

PRACTICE QUESTIONS

Linux Foundation / CNCF

CKAD

Certified Kubernetes Application Developer

SHARED BY [u/Sunny-Gecko-9532](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Linux Foundation / CNCF CKAD, Certified Kubernetes Application Developer

Shared by [u/Sunny-Gecko-9532](#) on aiexamcerts

10 practice questions for the Linux Foundation / CNCF CKAD exam, Certified Kubernetes Application Developer, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/linux-foundation-cncf/ckad. Spotted a mistake? Email support@aiexamcerts.com with the exam code CKAD and the question number.

1. A team wants to see CPU and memory consumption for each container in the pods of namespace shop. Which command gives this view once metrics-server is installed?
 - A `kubectl top pods --containers -n shop`
 - B `kubectl get events -n shop --watch` and read the resource usage columns
 - C `kubectl describe namespace shop`
 - D `kubectl auth can-i list pods -n shop`

Answer: A

`kubectl top` with the `--containers` flag reports resource usage per container, and it depends on metrics-server being present in the cluster. `kubectl get events` lists scheduling and lifecycle events, not resource metrics. The `describe namespace` and `auth can-i` commands do not report consumption at all.

2. An init container must finish successfully before the main containers in the same pod are started, and init containers run one after another in the order they are listed.
 - A True
 - B False

Answer: A (True)

Init containers run sequentially, each to successful completion, before any app containers start. A failed init container is retried according to the pod `restartPolicy`. This is useful for waiting on dependencies or preparing shared volumes.

3. How long does Kubernetes normally keep Event objects in the API?
 - A Indefinitely, until the cluster is deleted
 - B For a limited retention period set on the API server, typically about one hour
 - C Only for the duration of a single `kubectl` request, then discarded by the API client
 - D Until the next kubelet restart

Answer: B

Events are short-lived records, and the API server expires them after a configured retention period, commonly about one hour. Teams that need longer history export events to a logging system. Keeping them indefinitely is the tempting misconception, and it would bloat etcd.

4. A Service with clusterIP set to None is called a _____ Service, and DNS returns the pod addresses directly.

Answer: headless (also accepted: headless service)

A headless Service has no virtual IP, so cluster DNS returns the individual pod IPs for its selected pods. This is commonly used with StatefulSets to give each pod a stable identity. The answer is the term headless.

5. Which two statements about a Service of type ClusterIP are correct? (Choose two.)

- A It is reachable only from inside the cluster by default
- B It allocates a port on every node for external traffic
- C Its endpoints are the pods that match the Service selector and are Ready
- D It provides a public DNS name managed by the cloud provider
- E It requires an Ingress controller to function

Answer: A, C

A ClusterIP Service gets a virtual IP that only in-cluster clients can reach, and its endpoints are the Ready pods matching its selector. Allocating node ports is what NodePort does, and the cloud DNS name belongs to a LoadBalancer with external DNS. Ingress is an optional layer that is not needed for ClusterIP to work.

6. A namespace must reject any pod that runs as root or allows privilege escalation. Which mechanism enforces the Pod Security restricted profile for that namespace?

- A A namespace label pod-security.kubernetes.io/enforce set to restricted
- B A ResourceQuota that limits the number of pods allowed to run as root in the namespace
- C A LimitRange with a maxRoot default
- D A NetworkPolicy that blocks port 0

Answer: A

Pod Security Admission reads the pod-security.kubernetes.io/enforce label on a namespace and applies the chosen level such as baseline or restricted. ResourceQuota and LimitRange govern resource amounts, not security settings. NetworkPolicy controls traffic, so it cannot stop a pod from running as root.

7. A pod needs to call the Kubernetes API using a dedicated identity with least privilege, and the default token should not be mounted into unrelated pods. What is the best setup?
- A Bind cluster-admin to the default ServiceAccount in every namespace so that all workloads can reach the API without extra configuration
 - B Create a ServiceAccount, bind it with a Role, and set automountServiceAccountToken to false where the token is not needed
 - C Share the kubeconfig file from the admin user through a ConfigMap
 - D Run the pod with hostNetwork so it inherits the node identity

Answer: B

A dedicated ServiceAccount with a narrow RoleBinding follows least privilege, and disabling automatic token mounting removes the credential from pods that do not call the API. Binding cluster-admin to default widens access for every pod in the namespace. Sharing an admin kubeconfig or using hostNetwork both grant access that the workload does not need.

8. A Helm release that was upgraded can be returned to an earlier revision with helm rollback, because Helm keeps a history of release revisions.
- A True
 - B False

Answer: A (True)

Helm stores each release revision as a Secret in the release namespace, and helm rollback restores the manifests from a chosen earlier revision. Rollback does not reverse data changes made by the application. It is a standard way to recover from a bad chart upgrade.

9. After a rollout, the new pods stay in CrashLoopBackOff. Which single action best helps identify the cause from the pod's own state?
- A kubectl delete namespace shop and recreate the Deployment
 - B kubectl scale deployment to 10 replicas
 - C kubectl describe pod and read the Events and Last State sections
 - D kubectl label pods --all status=ok

Answer: C

kubectl describe pod shows the Last State with exit code and reason, the restart count, and recent events such as failed probes or image pull errors. Deleting the namespace destroys evidence and does not diagnose anything. Scaling or relabeling the pods does not reveal why the container exits.

10. Which container securityContext setting stops a setuid binary from gaining more privileges than its parent process?
- A readOnlyRootFilesystem: true
 - B runAsUser: 1000 with a fixed non-root group so files are owned by that identity
 - C allowPrivilegeEscalation: false
 - D privileged: false

Answer: C

Setting allowPrivilegeEscalation to false sets the no_new_privs flag, so setuid and setgid binaries cannot raise privileges. Running as UID 1000 changes the starting identity but does not block a setuid binary from elevating. Privileged set to false is the default and does not restrict escalation by itself.