Vendor: Linux Foundation

Exam Code: KCSA

Exam Name: Kubernetes and Cloud Native Security Associate

Version: DEMO

QUESTION 1
You are responsible for securing the kubelet component in a Kubernetes cluster. Which of the following statements about kubelet security is correct?

A. Kubelet runs as a privileged container by default.
B. Kubelet does not have any built-in security features.
C. Kubelet supports TLS authentication and encryption for secure communication with the API server.
D. Kubelet requires root access to interact with the host system.

Answer: C
Explanation:
The kubelet supports TLS for encrypting communication and authenticating both itself to the API server and the API server to itself, part of its built-in security mechanisms.

QUESTION 2
Which step would give an attacker a foothold in a cluster but no long-term persistence?

A. Modify Kubernetes objects stored within etcd.
B. Modify file on host filesystem.
C. Starting a process in a running container.
D. Create restarting container on host using Docker.

Answer: C
Explanation:
Starting a process inside an already-running container gives an attacker temporary access limited to the container's lifecycle, but does not survive a container restart or persist in any stored configuration, unlike modifying etcd, the host filesystem, or creating a new Docker container.

QUESTION 3
In a cluster that contains Nodes with multiple container runtimes installed, how can a Pod be configured to be created on a specific runtime?

A. By using a command-line flag when creating the Pod.
B. By modifying the Docker daemon configuration.
C. By setting the container runtime as an environment variable in the Pod.
D. By specifying the container runtime in the Pod's YAML file.

Answer: D
Explanation:
A Pod can specify its desired container runtime via the runtimeClassName field in its YAML spec, which references a predefined RuntimeClass object mapped to a specific container runtime.

QUESTION 4
Why does the default base64 encoding that Kubernetes applies to the contents of Secret resources provide inadequate protection?

A. Base64 encoding is vulnerable to brute-force attacks.
B. Base64 encoding relies on a shared key which can be easily compromised.
C. Base64 encoding does not encrypt the contents of the Secret, only obfuscates it.

D. Base64 encoding is not supported by all Secret Stores.

Answer: C
Explanation:
Base64 is a reversible encoding scheme, not an encryption method, so anyone who can read the Secret object can trivially decode its contents; it provides no confidentiality on its own.

QUESTION 5
Why might NetworkPolicy resources have no effect in a Kubernetes cluster?

A. NetworkPolicy resources are only enforced if the Kubernetes scheduler supports them.
B. NetworkPolicy resources are only enforced if the networking plugin supports them.
C. NetworkPolicy resources are only enforced for unprivileged Pods.
D. NetworkPolicy resources are only enforced if the user has the right RBAC permissions.

Answer: B
Explanation:
NetworkPolicy is an API object, but enforcement depends entirely on the CNI networking plugin implementing support for it; if the plugin doesn't support NetworkPolicy, the resources are created but have no actual effect.

QUESTION 6
Which security knowledge-base focuses specifically on offensive tools, techniques, and procedures?

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

Answer: A
Explanation:
MITRE ATT&CK is a curated knowledge base that catalogs real-world adversary tactics, techniques, and procedures (TTPs) used in attacks, distinguishing it from frameworks focused on defensive controls or web application vulnerabilities.

QUESTION 7
What does the 'cluster-admin' ClusterRole enable when used in a RoleBinding?

A. It gives full control over every resource in the role binding's namespace, not including the namespace object for isolation purposes.
B. It gives full control over every resource in the cluster and in all namespaces.
C. It gives full control over every resource in the role binding's namespace, including the namespace itself.
D. It allows read/write access to most resources in the role binding's namespace. This role does not allow write access to resource quota, to the namespace itself, and to EndpointSlices (or Endpoints).

Answer: B
Explanation:
The built-in cluster-admin ClusterRole grants superuser-level permissions across all resources in

all namespaces and cluster-scoped resources, regardless of whether it's bound via a ClusterRoleBinding or a namespaced RoleBinding - a RoleBinding referencing it grants full control within that namespace, but the role itself is inherently cluster-wide in scope and highly permissive.

QUESTION 8
Which of the following statements regarding a container run with privileged: true is correct?

A. A container run with privileged: true within a cluster can access all Secrets used within that cluster.
B. A container run with privileged: true within a Namespace can access all Secrets used within that Namespace.
C. A container run with privileged: true on a node can access all Secrets used on that node.
D. A container run with privileged: true has no additional access to Secrets than if it were run with privileged: false.

Answer: D
Explanation:
The privileged: true setting grants additional kernel capabilities and device access on the host, but it does not by itself grant any additional RBAC permissions to read Kubernetes Secret objects via the API - Secret access is governed separately by RBAC.

QUESTION 9
A Kubernetes cluster tenant can launch privileged pods in contravention of the restricted Pod Security Standard mandated for cluster tenants and enforced by the built-in PodSecurity 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 tampering with the namespace labels.
C. By deleting the PodSecurity admission controller deployment running in their namespace.
D. By using higher-level access credentials obtained reading secrets from another namespace.

Answer: B
Explanation:
Since Pod Security Admission enforcement is controlled entirely by labels on the namespace object, a tenant with full CRUD access to that namespace object can simply change or remove the enforcing label (e.g., from restricted to privileged), bypassing the intended policy.

QUESTION 10
In Kubernetes, what is Public Key Infrastructure used for?

A. To manage certificates and ensure secure communication in a Kubernetes cluster.
B. To automate the scaling of containers in a Kubernetes cluster.
C. To manage networking in a Kubernetes cluster.
D. To monitor and analyze performance metrics of a Kubernetes cluster.

Answer: A
Explanation:
Kubernetes relies on PKI to issue and manage X.509 certificates used for authenticating components (API server, kubelet, etcd) and encrypting communication between them via TLS.

QUESTION 11
As a Kubernetes and Cloud Native Security Associate, a user can set up audit logging in a cluster. What is the risk of logging every event at the full RequestResponse level?

A. No risk, as it provides the most comprehensive audit trail.
B. Increased storage requirements and potential impact on performance.
C. Improved security and easier incident investigation.
D. Reduced storage requirements and faster performance.

Answer: B
Explanation:
The RequestResponse audit level logs the complete request and response bodies for every event, which generates a large volume of data, significantly increasing storage needs and potentially degrading API server performance.

QUESTION 12
Given a standard Kubernetes cluster architecture comprising a single control plane node and three worker nodes, which of the following data flows crosses a trust boundary?

A. From kubelet to Container Runtime
B. From kubelet to API Server
C. From kubelet to Controller Manager
D. From API Server to Container Runtime

Answer: B
Explanation:
The kubelet on a worker node communicating with the API server on the control plane node crosses the trust boundary between the worker node's local components and the cluster's central control plane, requiring authentication and authorization.

QUESTION 13
To restrict the kubelet's rights to the Kubernetes API, what authorization mode should be set on the Kubernetes API server?

A. Node
B. AlwaysAllow
C. kubelet
D. Webhook

Answer: A
Explanation:
The Node authorization mode is specifically designed to authorize kubelet API requests, restricting each kubelet's permissions to only the resources (Pods, Nodes, Secrets, etc.) related to its own node.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**