Professional Cloud DevOps Engineer Actual Exam Questions

## Question #: 170

Q: Your company allows teams to self-manage Google Cloud projects, including project-level Identity and Access Management (IAM). You are concerned that the team responsible for the Shared VPC project might accidentally delete the project, so a lien has been placed on the project. You need to design a solution to restrict Shared VPC project deletion to those with the resourcemanager.projects.updateLiens permission at the organization level. What should you do?

* A. Instruct teams to only perform IAM permission management as code with Terraform.
* B. Enable VPC Service Controls for the container.googleapis.com API service.
* C. Revoke the resourcemanager.projects.updateLiens permission from all users associated with the project.
* D. Enable the compute.restrictXpnProjectLienRemoval organization policy constraint.

Solution: D

## Question #: 171

Q: You are developing an application that consists of several microservices running in a Google Kubernetes Engine cluster. One microservice needs to connect to a third-party database running on-premises. You need to store credentials to the database and ensure that these credentials can be rotated while following security best practices. What should you do?

* A. Store the credentials in a sidecar container proxy, and use it to connect to the third-party database.
* B. Configure a service mesh to allow or restrict traffic from the Pods in your microservice to the database.
* C. Store the credentials in an encrypted volume mount, and associate a Persistent Volume Claim with the client Pod.
* D. Store the credentials as a Kubernetes Secret, and use the Cloud Key Management Service plugin to handle encryption and decryption.

Solution: D

## Question #: 172

Q: Your organization is running multiple Google Kubernetes Engine (GKE) clusters in a project. You need to design a highly-available solution to collect and query both domain-specific workload metrics and GKE default metrics across all clusters, while minimizing operational overhead. What should you do?

* A. Use Prometheus operator to install Prometheus in every cluster and scrape the metrics. Configure remote-write to one central Prometheus. Query the central Prometheus instance.
* B. Enable managed collection on every GKE cluster. Query the metrics in BigQuery.
* C. Use Prometheus operator to install Prometheus in every cluster and scrape the metrics. Ensure that a Thanos sidecar is enabled on every Prometheus instance. Configure Thanos in the central cluster. Query the central Thanos instance.
* D. Enable managed collection on every GKE cluster. Query the metrics in Cloud Monitoring.

Solution: D

## Question #: 173

Q: Your company stores a large volume of infrequently used data in Cloud Storage. The projects in your company's CustomerService folder access Cloud Storage frequently, but store very little data. You want to enable Data Access audit logging across the company to identify data usage patterns. You need to exclude the CustomerService folder projects from Data Access audit logging. What should you do?

* A. Enable Data Access audit logging for Cloud Storage at the organization level, and configure exempted principals to include users of the CustomerService folder.
* B. Enable Data Access audit logging for Cloud Storage at the organization level, with no additional configuration.
* C. Enable Data Access audit logging for Cloud Storage for all projects and folders other than the CustomerService folder.
* D. Enable Data Access audit logging for Cloud Storage for all projects and folders, and configure exempted principals to include users of the CustomerService folder.

Solution: C

## Question #: 174

Q: You have an application running in production on Cloud Run. Your team recently finished developing a new version (revision B) of the application. You want to test the new revision on 10% of your clients by using the least amount of effort. What should you do?

* A. Deploy the new revision to the existing service without traffic allocated. Tag the revision and share the URL with 10% of your clients.
* B. Create a new service, and deploy the new revisions on the new service. Deploy a new revision of the old application where the application routes a percentage of the traffic to the new service.
* C. Create a new service, and deploy the new revision on that new service. Create a load balancer to split the traffic between the old service and the new service.
* D. Deploy the new revision to the existing service without traffic allocated. Split the traffic between the old revision and the new revision.

Solution: D

## Question #: 175

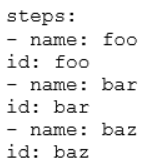
Q: You are designing a new multi-tenant Google Kubernetes Engine (GKE) cluster for a customer. Your customer is concerned with the risks associated with long-lived credentials use. The customer requires that each GKE workload has the minimum Identity and Access Management (IAM) permissions set following the principle of least privilege (PoLP). You need to design an IAM impersonation solution while following Google-recommended practices. What should you do?

* A. 1. Create a Google service account.  
  2. Create a node pool, and set the Google service account as the default identity.  
  3. Ensure that workloads can only run on the designated node pool by using node selectors, taints, and tolerations.  
  4. Repeat for each workload.
* B. 1. Create a Google service account.  
  2. Create a node pool without taints, and set the Google service account as the default identity.  
  3. Grant IAM permissions to the Google service account.
* C. 1. Create a Google service account.  
  2. Create a Kubernetes service account in a Workload Identity-enabled cluster.  
  3. Link the Google service account with the Kubernetes service account by using the roles/iam.workloadIdentityUser role and iam.gke.io/gcp-service-account annotation.  
  4. Map the Kubernetes service account to the workload.  
  5. Repeat for each workload.
* D. 1. Create a Google service account.  
  2. Create a service account key for the Google service account.  
  3. Create a Kubernetes secret with a service account key.  
  4. Ensure that workload mounts the secret and set the GOOGLE\_APPLICATION\_CREDENTIALS environment variable to point at the mount path.  
  5. Repeat for each workload.

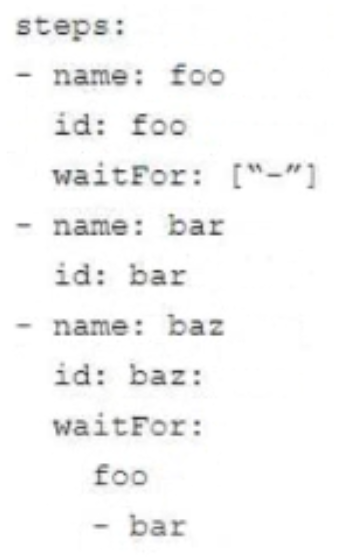
Solution: C

## Question #: 176

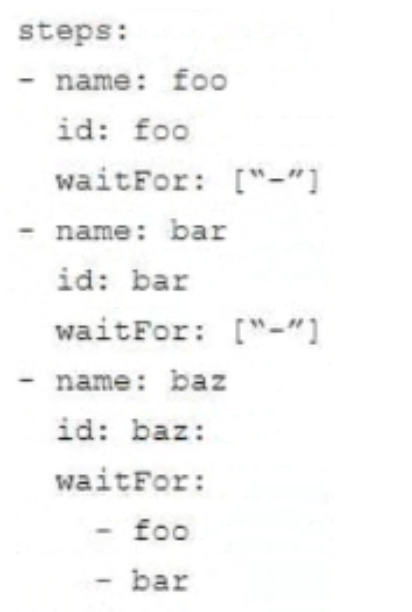
Q: You are configuring a Cl pipeline in Cloud Build When you test the pipeline, the following cloudbuild.yaml definition results in 5 minutes each on the foo step and bar step

  
The foo step and bar step are independent of each other. The baz step needs both the foo and bar steps to be completed before starting. You want to use parallelism to reduce build times What should you do?

* A. Modify the build script to add -  
  options:  
  machineType: 'E2\_HIGHCPU\_8'
* B. Modify the build script to add -  
  options:  
  machineType: 'E2\_HIGHCPU\_32'
* C. Change the build script to:



* D. Change the build script to:



Solution: D

## Question #: 177

Q: You receive a Cloud Monitoring alert indicating potential malicious activity on a node in your Google Kubernetes Engine (GKE) cluster. The alert suggests a possible compromised container running on that node. You need to isolate this node to prevent further compromise while investigating the issue. You also want to minimize disruption to applications running on the cluster. What should you do?

* A. Taint the suspicious node to prevent Pods that have interacted with it from being scheduled on other nodes in the cluster
* B. Scale down the deployment associated with the compromised container to zero other nodes
* C. Restart the node to disrupt the malicious activity, and force all Pods to be restructured on other nodes.
* D. Cordon the node to prevent new Pods from being scheduled, the drain the node to safely remove existing Pods and reschedule them to other nodes.

Solution: D

## Question #: 178

Q: Your company has an application deployed on Google Kubernetes Engine (GKE) consisting of 12 microservices. Multiple teams are working concurrently on various features across three envi-ronments: Dev, Staging, and Prod. Developers report dependency test failures and delayed re-leases due to deployments from multiple feature branches in the shared Dev GKE cluster.  
  
You need to implement a cost-effective solution for developers to test their microservice features in a stable development environment isolated from other development activities. What should you do?

* A. Automate CI pipelines by using Cloud Build for container image creation and Kubernetes manifest updates from main branch merge requests. Integrate with Config Sync to test new im-ages in dynamically created namespaces on the Dev GKE cluster with autoscaling enabled. Im-plement a post-test namespace cleanup routine.
* B. Automate CI pipelines by using Cloud Build to create container images and update Kuber-netes manifests for each commit. Use Cloud Deploy for progressive delivery to Dev, Staging, and Prod GKE clusters. Enable Config Sync for consistent Kubernetes configurations across en-vironments.
* C. Use Cloud Build to automate CI pipelines and update Kubernetes manifest files from feature branch commits. Integrate with Config Sync to test new images in dynamically created namespaces on the Dev GKE cluster with autoscaling enabled. Implement a post-test namespace cleanup routine.
* D. Use Cloud Build to automate CI pipelines and update Kubernetes manifest files from feature branch commits. Integrate with Config Sync to test new images in dynamically created GKE Dev clusters for each feature branch, which are deleted upon merge request.

Solution: A

## Question #: 179

Q: You are troubleshooting a failed deployment in your CI/CD pipeline. The deployment logs indicate that the application container failed to start due to a missing environment variable. You need to identify the root cause and implement a solution within your CI/CD workflow to prevent this issue from recurring. What should you do?

* A. Use a canary deployment strategy.
* B. Implement static code analysis in the CI pipeline.
* C. Run integration tests in the CI pipeline.
* D. Enable Cloud Audit Logs for the deployment.

Solution: C

## Question #: 180

Q: You work for a company that offers a free photo processing application. You are designing the infrastructure for the backend service that processes the photos. The service:  
• Uses Cloud Storage to store both unprocessed and processed photos.  
• Can resume processing photos in the event of a failure.  
• Is not suitable for containerization.  
  
There is no SLO for the time taken to process a photo. You need to choose the most cost-effective solution for running the service. What should you do?

* A. Deploy the service by using Cloud Run.
* B. Deploy the service by using standard VMs with a 3-year committed use discount.
* C. Deploy the service by using GKE.
* D. Deploy the service by using Spot VMs.

Solution: D

## Question #: 181

Q: You manage a critical API running on Cloud Run that serves an average of 10,000 requests per minute. You need to define service level objectives (SLOs) for availability and latency to ensure that the API meets user expectations, which include 99.9% availability and a maximum latency of 200 milliseconds for 95% of requests. You also need to ensure these SLOs are actively monitored and measured. What should you do?

* A. Configure Cloud Monitoring to send alerts when average API latency exceeds 150 ms or the error rate surpasses 0.1%.
* B. Prioritize latency as the only SLO, targeting 100 ms for 99% of requests.
* C. Set SLOs for 99% availability at 99% and 500 ms latency for 90% of requests. Use Cloud Monitoring to track SLOs and alert on violations.
* D. Set SLOs for the API by using availability and latency service level indicators. Use Cloud Monitoring to track SLOs and alert on violations.

Solution: D

## Question #: 182

Q: You are running a web application that connects to an AlloyDB cluster by using a private IP address in your default VPC. You need to run a database schema migration in your CI/CD pipeline by using Cloud Build before deploying a new version of your application. You want to follow Google-recommended security practices. What should you do?

* A. Set up a Cloud Build private pool to access the database through a static external IP address. Configure the database to only allow connections from this IP address. Execute the schema migration script in the private pool.
* B. Create a service account that has permission to access the database. Configure Cloud Build to use this service account and execute the schema migration script in a private pool.
* C. Add the database username and password to Secret Manager. When running the schema migration script, retrieve the username and password from Secret Manager.
* D. Add the database username and encrypted password to the application configuration file. Use these credentials in Cloud Build to execute the schema migration script.

Solution: B

## Question #: 183

Q: You use Artifact Registry to store container images built with Cloud Build. You need to ensure that all existing and new images are continuously scanned for vulnerabilities. You also want to track who pushed each image to the registry. What should you do?

* A. Configure Artifact Registry to automatically scan new images and periodically re-scan all images. Use Cloud Audit Logs to track image uploads and identify the user who pushed each image.
* B. Configure Artifact Registry to send vulnerability scan results to a Cloud Storage bucket. Use a separate script to parse results and notify a security team.
* C. Configure Artifact Registry to automatically re-scan images daily. Enable Cloud Audit Logs to track these scans, and use Logs Explorer to identify vulnerabilities.
* D. Configure Artifact Registry to automatically trigger vulnerability scans for new image tags, and view scan results. Use Cloud Audit Logs to track image tag creation events.

Solution: A

## Question #: 184

Q: You manage a retail website for your company. The website consists of several microservices running in a GKE Standard node pool with node autoscaling enabled. Each microservice has resource limits and a Horizontal Pod Autoscaler configured. During a busy period, you receive alerts for one of the microservices. When you check the Pods, half of them have the status OOMKilled, and the number of Pods is at the minimum autoscaling limit. You need to resolve the issue. What should you do?

* A. Update the node pool to use a machine type with more memory.
* B. Increase the maximum number of nodes in the node pool.
* C. Increase the maximum replica limit of the Horizontal Pod Autoscaler.
* D. Increase the memory resource limit of the microservice.

Solution: D

## Question #: 185

Q: You are configuring a Cl pipeline. The build step for your Cl pipeline integration testing requires access to APIs inside your private VPC network. Your security team requires that you do not expose API traffic publicly. You need to implement a solution that minimizes management overhead. What should you do?

* A. Use Cloud Build private pools to connect to the private VPC.
* B. Use Cloud Build to create a Compute Engine instance in the private VPC. Run the integration tests on the VM by using a startup script.
* C. Use Cloud Build as a pipeline runner. Configure a cross-region internal Application Load Balancer for API access.
* D. Use Cloud Build as a pipeline runner. Configure a global external Application Load Balancer with a Google Cloud Armor policy for API access.

Solution: A

## Question #: 186

Q: You are deploying a new version of your application to a multi-zone Google Kubernetes Engine (GKE) cluster. The deployment is progressing smoothly, but you notice that some Pods in a specific zone are experiencing higher error rates. You need to selectively roll back the update for the Pods experiencing errors with minimal impact to users. What should you do?

* A. Scale down the Pods in the affected zone. Redeploy the new version of the application.
* B. Drain the affected nodes. Redeploy the new version of the application to the remaining nodes.
* C. Modify the Deployment to use the Pod template from the previous version of your application. Perform a rolling update to replace the Pods in the affected zone.
* D. Use the kubectl rollout undo command to roll back the entire deployment. Redeploy the new version of the application, excluding the affected zone.

Solution: C

## Question #: 187

Q: You work for a healthcare company and regulations require you to create all resources in a United States-based region. You attempted to create a secret in Secret Manager but received the following error message:  
  
Constraint constraints/gcp.resourceLocations violated for [orgpolicy:projects/000000] attempting to create a secret in [global]  
  
You need to resolve the error while remaining compliant with regulations. What should you do?

* A. Remove the organization policy referenced in the error message.
* B. Create the secret with an automatic replication policy.
* C. Create the secret with a user-managed replication policy.
* D. Add the global region to the organization policy referenced in the error message.

Solution: C

## Question #: 188

Q: You are responsible for creating development environments for your company's development team. You want to create environments with identical IDEs for all developers while ensuring that these environments are not exposed to public networks. You need to choose the most cost-effective solution without impacting developer productivity. What should you do?

* A. Create multiple Compute Engine VM instances with a public IP address and use a Public NAT gateway. Configure an instance schedule to shut down the VMs.
* B. Create multiple Compute Engine VM instances without a public IP address. Configure an instance schedule to shut down the VMs.
* C. Create a Cloud Workstations private cluster. Create a workstation configuration with an idieTimeour parameter.
* D. Create a Cloud Workstations private cluster. Create a workstation configuration with a runningTimeout parameter.

Solution: D

## Question #: 189

Q: Your company uses Cloud Deploy with multiple delivery pipelines for deploying applications to different environments. Your development team currently lacks access to any of these pipelines. You need to grant the team access to only the development delivery pipeline, while following Google-recommended practices. What should you do?

* A. In the Google Cloud console, grant the development team the roles/clouddeploy.operator role. Add deny conditions to all pipelines other than the development delivery pipeline.
* B. In the Google Cloud console, create a custom IAM role with all clouddeploy.automations.\* permissions and an allow policy for only the development delivery pipeline. Grant this IAM role to the development team.
* C. Grant the development team the roles/clouddeploy.operator role in a policy file. Apply the policy file to the development target.
* D. Grant the development team the roles/clouddeploy.developer role in a policy file. Apply this policy file to the development delivery pipeline.

Solution: D

## Question #: 190

Q: Your company has recently experienced several production service issues. You need to create a Cloud Monitoring dashboard to troubleshoot the issues, and you want to use the dashboard to distinguish between failures in your own service and those caused by a Google Cloud service that you use. What should you do?

* A. Create a log-based metric to track cloud service errors, and display the metric on the dashboard.
* B. Create a logs widget to display system errors from Cloud Logging on the dashboard.
* C. Create an alerting policy for the system error metrics.
* D. Enable Personalized Service Health annotations on the dashboard.

Solution: D

## Question #: 191

Q: Your company wants to implement a CD pipeline in Cloud Deploy for a web service deployed to GKE. The web service currently does not have any automated testing. The Quality Assurance team must manually verify any new releases of the web service before any production traffic is processed. You need to design the CD pipeline. What should you do?

* A. Create a single pipeline stage, and use a standard deployment strategy.
* B. Create a single pipeline stage, and use a canary deployment strategy.
* C. Create two pipeline stages, and use a canary deployment strategy.
* D. Create two pipeline stages, and use a standard deployment strategy.

Solution: D

## Question #: 192

Q: You manage your company’s primary revenue-generating application. You have an error budget policy in place that freezes production deployments when the application is close to breaching its SLO. A number of issues have recently occurred, and the application has exhausted its error budget. You need to deploy a new release to the application that includes a feature urgently required by your largest customer. You have been told that the release has passed all unit tests. What should you do?

* A. Delay the deployment of the feature until the error budget is replenished.
* B. Re-run the unit tests, and start the deployment of the feature if the tests pass.
* C. Start the deployment of the feature immediately.
* D. Deploy the feature to a subset of users, and gradually roll out to all users if there are no errors reported.

Solution: A

## Question #: 193

Q: You work for a company that manages highly sensitive user data. You are designing the Google Kubernetes Engine (GKE) infrastructure for your company, including several applications that will be deployed in development and production environments. Your design must protect data from unauthorized access from other applications, while minimizing the amount of management overhead required. What should you do?

* A. Create one cluster for the organization with separate namespaces for each application and environment combination.
* B. Create one cluster for each application with separate namespaces for production and development environments.
* C. Create one cluster for each environment (development and production) with each application in its own namespace within each cluster.
* D. Create one cluster for the organization with separate namespaces for each application.

Solution: C

## Question #: 194

Q: You are developing a Node.js utility on a workstation in Cloud Workstations by using Code OSS. The utility is a simple web page, and you have already confirmed that all necessary firewall rules are in place. You tested the application by starting it on port 3000 on your workstation in Cloud Workstations, but you need to be able to access the web page from your local machine. You need to follow Google-recommended security practices. What should you do?

* A. Use a browser running on a bastion host VM.
* B. Run the gcloud compute start-iap-tunnel command to the Cloud Workstations VM.
* C. Allow public IP addresses in the Cloud Workstations configuration.
* D. Click the preview link in the Code OSS panel.

Solution: D

## Question #: 195

Q: Your team is preparing to launch a new API in Cloud Run. The API uses an OpenTelemetry agent to send distributed tracing data to Cloud Trace to monitor the time each request takes. The team has noticed inconsistent trace collection. You need to resolve the issue. What should you do?

* A. Use an HTTP health check.
* B. Configure CPU to be always-allocated.
* C. Increase the CPU limit in Cloud Run from 2 to 4.
* D. Configure CPU to be allocated only during request processing.

Solution: B