Google Cloud

Partner Certification Academy


# Professional Cloud Developer

v2309

## Quiz questions*

## Container Best Practices & Security Command Center

** These are for practice only and are not actual exam questions*

Question: What is the primary purpose of Container Threat Detection in Google Cloud's Security Command Center?

- A. To monitor network traffic for suspicious activity.
- B. To continuously monitor the state of Container-Optimized OS node images and detect runtime attacks.
- C. To scan container images for vulnerabilities.
- D. To provide firewall rules for containerized applications.

Question: Which of the following is NOT a detection capability of Container Threat Detection?

- A. Detecting suspicious binaries and libraries.
- B. Using natural language processing (NLP) to detect malicious bash scripts.
- C. Monitoring network traffic for anomalies.
- D. Observing malicious URLs in the argument list of a running process.

Question: What happens when the detector service in Container Threat Detection identifies an incident?

- A. The incident is stored in a persistent database for future analysis.
- B. The incident is written as a finding in Security Command Center and optionally to Cloud Logging.
- C. An email notification is sent to the Google Cloud project owner.
- D. The compromised container is automatically shut down.

Question: What is the primary function of Binary Authorization in Google Cloud?

- A. To encrypt container images for secure storage.
- B. To ensure only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run.
- C. To compress container images for faster deployment.
- D. To monitor container runtime for potential threats.

Question: How does Binary Authorization help in enhancing container security?

- A. By scanning container images for malware.
- B. By enforcing runtime policies on containers.
- C. By ensuring only verified containers are admitted into the environment and remain trusted during runtime.
- D. By providing firewall rules for containerized applications.

Question: Which feature of Binary Authorization allows users to test policy changes without enforcing them?

- A. Cloud KMS support
- B. Dry run support
- C. Breakglass support
- D. Cloud Security Command Center integration

Question: Which of the following is a recommended practice for handling logs in containers?

- A. Write logs to a specific file and handle log rotation manually.
- B. Forward logs to a remote server for centralization.
- C. Write logs to stdout and stderr.
- D. Implement advanced logging mechanisms within the application.

Question: What is the primary purpose of logging directly in JSON format with different fields?

- A. To beautify the logs for better readability.
- B. To reduce the size of the log files.
- C. To search logs more effectively based on fields.
- D. To encrypt the logs for security purposes.

Question: Which of the following is NOT a characteristic of containers as per best practices?

- A. Stateless
- B. Immutable
- C. Updatable
- D. Configurable externally

Question: Why should you avoid using privileged containers?

- A. They consume more resources.
- B. They have access to all devices of the host machine, bypassing security features.
- C. They are not supported by Kubernetes.
- D. They are slower than non-privileged containers.

Question: What is the primary difference between black-box monitoring and white-box monitoring?

- A. Black-box monitoring is for non-containerized applications, while white-box is for containerized applications.
- B. Black-box monitoring examines the application from the outside, while white-box monitoring examines it with privileged access.
- C. Black-box monitoring is less secure than white-box monitoring.
- D. White-box monitoring is only possible with Prometheus.

Question: Which of the following is a popular option in the Kubernetes community for white-box monitoring?

- A. Cloud Logging
- B. Fluent Bit
- C. Prometheus
- D. Cloud Storage

Question: What does it mean for a container to be stateless?

- A. It can be updated during its lifecycle.
- B. It stores persistent data inside the container.
- C. It can be shut down and destroyed without fear of data loss.
- D. It requires manual configuration for each deployment.

Question: What is the primary purpose of using the sidecar pattern for monitoring in containerized applications?

- A. To reduce the resource consumption of the main application.
- B. To export metrics in the right format for standardized monitoring.
- C. To provide a backup for the main application in case of failures.
- D. To handle network traffic and load balancing.

Question: In Kubernetes, what does the /healthz HTTP endpoint indicate when it receives a request?

- A. The application's current version.
- B. The application's readiness to receive traffic.
- C. The application's health status.
- D. The application's memory consumption.

Question: Why is it recommended to avoid running processes as root inside containers?

- A. To increase the performance of the container.
- B. To prevent potential vulnerabilities that could give root access to the host machine.
- C. To ensure compatibility with all operating systems.
- D. To reduce the size of the container image.

Question: What is the potential issue with using the "latest" tag for Docker images in Kubernetes manifests?

- A. It always pulls the oldest version of the image.
- B. It can lead to unpredictable and non-reproducible builds.
- C. It increases the deployment time.

- D. It is not supported by Kubernetes.

Question: Why is it essential to properly tag container images?

- A. To ensure the image is publicly accessible.
- B. To identify different versions of the same application.
- C. To increase the size of the container image.
- D. To automatically deploy the image to production.

Question: Which of the following is NOT a recommended practice when tagging container images?

- A. Using the latest tag for all images.
- B. Using semantic versioning for tags.
- C. Including the Git commit hash in the tag.
- D. Using distinct tags for development and production images.

Question: What advantage does including the Git commit hash in the container image tag provide?

- A. It ensures the image is built from the latest code.
- B. It provides a direct link between the container image and the source code version.
- C. It reduces the size of the container image.
- D. It automatically updates the container image in production.

# Answers to Quiz questions

## **Container Best Practices & Security Command Center**

Question: What is the primary purpose of Container Threat Detection in Google Cloud's Security Command Center?

- A. To monitor network traffic for suspicious activity.
- B. To continuously monitor the state of Container-Optimized OS node images and detect runtime attacks.
- C. To scan container images for vulnerabilities.
- D. To provide firewall rules for containerized applications.

Correct Answer: B. To continuously monitor the state of Container-Optimized OS node images and detect runtime attacks.

Explanation: Container Threat Detection is designed to continuously monitor the state of Container-Optimized OS node images. It evaluates all changes and remote access attempts to detect potential runtime attacks in near-real time. Resource: Container Threat Detection conceptual overview | Security Command Center - Google Cloud

Question: Which of the following is NOT a detection capability of Container Threat Detection?

- A. Detecting suspicious binaries and libraries.
- B. Using natural language processing (NLP) to detect malicious bash scripts.
- C. Monitoring network traffic for anomalies.
- D. Observing malicious URLs in the argument list of a running process.

Correct Answer: C. Monitoring network traffic for anomalies.

Explanation: While Container Threat Detection can detect suspicious binaries, libraries, and use NLP to identify malicious bash scripts, it does not monitor network traffic for anomalies.

Resource: Container Threat Detection conceptual overview | Security Command Center - Google Cloud

Question: What happens when the detector service in Container Threat Detection identifies an incident?

- A. The incident is stored in a persistent database for future analysis.
- B. The incident is written as a finding in Security Command Center and optionally to Cloud Logging.
- C. An email notification is sent to the Google Cloud project owner.
- D. The compromised container is automatically shut down.

Correct Answer: B. The incident is written as a finding in Security Command Center and optionally to Cloud Logging.

Explanation: If the detector service identifies an incident, it is recorded as a finding in the Security Command Center. Additionally, there's an option to log the incident in Cloud Logging.
Resource: Container Threat Detection conceptual overview | Security Command Center - Google Cloud

Question: What is the primary function of Binary Authorization in Google Cloud?

- A. To encrypt container images for secure storage.
- B. To ensure only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run.
- C. To compress container images for faster deployment.
- D. To monitor container runtime for potential threats.

Correct Answer: B. To ensure only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run.

Explanation: Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on GKE or Cloud Run. It allows users to require images to be signed by trusted authorities during development and enforces signature validation during deployment.
Resource: Binary Authorization | Google Cloud

Question: How does Binary Authorization help in enhancing container security?

- A. By scanning container images for malware.
- B. By enforcing runtime policies on containers.
- C. By ensuring only verified containers are admitted into the environment and remain trusted during runtime.
- D. By providing firewall rules for containerized applications.

Correct Answer: C. By ensuring only verified containers are admitted into the environment and remain trusted during runtime.

Explanation: Binary Authorization helps DevOps teams implement a proactive container security posture by ensuring only verified containers are admitted into the environment and that they remain trusted during runtime.
Resource: Binary Authorization | Google Cloud

Question: Which feature of Binary Authorization allows users to test policy changes without enforcing them?

- A. Cloud KMS support
- B. Dry run support
- C. Breakglass support
- D. Cloud Security Command Center integration

Correct Answer: B. Dry run support

Explanation: Dry run support in Binary Authorization allows users to test changes to their policy in non-enforcing mode before deploying. This helps in understanding the impact of policy changes without actually blocking deployments.
Resource: Binary Authorization | Google Cloud

Question: Which of the following is a recommended practice for handling logs in containers?

- A. Write logs to a specific file and handle log rotation manually.
- B. Forward logs to a remote server for centralization.
- C. Write logs to stdout and stderr.
- D. Implement advanced logging mechanisms within the application.

Correct Answer: C. Write logs to stdout and stderr.

Explanation: Containers offer an easy and standardized way to handle logs because you can write them to stdout and stderr. Docker captures these log lines and allows you to access them using the docker logs command. This eliminates the need for advanced logging mechanisms within the application.
Resource: Best practices for operating containers

Question: What is the primary purpose of logging directly in JSON format with different fields?

- A. To beautify the logs for better readability.
- B. To reduce the size of the log files.
- C. To search logs more effectively based on fields.
- D. To encrypt the logs for security purposes.

Correct Answer: C. To search logs more effectively based on fields.

Explanation: Logging directly in JSON format with different fields allows for more effective searching of logs based on those fields. This structured format makes it easier to filter and analyze logs.
Resource: Best practices for operating containers

Question: Which of the following is NOT a characteristic of containers as per best practices?

- A. Stateless
- B. Immutable
- C. Updatable
- D. Configurable externally

Correct Answer: C. Updatable

Explanation: Containers are designed to be stateless and immutable. They are not meant to be updated during their life. Instead, if updates or patches are needed, a new image should be built and redeployed.
Resource: Best practices for operating containers

Question: Why should you avoid using privileged containers?

- A. They consume more resources.
- B. They have access to all devices of the host machine, bypassing security features.
- C. They are not supported by Kubernetes.
- D. They are slower than non-privileged containers.

Correct Answer: B. They have access to all devices of the host machine, bypassing security features.

Explanation: Privileged containers have access to all the devices of the host machine, which means they can bypass almost all the security features of containers. This poses a security risk.

Resource: Best practices for operating containers

Question: What is the primary difference between black-box monitoring and white-box monitoring?

- A. Black-box monitoring is for non-containerized applications, while white-box is for containerized applications.
- B. Black-box monitoring examines the application from the outside, while white-box monitoring examines it with privileged access.
- C. Black-box monitoring is less secure than white-box monitoring.
- D. White-box monitoring is only possible with Prometheus.

Correct Answer: B. Black-box monitoring examines the application from the outside, while white-box monitoring examines it with privileged access.

Explanation: Black-box monitoring refers to examining the application as if you were an end user, from the outside. White-box monitoring, on the other hand, examines the application with some kind of privileged access, gathering metrics that an end user cannot view.
Resource: Best practices for operating containers

Question: Which of the following is a popular option in the Kubernetes community for white-box monitoring?

- A. Cloud Logging
- B. Fluent Bit
- C. Prometheus
- D. Cloud Storage

Correct Answer: C. Prometheus

Explanation: Prometheus is a popular system in the Kubernetes community for white-box monitoring. It can automatically discover the pods it needs to monitor and expects a specific format for the metrics it scrapes.

Resource: Best practices for operating containers

Question: What does it mean for a container to be stateless?

- A. It can be updated during its lifecycle.
- B. It stores persistent data inside the container.
- C. It can be shut down and destroyed without fear of data loss.
- D. It requires manual configuration for each deployment.

Correct Answer: C. It can be shut down and destroyed without fear of data loss.

Explanation: Being stateless means that any state (persistent data) is stored outside of the container. This ensures that the container can be cleanly shut down and destroyed at any time without the fear of losing data.
Resource: Best practices for operating containers

Question: What is the primary purpose of using the sidecar pattern for monitoring in containerized applications?

- A. To reduce the resource consumption of the main application.
- B. To export metrics in the right format for standardized monitoring.
- C. To provide a backup for the main application in case of failures.
- D. To handle network traffic and load balancing.

Correct Answer: B. To export metrics in the right format for standardized monitoring.

Explanation: The sidecar pattern is used to export metrics in the format and protocol that the global monitoring system understands. It allows for standardized monitoring without modifying the main application.
Resource: Best practices for operating containers

Question: In Kubernetes, what does the /healthz HTTP endpoint indicate when it receives a request?

- A. The application's current version.
- B. The application's readiness to receive traffic.
- C. The application's health status.
- D. The application's memory consumption.

Correct Answer: C. The application's health status.

Explanation: The /healthz HTTP endpoint in Kubernetes is used as a liveness probe to indicate the health status of the application. A "200 OK" response means the application is considered healthy.
Resource: Best practices for operating containers

Question: Why is it recommended to avoid running processes as root inside containers?

- A. To increase the performance of the container.
- B. To prevent potential vulnerabilities that could give root access to the host machine.
- C. To ensure compatibility with all operating systems.
- D. To reduce the size of the container image.

Correct Answer: B. To prevent potential vulnerabilities that could give root access to the host machine.

Explanation: Running processes as root inside containers can pose a security risk. If an attacker finds a vulnerability, they could potentially gain root access to the host machine.
Resource: Best practices for operating containers

Question: What is the potential issue with using the "latest" tag for Docker images in Kubernetes manifests?

- A. It always pulls the oldest version of the image.
- B. It can lead to unpredictable and non-reproducible builds.
- C. It increases the deployment time.
- D. It is not supported by Kubernetes.

Correct Answer: B. It can lead to unpredictable and non-reproducible builds.

Explanation: The "latest" tag can be moved frequently from image to image. Using it can result in different nodes running different images that were all tagged "latest" at one point, leading to unpredictability.
Resource: Best practices for operating containers

Question: Why is it essential to properly tag container images?

- A. To ensure the image is publicly accessible.
- B. To identify different versions of the same application.
- C. To increase the size of the container image.
- D. To automatically deploy the image to production.

Correct Answer: B. To identify different versions of the same application.

Explanation: Properly tagging container images allows developers and operators to distinguish between different versions of the same application, ensuring that the correct version is deployed and run in various environments.
Resource: Best practices for building containers

Question: Which of the following is NOT a recommended practice when tagging container images?

- A. Using the latest tag for all images.
- B. Using semantic versioning for tags.
- C. Including the Git commit hash in the tag.
- D. Using distinct tags for development and production images.

Correct Answer: A. Using the latest tag for all images.

Explanation: Relying solely on the "latest" tag can lead to confusion and potential deployment of incorrect versions. It's essential to use more descriptive tags, such as semantic versioning or Git commit hashes, to clearly identify image versions.
Resource: Best practices for building containers

Question: What advantage does including the Git commit hash in the container image tag provide?

- A. It ensures the image is built from the latest code.
- B. It provides a direct link between the container image and the source code version.
- C. It reduces the size of the container image.
- D. It automatically updates the container image in production.

Correct Answer: B. It provides a direct link between the container image and the source code version.

Explanation: Including the Git commit hash in the container image tag creates a clear association between the image and a specific version of the source code. This practice aids in traceability and ensures that the correct version of the code is being used.
Resource: Best practices for building containers