Professional Cloud Developer Sample Questions

The Cloud Developer sample questions will familiarize you with the format of exam questions and example content that may be covered on the exam.

The sample questions do not represent the range of topics or level of difficulty of questions presented on the exam. Performance on the sample questions should not be used to predict your Cloud Developer exam result.

Registration

First Name *

Mohammad

Last Name *

Muzammil

Primary Email *

mohdmuzammil74779@gmail.com

Recovery Email

mohammadm@sidgs.com

Organization (Employer or School) *

SID Global Solutions

Organization email (an email associated with your current organization)

mohammadm@sidgs.com

Country *

India ▾

Primary Relationship to Google *

Partner ▾

Send me offers, updates and useful tips for getting the most out of Google Cloud training and certification products and services. *

Yes ▾

✗ You are developing an online gaming platform as a microservices application on GKE. Users on social media are complaining about long loading times for certain URL requests to the application. You need to investigate performance bottlenecks in the application and identify which HTTP requests have a significantly high latency span in user requests. What should you do?

○ A. Instrument your microservices by installing the OpenTelemetry tracing package. Update your application code to send traces to Trace for inspection and analysis. Create an analysis report on Trace to analyze user requests.

○ B. Update your microservices to log HTTP request methods and URL paths to STDOUT. Use the logs router to send container logs to Cloud Logging. Create filters in Cloud Logging to evaluate the latency of user requests across different methods and URL paths.

● C. Configure GKE workload metrics using kubectl. Select all Pods to send their metrics to Cloud Monitoring. Create a custom dashboard of application metrics in Cloud Monitoring to determine performance bottlenecks of your GKE cluster. ✗

○ D. Install tcpdump on your GKE nodes. Run tcpdump to capture network traffic over an extended period of time to collect data. Analyze the data files using Wireshark to determine the cause of high latency.

Correct answer

● A. Instrument your microservices by installing the OpenTelemetry tracing package. Update your application code to send traces to Trace for inspection and analysis. Create an analysis report on Trace to analyze user requests.

Feedback

A is correct because it describes Google's recommended approach to capture latency spans in user requests (https://cloud.google.com/trace/docs/analysis-reports).
B is not correct as STDOUT logs do not provide convenient data format to capture latency data.
C is not correct as pod-wide metrics might not capture tracing data for specific URL requests.
D is not correct as installing tcpdump on GKE nodes is not a recommended practice.

https://cloud.google.com/... https://cloud.google.com/...

✗ You need to containerize a web application that will be hosted on Google Cloud behind a global load balancer with SSL certificates. You don’t have the time to develop authentication at the application level, and you want to offload SSL encryption and management from your application. You want to configure the architecture using managed services where possible. What should you do?

○ A. Host the application on GKE, and use Identity-Aware Proxy (IAP) with Cloud Load Balancing and Google-managed certificates.

○ B. Host the application on GKE, and deploy an NGINX Ingress Controller to handle authentication.

● C. Host the application on GKE, and deploy cert-manager to manage SSL certificates. ✗

○ D. Host the application on Compute Engine, and configure Cloud Endpoints for your application.

Correct answer

● A. Host the application on GKE, and use Identity-Aware Proxy (IAP) with Cloud Load Balancing and Google-managed certificates.

Feedback

A is correct because it uses the most managed services (GKE, IAP, and CLB with Google-managed certificates).
B is not correct because NGINX Ingress doesn’t handle SSL certificate rotation
C is not correct because it doesn’t handle authentication for the application, only SSL certification rotation.
D is not correct because while it's technically possible to run containers on Compute Engine, the better solution is to use GKE for containers.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You manage a microservice-based ecommerce platform on Google Cloud that sends confirmation emails to a third-party email service provider using a Cloud Function. Your company just launched a marketing campaign, and some customers are reporting that they have not received order confirmation emails. You discover that the services triggering the Cloud Function are receiving HTTP 500 errors. You need to change the way emails are handled to minimize email loss. What should you do?

○ A. Increase the Cloud Function’s timeout to nine minutes.

○ B. Configure the sender application to publish the outgoing emails in a message to a Pub/Sub topic. Update the Cloud Function configuration to consume the Pub/Sub queue.

● C. Configure the sender application to retry the execution of the Cloud Function every one second if a request fails. ✗

○ D. Configure the sender application to write emails to Memorystore and then trigger the Cloud Function. When the function is triggered, it reads the email details from Memorystore and sends them to the email service.

Correct answer

● B. Configure the sender application to publish the outgoing emails in a message to a Pub/Sub topic. Update the Cloud Function configuration to consume the Pub/Sub queue.

Feedback

A is not correct because increasing the timeout will not fix the issue. The issue is caused by the rapid increase in inbound traffic and the requests timing out while waiting for new Cloud Function instances to be created.
B is correct because it will decouple the Cloud Functions from the microservices sending emails and will allow Cloud Functions to scale at their own pace.
C is not correct because this will not decouple the applications. Although this is possible, a number of microservices might trigger the ‘email’ Cloud Function. Changing all these microservices will introduce code duplication, require development effort, and use unnecessary compute cycles.
D is not correct because this does not solve the problem. Rapid increase of traffic will again result in similar scaling challenges.

https://cloud.google.com/…

✓ You are developing a web application that contains private images and videos stored in a Cloud Storage bucket. Your users are anonymous and do not have Google Accounts. You want to use your application-specific logic to control access to the images and videos. How should you configure access?

● A. Generate a signed URL that grants read access to the bucket. Allow users to access the URL after authenticating through your web application. ✓

○ B. Configure Identity-Aware Proxy (IAP) to authenticate users into the web application. Allow users to access the bucket after authenticating through IAP.

○ C. Grant the Storage Object Viewer IAM role to allUsers. Allow users to access the bucket after authenticating through your web application.

○ D. Cache each web application user's IP address to create a named IP table using Google Cloud Armor. Create a Google Cloud Armor security policy that allows users to access the backend bucket.

Feedback

A is correct because Cloud Storage is designed to store unstructured data like images and videos. In some scenarios, you might not want to require your users to have a Google Account in order to access Cloud Storage, but you still want to control access using your application-specific logic. The way to address this use case is to provide a signed URL to a user, which gives the user read, write, or delete access to that resource for a limited time.
B is incorrect because IAP only allows users with correct IAM access to authenticate. In this case, our users are anonymous.
C is incorrect because it gives unnecessary access to the public.
D is incorrect because it's unnecessarily complicated, and IP addresses are an unreliable resource.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✗ You work on an application that relies on Cloud Spanner as its main datastore. New application features have occasionally caused performance regressions. You want to prevent performance issues by running an automated performance test with Cloud Build for each commit made. If multiple commits are made at the same time, the tests might run concurrently. What should you do?

○ A. Create a project with a Cloud Spanner instance and the required data. Adjust the Cloud Build build file to automatically restore the data to its previous state after the test is complete.

○ B. Create a new project with a random name for every build. Load the required data. Delete the project after the test is complete.

○ C. Create a new Cloud Spanner instance for every build. Load the required data. Delete the Cloud Spanner instance after the test is complete.

● D. Start the Cloud Spanner emulator locally. Load the required data. Shut down the emulator after the test is complete. ✗

Correct answer

● C. Create a new Cloud Spanner instance for every build. Load the required data. Delete the Cloud Spanner instance after the test is complete.

Feedback

A is not correct because Cloud Build can run builds in parallel. Multiple commits from multiple devs might cause multiple builds to run simultaneously, potentially affecting the results.
B is not correct because creating projects is rate limited and a highly privileged operation within an organization.
C is correct because it provides the test isolation needed to detect performance issues.
D is not correct because the emulator does not have the same scalability / performance characteristics as the real service.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✗ You need to deploy an internet-facing microservices application to GKE. You want to validate new features using the A/B testing method. You have the following requirements for deploying new container image releases:

1. There is no downtime when new container images are deployed.

2. New production releases are tested and verified using a subset of production users.

What should you do?

○ A. 1. Configure your CI/CD pipeline to update the Deployment manifest file by replacing the container version with the latest version. 2. Recreate the Pods in your cluster by applying the Deployment manifest file. 3. Validate the application's performance by comparing its functionality with the previous release version, and roll back if an issue arises.

○ B. 1. Install the Anthos Service Mesh on your GKE cluster. 2. Create two Deployments on the GKE cluster, and label them with different version names. 3. Create a VirtualService with a routing rule to send a small percentage of traffic to the Deployment that references the new version of the application.

○ C. 1. Create a second namespace on GKE for the new release version. 2. Create a Deployment configuration for the second namespace with the desired number of Pods. 3. Deploy new container versions in the second namespace. 4. Update the Ingress configuration to route traffic to the namespace with the new container versions.

● D. 1. Implement a rolling update pattern by replacing the Pods gradually with the new release version. 2. Validate the application's performance for the new subset of users during the rollout, and roll back if an issue arises. ✗

Correct answer

● B. 1. Install the Anthos Service Mesh on your GKE cluster. 2. Create two Deployments on the GKE cluster, and label them with different version names. 3. Create a VirtualService with a routing rule to send a small percentage of traffic to the Deployment that references the new version of the application.

Feedback

A is not correct because the approach would not allow testing the new release with a subset of users at the same time as having the previous release in place.
B is correct because Istio traffic management is a convenient tool to implement routing rules for A/B testing. Reference: https://cloud.google.com/service-mesh/docs/by-example/canary-deployment
C is not correct because the approach would not allow testing the new release with a subset of users at the same time as having the previous release in place.

D is not correct because the deployment pattern does not allow to reliably test a new version with a subset of production users while the previous release is still in place.

https://istio.io/latest/docs…

https://cloud.google.com/…

https://cloud.google.com/…

✗ Your team is writing a backend application to implement the business logic for an interactive voice response (IVR) system that will support a payroll application.

The IVR system has the following technical characteristics:

- Each customer phone call is associated with a unique IVR session.

- The IVR system creates a separate persistent gRPC connection to the backend for each session.

- If the connection is interrupted, the IVR system establishes a new connection, causing a slight latency for that call.

You need to determine which compute environment should be used to deploy the backend application. Using current call data, you determine that:

- Call duration ranges from 1 to 30 minutes.

- Calls are typically made during business hours.

- There are significant spikes of calls around certain known dates (e.g., pay days), or when large payroll changes occur.

You want to minimize cost, effort, and operational overhead. Where should you deploy the backend application?

○ A. Cloud Run

○ B. Cloud Functions

● C. GKE cluster in Standard mode ✗

○ D. Compute Engine

Correct answer

● A. Cloud Run

Feedback

A is correct because Cloud Run supports sessions of up to 60 minutes, supports gRPC, scales to zero and is zero-ops.

B is not correct because Cloud Functions are limited to 9 minutes of run time, and Cloud Functions don’t support gRPC.
C is not correct because GKE Standard will have higher costs and higher management overhead.
D is not correct because Compute Engine has higher costs and higher management overhead.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are a developer at a large organization. You are deploying a web application to GKE. The DevOps team has built a CI/CD pipeline that uses Cloud Deploy to deploy the application to Dev, Test, and Prod clusters in GKE. After Cloud Deploy successfully deploys the application to the Dev cluster, you want to automatically promote it to the Test cluster. How should you configure this process following Google-recommended best practices?

○ A. 1. Create a Cloud Build trigger that listens for SUCCEEDED Pub/Sub messages from the clouddeploy-operations topic. 2. Configure Cloud Build to include a step that promotes the application to the Test cluster.

○ B. 1. Create a Cloud Function that calls the Google Cloud Deploy API to promote the application to the Test cluster. 2. Configure this function to be triggered by SUCCEEDED Pub/Sub messages from the cloud-builds topic.

○ C. 1. Create a Cloud Function that calls the Google Cloud Deploy API to promote the application to the Test cluster. 2. Configure this function to be triggered by SUCCEEDED Pub/Sub messages from the clouddeploy-operations topic.

● D. 1. Create a Cloud Build pipeline that uses the gke-deploy builder. 2. Create a Cloud Build trigger that listens to SUCCEEDED Pub/Sub messages from the cloud-builds topic. 3. Configure this pipeline to run a deployment step to the Test cluster. ✗

Correct answer

● A. 1. Create a Cloud Build trigger that listens for SUCCEEDED Pub/Sub messages from the clouddeploy-operations topic. 2. Configure Cloud Build to include a step that promotes the application to the Test cluster.

Feedback

A is correct as it is the Google-recommended approach to integrate with CI pipelines.
B is not correct because the question is around Cloud Deploy rather than Cloud Build.
C is not correct because it is not the recommended approach. This would add extra complexity and management of Cloud Functions.
D is not correct because the question is around Cloud Deploy rather than Cloud Build.

https://cloud.google.com/...

https://cloud.google.com/...

✓ You are developing a new application. You want the application to be triggered only when a given file is updated in your Cloud Storage bucket. Your trigger might change, so your process must support different types of triggers. You want the configuration to be simple so that multiple team members can update the triggers in the future. What should you do?

○ A. Configure a Cloud Function that executes your application and is triggered when an object is updated in Cloud Storage.

● B. Create an Eventarc trigger that monitors your Cloud Storage bucket for a specific filename, and set the target as Cloud Run. ✓

○ C. Configure a Firebase function that executes your application and is triggered when an object is updated in Cloud Storage.

○ D. Configure Cloud Storage events to be sent to Pub/Sub, and use Pub/Sub events to trigger a Cloud Build job that executes your application.

Feedback

A is not correct because you can't filter by filenames; it will send all changes made to the bucket.
B is correct because Eventarc supports flexible filters and you can create triggers based on filename patterns.
C is not correct because you can't filter by filenames; it will send all changes to the bucket.
D is not correct because even though you can filter by different names, the configuration has multiple levels of triggers which is overly complicated.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://firebase.google.co…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are a developer at a large organization. You have an application written in Go running in a production GKE cluster. You need to add a new feature that requires access to BigQuery. You want to grant BigQuery access to your GKE cluster following Google-recommended best practices. What should you do?

○ A. Create a Google service account with BigQuery access. Add the JSON key to Secret Manager, and use the Go client library to access the JSON key.

○ B. Create a Google service account with BigQuery access. Add the Google service account JSON key as a Kubernetes secret, and configure the application to use this secret.

● C. Create a Google service account with BigQuery access. Add the Google service account JSON key to Secret Manager, and use an init container to access the secret for the application to use. ✗

○ D. Create a Google service account and a Kubernetes service account. Configure Workload Identity on the GKE cluster, and reference the Kubernetes service account on the application Deployment.

Correct answer

● D. Create a Google service account and a Kubernetes service account. Configure Workload Identity on the GKE cluster, and reference the Kubernetes service account on the application Deployment.

Feedback

A is not correct because it is not a recommended best practice with GKE, however when using Secrets Manager outside of GKE this would be the recommended approach.
B is not correct because secret data in GKE is not encrypted, just obfuscated, so storing secrets in this way is a security risk.
C is not correct because the recommended process when using Secret Manager, the best practice for this option we recommend using the Secret Manager API directly (using one of the provided client libraries, or by following the REST or gRPC documentation).
D is correct. This is the best way to consume Google Cloud services without having to pass credential variables around.

https://cloud.google.com/…

https://cloud.google.com/…

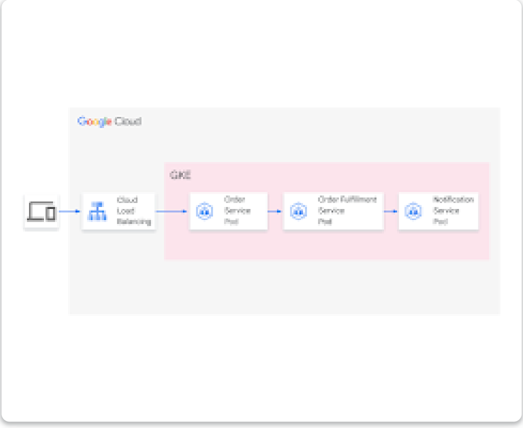
✓ You are developing a flower ordering application. Currently you have three microservices:

- Order Service (receives the orders)

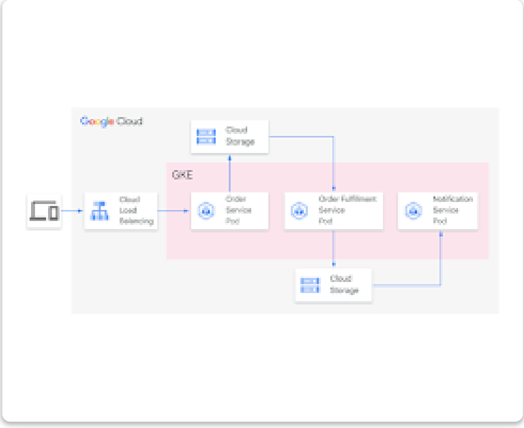
- Order Fulfillment Service (processes the orders)

- Notification Service (notifies the customer when the order is filled)

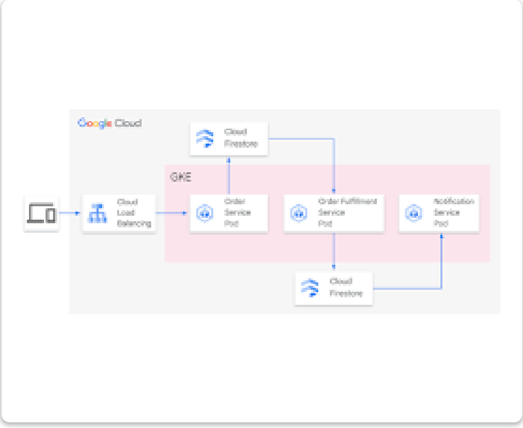
You need to determine how the services will communicate with each other. You want incoming orders to be processed quickly, and you need to collect order information for fulfillment. You also want to make sure orders are not lost between your services and are able to communicate asynchronously. How should the requests be processed?

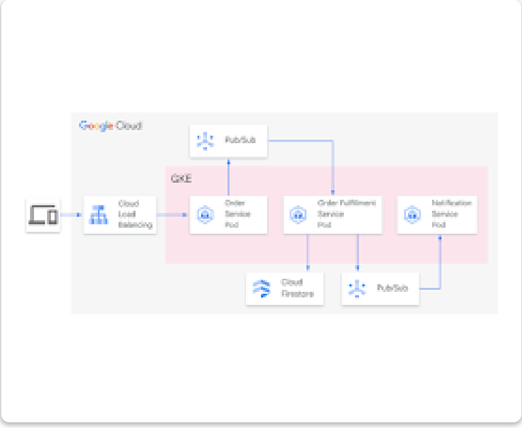


○ A. Order request → Order Service → Order Fulfillment Service → Notification Service



○ B. Order request → Order Service → Cloud Storage bucket → Order Fulfillment Service → Cloud Storage bucket → Notification Service





○ C. Order request → Order Service → Firestore database

● D. Order request → Order Service → Pub/Sub queue → ✓

→ Order Fulfillment Service → Firestore database → Notification Service

Order Fulfillment Service → Firestore database → Pub/Sub queue → Notification Service

Feedback

A is not correct because without using a queuing service, orders may be lost if a service is broken.
B is not correct because it uses a blob storage to trigger events and to store orders. This puts more responsibility on each service to make sure orders are fulfilled, and communication would not be asynchronous.
C is not correct because using a NoSQL DB as a queuing service would not make it asynchronous communication between the services. Some services would have to constantly poll to get new orders.
D is correct because it uses Pub/Sub for inter-service communication which is asynchronous, and Firestore is a NoSQL DB for storing orders.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are developing a Java Web Server that needs to interact with the Cloud Storage API on your users' behalf. Users should be able to authenticate to the Cloud Storage API using their Google identities. Which workflow should you implement in your web application?

○ A. 1. When a user arrives at your application, prompt them for their Google username and password. 2. Store an SHA password hash in your application's database along with the user's username. 3. The application authenticates to the Cloud Storage API using HTTPs requests with the user's username and password hash in the Authorization request header.

● B. 1. When a user arrives at your application, prompt them for their Google username and password. 2. Forward the user's username and password in an HTTPS request to the Google authorization server, and request an access token. 3. The Google server validates the user's credentials and returns an access token to the application. 4. The application uses the access token to call the Cloud Storage API. ✗

○ C. 1. When a user arrives at your application, route them to an Oauth consent screen with a list of requested permissions that prompts the user to sign in with SSO to their Google Account. 2. After the user signs in and provides consent, your application receives an authorization code from a Google server. 3. The Google server returns the authorization code to the user, which is stored in the browser's cookies. 4. The user authenticates to the Cloud Storage API using the authorization code in the cookie.

○ D. 1. When a user arrives at your application, route them to an Oauth consent screen with a list of requested permissions that prompts the user to sign in with SSO to their Google Account. 2. After the user signs in and provides consent, your application receives an authorization code from a Google server. 3. The application requests a Google Server to exchange the authorization code with an access token. 4. The Google server responds with the access token that is used by the application to call the Cloud Storage API.

Correct answer

● D. 1. When a user arrives at your application, route them to an Oauth consent screen with a list of requested permissions that prompts the user to sign in with SSO to their Google Account. 2. After the user signs in and provides consent, your application receives an authorization code from a Google server. 3. The application requests a Google Server to exchange the authorization code with an access token. 4. The Google server responds with the access token that is used by the application to call the Cloud Storage API.

Feedback

A is incorrect because it is not a best practice and discouraged to prompt a user directly for Google credentials.
B is incorrect because it is not a best practice and discouraged to prompt a user directly

for Google credentials.
C is incorrect because the web application needs to interact with the Google API and cannot use client-side credentials to do that from the web server.
D is correct because it accurately describes the OAuth 2.0 flow to authenticate a user to the Cloud Storage API (Reference: https://developers.google.com/identity/protocols/oauth2#scenarios).

https://developers.google.…

✗ You have an application running on GKE. The application is currently using a logging library and is outputting to standard output. You need to export the logs to Cloud Logging, and you need the logs to include metadata about each request. You want to use the simplest method to accomplish this. What should you do?

○ A. Update your application to output logs in JSON format, and add the necessary metadata to the JSON.

● B. Change your application's logging library to the Cloud Logging library, and configure your application to export logs to Cloud Logging. ✗

○ C. Install the Fluent Bit agent on each of your GKE nodes, and have the agent export all logs from /var/log.

○ D. Update your application to output logs in CSV format, and add the necessary metadata to the CSV.

Correct answer

● A. Update your application to output logs in JSON format, and add the necessary metadata to the JSON.

Feedback

A is correct because it's the easiest way to get a rich format into Cloud Logging. GKE automatically forwards logs sent to stdout to Cloud Logging. As long as it has the right JSON format, Cloud Logging will ingest the rich message
B is not correct because it would require a lot of extra work to replace the library, and replicate the extra information (such as pod name) that the GKE logs exporter automatically provides.
C is not correct because this is only needed for pods (normally special/privileged pods) that write directly to the GKE file system.
D is not correct because Cloud Logging doesn't support ingesting CSV.

https://cloud.google.com/… https://cloud.google.com/…

✓ You are a developer at a financial institution. You use Cloud Shell to interact with Google Cloud services. User data is currently stored on an ephemeral disk; however, a recently passed regulation mandates that you can no longer store sensitive information on an ephemeral disk. You need to implement a new storage solution for your user data. You want to minimize code changes. Where should you store your user data?

○ A. Store user data on a Cloud Shell home disk, and log in at least every 120 days to prevent its deletion.

● B. Store user data on a persistent disk in a Compute Engine instance. ✓

○ C. Store user data in a Cloud Storage bucket.

○ D. Store user data in BigQuery tables.

Feedback

A is not correct because the disk might be deleted if the developer is not logging in regularly.
B is correct because it would be the least complex way to achieve the goal.
C is not correct because it would require updating your application.
D is not correct because BigQuery storage is best for relational or JSON data, not unstructured files.

https://cloud.google.com/...

✓ Your team is developing unit tests for Cloud Function code. The code is stored in a Cloud Source Repositories repository. You are responsible for implementing the tests. Only a specific service account has the necessary permissions to deploy the code to Cloud Functions. You want to ensure that the code cannot be deployed without first passing the tests. How should you configure the unit testing process?

○ A. Configure Cloud Build to deploy the Cloud Function. If the code passes the tests, a deployment approval is sent to you.

○ B. Configure Cloud Build to deploy the Cloud Function, using the specific service account as the build agent. Run the unit tests after successful deployment.

○ C. Configure Cloud Build to run the unit tests. If the code passes the tests, the developer deploys the Cloud Function.

● D. Configure Cloud Build to run the unit tests, using the specific service account as the build agent. If the code passes the tests, Cloud Build deploys the Cloud Function. ✓

Feedback

A is not correct since you will not have the necessary permissions to deploy the code without using the specific service account as the Build Agent.
B is not correct since you are deploying the code before testing it.
C is not correct. Even if you are testing all the code, if the developers are responsible for deploying the code, they could deploy code that failed on Cloud Build. Plus, Cloud Build wouldn't have the necessary permissions to deploy the code without using the specific service account as the Build Agent.
D is correct since the same Cloud Build will run the unit tests and deploy the code, ensuring that only the approved code is deployed. Plus, since it is using the specific service account as the build agent, Cloud Build will have the correct permissions.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗

You are deploying a Python application to Cloud Run using Cloud Build. The Cloud Build pipeline is shown below:

```
steps:
  - name: python
    entrypoint: pip
    args: ["install", "-r", "requirements.txt", "--user"]

  - name: 'gcr.io/cloud-builders/docker'
    args: ['build', '-t',
          'us-central1-docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}', '.']

  - name: 'gcr.io/cloud-builders/docker'
    args: ['push', 'us-central1-docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}']

  - name: google/cloud-sdk
    args: ['gcloud', 'run', 'deploy', 'helloworld-${SHORT_SHA}',
           '--image=us-central1-docker.pkg.dev/${PROJECT_ID}/${_REPO_NAME}/myimage:${SHORT_SHA}',
           '--region', 'us-central1', '--platform', 'managed',
           '--allow-unauthenticated']
```

You want to optimize deployment times and avoid unnecessary steps. What should you do?

○ A. Add the --cache-from argument to the Docker build step in your build config file.

○ B. Deploy a new Docker registry in a VPC, and use Cloud Build worker pools inside the VPC to run the build pipeline.

○ C. Store image artifacts in a Cloud Storage bucket in the same region as the Cloud Run instance.

● D. Remove the step that pushes the container to Artifact Registry. ✗

Correct answer

● A. Add the --cache-from argument to the Docker build step in your build config file.

Feedback

A is correct because specifying a cached image is a valid method to speed up subsequent builds (https://cloud.google.com/build/docs/speeding-up-builds#using_a_cached_docker_image)
B is not correct because running Cloud Build with private worker pools in a VPC does not speed up build tasks, specifically not in this case, since neither the code repository nor Cloud Run are hosted in the VPC.
C is not correct because Cloud Run requires container images to be present in a valid Artifact Registry.
D is not correct because Cloud Run requires container images to be present in a valid Artifact Registry.

https://cloud.google.com/… https://cloud.google.com/…

✓ You are planning to add unit tests to your application. You need to be able to assert that published Pub/Sub messages are processed by your subscriber in order. You want the unit tests to be cost-effective and reliable. What should you do?

○ A. Create a topic and subscription for each tester.

○ B. Implement a mocking framework.

● C. Use the Pub/Sub emulator. ✓

○ D. Add a filter by tester to the subscription.

Feedback

A is not correct because you would incur additional costs.
B is not correct because mocking will not simulate Pub/Sub behavior.
C is correct because it enables isolated tests without additional cost.
D is not correct because you would incur additional costs.

https://cloud.google.com/…

✗ Before promoting your new application code to production, you want to conduct testing across a variety of different users. Although this plan is risky, you want to test the new version of the application with production users and you want to control which users are forwarded to the new version of the application based on their operating system. If bugs are discovered in the new version, you want to roll back the newly deployed version of the application as quickly as possible. What should you do?

○ A. Deploy your application on Cloud Run. Use traffic splitting to direct a subset of user traffic to the new version based on the revision tag.

○ B. Deploy your application on Compute Engine. Use Traffic Director to direct a subset of user traffic to the new version based on predefined weights.

○ C. Deploy your application on GKE with Service Mesh. Use traffic splitting to direct a subset of user traffic to the new version based on the user-agent header.

● D. Deploy your application on App Engine. Use traffic splitting to direct a subset of user traffic to the new version based on the IP address. ✗

Correct answer

● C. Deploy your application on GKE with Service Mesh. Use traffic splitting to direct a subset of user traffic to the new version based on the user-agent header.

Feedback

A is not correct because the revision tag is just a Cloud Run label and doesn’t link to users.
B is not correct because the weight split is not flexible and users are chosen randomly.
C is correct because it provides the most control - you can choose which user types are sent to the new version.
D is not correct because with App Engine you only have two options: cookie splitting or IP address, neither of which are flexible, and users are chosen randomly.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://istio.io/latest/docs...

✓ You are responsible for deploying a new API. That API will have three different URL paths:

- *https://yourcompany.com/students*

- *https://yourcompany.com/teachers*

- *https://yourcompany.com/classes*

You need to configure each API URL path to invoke a different function in your code. What should you do?

● A. Create three Cloud Functions as three backend services exposed using an HTTPS load balancer. ✓

○ B. Create one Cloud Function exposed directly.

○ C. Create one Cloud Function as a backend service exposed using an HTTPS load balancer.

○ D. Create three Cloud Functions exposed directly.

Feedback

A is correct since you will need an HTTPS Load Balancer to handle the different paths on a custom domain.
B is not correct since only one entry point is allowed per Cloud Functions.
C is not correct. You must have only one entry point per Cloud Function, so you would need 3 Cloud Functions. However, custom domains are not available on Cloud Functions.
D is not correct since you are not able to have custom domains on Cloud Function, neither paths.

https://cloud.google.com/… https://cloud.google.com/…

✗ You are developing an event-driven application. You have created a topic to receive messages sent to Pub/Sub. You want those messages to be processed in real time. You need the application to be independent from any other system and only incur compute costs when new messages arrive. You want to configure the simplest and most efficient architecture. What should you do?

○ A. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to process new messages in the topic.

● B. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to invoke the Cloud Function. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it. ✗

○ C. Deploy the application on Compute Engine. Use a Pub/Sub push subscription to process new messages in the topic.

○ D. Deploy the application on GKE. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it.

Correct answer

● A. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to process new messages in the topic.

Feedback

A is correct because Cloud Functions with a Pub/Sub trigger will run as soon as a new message arrives (Push) and it will only have a cost if new messages arrive at the topic.
B is not correct. You should use the PubSubMessage present on the request. Using the client library with this approach can lead to duplicated processing.
C is not correct since one of the requirements is to only pay for compute processing time when messages arrive. It's also a more complex approach.
D is not correct since one of the requirements is to only pay for compute processing time when messages arrive. It's also a more complex approach.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ Your team has created an application that is deployed in a single GKE cluster. The application is split into two different Deployments, each with their own Service and accessed using a different HTTP path.

A legacy client running on-premises needs to access the application through Cloud Interconnect through a single IP address. How should you expose the application? (choose two)

□ A. Create a Gateway with the Gateway Class Name: gke-l7-rilb specification.

☑ B. Create a Service with the networking.gke.io/load-balancer-type: "Internal" annotation. ✗

□ C. Create a Service of type LoadBalancer.

☑ D. Create a Service of type NodePort. ✗

□ E. Create a Service with a selector that matches both Deployments.

□ F. Create a HTTPRoute pointing to both Services.

Correct answer

☑ A. Create a Gateway with the Gateway Class Name: gke-l7-rilb specification.

☑ F. Create a HTTPRoute pointing to both Services.

Feedback

A is correct because an internal HTTP load balancer is most suited for HTTP applications that are accessed internally (through the interconnect).
B is not correct because an internal Service can’t do URL-based routing.
C is not correct because a load balancer will be required for each Deployment, resulting in two IPs.
D is not correct because a NodePort will result in a port open across all nodes (x2 for the second Deployment).
E is not correct because selecting both Deployments will cause the client to randomly hit one of the two Deployments.
F is correct because it allows mapping the two Deployments into a single IP according to the path each Deployment runs on. This single frontend will expose a single IP for both Deployments.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://kubernetes.io/doc…

✗ You are developing an application using different microservices that must remain internal to the cluster. You want the ability to configure each microservice with a specific number of replicas. You also want the ability to address a specific microservice from any other microservice in a uniform way, regardless of the number of replicas the microservice scales to. You plan to implement this solution on GKE. What should you do?

○ A. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using a Service, and use the Service DNS name to address it from other microservices within the cluster.

● B. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using an Ingress, and use the Ingress IP address to address the Deployment from other microservices within the cluster. ✗

○ C. Deploy each microservice as a Pod. Expose the Pod in the cluster using a Service, and use the Service DNS name to address the microservice from other microservices within the cluster.

○ D. Deploy each microservice as a Pod. Expose the Pod in the cluster using an Ingress, and use the Ingress IP address to address the Pod from other microservices within the cluster.

Correct answer

● A. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using a Service, and use the Service DNS name to address it from other microservices within the cluster.

Feedback

A Is correct because the Service will have a DNS entry inside the cluster that other microservices can use to address the pods of the Deployment that the Service is targetting.
B Is not correct because an Ingress exposes a Service using an external or internal HTTP(s) load balancer, and it does not apply directly to a Deployment.
C is not correct because a Pod is a single instance of the microservice, whereas a Deployment can be configured with a number of replicas.
D is not correct because it combines the mistakes of options B and C.

https://cloud.google.com/…

✗ Your application is running as a container in a GKE cluster. You need to add a secret to your application using a secure approach that prevents the secret being revealed by calls to the Kubernetes API server. What should you do?

● A. Create a Kubernetes Secret, and pass the Secret as an environment variable to the container. ✗

○ B. Enable GKE Application-layer Secrets Encryption on the cluster using a Cloud Key Management Service (KMS) key.

○ C. Store the Secret in Cloud KMS. Create a Google service account to read the Secret from Cloud KMS. Export the service account key in JSON format, and mount the JSON file on the container as a ConfigMap volume which can read the Secret from Cloud KMS.

○ D. Store the Secret in Secret Manager. Create a Google service account to read the Secret from Secret Manager. Create a Kubernetes service account to run the container. Use Workload Identity to authenticate as the Google service account.

Correct answer

● D. Store the Secret in Secret Manager. Create a Google service account to read the Secret from Secret Manager. Create a Kubernetes service account to run the container. Use Workload Identity to authenticate as the Google service account.

Feedback

A is not correct because a Kubernetes Secret only encodes the string, and anyone who can read the secret will be able to decode it.
B is not correct because GKE Application-layer Secrets Encryption still presents the Secret as a base64-encoded string from the Kubernetes API server.
C is not correct, because Cloud KMS is used to store the encryption keys, not the actual Secret. You are also passing in the Google service account key as a volume, which anyone can read if they can read Secrets.
D is correct because it offers a secure service to store the Secret and also a secure approach to obtaining the Secret with Workload Identity.

https://cloud.google.com/… https://cloud.google.com/…

https://kubernetes.io/doc… https://cloud.google.com/…

✗ You manage a microservices application on GKE using Istio. You secure the communication channels between your microservices by implementing an Istio AuthorizationPolicy, a Kubernetes NetworkPolicy, and mTLS on your GKE cluster. You discover that HTTP requests between two Pods to specific URLs fail, while other requests between the pods to other URLs succeed. What is the cause of the connection issue?

● A. A Kubernetes NetworkPolicy resource is blocking HTTP traffic between the Pods. ✗

○ B. The Pod initiating the HTTP requests is attempting to connect to the target Pod via an incorrect TCP port.

○ C. The AuthorizationPolicy of your cluster is blocking HTTP requests for specific paths within your application.

○ D. The cluster has mTLS configured in permissive mode, but the Pod's sidecar proxy is sending unencrypted traffic in plain text.

Correct answer

● C. The AuthorizationPolicy of your cluster is blocking HTTP requests for specific paths within your application.

Feedback

A is not correct because Kubernetes NetworkPolicy resources allow you to block HTTP traffic between groups of pods but not for selected paths. (https://kubernetes.io/docs/concepts/services-networking/network-policies/).
B is not correct because if the client pod is using an incorrect port to communicate with the server, pod requests will time out for all URL paths.
C is correct because an Istio Authorization policy allows you to block HTTP methods between pods for specific URL paths (https://istio.io/latest/docs/tasks/security/authorization/authz-http/).
D is not correct because mTLS configuration using Istio should not cause HTTP requests to fail. In permissive mode (default configuration), a service can accept both plain text and mTLS encrypted traffic (https://istio.io/latest/docs/tasks/security/authentication/mtls-migration/).

https://istio.io/latest/docs…

https://kubernetes.io/doc…

https://istio.io/latest/docs…

✗ You are developing a microservice-based application that will run on GKE. Some of the services need to access different Google Cloud APIs. How should you set up authentication of these services in the cluster following Google-recommended best practices? (choose two)

☑ A. Use the service account attached to the GKE node. ✗

□ B. Enable Workload Identity on the cluster via the gcloud command-line tool.

□ C. Access the Google service account keys from Secret Manager.

□ D. Store the Google service account keys in Secret Manager.

☑ E. Use gcloud to bind the Google service accounts and the Kubernetes service accounts using roles/iam.workloadIdentityUser. ✓

Correct answer

☑ B. Enable Workload Identity on the cluster via the gcloud command-line tool.

☑ E. Use gcloud to bind the Google service accounts and the Kubernetes service accounts using roles/iam.workloadIdentityUser.

Feedback

A is incorrect. While it could work, all the services are using the same service account, there is no separation of permissions, and no detailed logging.
B and E together connect GKE and Google service accounts, so GKE can authenticate a service with a Google service account.
C is incorrect. While this is feasible, it’s not the recommended practice for workload identity because of the mandatory key rotation of the service accounts.
D is incorrect. While this is feasible, it’s not the recommended practice for workload identity because of the mandatory key rotation of the service accounts.
E and B together connect GKE and Google service accounts, so GKE can authenticate a service with a Google service account.

https://cloud.google.com/…

https://cloud.google.com/…

✓ Your company's product team has a new requirement based on customer demand to autoscale your stateless and distributed service running in a GKE cluster. You want to find a solution that minimizes changes because this feature will go live in two weeks. What should you do?

○ A. Deploy a Vertical Pod Autoscaler, and scale based on the CPU load.

○ B. Deploy a Vertical Pod Autoscaler, and scale based on a custom metric.

● C. Deploy a Horizontal Pod Autoscaler, and scale based on the CPU load. ✓

○ D. Deploy a Horizontal Pod Autoscaler, and scale based on a custom metric.

Feedback

A. Incorrect: This doesn't help with a distributed application.
B. Incorrect: This would work, but would require Cloud Monitoring integration and possible application modification. This would also not apply to a distributed application.
C. Correct: This will require the least number of changes to the code and fits the requirements.
D. Incorrect: This would work, but would require Cloud Monitoring integration and possible application modification.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ Your team is developing an ecommerce platform for your company. Users will log in to the website and add items to their shopping cart. Users will be automatically logged out after 30 minutes of inactivity. When users log back in, their shopping cart should be available. How should you store users' session and shopping cart information while following Google-recommended best practices?

● A. Store the session and shopping cart information in local memory and enable cookie-based session affinity in a global external HTTP(S) load balancer. ✗

○ B. Store the shopping cart information in an object on Cloud Storage where the object name is the session identifier.

○ C. Store the session and shopping cart information in BigQuery.

○ D. Store the session information in Memorystore for Redis, and store the shopping cart information in Firestore.

Correct answer

● D. Store the session information in Memorystore for Redis, and store the shopping cart information in Firestore.

Feedback

A is not correct because local memory is lost on process termination, so you would lose the cart information.
B is not correct because accessing a Cloud Storage bucket is slow and expensive for session information. This is not a Google Cloud best practice.
C is not correct because BigQuery wouldn't be able to handle the frequent updates made to carts and sessions.
D is correct because Memorystore is fast and a standard solution to store session information, and Firestore is ideal for small structured data such as a shopping cart. The user will be mapped to the shopping cart with a new session, if required.

https://cloud.google.com/…

https://cloud.google.com/…

☒ You need to build a public API that authenticates, enforces quotas, and reports metrics for API callers. Which tool should you use to complete this architecture?

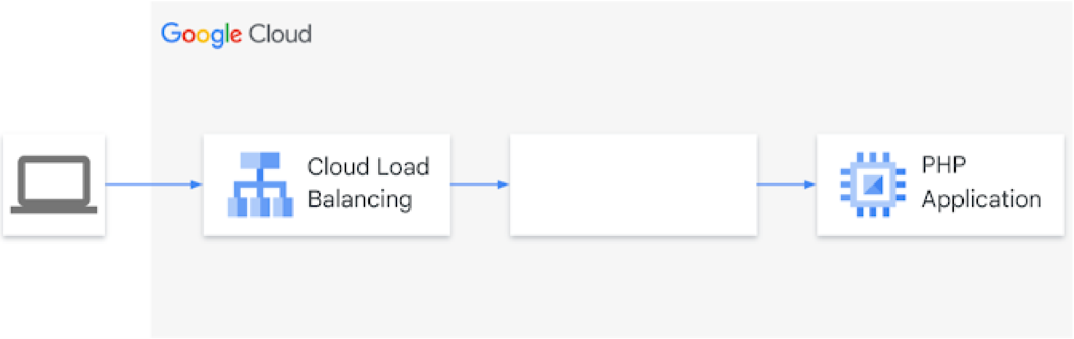


Diagram showing a Google Cloud architecture. An arrow from a “computer” to “Cloud Load Balancing”. An arrow from “Cloud Load Balancing” to an empty box. An arrow from the empty box to “PHP application”.

○ A. Cloud Run

○ B. Cloud Endpoints

● C. Identity-Aware Proxy ☒

○ D. GKE Ingress for HTTP(S) Load Balancing

Correct answer

● B. Cloud Endpoints

Feedback

A is incorrect. Cloud Run provides none of these features.
B is correct. All three features, authentication, quotas/rate limiting and metrics are the core features of Cloud Endpoints.
C is incorrect. IAP provides only authentication.
D is incorrect. GKE Ingress provides none of these features.

https://cloud.google.com/… https://cloud.google.com/…

✗ You recently developed a web application to transfer log data to a Cloud Storage bucket daily. Authenticated users will regularly review logs from the prior two weeks for critical events. After that, logs will be reviewed once annually by an external auditor. Data must be stored for a period of no less than 7 years. You want to propose a storage solution that meets these requirements and minimizes costs. What should you do? (Choose two)

☑ A. Use the Bucket Lock feature to set the retention policy on the data. ✓

☑ B. Run a scheduled job to set the storage class to Coldline for objects older than 14 days. ✗

□ C. Create a JSON Web Token (JWT) for users needing access to the Coldline storage buckets.

□ D. Create a lifecycle management policy to set the storage class to Coldline for objects older than 14 days.

□ E. Create a lifecycle management policy to set the storage class to Nearline for objects older than 14 days.

Correct answer

☑ A. Use the Bucket Lock feature to set the retention policy on the data.

☑ D. Create a lifecycle management policy to set the storage class to Coldline for objects older than 14 days.

Feedback

A is correct because the Bucket Lock feature will enforce the needed retention policy.
B is incorrect because storage classes should be set with a lifecycle management policy.
C is incorrect. JWTs can be used for authentication, but they should not be used to determine object lifecycle.
D is correct because a lifecycle management policy will change the storage class to minimize costs.
E is incorrect because Archive or Coldline storage is more economical than nearline if the data is only accessed annually.

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are developing an application that will store and access objects in a Cloud Storage bucket. To comply with regulatory requirements, you need to ensure that all objects are available for at least 7 years after their initial creation. Objects created more than 3 years ago are accessed very infrequently (less than once a year). You need to configure object storage while ensuring that storage cost is optimized. What should you do? (choose two)

☑ A. Set a retention policy on the bucket with a period of 7 years. ✓

□ B. Include the creation time in the prefix name of the object, and use IAM Conditions to provide only read access to objects within 7 years of the object creation date.

□ C. Enable Object Versioning to prevent objects from being accidentally deleted for 7 years after object creation.

□ D. Create an object lifecycle policy on the bucket that moves objects from Standard Storage to Archive Storage after 3 years.

☑ E. Implement a Cloud Function that checks the age of each object in the bucket and moves the objects older than 3 years to a second bucket with the Archive Storage class. Use Cloud Scheduler to trigger the Cloud Function on a daily schedule. ✗

Correct answer

☑ A. Set a retention policy on the bucket with a period of 7 years.

☑ D. Create an object lifecycle policy on the bucket that moves objects from Standard Storage to Archive Storage after 3 years.

Feedback

A is correct because Cloud Storage provides an option to configure a retention lifecycle rule.
B is incorrect because it is not a recommended way to implement data retention requirements.
C is incorrect because it does not guarantee that objects are not deleted within 7 years after object creation.
D is correct because it's the easiest and recommended way to implement a storage lifecycle policy to move objects from Standard to Archive tier.
E is incorrect because you do not require two buckets to store objects on two storage tiers.

https://cloud.google.com/...

✗ You are developing a web application that will run on Google Cloud. The rate of the incoming user traffic is expected to be unpredictable, with no traffic on most days and large spikes on other days. You need the application to automatically scale up and down, and you need to minimize the cost associated with running the application. What should you do?

○ A. Build the application with Firestore as the database. Deploy the application to Cloud Run.

● B. Build the application with Firestore as the database. Deploy the application to a GKE Standard cluster. ✗

○ C. Build the application with Cloud SQL as the database. Deploy the application to a GKE Autopilot cluster.

○ D. Build the application with Firestore as the database. Deploy the application to a Compute Engine managed instance group with autoscaling.

Correct answer

● A. Build the application with Firestore as the database. Deploy the application to Cloud Run.

Feedback

A is correct. Cloud Run supports scaling to zero. In addition, the cost for Firestore is storage only. So, when there is no traffic, there is zero operational cost.
B is incorrect because GKE doesn't scale to zero.
C is incorrect because GKE doesn't scale to zero). In addition there is a cost associated with running Cloud SQL.
D is incorrect. The Compute Engine manages instances that do not scale to zero. It needs a minimum of one instance to be running.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✓ Your company's development teams want to use various open source operating systems in their container images. When images are published, you need to scan them for Common Vulnerabilities and Exposures (CVEs). The scanning process must not impact software development agility. You want to use managed services where possible. What should you do?

● A. Enable the Container Analysis API to conduct vulnerability scans on images in Artifact Registry. ✓

○ B. Create a Cloud Run service that is triggered on a code check-in and scan the code for CVEs.

○ C. Disallow the use of non-commercially supported base images in your development environment.

○ D. Use Cloud Monitoring to review the output of Cloud Build to determine whether a vulnerable version has been used.

Feedback

A is correct. The Container Analysis API enables image scanning to scan for CVEs from the following sources: Debian, Ubuntu, Alpine, Red Hat Enterprise Edition, and the National Vulnerability Database.
B is incorrect. While this could work, it does not meet the criteria for a managed service
C is incorrect. While this would work, it's counterproductive to an agile software development culture and may impede progress.
D is incorrect. Cloud Monitoring could scan the logs but does not have insight into the Vulnerabilities.

https://cloud.google.com/…

https://cloud.google.com/…

✗

You are configuring a continuous integration pipeline using Cloud Build to automate the build of new container images . The pipeline builds the application from its source code, runs unit and integration tests in separate steps, and pushes the container to Artifact Registry.

The container build file is as follows:

```
FROM python:3.7-alpine
COPY . /app
WORKDIR /app
RUN pip install -r requirements.txt
CMD [ "gunicorn", "-w 4", "main:app" ]
```

You notice that Cloud Build runs are taking longer than expected to complete. You want to decrease the build time. What should you do? (choose two)

☐ A. Select a virtual machine (VM) size with higher CPU for Cloud Build runs.

☐ B. Deploy a Container Registry on a Compute Engine VM in a VPC, and use it to store the final images.

☑ C. Cache the container images for subsequent builds using the --cache-from argument in your build config file. ✓

☐ D. Change the base image in the build file to ubuntu:latest, and install Python 3.7 using a package manager utility.

☑ E. Store application source code on Cloud Storage, and configure the pipeline to use gsutil to download the source code. ✗

Correct answer

☑ A. Select a virtual machine (VM) size with higher CPU for Cloud Build runs.

☑ C. Cache the container images for subsequent builds using the --cache-from argument in your build config file.

Feedback

A is correct because a high-CPU virtual machine type can increase the speed of your build.
B is not correct because a Container Registry on a VM will not speed up the build.
C is correct because the same container is used in subsequent steps for testing and to be pushed to the registry.
D is not correct because an ubuntu container image will be significantly larger than the python:3.7-alpine image.
E is not correct because storing the application source code on Cloud Storage does not decrease the time to build the application.

https://cloud.google.com/… https://cloud.google.com/…

✗ You have developed an application and want to host it on Cloud Run. This application writes log records as text in local files. You want the logs to be written to Cloud Logging while minimizing the amount of code you have to maintain. What should you do?

● A. Import the Cloud Logging library in your code and use it to write logs. ✗

○ B. Use your programming language logger to write logs to Standard output (stdout) and Standard error (stderr) streams.

○ C. Expose the log files to www.mycompany.com/logs. Use a browser to manually download the files and upload them to Cloud Storage.

○ D. Using cron, schedule a job to copy the log files to Cloud Storage once a day.

Correct answer

● B. Use your programming language logger to write logs to Standard output (stdout) and Standard error (stderr) streams.

Feedback

A. This is incorrect. While it's technically possible to use the library, that would result in a lot of code to maintain.
B. This is correct. Cloud Run has direct integration to Cloud Logging via stdout and stderr.
C. This is incorrect. This task would have to be performed manually. Also this approach isn't the most secure.
D. This is incorrect. While data can be copied to Cloud Storage buckets, this doesn't help us with our goal of storing log data within Cloud Logging.

https://cloud.google.com/… https://cloud.google.com/…

✕ You want to migrate an on-premises container running in Knative to Google Cloud. You need to make sure that the migration doesn't affect your application's deployment strategy, and you want to use a fully managed service. Which Google Cloud service should you use to deploy your container?

○ A. Cloud Run

○ B. Compute Engine

● C. GKE ✕

○ D. App Engine flexible environment

Correct answer

● A. Cloud Run

Feedback

A. Correct: Cloud Run utilizes the Knative Serverless Framework and gives you the flexibility to run your workloads in any Knative supported cluster.
B. Incorrect: Using Compute Engine would mean that you are installing and maintaining GKE and Knative manually and the overhead would change the deployment strategy.
C. Incorrect: With GKE you still need to manage the worker nodes and it's not a fully managed service. Also you will need to perform heavy changes to your application deployment strategy.
D. Incorrect: While the App Engine Flexible environment can run containers, you will need to perform heavy changes to your application deployment strategy.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You have two Google Cloud projects - Project A and Project B. You need to create a Cloud Function in Project A that saves its output in a Cloud Storage bucket in Project B. You want to follow the principle of least privilege. What should you do?

● A. 1. Create a Google service account in Project B. 2. Assign this service account the roles/storage.objectCreator role on the storage bucket residing in Project B. 3. Deploy the Cloud Function in Project A using the service account from Project B. ✗

○ B. 1. Create a Google service account in Project A. 2. Assign this service account the roles/storage.objectCreator role on the storage bucket residing in Project B. 3. Deploy the Cloud Function using the service account from Project A.

○ C. 1. Determine the default App Engine service account (PROJECT_ID@appspot.gserviceaccount.com) in Project A. 2. Assign the default App Engine service account the roles/storage.objectCreator role on the storage bucket residing in Project B. 3. Deploy the Cloud Function using the default App Engine service account in Project A.

○ D. 1. Determine the default App Engine service account (PROJECT_ID@appspot.gserviceaccount.com) in Project B. 2. Assign the default App Engine service account the roles/storage.objectCreator role on the storage bucket residing in Project B. 3. Deploy the Cloud Function using the default App Engine service account in Project A.

Correct answer

● B. 1. Create a Google service account in Project A. 2. Assign this service account the roles/storage.objectCreator role on the storage bucket residing in Project B. 3. Deploy the Cloud Function using the service account from Project A.

Feedback

A is not correct because you cannot run a Cloud Function with a service account that is not in the same Google Cloud project.
B is correct because it follows the least privilege principle and for a Cloud Function, the service account must be created in the same project where the function is getting executed.
C is not correct, because it doesn't follow the least privilege principle and you could inadvertently give access to an App Engine application write access to your storage bucket.
D is not correct, it doesn't follow the least privilege principle and it's not possible since the service account is not in the same project where the Cloud Function is getting executed.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/...

✕ You are deploying your application on a GKE instance that communicates with Cloud SQL. You will use Cloud SQL Auth Proxy to allow your application to communicate to the database using the service account associated with the application's instance. You want to follow the principle of least privilege for the role assigned to the service account. What should you do?

● A. Assign the Project Editor role. ✕

○ B. Assign the Project Owner role.

○ C. Assign the Cloud SQL Client role.

○ D. Assign the Cloud SQL Editor role.

Correct answer

● C. Assign the Cloud SQL Client role.

Feedback

A is incorrect because the service account only needs to connect to Cloud SQL and the Google-recommended best practice is to provide the least amount of access required.
B is incorrect because the service account only needs to connect to Cloud SQL and the Google-recommended best practice is to provide the least amount of access required.
C is correct because the Cloud SQL Client role provided the minimum access required to connect to Cloud SQL.
D is incorrect because the service account only needs to connect to Cloud SQL and the Google-recommended best practice is to provide the least amount of access required.

https://cloud.google.com/... https://cloud.google.com/...

https://cloud.google.com/... https://cloud.google.com/...

✓ You recently developed an application. You need to call the Cloud Storage API from a Compute Engine instance that doesn't have a public IP address. What should you do?

○ A. Use Carrier Peering

○ B. Use VPC Network Peering

○ C. Use Shared VPC networks

● D. Use Private Google Access ✓

Feedback

A is not correct because Carrier Peering enables you to access Google applications, such as Google Workspace, by using a service provider to obtain enterprise-grade network services that connect your infrastructure to Google.
B is not correct because VPC Network Peering enables you to peer VPC networks so that workloads in different VPC networks can communicate in a private RFC 1918 space. Traffic stays within Google's network and doesn't traverse the public internet.
C is not correct because Shared VPC allows an organization to connect resources from multiple projects to a common VPC network so that they can communicate with each other securely and efficiently using internal IPs from that network.
D is correct because Private Google Access is an option available for each subnetwork. When it is enabled, instances in the subnetwork can communicate with public Google API endpoints even if the instances don't have external IP addresses.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗ Your application performs well when tested locally, but it runs significantly slower after you deploy it to a Compute Engine instance. You need to diagnose the problem with the least number of changes. What should you do?

○ A. File a ticket with Cloud Support indicating that the application performs faster locally.

● B. Use Cloud Debugger snapshots to look at a point-in-time execution of the application. ✗

○ C. Use Cloud Profiler to determine which functions within the application take the longest amount of time.

○ D. Add logging commands to the application and use Cloud Logging to check where the latency problem occurs.

Correct answer

● C. Use Cloud Profiler to determine which functions within the application take the longest amount of time.

Feedback

A is incorrect because the argument "it worked on my machine" but doesn't work on Google Cloud is never valid.
B is incorrect because Debugger snapshots only lets us review the application at a single point in time.
C is correct because it provides latency per function and historical latency information.
D is incorrect because while it works it requires a lot of work and is not the clear, optimal choice.

https://cloud.google.com/…

✓ You are developing an ecommerce web application that uses Cloud Run and Memorystore for Redis. When a user logs into the app, the application caches the user’s information (e.g., session, name, address, preferences), which is stored for quick retrieval during checkout. While testing your application in a browser, you get a 502 Bad Gateway error. You have determined that the application is not connecting to Memorystore. What is the reason for this error?

○ A. Your Memorystore for Redis instance was deployed without a public IP address.

● B. You configured your Serverless VPC Access connector in a different region than your Cloud Run service. ✓

○ C. The firewall rule allowing a connection between Cloud Run and Memorystore was removed during an infrastructure update by the DevOps team.

○ D. You configured your application to use a Serverless VPC Access connector on a different subnet in a different region than your Cloud Run service.

Feedback

A is not correct because Cloud Run connects to Memorystore via the Serverless VPC Connector. Connections are over private networks. Public addresses are not required.
B is correct. All of the components must be in the same region.
C is not correct because for connectivity between Cloud Run and Memorystore all that is required is a Serverless VPN Connector.
D is not correct. The Serverless VPC Connector is configured with a non-overlapping subnet that is not associated with the VPC.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✓ Your organization has recently begun an initiative to replatform their legacy applications onto GKE. You need to decompose a monolithic application into microservices. Multiple instances have read and write access to a configuration file, which is stored on a shared file system. You want to minimize the effort required to manage this transition, and you want to avoid rewriting the application code. What should you do?

○ A. Create a new Cloud Storage bucket, and mount it via FUSE in the container.

○ B. Create a new persistent disk, and mount the volume as a shared PersistentVolume.

● C. Create a new Filestore instance, and mount the volume as an nfs PersistentVolume. ✓

○ D. Create a new ConfigMap and volumeMount to store the contents of the configuration file.

Feedback

A is incorrect, because Cloud Storage FUSE does not support concurrency and file locking.
B is incorrect, because a persistent disk PersistentVolume is not read-write-many. It can only be read-write once or read-many.
C is correct, because it’s the only managed, supported read-write-many storage option available for file-system access in GKE.
D is incorrect, because the ConfigMap cannot be written to from the Pods.

https://kubernetes.io/doc…

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are configuring logging for a Cloud Run service that is in development. Your container instance writes structured logs to standard output (stdout) and standard error (stderr) streams. You want to correlate the automatically created request logs with your container logs. What should you do?

○ A. Instrument your application to submit traces to Cloud Trace.

● B. Use Snapshot Debugger to add logpoints with randomly generated unique identifiers for each request. ✗

○ C. Add the logging.googleapis.com/trace field to your log statements with the X-Cloud-Trace-Context header value.

○ D. Add the logging.googleapis.com/labels field to your log statements with a randomly generated unique identifier for each request.

Correct answer

● C. Add the logging.googleapis.com/trace field to your log statements with the X-Cloud-Trace-Context header value.

Feedback

A is not correct because Cloud Trace is for inspecting latency data
B is not correct because it adds temporary logging that remains active for up to 24 hours.
C is correct because it will create a “parent-child” relationship in Logs Explorer.
D is not correct because it will not relate the container logs to the automatically generated request logs. logging.googleapis.com/labels is primarily for user-generated structured logs and there is no corresponding element in the container logs to correlate.

https://cloud.google.com/… https://cloud.google.com/…

✗ You need to redesign the ingestion of audit events from your authentication service to allow it to handle a large increase in traffic. Currently, the audit service and the authentication service run in the same Compute Engine virtual machine. You plan to split each service into their own pool of Compute Engine VM instances and use Pub/Sub to send events from the authentication service to the audit service.

How should you set up the Pub/Sub topics and subscriptions to ensure that the system can handle a large volume of messages and can scale efficiently?

○ A. Create one Pub/Sub topic. Create one pull subscription.

○ B. Create one Pub/Sub topic. Create one pull subscription per audit service instance.

○ C. Create one Pub/Sub topic. Create one push subscription.

○ D. Create one Pub/Sub topic per authentication service instance. Create one pull subscription per topic.

● E. Create one Pub/Sub topic per authentication service instance. Create one push subscription per topic. ✗

Correct answer

● A. Create one Pub/Sub topic. Create one pull subscription.

Feedback

A is correct. This is the most flexible way to scale, allowing the authentication and audit services to be sized independently according to load.
B is incorrect. This will cause messages to be duplicated, one copy per subscription.
C is incorrect. This will allow the system to scale, but push subscriptions are less suited to handle large volumes of messages.
D is incorrect. This will allow the system to scale, however each audit service will listen to all subscriptions.
E. is incorrect. This will allow the system to scale, however it will require each audit service to listen to all subscriptions. Also push subscriptions are less suited to handle large volumes of messages.

https://cloud.google.com/…

✗

You are in the final stage of migrating an on-premises data center to Google Cloud. You are quickly approaching your deadline, and discover that a web API is running on a server slated for decommissioning. You need to recommend a solution to modernize this API while migrating to Google Cloud. The modernized web API must meet the following requirements:

- Autoscales during high traffic periods at the end of each month
- Written in Python 3.x
- Developers must be able to rapidly deploy new versions in response to frequent code changes

You want to minimize cost, effort, and operational overhead of running the service. What should you do?

○ A. Modernize and deploy the code on App Engine flexible environment.

○ B. Modernize and deploy the code on Cloud Run.

○ C. Deploy the modernized application to an n1-standard-1 Compute Engine instance.

● D. Ask the development team to rewrite the application to run as a container on GKE. ✗

Correct answer

● B. Modernize and deploy the code on Cloud Run.

Feedback

A is not correct. While this approach meets all of the requirements, it’s not the lowest cost one. With App Engine Flexible there is always at least one instance online.
B is correct. Cloud Run meets all of the requirements. It;s pay as you go designed to autoscale from 0-x instances, and has deployments that take seconds versus minutes.
C is not correct. While this is a solution, it does not meet all of the requirements. A single instance would not scale automatically. Finally, to accomplish all of the requirements it would require additional effort and ongoing server administration, setup, etc.
D is not correct. While this does meet all of the requirements, it’s not the lowest cost one nor the least effort.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✗ You are developing an application using a new programming language that does not have support for Cloud Client Libraries. Your application makes REST API calls to invoke Google Cloud services. The application runs on Cloud Run with an associated service account. You want to configure this service account to act as the authorization identity for the Google Cloud service calls. What should you do?

○ A. Include an API key with the application and pass the value in the Authorization header.

○ B. Retrieve the access token from the metadata server and pass the value in the Authorization header.

○ C. Use an API key for the service account as the value of the GOOGLE_APPLICATION_CREDENTIALS environment variable.

● D. Store the value for gcloud auth application-default print-access-token at startup in a file whose path is set in the GOOGLE_APPLICATION_CREDENTIALS environment variable. ✗

Correct answer

● B. Retrieve the access token from the metadata server and pass the value in the Authorization header.

Feedback

A is not correct because an API key is not the same as an authorization token and would not be honored if passed in the Authorization header of an HTTP request.
B is correct because the access token retrieved from the metadata server and passed in the Authorization header of an HTTP request to Google Cloud will be successful to present authentication as the service account.
C is not correct because GOOGLE_APPLICATION_CREDENTIALS should be set to the name of a file that contains the access token, not the value of an API key.
D is not correct because GOOGLE_APPLICATION_CREDENTIALS is used to point to a file containing an API key, not an access token.

https://developers.google.... https://cloud.google.com/...

https://cloud.google.com/...

✓ You are creating a web application designed to run on a Google Cloud runtime that writes a file to the user's Drive regardless of their account domain. You need to configure the application to authenticate to the Google Drive API. What should you do?

○ A. Use an OAuth Client ID with delegated domain-wide authority.

○ B. Use a service account with delegated domain-wide authority.

● C. Use an OAuth Client ID and https://www.googleapis.com/auth/drive.file scope to obtain an access token for each user. ✓

○ D. Use a service account and https://www.googleapis.com/auth/drive.file scope to generate a signed JSON Web Token (JWT).

Feedback

A is incorrect. OAuth Client IDs can't be granted domain-wide authority.
B is incorrect. This wouldn't work for all users (only users on domains that have granted it delegated domain-wide authority.)
C is correct. OAuth 2.0 web authorization will work with any user, while domain delegation only works for a single domain
D is incorrect. This wouldn't be writing to the user's drive. Also signed JWTs can't be used to authenticate to the Drive API.

https://developers.google....

✗ Your team is responsible for maintaining an application that aggregates news articles from many different sources. Your monitoring dashboard contains publicly accessible real-time reports and runs on a Compute Engine instance as a web application. External stakeholders and analysts need to access these reports via a secure channel without authentication. How should you configure this secure channel?

○ A. Use the service account key of the instance to encrypt the traffic.

○ B. Use Cloud Scheduler to trigger Cloud Build every hour to create an export from the reports. Store the reports in a public Cloud Storage bucket.

● C. Add an HTTP(S) load balancer in front of the monitoring dashboard. Configure Identity-Aware Proxy to secure the communication channel. ✗

○ D. Add an HTTP(S) load balancer in front of the monitoring dashboard. Set up a Google-managed SSL certificate on the load balancer for traffic encryption.

Correct answer

● D. Add an HTTP(S) load balancer in front of the monitoring dashboard. Set up a Google-managed SSL certificate on the load balancer for traffic encryption.

Feedback

A is incorrect. A service account cannot be used to encrypt HTTPS traffic.
B is incorrect. Periodical export would not meet the real-time requirement.
C is incorrect. IAP is not securing the communication channel, it authenticates the user. Technically Cloud Load Balancing already secures the channel but without an appropriate certificate.
D is correct. This provides an external HTTPS endpoint, and uses Google-managed services and a valid SSL certificate.

https://cloud.google.com/…

✗ Your team has developed a mobile web application where global users vote on popular topics. For each topic, you expect a very high volume of votes during each individual 30-minute voting window. You need to capture and count each topic's votes within every 30 minute window. You also need to store the votes for future analysis and reporting. What should you do?

○ A. Save the votes to Memorystore, and use Cloud Functions to insert the counts into BigQuery. Display the results in Google Data Studio.

○ B. Publish the votes to Pub/Sub, and use a Datafow pipeline to insert the counts and votes into BigQuery. Display the results in Google Data Studio.

● C. Publish the votes to Pub/Sub, and use Cloud Functions to insert the counts and votes into Cloud Storage. Display the results in Google Data Studio. ✗

○ D. Use Firebase to authenticate the mobile users, and publish the votes directly to Firestore. Export the votes to a CSV file, and import it into Sheets for reporting.

Correct answer

● B. Publish the votes to Pub/Sub, and use a Datafow pipeline to insert the counts and votes into BigQuery. Display the results in Google Data Studio.

Feedback

A. Incorrect. Memorystore is not a persistent data store and can potentially lose votes cast.
B. Correct. Pub/Sub supports the ingestion of millions of records per second and guarantees the delivery of the messages. Dataflow can aggregate votes within windows grouped by Topic. BigQuery should be used for analysis.
C. Incorrect. Windowing and grouping with Cloud Functions requires storing state in an intermediary datastore. Also storing the raw data in a blob store makes analysis with Data Studio inefficient.
D. Incorrect. There are limits to the grouping and analysis operations that Google Sheets can perform.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✗

Your team manages a web application that currently stores user session information in an on-premises PostgreSQL database. Your team decided to leave the database on-premises and migrate the web application to Google Cloud. You detected high latency after the migration. You need to conduct a few quick tests to collect data points and then provide suggestions to your Tech Lead to improve performance and make sure it's a cost-effective solution.

- First, you want to migrate the database to Google Cloud without changing the schema to see whether the latency is diminished.
- Next, you want to evaluate replacing PostgreSQL with a cloud managed NoSQL database to store user session information.

You want to use managed services and quickly gather your data points. What should you do?

○ A. Migrate the database to Cloud SQL. Then import the data into Cloud Storage.

○ B. Migrate the database to BigQuery. Then import the data into Firestore in Native mode.

○ C. Migrate the database to Cloud SQL. Then import the data into Firestore in Native mode.

● D. Create a Compute Engine virtual machine instance in Google Cloud, and install PostgreSQL and MongoDB Server software. Migrate the database to the new PostgreSQL, and then migrate the data to MongoDB. ✗

Correct answer

● C. Migrate the database to Cloud SQL. Then import the data into Firestore in Native mode.

Feedback

A is incorrect. Cloud Storage is not an effective NoSQL database for user session information.
B is incorrect. BigQuery is a data warehouse. It has limited update/delete capabilities for inserted rows and hence is a bad choice for user session data, which changes as the session with the user progresses.
C is correct. Cloud SQL is the managed PostgreSQL database and migration will not require any schema changes. Firestore in Native mode is recommended for storing user-session information and is a natural choice for this test.
D is incorrect. This doesn't use any managed service and will increase testing time since it will require database server management.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✓ You have written a Cloud Function in Node.js with source code stored in a Git repository. You want any committed changes to the source code to be automatically tested. You write a Cloud Build configuration that pushes the source code to a uniquely named Cloud Function, then calls the function as a test, and then deletes the Cloud Function as cleanup. You discover that if the test fails, the Cloud Function is not deleted. What should you do?

○ A. Change the order of the steps to delete the Cloud Function before performing the test.

○ B. Include a waitFor option in the Cloud Build step that deletes the Cloud Function test step as a required preceding step.

● C. Have the Cloud Build step write the Cloud Function results to a file and return 0. Add a step after the Cloud Function deletion that checks whether the file contains the expected results and fails if it doesn't. ✓

○ D. Have the Cloud Build test step set its outcome in an environment variable called result and return 0. Add a final step after the Cloud Function deletion that checks whether the environment variable contains the expected results.

Feedback

A is incorrect because if you delete a Cloud Function you cannot test it.

B is incorrect. The Cloud Build waitFor is used to synchronize steps. If a step identifies a previous step in a waitFor and the previous step fails then the Cloud Build as a whole will fail and the function won't be deleted.

C is correct. There is a persistent file system that is shared between steps in a Cloud Build, so the correct steps should be:
1. Deploy the Cloud Function.
2. Save the results of calling the Cloud Function to a file.
3. Delete the Cloud Function.
4. Test the content of the file.
Since step 2 can now never fail, step 3 is executed, and step 4 defines the outcome of the build as a whole.

D is incorrect. Environment variables exist locally in the container in which the step executes. When the step completes, the container is destroyed and takes its environment variables with it. These variables are thus not available in subsequent steps and hence can't be used as a communication between distinct steps.

https://cloud.google.com/...

https://cloud.google.com/...

https://cloud.google.com/...

✓ You have deployed a web application in a GKE cluster. You are reviewing the Cloud Monitoring metrics and find that your cluster’s CPU load fluctuates throughout the day. To maximize performance while minimizing cost, you want the number of pods and notes to automatically adjust. What should you do?

○ A. Modify the managed instance group (MIG) to enable Autoscaling to configure max and min amount of nodes based on CPU load.

● B. Enable Cluster Autoscaler on the GKE cluster, and configure the Horizontal Pod Autoscaler (HPA) to autoscale the workload based on CPU load. ✓

○ C. Enable Cluster Autoscaler on the GKE cluster, and configure the HPA to autoscale the workloads based on a custom metric.

○ D. Modify the MIG to enable Autoscaling to configure max and min amount of nodes based on CPU load, and configure the Vertical Pod Autoscaler (VPA) to scale workloads based on CPU load.

Feedback

A is not correct because you should not use Compute Engine's autoscaling feature on instance groups created by GKE.
B is the recommended approach to autoscale a Kubernetes Deployment.
C is not correct because CPU metrics are enabled by default and custom metrics are unnecessary.
D is not correct because you should not use Compute Engine's autoscaling feature on instance groups created by GKE.

https://cloud.google.com/…

https://cloud.google.com/…

https://cloud.google.com/…

✓ You have a Java application running on Cloud Run. Your application's error messages do not appear in the Error Reporting console. What should you do?

○ A. Ensure that Cloud Monitoring client libraries are bundled with the Java application.

○ B. Verify that application logs are being written to the correct regional storage bucket.

● C. Verify that application errors are being written to stderr. ✓

○ D. Log exceptions using System.out.println.

Feedback

A is not correct because no external libraries are required for error reporting in Cloud Run.
B. is not correct because Error Reporting does not analyze logs stored in regional log buckets or logs routed to other projects.
C is correct because errors must be written to stderr in Cloud Run to be recognized by Error Reporting.
D is not correct because system.out.println outputs to stdout, not stderr.

https://cloud.google.com/…

https://cloud.google.com/…

✗ You are analyzing your application’s performance. You observe that certain Cloud Bigtable tables in your cluster are used much more than others, causing inconsistent application performance for end users. You discover that some tablets have large sections of similarly named row keys and are heavily utilized, while other tablets are running idle. You discover that a user’s ZIP code is the first component of the row key, and your application is being heavily used by profiles originating from that ZIP code. You want to change how you generate row keys so that they are human readable and so that Cloud Bigtable demand is more evenly distributed within the cluster. What should you do?

● A. Use serially generated integer values. ✗

○ B. Use a subset of the MD5 hash of the row contents.

○ C. Use a concatenation of multiple human-readable attributes.

○ D. Use UNIX epoch-styled timestamps represented in milliseconds.

Correct answer

● C. Use a concatenation of multiple human-readable attributes.

Feedback

A is not correct because, depending on the distribution of the underlying values, serially generated integer values may lead to hotspotting.
B is not correct because this is no longer a recommended best practice: it makes it difficult to troubleshoot issues.
C is correct because using a sufficient number of delimited attributes can provide sufficient spreading.
D Is not correct because timestamps are poor candidates for row keys, and in this case inadvertently lead to ID collisions if multiple updates happening in the same millisecond execute in close succession.

https://cloud.google.com/...

https://cloud.google.com/...

✗ Your company has a successful multi-player game that has become popular in the US. Now, it wants to expand to other regions. It is launching a new feature that allows users to trade points. This feature will work for users across the globe. Your company's current MySQL backend is reaching the limit of the Compute Engine instance that hosts the game. Your company wants to migrate to a different database that will provide global consistency and high availability across the regions. Which database should they choose?

○ A. BigQuery

● B. Cloud SQL ✗

○ C. Cloud Spanner

○ D. Cloud Bigtable

Correct answer

● C. Cloud Spanner

Feedback

A is not correct because BigQuery can't be used as a transactional database.
B is not correct because Cloud SQL doesn't provide high availability across regions.
C is correct because only Cloud Spanner provides global consistency and availability.
D is not correct because Cloud Bigtable doesn't provide global availability.

✓ Your company plans to expand their analytics use cases. One of the new use cases requires your data analysts to analyze events using SQL on a near real–time basis. You expect rapid growth and want to use managed services as much as possible. What should you do?

● A. Create a Pub/Sub topic and a subscription. Stream your events from the source into the Pub/Sub topic. Leverage Dataflow to ingest these events into BigQuery. ✓

○ B. Create a Pub/Sub topic and a subscription. Stream your events from the source into the Pub/Sub topic. Leverage Dataflow to ingest these events into Cloud Storage.

○ C. Create a Pub/Sub topic and a subscription. Stream your events from the source into the Pub/Sub topic. Leverage Dataflow to ingest these events into Firestore in Datastore mode.

○ D. Create a Kafka instance on a large Compute Engine instance. Stream your events from the source into a Kafka pipeline. Leverage Dataflow to ingest these events into Cloud Storage.

Feedback

A is correct because all three products involved can scale to significant volumes, and writing the data to BigQuery allows for immediate analysis via SQL.
B is not correct because Cloud Storage is not ideal for inserting individual events and analyzing them via SQL.
C Is not correct because Firestore in Datastore mode is not ideal for inserting individual events and analyzing them.
D is not correct because this solution doesn't provide a fully managed solution.

https://cloud.google.com/… https://cloud.google.com/…

✓ Your application that is deployed on Cloud Run receives a large amount of traffic. You are concerned that deploying changes to the application could affect all users negatively. You want to avoid full-scale load testing due to cost concerns, but you still want to deploy new features as quickly as possible. Which approach should you take?

○ A. Schedule weekly load tests against the production application.

○ B. Use the local development environment to perform load testing outside Google Cloud.

○ C. Before allowing users to access new features, deploy as a new version and perform smoke tests. Then enable all users to access the new features.

● D. Use traffic splitting to have a smaller part of the users test out new features, and slowly adjust traffic splitting until all users get the new features. ✓

Feedback

A is incorrect because there are patterns to perform A/B testing and reduce the need for regular independent load tests.
B is incorrect because it does not accurately simulate the production environment.
C is incorrect because smoke tests are still exposing all users to new features immediately as described.
D is correct because traffic splitting allows real user testing without impacting all users and reduces load testing costs.

https://cloud.google.com/…

✗ Your website is deployed on Compute Engine. Your marketing team wants to test conversion rates between three different website designs. You are not able to make changes to your application code. What should you do?

○ A. Deploy website on Cloud Run and use traffic splitting.

○ B. Deploy website on Cloud Run as three separate revisions.

○ C. Deploy website on Cloud Functions as three separate functions.

● D. Deploy website on Cloud Functions and implement custom code to show different designs. ✗

Correct answer

● A. Deploy website on Cloud Run and use traffic splitting.

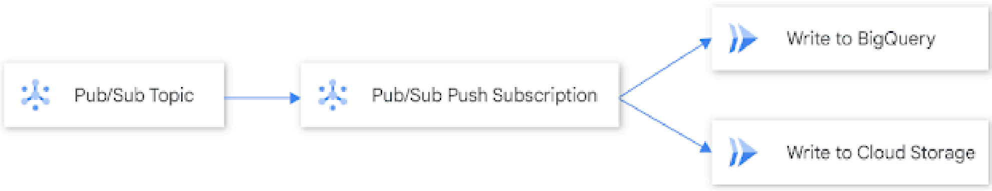
Feedback

A is correct because it allows routing traffic to a single domain and split traffic based on percentages.
B is not correct because the domain name will change based on the revision.
C and D are not correct because Cloud Functions cannot be used to deploy websites.

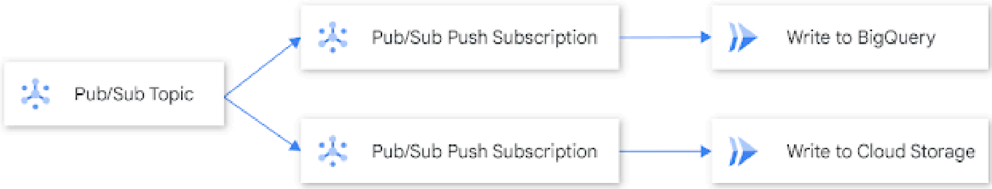
https://cloud.google.com/…

✗ Your team is using Cloud Run to write every Pub/Sub message to both a Cloud Storage object and a BigQuery table. You want to minimize operational overhead. Which architecture should you implement?

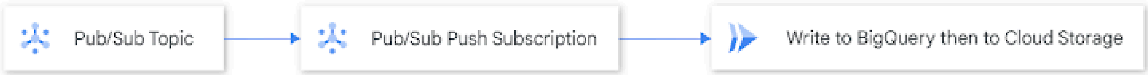
A. One topic, 1 subscription, 2 Cloud Run services



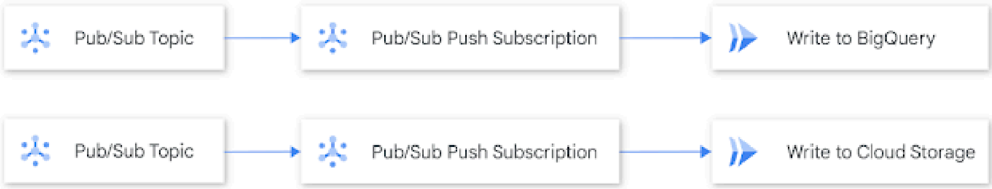
B. One topic, 2 subscriptions, 2 Cloud Run services



C. One topic, 1 Cloud Run service, 1 push subscription


Pub/Sub Topic
Pub/Sub Push Subscription
Write to BigQuery then to Cloud Storage

D. Two topics, 2 subscriptions, 2 Cloud Run services



● A. ✗

○ B.

○ C.

○ D.

Correct answer

● B.

Feedback

A is not correct because this will write half the messages to BigQuery and half to Cloud Storage, which doesn't meet the need.
B is correct because each App Engine service will get its own message to write and can retry/fail independently.
C is not correct because a failure in processing the message to one system can cause duplicate writes to BigQuery or Google Cloud Storage.
D is not correct because it duplicates the message send charges and requires that the message be sent twice to two different topics, which increases costs, the need to manage an additional topic and complexities on the client.

https://cloud.google.com/… https://cloud.google.com/…

✗ You are capturing important audit activity in Cloud Logging. You need to read the information from Cloud Logging to perform near real-time analysis of the logs. You will have multiple processes performing different types of analysis on the logging data. What should you do?

○ A. Write an app to read the logs directly from the Cloud Logging API.

○ B. Set up a Cloud Logging sink to Pub/Sub, and read the logs from a Pub/Sub topic.

● C. Write a Cloud Function endpoint to read directly from the Cloud Logging API, and copy the logs over to Dataproc. ✗

○ D. Set up a Cloud Logging sink to Cloud Storage, and read the logs from a Cloud Storage bucket.

Correct answer

● B. Set up a Cloud Logging sink to Pub/Sub, and read the logs from a Pub/Sub topic.

Feedback

A is not correct because the API has read limits and is not a suitable solution if you have multiple readers. (https://cloud.google.com/logging/quotas)
B is correct because this solution is near real time.
(https://cloud.google.com/logging/docs/export/using_exported_logs#pubsub-availability)
C is not correct because it is not an efficient solution.
(https://cloud.google.com/dataproc/docs/concepts/jobs/life-of-a-job
D is not correct because this solution is not real time.
(https://cloud.google.com/logging/docs/export/using_exported_logs#gcs-availability)

✓ You are writing an API endpoint to process orders from a web application and save the data into a collection in Firestore in Datastore mode. During application testing, you notice that when your application encounters an HTTP 5xx server error from the Datastore API, it catches this error and returns an HTTP 200 OK response code to the client, but does not store the data within Datastore. You want the consumers of your API endpoint to know that the write request was unsuccessful. What should you do?

○ A. Return an HTTP 204 No Content response.

○ B. Return an HTTP 406 Not Acceptable response.

● C. Return an HTTP 500 Internal Server Error response. ✓

○ D. Retry the Datastore API with exponential backoff until Firestore returns a HTTP 2xx response.

Feedback

A is not correct because 2xx codes indicate a success from the server.
B is not correct because 406 is sent specifically when a request's accept header is unfulfillable by the server.
C is correct because a 500-class response clearly communicates to clients that the API call was unsuccessful, and the client can re-submit independently.
D is not correct because it is unbounded as to when the Datastore API might respond with a non-500 class response.

https://www.restapitutoria…