

PRACTICE QUESTIONS

Linux Foundation / CNCF

CKS

Certified Kubernetes Security Specialist

SHARED BY [u/Steady-Jaguar-7156](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM Linux Foundation / CNCF CKS, Certified Kubernetes Security Specialist

Shared by [u/Steady-Jaguar-7156](#) 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. Before draining a worker node for kernel maintenance, an administrator wants to stop new pods from being scheduled there while leaving running pods alone. Which command does this?

- A `kubectl taint nodes <node> maintenance=true:NoExecute`
- B `kubectl cordon <node>`
- C `kubectl delete node <node>`
- D `kubectl label node <node> unschedulable=true`

Answer: B

`kubectl cordon` marks the node unschedulable so the scheduler skips it, and existing pods keep running until they are drained. A `NoExecute` taint evicts running pods that do not tolerate it, which goes further than the requirement. Deleting the node removes it from the cluster, and a label does not affect scheduling by itself.

2. In an `EncryptionConfiguration`, the provider that stores data without encryption and is used to read older plaintext Secrets is _____.

Answer: identity

The identity provider performs no encryption, so it is used either as the last fallback or to read Secrets that were written before encryption was enabled. The first provider in the list is used for new writes. Listing identity first would therefore leave new Secrets in plaintext.

3. Which `kubeadm` subcommand upgrades the control plane components on the first control plane node to a specified version?

- A `kubeadm init --upgrade`
- B `kubeadm join --upgrade`
- C `kubeadm upgrade apply`
- D `kubeadm reset --upgrade`

Answer: C

`kubeadm upgrade apply` with a target version upgrades the control plane static pods and cluster configuration on the first control plane node. Flags on `init`, `join` or `reset` do not perform an upgrade. `kubeadm init --upgrade` is tempting but is not a real upgrade path.

4. Granting cluster-admin to the system:authenticated group is a safe default for application teams.
- A True
 - B False

Answer: B (False)

The system:authenticated group contains every authenticated identity, so binding cluster-admin to it gives all of them full control. Least privilege requires narrow Roles per team. The statement is false.

5. Which two actions reduce the blast radius if one microservice is compromised? (Choose two.)
- A A default-deny NetworkPolicy with explicit allow rules for each needed flow
 - B Mounting the cluster-admin kubeconfig into the pod for convenience
 - C Running the container with privileged set to true
 - D Dropping unneeded Linux capabilities and running as a non-root user
 - E Giving every service the same ServiceAccount with broad permissions

Answer: A, D

Default-deny network policies stop a compromised pod from reaching services it has no reason to call, and dropped capabilities with a non-root user limit what the process can do on the host. Mounting an admin kubeconfig, running privileged and sharing a broad ServiceAccount each give the attacker more reach. These are the patterns to avoid.

6. Which capabilities setting best matches a restricted pod's default posture?
- A capabilities.add: [ALL] for full access so that the container can administer the whole host
 - B capabilities.add: [NET_ADMIN, SYS_ADMIN] for networking
 - C capabilities.drop: [ALL] with only the needed capabilities added back
 - D capabilities.drop: [NET_BIND_SERVICE] only

Answer: C

Dropping every capability and adding back only what the workload truly needs is the least-privilege pattern that the restricted profile expects. Adding all capabilities removes the isolation the profile is meant to keep. Dropping only one capability leaves most of the default set in place.

7. A pod spec sets hostPID: true. What is the main security concern?
- A The pod receives a public IP address automatically from the cloud provider's load balancer
 - B The pod gains write access to the etcd data directory
 - C The kubelet stops reporting the pod's status
 - D The container can see and signal processes running on the host

Answer: D

hostPID puts the container in the host's process namespace, so it can list and signal host processes and potentially escape isolation. A public IP is a cloud networking matter and not a result of this field. Access to etcd and kubelet reporting are not affected by hostPID.

8. The pod spec field that places the pod in the node's network namespace, and should normally be avoided, is _____.

Answer: hostNetwork

hostNetwork set to true lets the pod use the node's network stack and ports, which removes the isolation that per-pod networking gives. It is blocked by the restricted Pod Security level. Services and NetworkPolicies do not stop a pod from sharing the host network.

9. Which command signs a container image with Sigstore, using a key or a keyless identity?
- A trivy sign
 - B kubectI sign
 - C cosign sign
 - D docker trust sign

Answer: C

cosign sign attaches a signature to the image in the registry, using a local key or keyless signing with an OIDC identity. The other commands are either not real or belong to different signing systems. Verification then uses cosign verify against the same identity or key.

10. A Dockerfile's final stage runs as root and keeps compilers installed. What is the best change?
- A Add more RUN lines that install extra packages
 - B Replace every COPY with ADD for convenience
 - C Set an ENV variable named ROOT to 1 so that later build steps can detect root mode
 - D Use a multi-stage build with a minimal base and set USER to a non-root UID

Answer: D

A multi-stage build compiles in one stage and copies only the artifact into a minimal runtime image, and USER makes the process run as a non-root UID. Adding packages increases the attack surface. ADD and an environment variable do not change the privilege or contents of the final image.