PROFESSIONAL-CLOUD-DEVOPS-ENGINEER Q&As

Professional Cloud DevOps Engineer

Pass Google PROFESSIONAL-CLOUD-DEVOPS-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/professional-cloud-devops-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

You manage an application that is writing logs to Stackdriver Logging. You need to give some team members the ability to export logs. What should you do?

A. Grant the team members the IAM role of logging.configWriter on Cloud IAM.

B. Configure Access Context Manager to allow only these members to export logs.

C. Create and grant a custom IAM role with the permissions logging.sinks.list and logging.sink.get.

D. Create an Organizational Policy in Cloud IAM to allow only these members to create log exports.

Correct Answer: A

Reference: https://cloud.google.com/logging/docs/access-control

QUESTION 2

Your application runs on Google Cloud Platform (GCP). You need to implement Jenkins for deploying application releases to GCP. You want to streamline the release process, lower operational toil, and keep user data secure. What should you do?

A. Implement Jenkins on local workstations.

B. Implement Jenkins on Kubernetes on-premises.

C. Implement Jenkins on Google Cloud Functions.

D. Implement Jenkins on Compute Engine virtual machines.

Correct Answer: D

References: https://plugins.jenkins.io/google-compute-engine/

QUESTION 3

You support a popular mobile game application deployed on Google Kubernetes Engine (GKE) across several Google Cloud regions. Each region has multiple Kubernetes clusters. You receive a report that none of the users in a specific region can connect to the application. You want to resolve the incident while following Site Reliability Engineering practices. What should you do first?

A. Reroute the user traffic from the affected region to other regions that don\\'t report issues.

B. Use Stackdriver Monitoring to check for a spike in CPU or memory usage for the affected region.

C. Add an extra node pool that consists of high memory and high CPU machine type instances to the cluster.

D. Use Stackdriver Logging to filter on the clusters in the affected region, and inspect error messages in the logs.

Correct Answer: A

Reference: https://cloud.google.com/error-reporting/docs/viewing-errors

QUESTION 4

Your company runs applications in Google Kubernetes Engine (GKE). Several applications rely on ephemeral volumes. You noticed some applications were unstable due to the DiskPressure node condition on the worker nodes. You need to identify which Pods are causing the issue, but you do not have execute access to workloads and nodes. What should you do?

A. Check the node/ephemeral_storage/used_bytes metric by using Metrics Explorer.

B. Check the container/ephemeral_storage/used_bytes metric by using Metrics Explorer.

C. Locate all the Pods with emptyDir volumes. Use the df -h command to measure volume disk usage.

D. Locate all the Pods with emptyDir volumes. Use the df -sh * command to measure volume disk usage.

Correct Answer: A

node/ephemeral_storage/used_bytes GA Ephemeral storage usage GAUGE, INT64, By k8s_node Local ephemeral storage bytes used by the node. Sampled every 60 seconds.
https://cloud.google.com/monitoring/api/metrics_kubernetes

QUESTION 5

You are building and running client applications in Cloud Run and Cloud Functions. Your client requires that all logs must be available for one year so that the client can import the logs into their logging service. You must minimize required code changes. What should you do?

A. Deploy Falco or Twistlock on GKE to monitor for vulnerabilities on your running Pods.

B. Configure Identity and Access Management (IAM) policies to create a least privilege model on your GKE clusters.

C. Use Binary Authorization to attest images during your CI/CD pipeline.

D. Enable Container Analysis in Artifact Registry, and check for common vulnerabilities and exposures (CVEs) in your container images.

Correct Answer: A