Vendor: Google

Exam Code: Professional-Cloud-DevOps-Engineer

Exam Name: Google Cloud Certified - Professional Cloud DevOps Engineer Exam

Version: DEMO

QUESTION 1
You have a CI/CD pipeline that uses Cloud Build to build new Docker images and push them to Docker Hub. You use Git for code versioning. After making a change in the Cloud Build YAML configuration, you notice that no new artifacts are being built by the pipeline. You need to resolve the issue following Site
Reliability Engineering practices. What should you do?

A. Disable the CI pipeline and revert to manually building and pushing the artifacts.
B. Change the CI pipeline to push the artifacts is Container Registry instead of Docker Hub.
C. Upload the configuration YAML file to Cloud Storage and use Error Reporting to identify and fix the issue.
D. Run a Git compare between the previous and current Cloud Build Configuration files to find and fix the bug.

Answer: D

QUESTION 2
Your company follows Site Reliability Engineering principles. You are writing a postmortem for an incident, triggered by a software change, that severely affected users. You want to prevent severe incidents from happening in the future. What should you do?

A. Identify engineers responsible for the incident and escalate to their senior management.
B. Ensure that test cases that catch errors of this type are run successfully before new software releases.
C. Follow up with the employees who reviewed the changes and prescribe practices they should follow in the future.
D. Design a policy that will require on-call teams to immediately call engineers and management to discuss a plan of action if an incident occurs.

Answer: B

QUESTION 3
You support a high-traffic web application that runs on Google Cloud Platform (GCP). You need to measure application reliability from a user perspective without making any engineering changes to it. What should you do? (Choose two.)

A. Review current application metrics and add new ones as needed.
B. Modify the code to capture additional information for user interaction.
C. Analyze the web proxy logs only and capture response time of each request.
D. Create new synthetic clients to simulate a user journey using the application.
E. Use current and historic Request Logs to trace customer interaction with the application.

Answer: DE

QUESTION 4
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.

Answer: A

QUESTION 5
Your application services run in Google Kubernetes Engine (GKE). You want to make sure that only images from your centrally-managed Google Container Registry (GCR) image registry in the altostrat-images project can be deployed to the cluster while minimizing development time. What should you do?

A. Create a custom builder for Cloud Build that will only push images to gcr.io/altostrat-images.
B. Use a Binary Authorization policy that includes the whitelist name pattern gcr.io/altostrat-images/.
C. Add logic to the deployment pipeline to check that all manifests contain only images from gcr.io/altostrat-images.
D. Add a tag to each image in gcr.io/altostrat-images and check that this tag is present when the image is deployed.

Answer: B
Explanation:
https://cloud.google.com/binary-authorization/docs/example-policies

QUESTION 6
Your team has recently deployed an NGINX-based application into Google Kubernetes Engine (GKE) and has exposed it to the public via an HTTP Google Cloud Load Balancer (GCLB) ingress. You want to scale the deployment of the application's frontend using an appropriate Service Level Indicator (SLI). What should you do?

A. Configure the horizontal pod autoscaler to use the average response time from the Liveness and Readiness probes.
B. Configure the vertical pod autoscaler in GKE and enable the cluster autoscaler to scale the cluster as pods expand.
C. Install the Stackdriver custom metrics adapter and configure a horizontal pod autoscaler to use the number of requests provided by the GCLB.
D. Expose the NGINX stats endpoint and configure the horizontal pod autoscaler to use the request metrics exposed by the NGINX deployment.

Answer: C

QUESTION 7
Your company follows Site Reliability Engineering practices. You are the Incident Commander for a new, customer-impacting incident. You need to immediately assign two incident management roles to assist you in an effective incident response. What roles should you assign? (Choose two.)

A. Operations Lead
B. Engineering Lead
C. Communications Lead
D. Customer Impact Assessor
E. External Customer Communications Lead

Answer: AC
Explanation:
https://sre.google/workbook/incident-response/
The main roles in incident response are the Incident Commander (IC), Communications Lead (CL), and Operations or Ops Lead (OL).

QUESTION 8
You support an application running on GCP and want to configure SMS notifications to your team for the most critical alerts in Stackdriver Monitoring. You have already identified the alerting policies you want to configure this for. What should you do?

A. Download and configure a third-party integration between Stackdriver Monitoring and an SMS gateway. Ensure that your team members add their SMS/phone numbers to the external tool.
B. Select the Webhook notifications option for each alerting policy, and configure it to use a third-party integration tool. Ensure that your team members add their SMS/phone numbers to the external tool.
C. Ensure that your team members set their SMS/phone numbers in their Stackdriver Profile. Select the SMS notification option for each alerting policy and then select the appropriate SMS/phone numbers from the list.
D. Configure a Slack notification for each alerting policy. Set up a Slack-to-SMS integration to send SMS messages when Slack messages are received. Ensure that your team members add their SMS/phone numbers to the external integration.

Answer: C
Explanation:
https://cloud.google.com/monitoring/support/notification-options#creating_channels
To configure SMS notifications, do the following:
In the SMS section, click Add new and follow the instructions.
Click Save.
When you set up your alerting policy, select the SMS notification type and choose a verified phone number from the list.

QUESTION 9
You are managing an application that exposes an HTTP endpoint without using a load balancer. The latency of the HTTP responses is important for the user experience. You want to understand what HTTP latencies all of your users are experiencing. You use Stackdriver Monitoring. What should you do?

A. In your application, create a metric with a metricKind set to DELTA and a valueType set to DOUBLE. In Stackdriver's Metrics Explorer, use a Stacked Bar graph to visualize the metric.
B. In your application, create a metric with a metricKind set to CUMULATIVE and a valueType set to DOUBLE. In Stackdriver's Metrics Explorer, use a Line graph to visualize the metric.
C. In your application, create a metric with a metricKind set to GAUGE and a valueType set to DISTRIBUTION. In Stackdriver's Metrics Explorer, use a Heatmap graph to visualize the metric.
D. In your application, create a metric with a metricKind set to METRIC_KIND_UNSPECIFIED and a valueType set to INT64. In Stackdriver's Metrics Explorer, use a Stacked Area graph to visualize the metric.

Answer: C
Explanation:
https://cloud.google.com/monitoring/api/v3/kinds-and-types?hl=en

GAUGE Metric : In which value measures a specific instant in time
DELTA Metric : In which the value measures the change since it was last recorded
CUMULATIVE metric : In which the value constantly increases over time

QUESTION 10
Your team is designing a new application for deployment both inside and outside Google Cloud Platform (GCP). You need to collect detailed metrics such as system resource utilization. You want to use centralized GCP services while minimizing the amount of work required to set up this collection system. What should you do?

A. Import the Stackdriver Profiler package, and configure it to relay function timing data to Stackdriver for further analysis.
B. Import the Stackdriver Debugger package, and configure the application to emit debug messages with timing information.
C. Instrument the code using a timing library, and publish the metrics via a health check endpoint that is scraped by Stackdriver.
D. Install an Application Performance Monitoring (APM) tool in both locations, and configure an export to a central data storage location for analysis.

Answer: A
Explanation:
https://cloud.google.com/profiler/docs/about-profiler
Cloud Profiler is a statistical, low-overhead profiler that continuously gathers CPU usage and memory-allocation information from your production applications.

QUESTION 11
You need to reduce the cost of virtual machines (VM) for your organization. After reviewing different options, you decide to leverage preemptible VM instances.
Which application is suitable for preemptible VMs?

A. A scalable in-memory caching system.
B. The organization's public-facing website.
C. A distributed, eventually consistent NoSQL database cluster with sufficient quorum.
D. A GPU-accelerated video rendering platform that retrieves and stores videos in a storage bucket.

Answer: A
Explanation:
A GPU-accelerated video rendering platform that retrieves and stores videos in a storage bucket: Video rendering requires a stable and powerful infrastructure with persistent storage, which is not provided by preemptible VMs. Additionally, GPUs are not available on all preemptible VM instances.
https://cloud.google.com/compute/docs/instances/preemptible#preemptible-with-gpu

QUESTION 12
Your organization recently adopted a container-based workflow for application development. Your team develops numerous applications that are deployed continuously through an automated build pipeline to a Kubernetes cluster in the production environment. The security auditor is concerned that developers or operators could circumvent automated testing and push code changes to production without approval. What should you do to enforce approvals?

A. Configure the build system with protected branches that require pull request approval.

B. Use an Admission Controller to verify that incoming requests originate from approved sources.
C. Leverage Kubernetes Role-Based Access Control (RBAC) to restrict access to only approved users.
D. Enable binary authorization inside the Kubernetes cluster and configure the build pipeline as an attestor.

Answer: D

QUESTION 13
You support a stateless web-based API that is deployed on a single Compute Engine instance in the europe-west2-a zone. The Service Level Indicator (SLI) for service availability is below the specified Service Level Objective (SLO). A postmortem has revealed that requests to the API regularly time out. The time outs are due to the API having a high number of requests and running out memory. You want to improve service availability. What should you do?

A. Change the specified SLO to match the measured SLI
B. Move the service to higher-specification compute instances with more memory
C. Set up additional service instances in other zones and load balance the traffic between all instances
D. Set up additional service instances in other zones and use them as a failover in case the primary instance is unavailable

Answer: C
Explanation:
This option will provide redundancy and increase the availability of the service by distributing the traffic across multiple instances. Additionally, if one instance goes down, the load balancer will redirect the traffic to the other healthy instances, minimizing the impact on the service availability.

QUESTION 14
You are running a real-time gaming application on Compute Engine that has a production and testing environment. Each environment has their own Virtual Private Cloud (VPC) network. The application frontend and backend servers are located on different subnets in the environment's VPC. You suspect there is a malicious process communicating intermittently in your production frontend servers. You want to ensure that network traffic is captured for analysis. What should you do?

A. Enable VPC Flow Logs on the production VPC network frontend and backend subnets only with a sample volume scale of 0.5.
B. Enable VPC Flow Logs on the production VPC network frontend and backend subnets only with a sample volume scale of 1.0.
C. Enable VPC Flow Logs on the testing and production VPC network frontend and backend subnets with a volume scale of 0.5. Apply changes in testing before production.
D. Enable VPC Flow Logs on the testing and production VPC network frontend and backend subnets with a volume scale of 1.0. Apply changes in testing before production.

Answer: B
Explanation:
https://cloud.google.com/vpc/docs/flow-logs#log-sampling

QUESTION 15

Your team of Infrastructure DevOps Engineers is growing, and you are starting to use Terraform to manage infrastructure. You need a way to implement code versioning and to share code with other team members. What should you do?

A. Store the Terraform code in a version-control system. Establish procedures for pushing new versions and merging with the master.
B. Store the Terraform code in a network shared folder with child folders for each version release. Ensure that everyone works on different files.
C. Store the Terraform code in a Cloud Storage bucket using object versioning. Give access to the bucket to every team member so they can download the files.
D. Store the Terraform code in a shared Google Drive folder so it syncs automatically to every team member's computer. Organize files with a naming convention that identifies each new version.

Answer: A

QUESTION 16
You are using Stackdriver to monitor applications hosted on Google Cloud Platform (GCP). You recently deployed a new application, but its logs are not appearing on the Stackdriver dashboard. You need to troubleshoot the issue. What should you do?

A. Confirm that the Stackdriver agent has been installed in the hosting virtual machine.
B. Confirm that your account has the proper permissions to use the Stackdriver dashboard.
C. Confirm that port 25 has been opened in the firewall to allow messages through to Stackdriver.
D. Confirm that the application is using the required client library and the service account key has proper permissions.

Answer: A

QUESTION 17
Your organization recently adopted a container-based workflow for application development. Your team develops numerous applications that are deployed continuously through an automated build pipeline to the production environment. A recent security audit alerted your team that the code pushed to production could contain vulnerabilities and that the existing tooling around virtual machine (VM) vulnerabilities no longer applies to the containerized environment. You need to ensure the security and patch level of all code running through the pipeline. What should you do?

A. Set up Container Analysis to scan and report Common Vulnerabilities and Exposures.
B. Configure the containers in the build pipeline to always update themselves before release.
C. Reconfigure the existing operating system vulnerability software to exist inside the container.
D. Implement static code analysis tooling against the Docker files used to create the containers.

Answer: A
Explanation:
https://cloud.google.com/container-analysis/docs/container-analysis
Container Analysis is a service that provides vulnerability scanning and metadata storage for containers.

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