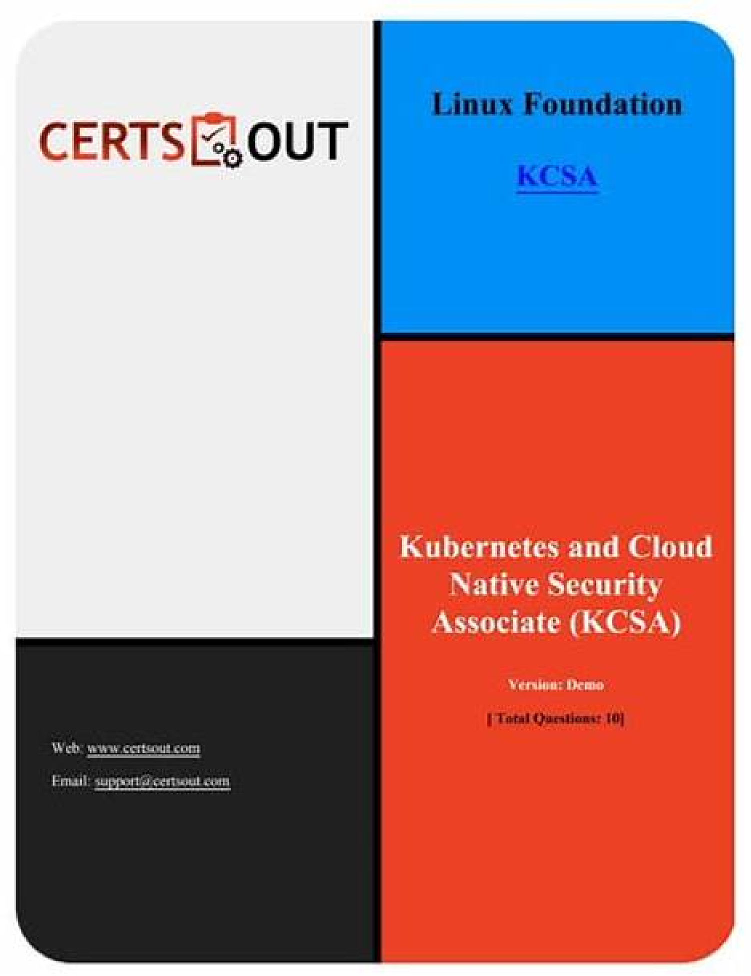
[Technology] Linux Foundation KCSA Exam Dumps For Good Success 2026



BONUS!!! Download part of DumpsValid KCSA dumps for free: https://drive.google.com/open?id=1HliAyl5RD_aXG31PobV_lXZovG3Mfag4

At present, our company has launched all kinds of KCSA study materials, which almost covers all official tests. Every KCSA exam questions are going through rigid quality check before appearing on our online stores. So you do not need to worry about trivial things and concentrate on going over our KCSA Exam Preparation. After careful preparation, you are bound to pass the KCSA exam. Just remember that all your efforts will finally pay off.

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	- 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.
Topic 3	- 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 4	- Kubernetes Cluster Component Security: This section of the exam measures the skills of a Kubernetes Administrator and focuses on securing the core components that make up a Kubernetes cluster. It encompasses the security configuration and potential vulnerabilities of essential parts such as the API server, etcd, kubelet, container runtime, and networking elements, ensuring each component is hardened against attacks.

>> KCSA Reliable Braindumps Questions <<

Valid KCSA Study Plan, KCSA Dumps Collection

In today's society, the pace of life is very fast. No matter what your current status is KCSA exam questions can save you the most time, and then pass the exam while still having your own life time. The users of the KCSA Study Materials are very extensive, but everyone has a common feature, that is, hope to obtain the KCSA certification in the shortest possible time. You can really do this in our KCSA learning guide.

Linux Foundation Kubernetes and Cloud Native Security Associate Sample Questions (Q15-Q20):

NEW QUESTION # 15
Which information does a user need to verify a signed container image?

- A. The image's SHA-256 hash and the public key of the signing authority.
- B. The image's digital signature and the public key of the signing authority.
- C. The image's SHA-256 hash and the private key of the signing authority.
- D. The image's digital signature and the private key of the signing authority.

Answer: B

Explanation:
* Container image signing (e.g., withcosign, Notary v2) uses asymmetric cryptography.
* Verification process:
* Retrieve theimage's digital signature.
* Validate the signature with thepublic keyof the signer.
* Exact extract (Sigstore Cosign Docs):
* "Verification of an image requires the signature and the signer's public key. The signature proves authenticity and integrity."
* Why others are wrong:
* A & B: The private key is only used by the signer, never shared.
* C: The hash alone cannot prove authenticity without the digital signature.
References:
Sigstore Cosign Docs: https://docs.sigstore.dev/cosign/overview

NEW QUESTION # 16
A Kubernetes cluster tenant can launch privileged Pods in contravention of therestricted Pod Security Standardmandated for cluster tenants and enforced by the built-inPodSecurity admission controller.

The tenant has full CRUD permissions on the namespace object and the namespaced resources. How did the tenant achieve this?

- A. The scope of the tenant role means privilege escalation is impossible.
- B. By deleting the PodSecurity admission controller deployment running in their namespace.
- C. By using higher-level access credentials obtained reading secrets from another namespace.
- D. By tampering with the namespace labels.

Answer: D

Explanation:
* ThePodSecurity admission controllerenforces Pod Security Standards (Baseline, Restricted, Privileged)based on namespace labels.
* If a tenant has full CRUD on the namespace object, they canmodify the namespace labelsto remove or weaken the restriction (e.g., setting pod-security.kubernetes.io/enforce=privileged).
* This allows privileged Pods to be admitted despite the security policy.
* Incorrect options:
* (A) is false - namespace-level access allows tampering.
* (C) is invalid - PodSecurity admission is not namespace-deployed, it's a cluster-wide admission controller.
* (D) is unrelated - Secrets from other namespaces wouldn't directly bypass PodSecurity enforcement.
References:
Kubernetes Documentation - Pod Security Admission
CNCF Security Whitepaper - Admission control and namespace-level policy enforcement weaknesses.

NEW QUESTION # 17
What was the name of the precursor to Pod Security Standards?

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

Answer: B

Explanation:
* Kubernetes originally had a feature calledPodSecurityPolicy (PSP), which provided controls to restrict pod behavior.
* Official docs:
* "PodSecurityPolicy was deprecated in Kubernetes v1.21 and removed in v1.25."
* "Pod Security Standards (PSS) replace PodSecurityPolicy (PSP) with a simpler, policy- driven approach."
* PSP was often complex and hard to manage, so it was replaced by Pod Security Admission (PSA) which enforcesPod Security Standards.
References:
Kubernetes Docs - PodSecurityPolicy (deprecated): https://kubernetes.io/docs/concepts/security/pod- security-policy/ Kubernetes Blog - PodSecurityPolicy Deprecation: https://kubernetes.io/blog/2021/04/06/podsecuritypolicy- deprecation-past-present-and-future/

NEW QUESTION # 18
Which of the following represents a baseline security measure for containers?

- A. Implementing access control to restrict container access.
- B. Configuring a static IP for each container.
- C. Configuring persistent storage for containers.
- D. Run containers as the root user.

Answer: A

Explanation:
* Access control (RBAC, least privilege, user restrictions)is abaseline container security best practice.
* Exact extract (Kubernetes Pod Security Standards - Baseline):
* "The baseline profile is designed to prevent known privilege escalations. It prohibits running privileged containers or containers as

root."
* Other options clarified:
* B: Static IPs not a security measure.
* C: Persistent storage is functionality, not security.
* D: Running as root is explicitlyinsecure.
References:
Kubernetes Docs - Pod Security Standards (Baseline): https://kubernetes.io/docs/concepts/security/pod- security-standards/

NEW QUESTION # 19
Which of the following is a control for Supply Chain Risk Management according to NIST 800-53 Rev. 5?

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

Answer: C

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 # 20
......

- Study KCSA Plan □ KCSA Latest Dumps □ Valid Dumps KCSA Sheet □ Open （ www.pdfvce.com ） enter ▷ KCSA ◁ and obtain a free download □Questions KCSA Pdf
- KCSA Exam Passing Score □ Valid KCSA Test Objectives □ Premium KCSA Files □ Easily obtain □ KCSA □ for free download through ➽ www.vce4dumps.com □ □KCSA Top Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, ncon.edu.sa, study.stcs.edu.np, quokkademy.com, Disposable vapes