

PRACTICE QUESTIONS

Linux Foundation / CNCF

CKS

Certified Kubernetes Security Specialist

SHARED BY [u/boldbison1986](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM Linux Foundation / CNCF CKS, Certified Kubernetes Security Specialist

Shared by u/boldbison1986 on aiexamcerts

10 practice questions for the Linux Foundation / CNCF CKS exam, Certified Kubernetes Security Specialist, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/linux-foundation-cncf/cks. Spotted a mistake? Email support@aiexamcerts.com with the exam code CKS and the question number.

1. A hardened node must reject anonymous calls to the kubelet API and authorize requests through the API server. Which kubelet configuration does this?
 - A readOnlyPort: 10255 left enabled so that unauthenticated monitoring tools can scrape the node
 - B cgroupDriver: systemd
 - C rotateCertificates: false
 - D authentication.anonymous.enabled: false with authorization.mode: Webhook

Answer: D

Disabling anonymous authentication and using the Webhook authorization mode sends kubelet requests through the API server's access review. The read-only port exposes unauthenticated data and is the opposite of what is needed. cgroupDriver affects resource management, and certificate rotation has nothing to do with anonymous access.

2. Enabling anonymous authentication on the kubelet is recommended so that the metrics server can scrape nodes without credentials.
 - A True
 - B False

Answer: B (False)

Anonymous kubelet access is a known exposure, and the metrics server should authenticate with a client certificate and an RBAC-backed identity instead. Hardened clusters disable anonymous authentication. The statement is therefore false.

3. Which command checks whether the ServiceAccount app-sa in namespace shop is allowed to delete Secrets in that namespace?
 - A kubectl auth can-i delete secrets --as=system:serviceaccount:shop:app-sa -n shop
 - B kubectl get secrets --as=app-sa
 - C kubectl describe serviceaccount app-sa and read its token and secret references in the output
 - D kubectl config view --raw

Answer: A

kubectl auth can-i with --as impersonates the ServiceAccount and asks the authorizer for the verb, resource and namespace. get secrets would try a real read rather than check delete permission, and it uses the wrong identity format. describe and config view do not evaluate permissions.

4. The seccomp profile type that applies the container runtime's default syscall filter is _____.

Answer: RuntimeDefault (also accepted: Runtime Default)

RuntimeDefault applies the container runtime's built-in seccomp filter, which blocks a set of risky system calls without custom work. Unconfined disables seccomp entirely, and Localhost loads a custom profile from the node. RuntimeDefault is the recommended baseline for most workloads.

5. Which two kube-apiserver settings help prevent unauthenticated access to the cluster? (Choose two.)

- A --anonymous-auth=false
- B --profiling=false
- C --authorization-mode=Node,RBAC
- D --enable-admission-plugins=AlwaysPullImages
- E --audit-log-maxage=30

Answer: A, C

Turning off anonymous authentication stops unauthenticated requests from being treated as a valid identity, and Node,RBAC ensures every request is authorized. Profiling and image pulling are unrelated to authentication. The audit retention setting helps investigations but does not block anyone.

6. Which Pod Security Admission mode admits violating pods but records each violation in the audit log?

- A audit
- B enforce
- C exempt
- D restricted

Answer: A

The audit mode lets violating pods through while writing the violation to the audit log, which helps teams find workloads before enforcing a level. enforce rejects violating pods outright. exempt is a list of users, namespaces or runtime classes that skip checks, and restricted is a level rather than a mode.

7. A service must accept traffic only from pods in the namespace named frontend. Which resource enforces this?
- A A Service of type ExternalName pointing at the frontend
 - B A NetworkPolicy with a namespaceSelector that matches the frontend namespace
 - C A ConfigMap listing the allowed namespaces
 - D A PodDisruptionBudget for the frontend pods that limits how many of them can be evicted at once

Answer: B

A NetworkPolicy with a namespaceSelector allows ingress only from pods in the matching namespace, and the CNI plugin enforces it. ExternalName is a DNS alias and does not filter traffic. A ConfigMap is only data, and a PodDisruptionBudget governs voluntary evictions.

8. Environment variables that carry a Secret value are safer than a mounted Secret file because they are never visible to child processes.
- A True
 - B False

Answer: B (False)

Environment variables are inherited by child processes and often leak into logs, crash dumps and diagnostic output, so they are generally considered riskier than files with tight permissions. The claim that they are never visible to child processes is false. The statement is false.

9. Which admission plugin calls an external service to approve or deny the use of an image?
- A ImagePolicyWebhook
 - B NodeRestriction
 - C ServiceAccount
 - D DefaultStorageClass

Answer: A

ImagePolicyWebhook sends image references to a webhook backend that returns allow or deny, which lets a cluster enforce its own image policy. NodeRestriction limits kubelet permissions, ServiceAccount attaches identities to pods, and DefaultStorageClass sets a storage default. Only the first is an image gate.

10. A pipeline must prove which commit produced a deployed image. What is the most useful practice?
- A Always push the image with the latest tag
 - B Record the commit SHA as an image label and attach a provenance attestation
 - C Rename the image file with the build date only, which is recorded in the registry index
 - D Store the registry password inside the image

Answer: B

A commit label and a signed provenance attestation tie the image to its source and build steps, which supports audits and rollbacks. The latest tag says nothing about origin. Renaming by date and embedding a password do not prove provenance, and the password would be a security problem.