responsible for ensuring the security of the Kubernetes cluster and its components.
- D. The Scheduler is responsible for managing the deployment and scaling of applications in the Kubernetes cluster.

Answer: B

Explanation:
* TheKubernetes Schedulerassigns Pods to nodes based on:
* Resource requests & availability (CPU, memory, GPU, etc.)
* Constraints (affinity, taints, tolerations, topology, policies)
* Exact extract (Kubernetes Docs - Scheduler):
* "The scheduler is a control plane process that assigns Pods to Nodes. Scheduling decisions take into account resource requirements, affinity/anti-affinity, constraints, and policies."
* Other options clarified:
* A: Monitoring cluster health is theController Manager's/kubelet's job.

* B: Security is enforced throughRBAC, admission controllers, PSP/PSA, not the scheduler.
* C: Deployment scaling is handled by theController Manager(Deployment/ReplicaSet controller).
References:
Kubernetes Docs - Scheduler: https://kubernetes.io/docs/concepts/scheduling-eviction/kube-scheduler/

NEW QUESTION # 59
In order to reduce the attack surface of the Scheduler, which default parameter should be set to false?

- A. --profiling
- B. --secure-kubeconfig
- C. --bind-address
- D. --scheduler-name

Answer: A

Explanation:
* Thekube-schedulerexposes aprofiling/debugging endpointwhen --profiling=true (default).
* This can unnecessarily increase the attack surface.
* Best practice: set --profiling=false in production.
* Exact extract (Kubernetes Docs - kube-scheduler flags):
* "--profiling (default true): Enable profiling via web interface host:port/debug/pprof/."
* Why others are wrong:
* --scheduler-name: just identifies the scheduler, not a security risk.
* --secure-kubeconfig: not a valid flag.
* --bind-address: changing it limits exposure but is not the default risk parameter for profiling.
References:
Kubernetes Docs - kube-scheduler options: https://kubernetes.io/docs/reference/command-line-tools- reference/kube-scheduler/

NEW QUESTION # 60
.....

If you buy and use the KCSA study materials from our company, you can complete the practice tests in a timed environment, receive grades and review test answers via video tutorials. You just need to download the software version of our KCSA Study Materials after you buy our study materials. You will have the right to start to try to simulate the real examination. We believe that the KCSA study materials from our company will not let you down.

- Linux Foundation KCSA Desktop Practice Test Software □ Search for ➥ KCSA □ and easily obtain a free download on 《 www.pdfvce.com 》 □KCSA Latest Real Exam
- Certificate KCSA Exam □ KCSA Reliable Dumps Book □ KCSA Reliable Dumps Book □ Search for □ KCSA □ and download it for free immediately on ➥ www.prep4away.com □□□ □KCSA Latest Test Experience
- tacliinshecourses.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, daotao.wisebusiness.edu.vn, bbs.teachersbbs.com, practicalmind.net, www.stes.tyc.edu.tw, cou.alnoor.edu.iq, mekkawyacademy.com, Disposable vapes