Overview of Cloud Native Security

Cloud Provider and Infrastructure Security

Question 1

What is a primary security advantage of using a cloud provider's managed Kubernetes service?

- (A) Automatic scaling of CPU and memory resources.
- (B) Built-in integration with developer IDE tools.
- (C) Regular security patching and updates.
- (D) Unlimited data storage capacities.

Answer

(C) Regular security patching and updates.

Question 2

Which of the following is a recommended practice to secure Kubernetes infrastructure on a cloud provider?

- (A) Utilize public container images from unverified sources.
- (B) Regularly audit and apply Kubernetes security patches.
- (C) Enable anonymous access to Kubernetes API endpoints.
- (D) Run all pods with root privileges by default.

Answer

(B) Regularly audit and apply Kubernetes security patches.

Controls and Frameworks

Question 1

Which of the following is a primary purpose of security controls in a Kubernetes environment?

- (A) To automate deployment processes.
- (B) To manage network traffic between pods.
- (C) To ensure compliance with legal and regulatory requirements.
- (D) To provide user authentication and authorization.

Answer

(C) To ensure compliance with legal and regulatory requirements. **(D)** To provide user authentication and authorization.

Question 2
Which of the following are well-known frameworks used for security management in cloud-native environments?

- (A) OWASP
- (B) HIPAA
- (C) MITRE ATTACK
- (D) PCI DSS

Answer

(A) OWASP **(C)** MITRE ATTACK

The 4Cs of Cloud Native Security

Question 1
Which of the following is not one of the 4Cs of Cloud Native Security?

- (A) Code
- (B) Culture
- (C) Cloud
- (D) Cluster
- (E) Container

Answer

(B) Culture

Question 2
In the context of the 4Cs of Cloud Native Security, what does the “Cluster” focus on?

- (A) Securing interactions with external APIs.
- (B) Managing container runtime vulnerabilities.
- (C) Protecting the infrastructure that the applications run on.
- (D) Implementing continuous integration pipelines.

Answer

(C) Protecting the infrastructure that the applications run on.

Isolation Techniques

Question 1

What is a namespace in Kubernetes used for?

- (A) Installing additional software packages.
- (B) Isolating resources within a cluster.
- (C) Managing storage volumes.
- (D) Running scheduled tasks.

Answer

(B) Isolating resources within a cluster.

Question 2

Which of the following is a technique to provide isolation for applications running within Kubernetes?

- (A) Network policies.
- (B) Storage classes.
- (C) Replica sets.
- (D) Persistent volumes.

Answer

(A) Network policies.

Artifact Repository and Image Security

Question 1

Which of the following practices enhance container image security?

- (A) Using the latest version of images without verification.
- (B) Setting up image vulnerability scanning.
- (C) Allowing images from any public repository.
- (D) Identifying a trusted source for base images.

Answer

(B) Setting up image vulnerability scanning. **(D)** Identifying a trusted source for base images.

Question 2

What is a key benefit of using an artifact repository in a Kubernetes environment?

- (A) It allows for storing logs from the Kubernetes clusters.
- (B) It helps improve the security and integrity of deployment artifacts.
- (C) It provides automatic scaling of Kubernetes nodes.
- (D) It facilitates communication between microservices.

Answer

(B) It helps improve the security and integrity of deployment artifacts.

Workload and Application Code Security

Question 1

What is an effective method for securing application code in Kubernetes?

- (A) Using integrated development environments (IDEs).
- (B) Implementing code reviews and static analysis tools.
- (C) Running applications with root privileges.
- (D) Disabling network encryption.

Answer

(B) Implementing code reviews and static analysis tools.

Question 2

Which approach enhances workload security in Kubernetes clusters?

- (A) Deploying all applications in the default namespace.
- (B) Regularly applying security patches and updates to container images.
- (C) Using privileged containers for all applications.
- (D) Allowing unrestricted network access to pods.

Answer

(B) Regularly applying security patches and updates to container images.

Kubernetes Cluster Component Security

API Server

Question 1

Which of the following can be used to secure communication between the API Server and other Kubernetes components?

- (A) Network policies.
- (B) TLS certificates.
- (C) iptables configuration.
- (D) Role-based access control.

Answer

(B) TLS certificates

Question 2

What mechanism does the Kubernetes API Server use to authenticate user requests?

- (A) API Tokens.
- (B) Username and password.
- (C) SSH keys.
- (D) OAuth tokens.

Answer

(A) API Tokens (D) OAuth tokens

Controller Manager

Question 1

What function does the Kubernetes Controller Manager serve in maintaining desired state configurations?

- (A) It handles communication between Pods.
- (B) It manages routine tasks such as node health checks and replication.
- (C) It provides a web interface for monitoring cluster resources.
- (D) It allows direct configuration of the cluster's network policies.

Answer

(B) It manages routine tasks such as node health checks and replication.

Question 2

Which security measure is essential for protecting the Kubernetes Controller Manager?

- (A) Enabling Role-Based Access Control (RBAC) for API authorization.
- (B) Using a firewall to block all external traffic to nodes.
- (C) Running the Controller Manager on a separate physical server.
- (D) Disabling all logging mechanisms to minimize data exposure.

Answer

(A) Enabling Role-Based Access Control (RBAC) for API authorization.

Scheduler

Question 1

What is the primary function of the Kubernetes Scheduler in a cluster?

- (A) To manage network policies.
- (B) To control access to the Kubernetes API.
- (C) To assign Pods to nodes based on resource availability and constraints.
- (D) To store and manage container images.

Answer

(C) To assign Pods to nodes based on resource availability and constraints.

Question 2

Which of the following contributes to Kubernetes Scheduler's decision when determining node assignment for a Pod?

- (A) Node's label selectors that match the Pod's node affinity.
- (B) Network bandwidth usage across the nodes.

- (C) Pod's image pull policy.
- (D) Node's hardware specifications that match the Pod's requests.

Answer

(A) Node's label selectors that match the Pod's node affinity. **(D)** Node's hardware specifications that match the Pod's requests.

Kubelet

Question 1

Which of the following options helps enhance the security of the Kubelet on a Kubernetes node?

- (A) Running the Kubelet under a non-root user account.
- (B) Enabling the read-only port.
- (C) Configuring API Server authentication.
- (D) Using TLS for Kubelet API server communication.

Answer

(A) Running the Kubelet under a non-root user account. **(D)** Using TLS for Kubelet API server communication.

Question 2

What is a potential security risk if the Kubelet's anonymous-auth is enabled?

- (A) Unauthorized access to sensitive data on the node.
- (B) Increased latency in pod scheduling.
- (C) Debugging and troubleshooting becomes easier.
- (D) Enhancing cluster performance by offloading tasks to the node.

Answer

(A) Unauthorized access to sensitive data on the node.

Container Runtime

Question 1

What role does the container runtime play in Kubernetes?

- (A) It manages the cluster networking.

- (B) It schedules pods and other workloads.
- (C) It starts and stops containers on a node.
- (D) It provides persistent storage services.

Answer

(C) It starts and stops containers on a node.

Question 2
Which of the following is a common container runtime used in Kubernetes?

- (A) Syslog
- (B) CRI-O
- (C) HDFS
- (D) Nagios

Answer

(B) CRI-O

KubeProxy

Question 1:
What is the primary role of KubeProxy in a Kubernetes cluster?

- (A) To manage network storage volumes.
- (B) To schedule pod placement on nodes.
- (C) To manage network access for services/interfaces.
- (D) To deploy applications automatically.

Answer

(C) To manage network access for services/interfaces.

Question 2:
Which of the following is a key security concern related to KubeProxy?

- (A) Ensuring communication encryption between nodes.
- (B) Controlling access to the Kubernetes API server.
- (C) Securing service accounts used by proxy services.
- (D) Managing access controls for network policies.

Answer

(A) Ensuring communication encryption between nodes.

Pod

Question 1

Which of the following is a primary security concern for pods in a Kubernetes cluster?

- (A) Version compatibility with the operating system.
- (B) Network latency between nodes.
- (C) Container vulnerabilities and privilege escalation.
- (D) The graphical user interface performance.

Answer

(C) Container vulnerabilities and privilege escalation.

Question 2

How can you implement security controls to restrict the actions of pods in a Kubernetes cluster?

- (A) By using Network Policies to control pod communication.
- (B) By configuring persistent volume claims.
- (C) By setting high availability for the scheduler.
- (D) By encrypting the kube-proxy logs.

Answer

(A) By using Network Policies to control pod communication.

Etcd

Question 1

Which of the following best describes the role of etcd in a Kubernetes cluster?

- (A) It serves as the user interface for managing containers.
- (B) It is a database that stores the cluster configuration and state.
- (C) It acts as the scheduler for deploying resources in a cluster.
- (D) It functions as the network load balancer.

Answer

(B) It is a database that stores the cluster configuration and state.

Question 2
How can you secure etcd data to prevent unauthorized access in a Kubernetes cluster?

- (A) By deploying etcd on the same node as the kubelet.
- (B) By enabling HTTP communication between Kubernetes components and etcd.
- (C) By configuring etcd to use TLS encryption for data in transit.
- (D) By restricting etcd access to only the master nodes.

Answer

(C) By configuring etcd to use TLS encryption for data in transit. **(D)** By restricting etcd access to only the master nodes.

Container Networking

Question 1
When securing container networking in a Kubernetes cluster, which of the following are important considerations?

- (A) Network policies for traffic control.
- (B) Container runtime security.
- (C) DNS configuration for resolution.
- (D) Authentication and authorization controls.

Answer

(A) Network policies for traffic control. **(D)** Authentication and authorization controls.

Question 2
Which Kubernetes resource is specifically used to manage network traffic into and out of a Pod in a cluster?

- (A) ConfigMap
- (B) NetworkPolicy
- (C) RoleBinding
- (D) Volume

Answer

(B) NetworkPolicy

Client Security

Question 1

What is the primary protocol used by clients to communicate securely with the Kubernetes API server?

- (A) FTP
- (B) HTTP
- (C) HTTPS
- (D) SSH

Answer

(C) HTTPS

Question 2

Which of the following methods can be used to authenticate API requests to the Kubernetes API server?

- (A) Username and password
- (B) Client certificates
- (C) Bearer tokens
- (D) All of the above

Answer

(D) All of the above

Storage

Question 1

Which of the following is a primary security concern when using persistent storage in Kubernetes?

- (A) Storage performance degradation.
- (B) Unauthorized access to sensitive data.
- (C) Lack of storage capacity.
- (D) High storage costs.

Answer

(B) Unauthorized access to sensitive data.

Question 2
How can Kubernetes Secrets improve the security of storage configurations within a cluster?

- (A) By enhancing data encryption.
- (B) By providing a mechanism to store sensitive information, like passwords, in a secure manner.
- (C) By increasing storage space.
- (D) By improving the speed of data retrieval.

Answer

(B) By providing a mechanism to store sensitive information, like passwords, in a secure manner.

Kubernetes Security Fundamentals

Pod Security Standards

Question 1 What is the purpose of Kubernetes Pod Security Standards?

- (A) To restrict the version of Kubernetes that can be used.
- (B) To provide guidelines for the isolation of Kubernetes workloads to protect the system from malicious pods.
- (C) To ensure that only certain container registries can be used.
- (D) To specify which Kubernetes resources can be accessed by nodes.

Answer

(B) To provide guidelines for the isolation of Kubernetes workloads to protect the system from malicious pods.

Question 2 Which of the following is a valid enforcement level in Kubernetes Pod Security Standards?

- (A) Restricted
- (B) Basic
- (C) Closed
- (D) Enforced

Answer

(A) Restricted

Pod Security Admissions

Question 1

Which of the following accurately describes the role of Pod Security Admissions in Kubernetes?

- (A) They are responsible for scheduling pods to appropriate nodes.
- (B) They enforce policies that dictate what pods can run and how they can operate within a cluster.
- (C) They manage the lifecycle of Kubernetes nodes.
- (D) They handle communication between pods.

Answer

(B) They enforce policies that dictate what pods can run and how they can operate within a cluster.

Question 2

What is a primary benefit of using Pod Security Admissions in a Kubernetes environment?

- (A) They improve the efficiency of networking between pods.
- (B) They ensure compliance with organizational security policies by controlling pod-level access and operations.
- (C) They facilitate the dynamic scaling of pods based on resource usage.
- (D) They provide automatic updates to the Kubernetes version used in the cluster.

Answer

(B) They ensure compliance with organizational security policies by controlling pod-level access and operations.

Authentication

Question 1

What is the primary purpose of a Kubernetes ServiceAccount?

- (A) To monitor network traffic.
- (B) To authenticate nodes to the API server.

- (C) To grant permissions to applications running in a pod.
- (D) To authenticate external users to the cluster.

Answer

(C) To grant permissions to applications running in a pod.

Question 2

Which authentication method allows Kubernetes to integrate with an external identity provider?

- (A) Client certificates.
- (B) Service Accounts.
- (C) Integrating with OIDC (OpenID Connect).
- (D) Static Bearer Token.

Answer

(C) Integrating with OIDC (OpenID Connect).

Authorization

Question 1

Which of the following Kubernetes components is responsible for making authorization decisions?
- (A) API Server - (B) Scheduler - (C) Controller Manager - (D) Kubelet

Answer

(A) API Server

Question 2

In Kubernetes, which of these is a role-based access control (RBAC) component?
- (A) ClusterRole - (B) PodSecurityPolicy - (C) ServiceAccount - (D) Namespace

Answer

(A) ClusterRole

Secrets

Question 1

What is the primary purpose of Kubernetes Secrets?

- (A) To store sensitive information such as passwords, tokens, and keys.
- (B) To monitor the health of Kubernetes nodes.
- (C) To provide high availability for pods.
- (D) To configure network policies for namespaces.

Answer

(A) To store sensitive information such as passwords, tokens, and keys.

Question 2

How can Kubernetes Secrets enhance security compared to storing sensitive data directly in environment variables?

- (A) They offer encryption at rest.
- (B) They provide automatic backup of sensitive data.
- (C) They allow granular access controls to sensitive information.
- (D) They integrate with third-party identity providers.

Answer

(A) They offer encryption at rest. **(C)** They allow granular access controls to sensitive information.

Isolation and Segmentation

Question 1

Which Kubernetes feature can be used to limit the scope and traffic within certain namespaces to enhance isolation?

- (A) Network Policies
- (B) ConfigMaps
- (C) Persistent Volumes
- (D) Node Selectors

Answer

(A) Network Policies

Question 2

What is the primary benefit of using Kubernetes namespaces for isolation and segmentation in a cluster?

- (A) They provide high availability for applications.

- (B) They allow you to create new API objects.
- (C) They enable resource and access constraints within a cluster.
- (D) They speed up pod deployment.

Answer

(C) They enable resource and access constraints within a cluster.

Audit Logging

Question 1

Which Kubernetes component is primarily responsible for storing audit logs?

- (A) kube-scheduler
- (B) etcd
- (C) kube-apiserver
- (D) kube-controller-manager

Answer

(C) kube-apiserver

Question 2

What is the main purpose of Kubernetes audit logs?

- (A) To monitor network traffic
- (B) To track changes in resource usage over time
- (C) To maintain a record of the sequence of activities affecting the cluster
- (D) To automatically scale the deployment of pods based on user demand

Answer

(C) To maintain a record of the sequence of activities affecting the cluster

Network Policy

Question 1
How does a Network Policy in Kubernetes help enhance security within a cluster?

- (A) By restricting network traffic to and from pods based on label selectors.
- (B) By encrypting all network traffic.
- (C) By automatically updating DNS records.
- (D) By providing a default deny-all rule for cluster communication.

Answer

(A) By restricting network traffic to and from pods based on label selectors.

Question 2
Which of the following is true regarding Kubernetes Network Policies?

- (A) Network Policies can be used to control traffic between different namespaces.
- (B) Network Policies are enforced by default in all Kubernetes clusters.
- (C) Network Policies replace the need for firewalls.
- (D) Network Policies can specify deny rules but not allow rules.

Answer

(A) Network Policies can be used to control traffic between different namespaces.

Kubernetes Threat Model

Kubernetes Trust Boundaries and Data Flow

Question 1
In the context of Kubernetes, what are trust boundaries primarily concerned with?

- (A) The physical separation of Kubernetes nodes.
- (B) The demarcation points where security controls are required to restrict access and ensure data integrity.
- (C) Defining the API schema for different Kubernetes objects.
- (D) The configuration management of Kubernetes services.

Answer

(B) The demarcation points where security controls are required to restrict access and ensure data integrity.

Question 2
Which of the following components might be involved in the data flow across trust boundaries in a Kubernetes environment?

- (A) Service Accounts.
- (B) Pods and Containers.
- (C) Kubernetes Control Plane.
- (D) Network Policies.

Answer

(B) Pods and Containers. **(D)** Network Policies.

Persistence

Question 1
Which of the following is a method used to establish persistence in a Kubernetes cluster?

- (A) Using a PersistentVolume to store critical data.
- (B) Implementing network policies.
- (C) Running applications in a Kubernetes Job.
- (D) Configuring Role-Based Access Control (RBAC).

Answer

(A) Using a PersistentVolume to store critical data.

Question 2
What role can the use of ConfigMaps play in persistence within a Kubernetes threat model?

- (A) ConfigMaps provide a mechanism to store sensitive information securely.
- (B) They allow attackers to store malicious scripts for persistent backdoors.
- (C) They ensure that application configurations persist across pod restarts.
- (D) ConfigMaps enforce strict network security policies.

Answer

(C) They ensure that application configurations persist across pod restarts.

Denial of Service

Question 1

Which of the following can be a potential Denial of Service (DoS) threat in a Kubernetes environment?

- (A) Misconfigured Resource Quotas
- (B) Properly configured Network Policies
- (C) Single user access for all deployments
- (D) Efficient load balancing

Answer

(A) Misconfigured Resource Quotas **(C)** Single user access for all deployments

Question 2

How can limiting the number of concurrent connections help mitigate Denial of Service attacks in Kubernetes?

- (A) It improves network throughput.
- (B) It prevents any single user from monopolizing resources.
- (C) It allows easier scaling of resources.
- (D) It reduces resource utilization.

Answer

(B) It prevents any single user from monopolizing resources.

Malicious Code Execution and Compromised Applications in Containers

Question 1

What is a common method attackers use to execute malicious code within a Kubernetes cluster?

- (A) Utilizing Kubernetes API server to directly execute commands.
- (B) Exploiting vulnerabilities in container images to insert malicious scripts.
- (C) Leveraging Kubernetes Control Loop to overwrite container definitions.
- (D) Increasing resource limits to cause a denial of service.

Answer

(B) Exploiting vulnerabilities in container images to insert malicious scripts.

Question 2
How can compromised applications in containers be detected within a Kubernetes environment?

- (A) Monitoring network traffic for suspicious patterns.
- (B) Adjusting all nodes to non-root user restrictions.
- (C) Using Kubernetes API server logs to track service account activity.
- (D) Implementing regular Kubernetes version upgrades.

Answer

(A) Monitoring network traffic for suspicious patterns. **(C)** Using Kubernetes API server logs to track service account activity.

Attacker on the Network

Question 1
What could an attacker on the network potentially exploit in a Kubernetes cluster to gain unauthorized access?

- (A) Insecure etcd endpoints.
- (B) Properly configured Network Policies.
- (C) Unsecured API server.
- (D) Encrypted communication channels.

Answer

(A) Insecure etcd endpoints. **(C)** Unsecured API server.

Question 2
Which of the following practices helps prevent network attacks in a Kubernetes environment?

- (A) Disabling RBAC.
- (B) Implementing network segmentation and isolation.
- (C) Using unverified container images.
- (D) Encrypting traffic between components.

Answer

(B) Implementing network segmentation and isolation. **(D)** Encrypting traffic between components.

Access to Sensitive Data

Question 1

Which of the following practices improves the protection of sensitive data in Kubernetes?

- (A) Using ConfigMaps to store all confidential data.
- (B) Encrypting secrets at rest in etcd.
- (C) Allowing all users access to secrets.
- (D) Storing secrets directly in environment variables.

Answer

(B) Encrypting secrets at rest in etcd.

Question 2

What is a best practice to control access to sensitive data in a Kubernetes cluster?

- (A) Assigning secrets viewing permissions to all pods by default.
- (B) Using Role-Based Access Control (RBAC) to limit access to secrets.
- (C) Storing sensitive information in persistent volumes.
- (D) Disabling audit logs to prevent sensitive information leakage.

Answer

(B) Using Role-Based Access Control (RBAC) to limit access to secrets.

Privilege Escalation

Question 1

In the context of Kubernetes, which of the following strategies can help prevent privilege escalation?

- (A) Use RBAC (Role-Based Access Control) to limit permissions.
- (B) Allow pods to run as root by default.
- (C) Grant cluster-admin rights to every user.
- (D) Disable the use of service accounts in pods.

Answer

(A) Use RBAC (Role-Based Access Control) to limit permissions.

Question 2

Which of the following practices can lead to privilege escalation in a Kubernetes cluster?

- (A) Creating wide-open RBAC roles with wildcard permissions.
- (B) Enforcing strict Network Policies for pod communication.
- (C) Running each pod in its own namespace with restricted roles.
- (D) Limiting the use of hostPath in Pod specifications.

Answer

(A) Creating wide-open RBAC roles with wildcard permissions.

Platform Security

Supply Chain Security

Question 1

Which of the following practices is essential for ensuring supply chain security in Kubernetes?

- (A) Keeping software dependencies up-to-date with the latest versions.
- (B) Reducing CPU and memory limits for containers.
- (C) Utilizing a reverse proxy for incoming traffic.
- (D) Restricting network access using NetworkPolicies.

Answer

(A) Keeping software dependencies up-to-date with the latest versions.

Question 2

What role does a Software Bill of Materials (SBOM) play in Kubernetes supply chain security?

- (A) It automates the creation of Kubernetes Pods on demand.
- (B) It provides a detailed list of all software components used within an application.
- (C) It automatically scales Kubernetes nodes based on CPU usage.
- (D) It manages user access and permissions within a Kubernetes cluster.

Answer

(B) It provides a detailed list of all software components used within an application.

Image Repository

Question 1

Which command is used to authenticate with a private Docker registry in Kubernetes?

- (A) `kubectl create secret docker-registry`
- (B) `kubectl apply -f`
- (C) `kubectl set image`
- (D) `kubectl rollout restart`

Answer

(A) ‘kubectl create secret docker-registry‘

Image Repository

Question 2

What is the purpose of imagePullSecrets in Kubernetes?

- (A) To store Docker images securely in a Kubernetes deployment.
- (B) To automate rolling updates for Kubernetes pods.
- (C) To authenticate with private container registries.
- (D) To mount volumes within a Kubernetes pod.

Answer

(C) To authenticate with private container registries.

Observability

Question 1

Which component is primarily responsible for collecting metrics from Kubernetes nodes?

- (A) Kube-scheduler
- (B) Kube-proxy
- (C) Kubelet

- (D) Etcd

Answer

(C) Kubelet

Question 2

What tool is commonly used in Kubernetes to visualize and monitor cluster metrics?

- (A) Prometheus
- (B) Helm
- (C) Minikube
- (D) Kubectl

Answer

(A) Prometheus

Service Mesh

Question 1

What is a primary benefit of using a service mesh in a Kubernetes environment?

- (A) It enhances the speed of the physical network.
- (B) It provides automatic load balancing for HTTP, gRPC, TCP, and more.
- (C) It reduces the number of services needed in the environment.
- (D) It increases the RAM available to each container.

Answer

(B) It provides automatic load balancing for HTTP, gRPC, TCP, and more.

Question 2

Which of the following is a common feature of service mesh solutions?

- (A) Autoscaling of Kubernetes nodes.
- (B) End-to-end encryption of data in transit between services.
- (C) Creation of persistent volumes in the cluster.
- (D) Directly managing container lifecycle inside pods.

Answer

(B) End-to-end encryption of data in transit between services.

PKI

Question 1

In the context of Kubernetes, what does a Public Key Infrastructure (PKI) primarily provide?

- (A) Toolkit for developing cloud-native applications.
- (B) Authentication and secure communication.
- (C) Container runtime environment.
- (D) Database management system.

Answer

(B) Authentication and secure communication.

Question 2

Which component in the Kubernetes control plane is responsible for generating and signing certificates used in PKI?

- (A) kubelet
- (B) kube-scheduler
- (C) kube-apiserver
- (D) kube-controller-manager

Answer

(D) kube-controller-manager

Connectivity

Question 1

Which component in Kubernetes is responsible for assigning IP addresses to pods to facilitate connectivity?

- (A) Kube-scheduler.
- (B) Kube-controller-manager.
- (C) Kube-proxy.
- (D) Kubelet.
- (E) CNI plugin.

Answer

(E) CNI plugin

Question 2
What role does the `kube-proxy` play in Kubernetes networking?

- (A) It schedules pods to run on nodes.
- (B) It maintains network rules on nodes to allow communication to your Pods.
- (C) It assigns IP addresses to pods.
- (D) It manages service accounts and roles.
- (E) It monitors the health of pods and nodes.

Answer

(B) It maintains network rules on nodes to allow communication to your Pods.

Admission Control

Question 1
Which of the following statements accurately describe the purpose of admission controllers in Kubernetes?

- (A) They automatically update the Kubernetes control plane components.
- (B) They intercept requests to the Kubernetes API Server before they are persisted in etcd.
- (C) They automatically scale the pods in a Kubernetes cluster.
- (D) They enforce certain policies on the requests to create or modify resources.

Answer

(B) They intercept requests to the Kubernetes API Server before they are persisted in etcd. **(D)** They enforce certain policies on the requests to create or modify resources.

Question 2
What are some common use cases for admission controllers in a Kubernetes environment?

- (A) To provide detailed logging of all Kubernetes API requests.
- (B) To ensure that certain security policies are enforced on resources before they are created.
- (C) To modify the content of resources submitted to the API before they are processed.
- (D) To replace the kube-scheduler in scheduling decisions.

Answer

(B) To ensure that certain security policies are enforced on resources before they are created.
(C) To modify the content of resources submitted to the API before they are processed.

Compliance and Security Frameworks

Compliance Frameworks

Question 1

Which of the following is a compliance framework specifically focused on protecting personal data and privacy in the European Union?

- (A) SOC 2
- (B) PCI DSS
- (C) HIPAA
- (D) GDPR

Answer

(D) GDPR

Question 2

Which compliance framework focuses on ensuring that organizations follow best practices for information security management?

- (A) ISO/IEC 27001
- (B) GDPR
- (C) CCPA
- (D) FISMA

Answer

(A) ISO/IEC 27001

Threat Modelling Frameworks

Question 1

Which of the following is a primary benefit of using threat modeling frameworks in Kubernetes environments?

- (A) Improved application performance.
- (B) Early identification of potential security threats.
- (C) Easier database management.
- (D) Faster application deployment.

Answer

(B) Early identification of potential security threats.

Question 2
What is a common characteristic of security frameworks like STRIDE and PASTA when applied to Kubernetes?

- (A) They focus only on network security.
- (B) They integrate seamlessly with all programming languages.
- (C) They help identify and address potential security threats throughout the development lifecycle.
- (D) They are exclusively designed for Windows environments.

Answer

(C) They help identify and address potential security threats throughout the development lifecycle.

Supply Chain Compliance

Question 1
What is a key benefit of implementing supply chain security compliance in Kubernetes environments?

- (A) It increases application performance significantly.
- (B) It ensures that container images are built from trusted sources.
- (C) It simplifies the Kubernetes deployment process by removing unnecessary steps.
- (D) It allows developers to bypass cluster security protocols more easily.

Answer

(B) It ensures that container images are built from trusted sources.

Question 2
Which of the following practices is essential for maintaining Kubernetes supply chain compliance?

- (A) Using unverified third-party container images for deployment.
- (B) Regularly scanning container images for vulnerabilities and compliance.
- (C) Allowing unrestricted access to Kubernetes cluster resources.
- (D) Disabling logging to enhance system performance.

Answer

(B) Regularly scanning container images for vulnerabilities and compliance.

Automation and Tooling

Question 1:
Which of the following Kubernetes tools can be used to automate compliance checks and enforce security policies within clusters?

- (A) Kubeadm
- (B) Kubesec
- (C) Kube-bench
- (D) Helm

Answer

(B) Kubesec **(C)** Kube-bench

Question 2:
Which of the following is a commonly used tool that integrates with Kubernetes to automate security testing for vulnerabilities in container images?

- (A) Istio
- (B) Falco
- (C) Aqua Security
- (D) ArgoCD

Answer

(C) Aqua Security

