



**"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."**

**[www.atmicnetworks.com](http://www.atmicnetworks.com)**

Warning: Keep connected with our support team for latest updates

### Question: 1

HipLocal's .net-based auth service fails under intermittent load. What should they do?

- A. Use App Engine for autoscaling.
- B. Use Cloud Functions for autoscaling.
- C. Use a Compute Engine cluster for the service.
- D. Use a dedicated Compute Engine virtual machine instance for the service.

**Answer: D**

Explanation:

Reference: <https://www.qwiklabs.com/focuses/611?parent=catalog>

### Question: 2

HipLocal's APIs are showing occasional failures, but they cannot find a pattern. They want to collect **SOME** metrics to help them troubleshoot.

What should they do?

- A. Take frequent snapshots of all of the VMs.
- B. Install the Stackdriver Logging agent on the VMs.
- C. Install the Stackdriver Monitoring agent on the VMs.
- D. Use Stackdriver Trace to look for performance bottlenecks.

**Answer: C**

Explanation:

### Question: 3

HipLocal has connected their Hadoop infrastructure to GCP using Cloud Interconnect in order to query data stored on persistent disks.

Which IP strategy should they use?

- A. Create manual subnets.
- B. Create an auto mode subnet.
- C. Create multiple peered VPCs.
- D. Provision a single instance for NAT.

**Answer: A**

Explanation:

### Question: 4

Which service should HipLocal use to enable access to internal apps?

- A. Cloud VPN
- B. Cloud Armor
- C. Virtual Private Cloud
- D. Cloud Identity-Aware Proxy

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/iap/docs/cloud-iap-for-on-prem-apps-overview>

### Question: 5

HipLocal wants to reduce the number of on-call engineers and eliminate manual scaling.

Which two services should they choose? (Choose two.)

- A. Use Google App Engine services.
- B. Use serverless Google Cloud Functions.
- C. Use Knative to build and deploy serverless applications.
- D. Use Google Kubernetes Engine for automated deployments.
- E. Use a large Google Compute Engine cluster for deployments.

**Answer: BC**

Explanation:

### Question: 6

In order to meet their business requirements, how should HipLocal store their application state?

- A. Use local SSDs to store state.
- B. Put a memcache layer in front of MySQL.
- C. Move the state storage to Cloud Spanner.
- D. Replace the MySQL instance with Cloud SQL.

**Answer: B**

Explanation:

### Question: 7

Which service should HipLocal use for their public APIs?

- A. Cloud Armor
- B. Cloud Functions
- C. Cloud Endpoints
- D. Shielded Virtual Machines

**Answer: D**

Explanation:

### Question: 8

HipLocal wants to improve the resilience of their MySQL deployment, while also meeting their business and technical requirements.

Which configuration should they choose?

- A. Use the current single instance MySQL on Compute Engine and several read-only MySQL servers on Compute Engine.
- B. Use the current single instance MySQL on Compute Engine, and replicate the data to Cloud SQL in an external master configuration.
- C. Replace the current single instance MySQL instance with Cloud SQL, and configure high availability.
- D. Replace the current single instance MySQL instance with Cloud SQL, and Google provides redundancy without further configuration.

**Answer: B**

Explanation:

### Question: 9

Which database should HipLocal use for storing user activity?

- A. BigQuery
- B. Cloud SQL
- C. Cloud Spanner
- D. Cloud Datastore

**Answer: A**

Explanation:

### Question: 10

HipLocal is configuring their access controls.

Which firewall configuration should they implement?

- A. Block all traffic on port 443.
- B. Allow all traffic into the network.
- C. Allow traffic on port 443 for a specific tag.
- D. Allow all traffic on port 443 into the network.

**Answer: D**

Explanation:

### Question: 11

HipLocal's data science team wants to analyze user reviews.

How should they prepare the data?

- A. Use the Cloud Data Loss Prevention API for redaction of the review dataset.
- B. Use the Cloud Data Loss Prevention API for de-identification of the review dataset.
- C. Use the Cloud Natural Language Processing API for redaction of the review dataset.
- D. Use the Cloud Natural Language Processing API for de-identification of the review dataset.

**Answer: B**

Explanation:

<https://cloud.google.com/dlp/docs/deidentify-sensitive-data>

### Question: 12

In order for HipLocal to store application state and meet their stated business requirements, which database service should they migrate to?

- A. Cloud Spanner
- B. Cloud Datastore
- C. Cloud Memorystore as a cache
- D. Separate Cloud SQL clusters for each region

**Answer: D**

Explanation:

### Question: 13

For this question, refer to the HipLocal case study.

How should HipLocal redesign their architecture to ensure that the application scales to support a large increase in users?

- A. Use Google Kubernetes Engine (GKE) to run the application as a microservice. Run the MySQL database on a dedicated GKE node.
- B. Use multiple Compute Engine instances to run MySQL to store state information. Use a Google Cloud-managed load balancer to distribute the load between instances. Use managed instance groups for scaling.
- C. Use Memorystore to store session information and CloudSQL to store state information. Use a Google Cloud-managed load balancer to distribute the load between instances. Use managed instance groups for scaling.
- D. Use a Cloud Storage bucket to serve the application as a static website, and use another Cloud Storage

bucket to store user state information.

**Answer: D**

Explanation:

### Question: 14

For this question, refer to the HipLocal case study.

How should HipLocal increase their API development speed while continuing to provide the QA team with a stable testing environment that meets feature requirements?

- A. Include unit tests in their code, and prevent deployments to QA until all tests have a passing status.
- B. Include performance tests in their code, and prevent deployments to QA until all tests have a passing status.
- C. Create health checks for the QA environment, and redeploy the APIs at a later time if the environment is unhealthy.
- D. Redeploy the APIs to App Engine using Traffic Splitting. Do not move QA traffic to the new versions if errors are found.

**Answer: B**

Explanation:

### Question: 15

For this question, refer to the HipLocal case study.

HipLocal's application uses Cloud Client Libraries to interact with Google Cloud. HipLocal needs to configure authentication and authorization in the Cloud Client Libraries to implement least privileged access for the application. What should they do?

- A. Create an API key. Use the API key to interact with Google Cloud.
- B. Use the default compute service account to interact with Google Cloud.
- C. Create a service account for the application. Export and deploy the private key for the application. Use the service account to interact with Google Cloud.
- D. Create a service account for the application and for each Google Cloud API used by the application. Export and deploy the private keys used by the application. Use the service account with one Google Cloud API to interact with Google Cloud.

**Answer: A**

Explanation:

## Question: 16

For this question refer to the HipLocal case study.

HipLocal wants to reduce the latency of their services for users in global locations. They have created read replicas of their database in locations where their users reside and configured their service to read traffic using those replicas. How should they further reduce latency for all database interactions with the least amount of effort?

- A. Migrate the database to Bigtable and use it to serve all global user traffic.
- B. Migrate the database to Cloud Spanner and use it to serve all global user traffic.
- C. Migrate the database to Firestore in Datastore mode and use it to serve all global user traffic.
- D. Migrate the services to Google Kubernetes Engine and use a load balancer service to better scale the application.

**Answer: D**

Explanation:

## Question: 17

For this question, refer to the HipLocal case study.

Which Google Cloud product addresses HipLocal's business requirements for service level indicators and objectives?

- A. Cloud Profiler
- B. Cloud Monitoring
- C. Cloud Trace
- D. Cloud Logging

**Answer: B**

Explanation:

<https://cloud.google.com/stackdriver/docs/solutions/slo-monitoring#defn-sli>

## Question: 18

For this question, refer to the HipLocal case study.

A recent security audit discovers that HipLocal's database credentials for their Compute Engine- hosted MySQL databases are stored in plain text on persistent disks. HipLocal needs to reduce the risk of these credentials being stolen. What should they do?

- A. Create a service account and download its key. Use the key to authenticate to Cloud Key Management

Service (KMS) to obtain the database credentials.

- B. Create a service account and download its key. Use the key to authenticate to Cloud Key Management Service (KMS) to obtain a key used to decrypt the database credentials.
- C. Create a service account and grant it the roles/iam.serviceAccountUser role. Impersonate as this account and authenticate using the Cloud SQL Proxy.
- D. Grant the roles/secretmanager.secretAccessor role to the Compute Engine service account. Store and access the database credentials with the Secret Manager API.

**Answer: D**

Explanation:

<https://cloud.google.com/secret-manager/docs/overview>

## Question: 19

For this question, refer to the HipLocal case study.

HipLocal is expanding into new locations. They must capture additional data each time the application is launched in a new European country. This is causing delays in the development process due to constant schema changes and a lack of environments for conducting testing on the application changes. How should they resolve the issue while meeting the business requirements?

- A. Create new Cloud SQL instances in Europe and North America for testing and deployment. Provide developers with local MySQL instances to conduct testing on the application changes.
- B. Migrate data to Bigtable. Instruct the development teams to use the Cloud SDK to emulate a local Bigtable development environment.
- C. Move from Cloud SQL to MySQL hosted on Compute Engine. Replicate hosts across regions in the Americas and Europe. Provide developers with local MySQL instances to conduct testing on the application changes.
- D. Migrate data to Firestore in Native mode and set up instan

**Answer: B**

Explanation:

## Topic 2, Misc. Questions

## Question: 20

You want to upload files from an on-premises virtual machine to Google Cloud Storage as part of a data migration. These files will be consumed by Cloud DataProc Hadoop cluster in a GCP environment.

Which command should you use?

- A. gsutil cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- B. gcloud cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- C. hadoop fs cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/
- D. gcloud dataproc cp [LOCAL\_OBJECT] gs://[DESTINATION\_BUCKET\_NAME]/

**Answer: A**

Explanation:

The gsutil cp command allows you to copy data between your local file. storage. boto files generated by running "gsutil config"

### Question: 21

You migrated your applications to Google Cloud Platform and kept your existing monitoring platform.

You now

find that your notification system is too slow for time critical problems.

What should you do?

- A. Replace your entire monitoring platform with Stackdriver.
- B. Install the Stackdriver agents on your Compute Engine instances.
- C. Use Stackdriver to capture and alert on logs, then ship them to your existing platform.
- D. Migrate some traffic back to your old platform and perform AB testing on the two platforms concurrently.

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/monitoring/>

### Question: 22

You are planning to migrate a MySQL database to the managed Cloud SQL database for Google Cloud. You have Compute Engine virtual machine instances that will connect with this Cloud SQL instance. You do not want to whitelist IPs for the Compute Engine instances to be able to access Cloud SQL.

What should you do?

- A. Enable private IP for the Cloud SQL instance.
- B. Whitelist a project to access Cloud SQL, and add Compute Engine instances in the whitelisted project.
- C. Create a role in Cloud SQL that allows access to the database from external instances, and assign the Compute Engine instances to that role.
- D. Create a CloudSQL instance on one project. Create Compute engine instances in a different project. Create a VPN between these two projects to allow internal access to CloudSQL.

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/sql/docs/mysql/connect-external-app>

### Question: 23

You have deployed an HTTP(s) Load Balancer with the gcloud commands shown below.

```
export NAME=load-balancer
```

```

# create network
gcloud compute networks create ${WE}

# add instance
gcloud compute instances create ${NAME}-backend-instance-1 --subnet ${@ONE} --no address

# create the instance group
gcloud compute instance-groups unmanaged create S${NAME}-i
gcloud compute instance-groups unmanaged set-named-ports ${NAME}-i --named-ports http:80
gcloud compute instance-groups unmanaged add-instances ${NAME}-i --instances S${NAME}-instance-1

# configure health checks
gcloud compute health-checks create http ${NAME}-http-hc --port 80

# create backend service
gcloud compute backend-services create S${NAME}-http-bes --health-checks S${NAME}-http-hc --protocol HTTP --port-name http --global
gcloud compute backend-services add-backend S${NAME}-http-bes --instance-group S${NAME}-i --balancing-mode RATE --max-rate 100000 --
capacity-scaler 1.0 --global --instance-group-zone us-east1-d

# create url maps and forwarding rule
gcloud compute url-maps create S${NAME}-http-urlmap --default-service S${NAME}-http-bes
gcloud compute target-http-proxies create S${NAME}-http-proxy --url-map S${NAME}-http-urlmap
gcloud compute forwarding-rules create S${NAME}-http-fw --global --ip-protocol ICP --target-http-proxy S${NAME}-http-proxy --ports 80

```

Health checks to port 80 on the Compute Engine virtual machine instance are failing and no traffic is sent to your instances. You want to resolve the problem.

Which commands should you run?

- A. `gcloud compute instances add-access-config ${NAME}-backend-instance-1`
- B. `gcloud compute instances add-tags ${NAME}-backend-instance-1 --tags http-server`
- C. `gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS`
- D. `gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --destination-ranges 130.211.0.0/22,35.191.0.0/16 --direction EGRESS`

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/vpc/docs/special-configurations>

## Question: 24

Your website is deployed on Compute Engine. Your marketing team wants to test conversion rates between 3 different website designs.

Which approach should you use?

- A. Deploy the website on App Engine and use traffic splitting.
- B. Deploy the website on App Engine as three separate services.
- C. Deploy the website on Cloud Functions and use traffic splitting.
- D. Deploy the website on Cloud Functions as three separate functions.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/appengine/docs/standard/python/splitting-traffic>

## Question: 25

You need to copy directory local-scripts and all of its contents from your local workstation to a Compute Engine virtual machine instance.

Which command should you use?

- A. `gsutil cp --project "my-gcp-project" -r ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone "us-east1-b"`
- B. `gsutil cp --project "my-gcp-project" -R ~/local-scripts/ gcp-instance-name:~/server-scripts/ --zone "us-east1-b"`
- C. `gcloud compute scp --project "my-gcp-project" --recurse ~/local-scripts/ gcpinstance-name:~/server-scripts/ --zone "us-east1-b"`
- D. `gcloud compute mv --project "my-gcp-project" --recurse ~/local-scripts/ gcpinstance-name:~/server-scripts/ --zone "us-east1-b"`

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/sdk/gcloud/reference/compute/copy-files>

## Question: 26

You are deploying your application to a Compute Engine virtual machine instance with the Stackdriver

Monitoring Agent installed. Your application is a unix process on the instance. You want to be alerted

if the unix process has not run for at least 5 minutes. You are not able to change the application to generate metrics or logs.

Which alert condition should you configure?

- A. Uptime check
- B. Process health
- C. Metric absence
- D. Metric threshold

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/monitoring/alerts/concepts-indepth>

## Question: 27

You have two tables in an ANSI-SQL compliant database with identical columns that you need to quickly combine into a single table, removing duplicate rows from the result set.

What should you do?

- A. Use the JOIN operator in SQL to combine the tables.

- B. Use nested WITH statements to combine the tables.
- C. Use the UNION operator in SQL to combine the tables.
- D. Use the UNION ALL operator in SQL to combine the tables.

**Answer: C**

Explanation:

Reference: [https://www.techonthenet.com/sql/union\\_all.php](https://www.techonthenet.com/sql/union_all.php)

### Question: 28

You have an application deployed in production. When a new version is deployed, some issues don't arise until the application receives traffic from users in production. You want to reduce both the impact and the number of users affected.

Which deployment strategy should you use?

- A. Blue/green deployment
- B. Canary deployment
- C. Rolling deployment
- D. Recreate deployment

**Answer: A**

Explanation:

Reference: <https://thenewstack.io/deployment-strategies/>

### Question: 29

Your company wants to expand their users outside the United States for their popular application.

The

company wants to ensure 99.999% availability of the database for their application and also wants to minimize the read latency for their users across the globe.

Which two actions should they take? (Choose two.)

- A. Create a multi-regional Cloud Spanner instance with "nam-asia-eur1" configuration.
- B. Create a multi-regional Cloud Spanner instance with "nam3" configuration.
- C. Create a cluster with at least 3 Spanner nodes.
- D. Create a cluster with at least 1 Spanner node.
- E. Create a minimum of two Cloud Spanner instances in separate regions with at least one node.
- F. Create a Cloud Dataflow pipeline to replicate data across different databases.

**Answer: BF**

Explanation:

### Question: 30

You need to migrate an internal file upload API with an enforced 500-MB file size limit to App Engine. What

should you do?

- A. Use FTP to upload files.
- B. Use CPanel to upload files.
- C. Use signed URLs to upload files.
- D. Change the API to be a multipart file upload API.

**Answer: C**

Explanation:

Reference: [https://wiki.christophchamp.com/index.php?title=Google\\_Cloud\\_Platform](https://wiki.christophchamp.com/index.php?title=Google_Cloud_Platform)

### **Question: 31**

You are planning to deploy your application in a Google Kubernetes Engine (GKE) cluster. The application exposes an HTTP-based health check at /healthz. You want to use this health check endpoint to determine whether traffic should be routed to the pod by the load balancer. Which code snippet should you include in your Pod configuration?

**A.** `livenessProbe:`

`httpGet:`

`path: /healthz`

`port: 80`

`readinessProbe:`

`httpGet:`

`path: /healthz`

`port: 80`

`loadBalancerHealthCheck:`

`httpGet: path: /healthz port: 80`

**D** `healthcheck:`

`httpGet: path: /healthz port: 80`

- A. Option A
- B. Option B
- C. Option C

D. Option D

**Answer: B**

Explanation:

For the GKE ingress controller to use your readinessProbes as health checks, the Pods for an Ingress must exist at the time of Ingress creation. If your replicas are scaled to 0, the default health check will apply.

### Question: 32

Your teammate has asked you to review the code below. Its purpose is to efficiently add a large number of small rows to a BigQuery table.

```
BigQuery service = BigQueryOptions.newBuilder().build().getService();
```

```
public void writeToBigQuery(Collection<Map<String, String>> rows) {  
    for(Map<String, String> row : rows) {  
        InsertAllRequest insertRequest = InsertAllRequest.newBuilder(  
            "datasetId", "tableId",  
            InsertAllRequest.RowToInsert.of(row)).build();  
        service.insertAll(insertRequest);  
    }  
}
```

Which improvement should you suggest your teammate make?

- A. Include multiple rows with each request.
- B. Perform the inserts in parallel by creating multiple threads.
- C. Write each row to a Cloud Storage object, then load into BigQuery.
- D. Write each row to a Cloud Storage object in parallel, then load into BigQuery.

**Answer: B**

Explanation:

### Question: 33

You are developing a JPEG image-resizing API hosted on Google Kubernetes Engine (GKE). Callers of the service will exist within the same GKE cluster. You want clients to be able to get the IP address of the service.

What should you do?

- A. Define a GKE Service. Clients should use the name of the A record in Cloud DNS to find the service's cluster IP address.
- B. Define a GKE Service. Clients should use the service name in the URL to connect to the service.
- C. Define a GKE Endpoint. Clients should get the endpoint name from the appropriate environment variable in the client container.
- D. Define a GKE Endpoint. Clients should get the endpoint name from Cloud DNS.

**Answer: C**

Explanation:

**Question: 34**

You are using Cloud Build to build and test application source code stored in Cloud Source Repositories. The build process requires a build tool not available in the Cloud Build environment. What should you do?

- A. Download the binary from the internet during the build process.
- B. Build a custom cloud builder image and reference the image in your build steps.
- C. Include the binary in your Cloud Source Repositories repository and reference it in your build scripts.
- D. Ask to have the binary added to the Cloud Build environment by filing a feature request against the Cloud Build public Issue Tracker.

**Answer: B**

Explanation:

**Question: 35**

You are deploying your application to a Compute Engine virtual machine instance. Your application is configured to write its log files to disk. You want to view the logs in Stackdriver Logging without changing the application code. What should you do?

- A. Install the Stackdriver Logging Agent and configure it to send the application logs.
- B. Use a Stackdriver Logging Library to log directly from the application to Stackdriver Logging.
- C. Provide the log file folder path in the metadata of the instance to configure it to send the application logs.
- D. Change the application to log to /var/log so that its logs are automatically sent to Stackdriver Logging.

**Answer: A**

Explanation:

**Question: 36**

Your service adds text to images that it reads from Cloud Storage. During busy times of the year, requests to Cloud Storage fail with an HTTP 429 "Too Many Requests" status code. How should you handle this error?

- A. Add a cache-control header to the objects.
- B. Request a quota increase from the GCP Console.
- C. Retry the request with a truncated exponential backoff strategy.
- D. Change the storage class of the Cloud Storage bucket to Multi-regional.

**Answer: C**

Explanation:

Reference: <https://developers.google.com/gmail/api/v1/reference/quota>

### Question: 37

You are building an API that will be used by Android and iOS apps. The API must:

- Support HTTPS
- Minimize bandwidth cost
- Integrate easily with mobile apps

Which API architecture should you use?

- A. RESTful APIs
- B. MQTT for APIs
- C. gRPC-based APIs
- D. SOAP-based APIs

**Answer: A**

Explanation:

Reference: <https://www.devteam.space/blog/how-to-build-restful-api-for-your-mobile-app/>

### Question: 38

Your application takes an input from a user and publishes it to the user's contacts. This input is stored in a table in Cloud Spanner. Your application is more sensitive to latency and less sensitive to consistency.

How should you perform reads from Cloud Spanner for this application?

- A. Perform Read-Only transactions.
- B. Perform stale reads using single-read methods.
- C. Perform strong reads using single-read methods.
- D. Perform stale reads using read-write transactions.

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/solutions/best-practices-cloud-spanner-gaming-database>

### Question: 39

Your application is deployed in a Google Kubernetes Engine (GKE) cluster. When a new version of your application is released, your CI/CD tool updates the `spec.template.spec.containers[0].image` value to reference the Docker image of your new application version. When the Deployment object applies the change, you want to deploy at least 1 replica of the new version and maintain the previous replicas until the new replica is healthy.

Which change should you make to the GKE Deployment object shown below?

```
apiVersion: apps/v1
```

```
kind: Deployment
```

```
metadata:
```

```
name: ecommerce-frontend-deployment spec:
replicas: 3
selector: matchLabels:
  app: ecommerce-frontend
template:
  metadata labels
    app: ecommerce-frontend
spec:
  containers:
  - name: ecommerce-frontend-webapp
    image: ecommerce-frontend-webapp:1.7.9
  ports:
  - containerport: 80
```

- A. Set the Deployment strategy to RollingUpdate with maxSurge set to 0, maxUnavailable set to 1.
- B. Set the Deployment strategy to RollingUpdate with maxSurge set to 1, maxUnavailable set to 0.
- C. Set the Deployment strategy to Recreate with maxSurge set to 0, maxUnavailable set to 1.
- D. Set the Deployment strategy to Recreate with maxSurge set to 1, maxUnavailable set to 0.

**Answer: D**

Explanation:

### Question: 40

You plan to make a simple HTML application available on the internet. This site keeps information about FAQs for your application. The application is static and contains images, HTML, CSS, and Javascript. You want to make this application available on the internet with as few steps as possible. What should you do?

- A. Upload your application to Cloud Storage.
- B. Upload your application to an App Engine environment.
- C. Create a Compute Engine instance with Apache web server installed. Configure Apache web server to host the application.
- D. Containerize your application first. Deploy this container to Google Kubernetes Engine (GKE) and assign an external IP address to the GKE pod hosting the application.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/storage/docs/hosting-static-website>

### Question: 41

Your company has deployed a new API to App Engine Standard environment. During testing, the API is not behaving as expected. You want to monitor the application over time to diagnose the problem within the application code without redeploying the application.

Which tool should you use?

- A. Stackdriver Trace
- B. Stackdriver Monitoring
- C. Stackdriver Debug Snapshots
- D. Stackdriver Debug Logpoints

**Answer: B**

Explanation:

Reference: <https://rominirani.com/gcp-stackdriver-tutorial-debug-snapshots-traces-logging-and-logpoints-1ba49e4780e6>

### Question: 42

You want to use the Stackdriver Logging Agent to send an application's log file to Stackdriver from a Compute Engine virtual machine instance.

After installing the Stackdriver Logging Agent, what should you do first?

- A. Enable the Error Reporting API on the project.
- B. Grant the instance full access to all Cloud APIs.
- C. Configure the application log file as a custom source.
- D. Create a Stackdriver Logs Export Sink with a filter that matches the application's log entries.

**Answer: B**

Explanation:

### Question: 43

Your company has a BigQuery data mart that provides analytics information to hundreds of employees. One user of wants to run jobs without interrupting important workloads. This user isn't concerned about the time it takes to run these jobs. You want to fulfill this request while minimizing cost to the company and the effort required on your part.

What should you do?

- A. Ask the user to run the jobs as batch jobs.
- B. Create a separate project for the user to run jobs.
- C. Add the user as a job.user role in the existing project.
- D. Allow the user to run jobs when important workloads are not running.

**Answer: B**

Explanation:

### Question: 44

You want to notify on-call engineers about a service degradation in production while minimizing development time.

What should you do?

- A. Use Cloud Function to monitor resources and raise alerts.
- B. Use Cloud Pub/Sub to monitor resources and raise alerts.
- C. Use Stackdriver Error Reporting to capture errors and raise alerts.
- D. Use Stackdriver Monitoring to monitor resources and raise alerts.

**Answer: A**

Explanation:

### Question: 45

You are writing a single-page web application with a user-interface that communicates with a third-party API for content using XMLHttpRequest. The data displayed on the UI by the API results is less critical than other data displayed on the same web page, so it is acceptable for some requests to not have the API data displayed in the UI. However, calls made to the API should not delay rendering of other parts of the user interface. You want your application to perform well when the API response is an error or a timeout. What should you do?

- A. Set the asynchronous option for your requests to the API to false and omit the widget displaying the API results when a timeout or error is encountered.
- B. Set the asynchronous option for your request to the API to true and omit the widget displaying the API results when a timeout or error is encountered.
- C. Catch timeout or error exceptions from the API call and keep trying with exponential backoff until the API response is successful.
- D. Catch timeout or error exceptions from the API call and display the error response in the UI widget.

**Answer: A**

Explanation:

### Question: 46

You are creating an App Engine application that writes a file to any user's Google Drive.

How should the application authenticate to the Google Drive API?

- A. With an OAuth Client ID that uses the `https://www.googleapis.com/auth/drive.file` scope to obtain an access token for each user.
- B. With an OAuth Client ID with delegated domain-wide authority.
- C. With the App Engine service account and `https://www.googleapis.com/auth/drive.file` scope that generates a signed JWT.
- D. With the App Engine service account with delegated domain-wide authority.

**Answer: B**

Explanation:

Reference: <https://developers.google.com/drive/api/v3/about-auth>

### Question: 47

You are creating a Google Kubernetes Engine (GKE) cluster and run this command:

```
> gcloud container clusters create large-cluster --num-nodes 200
```

The command fails with the error:

```
insufficient regional quota to satisfy request: resource "CPUS": request requires '200.0*' and is short *176.0*. project has a quota of *24.0' with *24.0* available
```

You want to resolve the issue. What should you do?

- A. Request additional GKE quota in the GCP Console.
- B. Request additional Compute Engine quota in the GCP Console.
- C. Open a support case to request additional GKE quota.
- D. Decouple services in the cluster, and rewrite new clusters to function with fewer cores.

**Answer: A**

Explanation:

### Question: 48

You are parsing a log file that contains three columns: a timestamp, an account number (a string), and a transaction amount (a number). You want to calculate the sum of all transaction amounts for each unique account number efficiently.

Which data structure should you use?

- A. A linked list
- B. A hash table
- C. A two-dimensional array
- D. A comma-delimited string

**Answer: B**

Explanation:

### Question: 49

Your company has a BigQuery dataset named "Master" that keeps information about employee travel and expenses. This information is organized by employee department. That means employees should only be able

to view information for their department. You want to apply a security framework to enforce this requirement with the minimum number of steps.

What should you do?

- A. Create a separate dataset for each department. Create a view with an appropriate WHERE clause to select records from a particular dataset for the specific department. Authorize this view to access records from your Master dataset. Give employees the permission to this department-specific dataset.
- B. Create a separate dataset for each department. Create a data pipeline for each department to copy appropriate information from the Master dataset to the specific dataset for the department. Give employees the permission to this department-specific dataset.
- C. Create a dataset named Master dataset. Create a separate view for each department in the Master dataset. Give employees access to the specific view for their department.
- D. Create a dataset named Master dataset. Create a separate table for each department in the Master dataset. Give employees access to the specific table for their department.

**Answer: B**

Explanation:

### Question: 50

You have an application in production. It is deployed on Compute Engine virtual machine instances controlled by a managed instance group. Traffic is routed to the instances via a HTTP(s) load balancer. Your users are unable to access your application. You want to implement a monitoring technique to alert you when the application is unavailable.

Which technique should you choose?

- A. Smoke tests
- B. Stackdriver uptime checks
- C. Cloud Load Balancing - health checks
- D. Managed instance group - health checks

**Answer: B**

Explanation:

Reference: <https://medium.com/google-cloud/stackdriver-monitoring-automation-part-3-uptime-checks-476b8507f59c>

### Question: 51

You are load testing your server application. During the first 30 seconds, you observe that a previously inactive Cloud Storage bucket is now servicing 2000 write requests per second and 7500 read requests per second.

Your application is now receiving intermittent 5xx and 429 HTTP responses from the Cloud Storage JSON API as the demand escalates. You want to decrease the failed responses from the Cloud Storage API. What should you do?

- A. Distribute the uploads across a large number of individual storage buckets.
- B. Use the XML API instead of the JSON API for interfacing with Cloud Storage.
- C. Pass the HTTP response codes back to clients that are invoking the uploads from your application.
- D. Limit the upload rate from your application clients so that the dormant bucket's peak request rate is reached more gradually.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/storage/docs/request-rate>

### Question: 52

Your application is controlled by a managed instance group. You want to share a large read-only data set between all the instances in the managed instance group. You want to ensure that each instance can start quickly and can access the data set via its filesystem with very low latency. You also want to minimize the total cost of the solution. What should you do?

- A. Move the data to a Cloud Storage bucket, and mount the bucket on the filesystem using Cloud Storage FUSE.
- B. Move the data to a Cloud Storage bucket, and copy the data to the boot disk of the instance via a startup script.
- C. Move the data to a Compute Engine persistent disk, and attach the disk in read-only mode to multiple Compute Engine virtual machine instances.
- D. Move the data to a Compute Engine persistent disk, take a snapshot, create multiple disks from the snapshot, and attach each disk to its own instance.

**Answer: C**

Explanation:

### Question: 53

You are developing an HTTP API hosted on a Compute Engine virtual machine instance that needs to be invoked by multiple clients within the same Virtual Private Cloud (VPC). You want clients to be able to get the IP address of the service.

What should you do?

- A. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Clients should use this IP address to connect to the service.
- B. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Then, define an A record in Cloud DNS. Clients should use the name of the A record to connect to the service.
- C. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url `https://[INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal/`.
- D. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url `https://[API_NAME]/[API_VERSION]/`.

**Answer: D**

Explanation:

### Question: 54

Your application is logging to Stackdriver. You want to get the count of all requests on all `/api/alpha/*` endpoints.

What should you do?

- A. Add a Stackdriver counter metric for path:`/api/alpha/`.
- B. Add a Stackdriver counter metric for endpoint:`/api/alpha/*`.
- C. Export the logs to Cloud Storage and count lines matching `/api/alpha`.
- D. Export the logs to Cloud Pub/Sub and count lines matching `/api/alpha`.

**Answer: C**

Explanation:

### Question: 55

You want to re-architect a monolithic application so that it follows a microservices model. You want to accomplish this efficiently while minimizing the impact of this change to the business.

Which approach should you take?

- A. Deploy the application to Compute Engine and turn on autoscaling.
- B. Replace the application's features with appropriate microservices in phases.
- C. Refactor the monolithic application with appropriate microservices in a single effort and deploy it.
- D. Build a new application with the appropriate microservices separate from the monolith and replace it when it is complete.

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/solutions/migrating-a-monolithic-app-to-microservices-gke>

### Question: 56

Your existing application keeps user state information in a single MySQL database. This state information is very user-specific and depends heavily on how long a user has been using an application. The MySQL database is causing challenges to maintain and enhance the schema for various users.

Which storage option should you choose?

- A. Cloud SQL
- B. Cloud Storage
- C. Cloud Spanner
- D. Cloud Datastore/Firestore

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/solutions/migrating-mysql-to-cloudsql-concept>

### Question: 57

You are building a new API. You want to minimize the cost of storing and reduce the latency of serving images. Which architecture should you use?

- A. App Engine backed by Cloud Storage
- B. Compute Engine backed by Persistent Disk
- C. Transfer Appliance backed by Cloud Filestore
- D. Cloud Content Delivery Network (CDN) backed by Cloud Storage

**Answer: B**

Explanation:

### Question: 58

Your company's development teams want to use Cloud Build in their projects to build and push Docker images

to Container Registry. The operations team requires all Docker images to be published to a centralized, securely managed Docker registry that the operations team manages.

What should you do?

- A. Use Container Registry to create a registry in each development team's project. Configure the Cloud Build build to push the Docker image to the project's registry. Grant the operations team access to each development team's registry.
- B. Create a separate project for the operations team that has Container Registry configured. Assign appropriate permissions to the Cloud Build service account in each developer team's project to allow access to the operation team's registry.
- C. Create a separate project for the operations team that has Container Registry configured. Create a Service Account for each development team and assign the appropriate permissions to allow it access to the operations team's registry. Store the service account key file in the source code repository and use it to authenticate against the operations team's registry.
- D. Create a separate project for the operations team that has the open source Docker Registry deployed on a Compute Engine virtual machine instance. Create a username and password for each development team. Store the username and password in the source code repository and use it to authenticate against the operations team's Docker registry.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/container-registry/>

### Question: 59

You are planning to deploy your application in a Google Kubernetes Engine (GKE) cluster. Your application can scale horizontally, and each instance of your application needs to have a stable network identity and its own persistent disk.

Which GKE object should you use?

- A. Deployment
- B. StatefulSet
- C. ReplicaSet
- D. ReplicaController

**Answer: B**

Explanation:

Reference: <https://livebook.manning.com/book/kubernetes-in-action/chapter-10/46>

### Question: 60

You are using Cloud Build to build a Docker image. You need to modify the build to execute unit and run integration tests. When there is a failure, you want the build history to clearly display the stage at which the build failed.

What should you do?

- A. Add RUN commands in the Dockerfile to execute unit and integration tests.
- B. Create a Cloud Build build config file with a single build step to compile unit and integration tests.
- C. Create a Cloud Build build config file that will spawn a separate cloud build pipeline for unit and integration tests.
- D. Create a Cloud Build build config file with separate cloud builder steps to compile and execute unit and integration tests.

**Answer: D**

Explanation:

### Question: 61

Your code is running on Cloud Functions in project

- A. It is supposed to write an object in a Cloud Storage bucket owned by project B. However, the write call is failing with the error "403 Forbidden".

What should you do to correct the problem?

- A. Grant your user account the roles/storage.objectCreator role for the Cloud Storage bucket.
- B. Grant your user account the roles/iam.serviceAccountUser role for the service-PROJECTA@gcf-adminrobot.iam.gserviceaccount.com service account.
- C. Grant the service-PROJECTA@gcf-admin-robot.iam.gserviceaccount.com service account the roles/storage.objectCreator role for the Cloud Storage bucket.
- D. Enable the Cloud Storage API in project B.

**Answer: B**

Explanation:

**Question: 62**

Your application is running in multiple Google Kubernetes Engine clusters. It is managed by a Deployment in each cluster. The Deployment has created multiple replicas of your Pod in each cluster. You want to view the logs sent to stdout for all of the replicas in your Deployment in all clusters. Which command should you use?

- A. `kubectl logs [PARAM]`
- B. `gcloud logging read [PARAM]`
- C. `kubectl exec -it [PARAM] journalctl`
- D. `gcloud compute ssh [PARAM] --command= "sudo journalctl"`

**Answer: D**

Explanation:

### Question: 63

You are using Cloud Build to create a new Docker image on each source code commit to a Cloud Source Repositories repository. Your application is built on every commit to the master branch. You want to release specific commits made to the master branch in an automated method. What should you do?

- A. Manually trigger the build for new releases.
- B. Create a build trigger on a Git tag pattern. Use a Git tag convention for new releases.
- C. Create a build trigger on a Git branch name pattern. Use a Git branch naming convention for new releases.
- D. Commit your source code to a second Cloud Source Repositories repository with a second Cloud Build trigger. Use this repository for new releases only.

**Answer: C**

Explanation:

Reference: <https://docs.docker.com/docker-hub/builds/>

### Question: 64

You are designing a schema for a table that will be moved from MySQL to Cloud Bigtable. The MySQL table is as follows:

#### AccountActivity

**Account\_id int, Event\_timestamp datetime, Transaction\_type string. Amount numeric(18, 4) } primary key (Account\_id, Event\_timestamp)**

How should you design a row key for Cloud Bigtable for this table?

- A. Set Account\_id as a key.
- B. Set Account\_id\_Event\_timestamp as a key.
- C. Set Event\_timestamp\_Account\_id as a key.
- D. Set Event\_timestamp as a key.

**Answer: C**

Explanation:

### Question: 65

You want to view the memory usage of your application deployed on Compute Engine. What should you do?

- A. Install the Stackdriver Client Library.
- B. Install the Stackdriver Monitoring Agent.
- C. Use the Stackdriver Metrics Explorer.
- D. Use the Google Cloud Platform Console.

**Answer: C**

Explanation:

Reference: <https://stackoverflow.com/questions/43991246/google-cloud-platform-how-to-monitor-memory-usage-of-vm-instances>

### Question: 66

You have an analytics application that runs hundreds of queries on BigQuery every few minutes using BigQuery API. You want to find out how much time these queries take to execute. What should you do?

- A. Use Stackdriver Monitoring to plot slot usage.
- B. Use Stackdriver Trace to plot API execution time.
- C. Use Stackdriver Trace to plot query execution time.
- D. Use Stackdriver Monitoring to plot query execution times.

**Answer: D**

Explanation:

### Question: 67

You are designing a schema for a Cloud Spanner customer database. You want to store a phone number array field in a customer table. You also want to allow users to search customers by phone number. How should you design this schema?

- A. Create a table named Customers. Add an Array field in a table that will hold phone numbers for the customer.
- B. Create a table named Customers. Create a table named Phones. Add a CustomerId field in the Phones table to find the CustomerId from a phone number.
- C. Create a table named Customers. Add an Array field in a table that will hold phone numbers for the customer. Create a secondary index on the Array field.
- D. Create a table named Customers as a parent table. Create a table named Phones, and interleave this table into the Customer table. Create an index on the phone number field in the Phones table.

**Answer: C**

Explanation:

## Question: 68

You are deploying a single website on App Engine that needs to be accessible via the URL <http://www.altostrat.com/>. What should you do?

- A. Verify domain ownership with Webmaster Central. Create a DNS CNAME record to point to the App Engine canonical name `ghs.googlehosted.com`.
- B. Verify domain ownership with Webmaster Central. Define an A record pointing to the single global App Engine IP address.
- C. Define a mapping in `dispatch.yaml` to point the domain `www.altostrat.com` to your App Engine service. Create a DNS CNAME record to point to the App Engine canonical name `ghs.googlehosted.com`.
- D. Define a mapping in `dispatch.yaml` to point the domain `www.altostrat.com` to your App Engine service. Define an A record pointing to the single global App Engine IP address.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/appengine/docs/flexible/dotnet/mapping-custom-domains?hl=fa>

## Question: 69

You are running an application on App Engine that you inherited. You want to find out whether the application is using insecure binaries or is vulnerable to XSS attacks. Which service should you use?

- A. Cloud Amor
- B. Stackdriver Debugger
- C. Cloud Security Scanner
- D. Stackdriver Error Reporting

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/security-scanner>

## Question: 70

You are working on a social media application. You plan to add a feature that allows users to upload

images. These images will be 2 MB – 1 GB in size. You want to minimize their infrastructure operations overhead for this feature. What should you do?

- A. Change the application to accept images directly and store them in the database that stores other user information.

- B. Change the application to create signed URLs for Cloud Storage. Transfer these signed URLs to the client application to upload images to Cloud Storage.
- C. Set up a web server on GCP to accept user images and create a file store to keep uploaded files. Change the application to retrieve images from the file store.
- D. Create a separate bucket for each user in Cloud Storage. Assign a separate service account to allow write access on each bucket. Transfer service account credentials to the client application based on user information. The application uses this service account to upload images to Cloud Storage.

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/blog/products/storage-data-transfer/uploading-images-directly-to-cloud-storage-by-using-signed-url>

### Question: 71

Your application is built as a custom machine image. You have multiple unique deployments of the machine image. Each deployment is a separate managed instance group with its own template. Each deployment requires a unique set of configuration values. You want to provide these unique values to each deployment but use the same custom machine image in all deployments. You want to use out-of-the-box features of Compute Engine. What should you do?

- A. Place the unique configuration values in the persistent disk.
- B. Place the unique configuration values in a Cloud Bigtable table.
- C. Place the unique configuration values in the instance template startup script.
- D. Place the unique configuration values in the instance template instance metadata.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/compute/docs/instance-groups>

### Question: 72

Your application performs well when tested locally, but it runs significantly slower when you deploy it to App Engine standard environment. You want to diagnose the problem. What should you do?

- A. File a ticket with Cloud Support indicating that the application performs faster locally.
- B. Use Stackdriver Debugger Snapshots to look at a point-in-time execution of the application.
- C. Use Stackdriver Trace to determine which functions within the application have higher latency.
- D. Add logging commands to the application and use Stackdriver Logging to check where the latency problem OCCURS.

**Answer: D**

Explanation:

### Question: 73

You have an application running in App Engine. Your application is instrumented with Stackdriver Trace. The `/product-details` request reports details about four known unique products at `/sku-details` as shown below. You want to reduce the time it takes for the request to complete. What should you do?

#### Timeline



- A. Increase the size of the instance class.
- B. Change the Persistent Disk type to SSD.
- C. Change `/product-details` to perform the requests in parallel.
- D. Store the `/sku-details` information in a database, and replace the webservice call with a database query.

**Answer: C**

Explanation:

### Question: 74

Your company has a data warehouse that keeps your application information in BigQuery. The BigQuery data warehouse keeps 2 PBs of user data.

a. Recently, your company expanded your user base to include EU users and needs to comply with

these requirements:

Your company must be able to delete all user account information upon user request.

All EU user data must be stored in a single region specifically for EU users.

Which two actions should you take? (Choose two.)

- A. Use BigQuery federated queries to query data from Cloud Storage.
- B. Create a dataset in the EU region that will keep information about EU users only.
- C. Create a Cloud Storage bucket in the EU region to store information for EU users only.
- D. Re-upload your data using to a Cloud Dataflow pipeline by filtering your user records out.
- E. Use DML statements in BigQuery to update/delete user records based on their requests.

**Answer: C,E**

Explanation:

Reference: <https://cloud.google.com/solutions/bigquery-data-warehouse>

### Question: 75

Your App Engine standard configuration is as follows:

```
service: production
instance_class: B1
```

You want to limit the application to 5 instances. Which code snippet should you include in your configuration?

- A. `manual_scaling:instances: 5min_pending_latency: 30ms`
- B. `manual_scaling:max_instances: 5idle_timeout: 10m`
- C. `basic_scaling:instances: 5min_pending_latency: 30ms`
- D. `basic_scaling:max_instances: 5idle_timeout: 10m`

**Answer: C**

Explanation:

### Question: 76

Your analytics system executes queries against a BigQuery dataset. The SQL query is executed in batch and passes the contents of a SQL file to the BigQuery CLI. Then it redirects the BigQuery CLI output to another process. However, you are getting a permission error from the BigQuery CLI when the queries are executed. You want to resolve the issue. What should you do?

- A. Grant the service account BigQuery Data Viewer and BigQuery Job User roles.
- B. Grant the service account BigQuery Data Editor and BigQuery Data Viewer roles.
- C. Create a view in BigQuery from the SQL query and `SELECT*` from the view in the CLI.
- D. Create a new dataset in BigQuery, and copy the source table to the new dataset Query the new dataset and table from the CLI.

**Answer: B**

Explanation:

**Question: 77**

Your application is running on Compute Engine and is showing sustained failures for a small number of requests. You have narrowed the cause down to a single Compute Engine instance, but the instance is unresponsive to SSH. What should you do next?

- A. Reboot the machine.
- B. Enable and check the serial port output.
- C. Delete the machine and create a new one.
- D. Take a snapshot of the disk and attach it to a new machine.

**Answer: A**

Explanation:

**Question: 78**

You configured your Compute Engine instance group to scale automatically according to overall CPU usage. However, your application's response latency increases sharply before the cluster has finished adding up instances. You want to provide a more consistent latency experience for your end users by changing the configuration of the instance group autoscaler. Which two configuration changes should you make? (Choose two.)

- A. Add the label "AUTOSCALE" to the instance group template.
- B. Decrease the cool-down period for instances added to the group.
- C. Increase the target CPU usage for the instance group autoscaler.
- D. Decrease the target CPU usage for the instance group autoscaler.
- E. Remove the health-check for individual VMs in the instance group.

**Answer: A,C**

Explanation:

**Question: 79**

You have an application controlled by a managed instance group. When you deploy a new version of the application, costs should be minimized and the number of instances should not increase. You want to ensure that, when each new instance is created, the deployment only continues if the new instance is healthy. What should you do?

- A. Perform a rolling-action with maxSurge set to 1, maxUnavailable set to 0.
- B. Perform a rolling-action with maxSurge set to 0, maxUnavailable set to 1
- C. Perform a rolling-action with maxHealthy set to 1, maxUnhealthy set to 0.

D. Perform a rolling-action with maxHealthy set to 0, maxUnhealthy set to 1.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>

### Question: 80

Your application requires service accounts to be authenticated to GCP products via credentials stored on its host Compute Engine virtual machine instances. You want to distribute these credentials to the host instances as securely as possible. What should you do?

- A. Use HTTP signed URLs to securely provide access to the required resources.
- B. Use the instance's service account Application Default Credentials to authenticate to the required resources.
- C. Generate a P12 file from the GCP Console after the instance is deployed, and copy the credentials to the host instance before starting the application.
- D. Commit the credential JSON file into your application's source repository, and have your CI/CD process package it with the software that is deployed to the instance.

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/compute/docs/api/how-tos/authorization>

### Question: 81

Your application is deployed in a Google Kubernetes Engine (GKE) cluster. You want to expose this application publicly behind a Cloud Load Balancing HTTP(S) load balancer. What should you do?

- A. Configure a GKE Ingress resource.
- B. Configure a GKE Service resource.
- C. Configure a GKE Ingress resource with type: LoadBalancer.
- D. Configure a GKE Service resource with type: LoadBalancer.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/kubernetes-engine/docs/concepts/ingress>

## Question: 82

Your company is planning to migrate their on-premises Hadoop environment to the cloud. Increasing storage cost and maintenance of data stored in HDFS is a major concern for your company. You also want to make minimal changes to existing data analytics jobs and existing architecture. How should you proceed with the migration?

- A. Migrate your data stored in Hadoop to BigQuery. Change your jobs to source their information from BigQuery instead of the on-premises Hadoop environment.
- B. Create Compute Engine instances with HDD instead of SSD to save costs. Then perform a full migration of your existing environment into the new one in Compute Engine instances.
- C. Create a Cloud Dataproc cluster on Google Cloud Platform, and then migrate your Hadoop environment to the new Cloud Dataproc cluster. Move your HDFS data into larger HDD disks to save on storage costs.
- D. Create a Cloud Dataproc cluster on Google Cloud Platform, and then migrate your Hadoop code objects to the new cluster. Move your data to Cloud Storage and leverage the Cloud Dataproc connector to run jobs on that data.

**Answer: D**

Explanation:

## Question: 83

Your data is stored in Cloud Storage buckets. Fellow developers have reported that data downloaded from Cloud Storage is resulting in slow API performance. You want to research the issue to provide details to the GCP support team. Which command should you run?

- A. `gsutil test -o output.json gs://my-bucket`
- B. `gsutil perfdiag -o output.json gs://my-bucket`
- C. `gcloud compute scp example-instance:~/test-data -o output.json gs://my-bucket`
- D. `gcloud services test -o output.json gs://my-bucket`

**Answer: B**

Explanation:

Reference: <https://groups.google.com/forum/#!topic/gce-discussion/xBI9Jq5HDsY>

## Question: 84

You are using Cloud Build to promote a Docker image to Development, Test, and Production environments. You need to ensure that the same Docker image is deployed to each of these environments. How should you identify the Docker image in your build?

- A. Use the latest Docker image tag.
- B. Use a unique Docker image name.
- C. Use the digest of the Docker image.
- D. Use a semantic version Docker image tag.

**Answer: D**

Explanation:

### Question: 85

Your company has created an application that uploads a report to a Cloud Storage bucket. When the report is uploaded to the bucket, you want to publish a message to a Cloud Pub/Sub topic. You want to implement a solution that will take a small amount of effort to implement. What should you do?

- A. Configure the Cloud Storage bucket to trigger Cloud Pub/Sub notifications when objects are modified.
- B. Create an App Engine application to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.
- C. Create a Cloud Function that is triggered by the Cloud Storage bucket. In the Cloud Function, publish a message to the Cloud Pub/Sub topic.
- D. Create an application deployed in a Google Kubernetes Engine cluster to receive the file; when it is received, publish a message to the Cloud Pub/Sub topic.

**Answer: C**

Explanation:

: <https://cloud.google.com/storage/docs/pubsub-notifications>

### Question: 86

Your teammate has asked you to review the code below, which is adding a credit to an account balance in Cloud Datastore. Which improvement should you suggest your teammate make?

```
public Entity creditAccount(long accountId, long creditAmount) {  
    Entity account = datastore.get  
(keyFactory.newKey(accountId));  
    account = Entity.builder(account).set(  
        "balance", account.getLong("balance")  
+ creditAmount).build()  
    datastore.put(account);  
    return account;  
}
```

- A. Get the entity with an ancestor query.
- B. Get and put the entity in a transaction.

- C. Use a strongly consistent transactional database.
- D. Don't return the account entity from the function.

**Answer: A**

Explanation:

### Question: 87

Your company stores their source code in a Cloud Source Repositories repository. Your company wants to build and test their code on each source code commit to the repository and requires a solution that is managed and has minimal operations overhead.

Which method should they use?

- A. Use Cloud Build with a trigger configured for each source code commit.
- B. Use Jenkins deployed via the Google Cloud Platform Marketplace, configured to watch for source code commits.
- C. Use a Compute Engine virtual machine instance with an open source continuous integration tool, configured to watch for source code commits.
- D. Use a source code commit trigger to push a message to a Cloud Pub/Sub topic that triggers an App Engine service to build the source code.

**Answer: A**

Explanation:

<https://cloud.google.com/build/docs/automating-builds/create-manage-triggers#:~:text=A%20Cloud%20Build%20trigger%20automatically,changes%20that%20match%20certain%20criteria>.

### Question: 88

You are writing a Compute Engine hosted application in project A that needs to securely authenticate to a Cloud Pub/Sub topic in project B.

What should you do?

- A. Configure the instances with a service account owned by project B. Add the service account as a Cloud Pub/Sub publisher to project A.
- B. Configure the instances with a service account owned by project A. Add the service account as a publisher on the topic.
- C. Configure Application Default Credentials to use the private key of a service account owned by project B. Add the service account as a Cloud Pub/Sub publisher to project A.
- D. Configure Application Default Credentials to use the private key of a service account owned by project A. Add the service account as a publisher on the topic.

**Answer: B**

Explanation:

<https://cloud.google.com/pubsub/docs/access-control>

"For example, suppose a service account in Cloud Project A wants to publish messages to a topic in Cloud Project B. You could

accomplish this by granting the service account Edit permission in Cloud Project B"

## Question: 89

You are developing a corporate tool on Compute Engine for the finance department, which needs to authenticate users and verify that they are in the finance department. All company employees use G Suite.

What should you do?

- A. Enable Cloud Identity-Aware Proxy on the HTTP(s) load balancer and restrict access to a Google Group containing users in the finance department. Verify the provided JSON Web Token within the application.
- B. Enable Cloud Identity-Aware Proxy on the HTTP(s) load balancer and restrict access to a Google Group containing users in the finance department. Issue client-side certificates to everybody in the finance team and verify the certificates in the application.
- C. Configure Cloud Armor Security Policies to restrict access to only corporate IP address ranges. Verify the provided JSON Web Token within the application.
- D. Configure Cloud Armor Security Policies to restrict access to only corporate IP address ranges. Issue client side certificates to everybody in the finance team and verify the certificates in the application.

## Answer: A

Explanation:

[https://cloud.google.com/iap/docs/signed-headers-howto#securing\\_iap\\_headers](https://cloud.google.com/iap/docs/signed-headers-howto#securing_iap_headers)  
(<https://cloud.google.com/endpoints/docs/openapi/authenticating-users-google-id>).

[https://cloud.google.com/armor/docs/security-policy-overview#:~:text=Google%20Cloud%20Armor%20security%20policies%20enable%20you%20to%20allow%20or,Private%20Cloud%20\(VPC\)%20networks](https://cloud.google.com/armor/docs/security-policy-overview#:~:text=Google%20Cloud%20Armor%20security%20policies%20enable%20you%20to%20allow%20or,Private%20Cloud%20(VPC)%20networks)

"Google Cloud Armor security policies protect your application by providing Layer 7 filtering and by scrubbing incoming requests for common web attacks or other Layer 7 attributes to potentially block traffic before it reaches your load balanced backend services or backend buckets"

## Question: 90

Your API backend is running on multiple cloud providers. You want to generate reports for the network latency of your API.

Which two steps should you take? (Choose two.)

- A. Use Zipkin collector to gather data.
- B. Use Fluentd agent to gather data.
- C. Use Stackdriver Trace to generate reports.
- D. Use Stackdriver Debugger to generate report.
- E. Use Stackdriver Profiler to generate report.

## Answer: AC

Explanation:

<https://cloud.google.com/trace/docs/zipkin>

"receive traces from Zipkin clients and forward those traces to Cloud Trace for analysis."

[https://cloud.google.com/trace/docs/quickstart#analysis\\_reports\\_window](https://cloud.google.com/trace/docs/quickstart#analysis_reports_window)

### Question: 91

You have an application deployed in production. When a new version is deployed, you want to ensure that all production traffic is routed to the new version of your application. You also want to keep the previous version deployed so that you can revert to it if there is an issue with the new version.

Which deployment strategy should you use?

- A. Blue/green deployment
- B. Canary deployment
- C. Rolling deployment
- D. Recreate deployment

**Answer: A**

Explanation:

### Question: 92

You are porting an existing Apache/MySQL/PHP application stack from a single machine to Google Kubernetes Engine. You need to determine how to containerize the application. Your approach should follow Google-recommended best practices for availability. What should you do?

- A. Package each component in a separate container. Implement readiness and liveness probes.
- B. Package the application in a single container. Use a process management tool to manage each component.
- C. Package each component in a separate container. Use a script to orchestrate the launch of the components.
- D. Package the application in a single container. Use a bash script as an entrypoint to the container, and then spawn each component as a background job.

**Answer: A**

Explanation:

<https://cloud.google.com/blog/products/containers-kubernetes/7-best-practices-for-building-containers>  
<https://cloud.google.com/architecture/best-practices-for-building-containers>

"classic Apache/MySQL/PHP stack: you might be tempted to run all the components in a single container. However, the best practice is to use two or three different containers: one for Apache, one for MySQL, and potentially one for PHP if you are running PHP-FPM."

### Question: 93

You are developing an application that will be launched on Compute Engine instances into multiple distinct projects, each corresponding to the environments in your software development process (development, QA, staging, and production). The instances in each project have the same application code but a different configuration. During deployment, each instance should receive the application's configuration based on the environment it serves. You want to minimize the number of steps to configure this flow.

What should you do?

- A. When creating your instances, configure a startup script using the `gcloud` command to determine the project name that indicates the correct environment.
- B. In each project, configure a metadata key "environment" whose value is the environment it serves. Use your deployment tool to query the instance metadata and configure the application based on the "environment" value.
- C. Deploy your chosen deployment tool on an instance in each project. Use a deployment job to retrieve the appropriate configuration file from your version control system, and apply the configuration when deploying the application on each instance.
- D. During each instance launch, configure an instance custom-metadata key named "environment" whose value is the environment the instance serves. Use your deployment tool to query the instance metadata, and configure the application based on the "environment" value.

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/compute/docs/metadata/overview>

### Question: 94

You are developing an ecommerce application that stores customer, order, and inventory data as relational tables inside Cloud Spanner. During a recent load test, you discover that Spanner performance is not scaling linearly as expected. Which of the following is the cause?

- A. The use of 64-bit numeric types for 32-bit numbers.
- B. The use of the `STRING` data type for arbitrary-precision values.
- C. The use of Version 1 UUIDs as primary keys that increase monotonically.
- D. The use of `LIKE` instead of `STARTS_WITH` keyword for parameterized SQL queries.

**Answer: C**

Explanation:

### Question: 95

You are developing an application that reads credit card data from a Pub/Sub subscription. You have written code and

completed unit testing. You need to test the Pub/Sub integration before deploying to Google Cloud. What should you do?

- A. Create a service to publish messages, and deploy the Pub/Sub emulator. Generate random content in the publishing service, and publish to the emulator.
- B. Create a service to publish messages to your application. Collect the messages from Pub/Sub in production, and replay them through the publishing service.
- C. Create a service to publish messages, and deploy the Pub/Sub emulator. Collect the messages from Pub/Sub in production, and publish them to the emulator.
- D. Create a service to publish messages, and deploy the Pub/Sub emulator. Publish a standard set of testing messages from the publishing service to the emulator.

**Answer: D**

Explanation:

### Question: 96

You are designing an application that will subscribe to and receive messages from a single Pub/Sub topic and insert corresponding rows into a database. Your application runs on Linux and leverages preemptible virtual machines to reduce costs. You need to create a shutdown script that will initiate a graceful shutdown. What should you do?

- A. Write a shutdown script that uses inter-process signals to notify the application process to disconnect from the database.
- B. Write a shutdown script that broadcasts a message to all signed-in users that the Compute Engine instance is going down and instructs them to save current work and sign out.
- C. Write a shutdown script that writes a file in a location that is being polled by the application once every five minutes. After the file is read, the application disconnects from the database.
- D. Write a shutdown script that publishes a message to the Pub/Sub topic announcing that a shutdown is in progress. After the application reads the message, it disconnects from the database.

**Answer: D**

Explanation:

### Question: 97

You work for a web development team at a small startup. Your team is developing a Node.js application using Google Cloud services, including Cloud Storage and Cloud Build. The team uses a Git repository for version control. Your manager calls you over the weekend and instructs you to make an emergency update to one of the company's websites, and you're the only developer available. You need to access Google Cloud to make the update, but you don't have your work laptop. You are not allowed to store source code locally on a non-corporate computer. How should you set up your developer environment?

- A. Use a text editor and the Git command line to send your source code updates as pull requests from a public

computer.

- B. Use a text editor and the Git command line to send your source code updates as pull requests from a virtual machine running on a public computer.
- C. Use Cloud Shell and the built-in code editor for development. Send your source code updates as pull requests.
- D. Use a Cloud Storage bucket to store the source code that you need to edit. Mount the bucket to a public computer as a drive, and use a code editor to update the code. Turn on versioning for the bucket, and point it to the team's Git repository.

**Answer: C**

Explanation:

<https://cloud.google.com/shell/docs>

### Question: 98

Your team develops services that run on Google Kubernetes Engine. You need to standardize their log data using Google-recommended practices and make the data more useful in the fewest number of steps. What should you do? (Choose two.)

- A. Create aggregated exports on application logs to BigQuery to facilitate log analytics.
- B. Create aggregated exports on application logs to Cloud Storage to facilitate log analytics.
- C. Write log output to standard output (stdout) as single-line JSON to be ingested into Cloud Logging as structured logs.
- D. Mandate the use of the Logging API in the application code to write structured logs to Cloud Logging.
- E. Mandate the use of the Pub/Sub API to write structured data to Pub/Sub and create a Dataflow streaming pipeline to normalize logs and write them to BigQuery for analytics.

**Answer: AC**

Explanation:

[https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best\\_practices](https://cloud.google.com/stackdriver/docs/solutions/gke/managing-logs#best_practices)

### Question: 99

You are designing a deployment technique for your new applications on Google Cloud. As part of your deployment planning, you want to use live traffic to gather performance metrics for both new and existing applications. You need to test against the full production load prior to launch. What should you do?

- A. Use canary deployment
- B. Use blue/green deployment
- C. Use rolling updates deployment
- D. Use A/B testing with traffic mirroring during deployment

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/architecture/application-deployment-and-testing-strategies>

## Question: 100

You support an application that uses the Cloud Storage API. You review the logs and discover multiple HTTP 503 Service Unavailable error responses from the API. Your application logs the error and does not take any further action. You want to implement Google-recommended retry logic to improve success rates. Which approach should you take?

- A. Retry the failures in batch after a set number of failures is logged.
- B. Retry each failure at a set time interval up to a maximum number of times.
- C. Retry each failure at increasing time intervals up to a maximum number of tries.
- D. Retry each failure at decreasing time intervals up to a maximum number of tries.

**Answer: C**

Explanation:

<https://cloud.google.com/storage/docs/retry-strategy>

## Question: 101

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 system run in the same Compute Engine virtual machine. You plan to use the following Google Cloud tools in the new architecture:

Multiple Compute Engine machines, each running an instance of the authentication service

Multiple Compute Engine machines, each running an instance of the audit service

Pub/Sub to send the events from the authentication services.

How should you set up the 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 to allow the audit services to share the messages.
- B. Create one Pub/Sub topic. Create one pull subscription per audit service instance to allow the services to share the messages.
- C. Create one Pub/Sub topic. Create one push subscription with the endpoint pointing to a load balancer in front of the audit services.
- D. Create one Pub/Sub topic per authentication service. Create one pull subscription per topic to be used by one audit service.
- E. Create one Pub/Sub topic per authentication service. Create one push subscription per topic, with the endpoint pointing to one audit service.

**Answer: A**

Explanation:

<https://cloud.google.com/pubsub/docs/subscriber> "Multiple subscribers can make pull calls to the same "shared" subscription. Each subscriber will receive a subset of the messages."

## Question: 102

You are developing a marquee stateless web application that will run on Google Cloud. The rate of the incoming user traffic is expected to be unpredictable, with no traffic on some 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 in Python with Firestore as the database. Deploy the application to Cloud Run.
- B. Build the application in C# with Firestore as the database. Deploy the application to App Engine flexible environment.
- C. Build the application in Python with CloudSQL as the database. Deploy the application to App Engine standard environment.
- D. Build the application in Python with Firestore as the database. Deploy the application to a Compute Engine managed instance group with autoscaling.

**Answer: A**

Explanation:

## Question: 103

You have written a Cloud Function that accesses other Google Cloud resources. You want to secure the environment using the principle of least privilege. What should you do?

- A. Create a new service account that has Editor authority to access the resources. The deployer is given permission to get the access token.
- B. Create a new service account that has a custom IAM role to access the resources. The deployer is given permission to get the access token.
- C. Create a new service account that has Editor authority to access the resources. The deployer is given permission to act as the new service account.
- D. Create a new service account that has a custom IAM role to access the resources. The deployer is given permission to act as the new service account.

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/blog/products/application-development/least-privilege-for-cloud-functions-using-cloud-iam>

## Question: 104

You are a SaaS provider deploying dedicated blogging software to customers in your Google Kubernetes Engine (GKE)

cluster. You want to configure a secure multi-tenant platform to ensure that each customer has access to only their own blog and can't affect the workloads of other customers. What should you do?

- A. Enable Application-layer Secrets on the GKE cluster to protect the cluster.
- B. Deploy a namespace per tenant and use Network Policies in each blog deployment.
- C. Use GKE Audit Logging to identify malicious containers and delete them on discovery.
- D. Build a custom image of the blogging software and use Binary Authorization to prevent untrusted image deployments.

**Answer: B**

**Explanation:**

Reference: <https://cloud.google.com/kubernetes-engine/docs/concepts/multitenancy-overview>

### **Question: 105**

You have decided to migrate your Compute Engine application to Google Kubernetes Engine. You need to build a container image and push it to Artifact Registry using Cloud Build. What should you do? (Choose two.)

- A) Run `gcloud builds submit` in the directory that contains the application source code.
  - B) Run `gcloud run deploy app-name --image gcr.io/$PROJECT_ID/app-name` in the directory that contains the application source code.
  - C) Run `gcloud container images add-tag gcr.io/$PROJECT_ID/app-name gcr.io/$PROJECT_ID/app-name:latest` in the directory that contains the application source code.
  - D) In the application source directory, create a file named `cloudbuild.yaml` that contains the following contents:

```
steps:  
- name: 'gcr.io/cloud-builders/docker'  
  args: ['build', '-f', 'ger.io/$PROJECT_ID/app-name', '.']  
- name: 'gcr.io/cloud-builders/docker'  
  args: ['push', 'ger.io/$PROJECT_ID/app-name']
```
  - E) In the application source directory, create a file named `cloudbuild.yaml` that contains the following contents:

```
steps:  
- name: 'gcr.io/cloud-builders/gcloud'  
  args: ['app', 'deploy'] timeout: '1600s'
```
- A. Option A
  - B. Option B
  - C. Option C
  - D. Option D
  - E. Option E

**Answer: A, D**

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/builds/submit>  
<https://cloud.google.com/artifact-registry/docs/configure-cloud-build>

### Question: 106

You are developing an internal application that will allow employees to organize community events within your company. You deployed your application on a single Compute Engine instance. Your company uses Google Workspace (formerly G Suite), and you need to ensure that the company employees can authenticate to the application from anywhere. What should you do?

- A. Add a public IP address to your instance, and restrict access to the instance using firewall rules. Allow your company's proxy as the only source IP address.
- B. Add an HTTP(S) load balancer in front of the instance, and set up Identity-Aware Proxy (IAP). Configure the IAP settings to allow your company domain to access the website.
- C. Set up a VPN tunnel between your company network and your instance's VPC location on Google Cloud. Configure the required firewall rules and routing information to both the on-premises and Google Cloud networks.
- D. Add a public IP address to your instance, and allow traffic from the internet. Generate a random hash, and create a subdomain that includes this hash and points to your instance. Distribute this DNS address to your company's employees.

**Answer: B**

Explanation:

<https://cloud.google.com/blog/topics/developers-practitioners/control-access-your-web-sites-identity-aware-proxy>

### Question: 107

Your development team is using Cloud Build to promote a Node.js application built on App Engine from your staging environment to production. The application relies on several directories of photos stored in a Cloud Storage bucket named webphotos-staging in the staging environment. After the promotion, these photos must be available in a Cloud Storage bucket named webphotos-prod in the production environment. You want to automate the process where possible. What should you do?

- A) Manually copy the photos to webphotos-prod.
- B) Add a startup script in the application's app.yaml file to move the photos from webphotos-staging to webphotos-prod.
- C) Add a build step in the cloudbuild.yaml file before the promotion step with the arguments:

```
- name: ger.io/cloud-builders/gsutil
  args: ['cp', '-r', 'gs://webphotos-staging *',
        'gs://webphotos-prod']
  waitFor: ['-']
```

D)

Add a build step in the cloudbuild.yaml file before the promotion step with the arguments:

```
- name: ger.io/cloud-builders/gcloud
  args: [ 'cp', '-A', 'gs://webphotos-staging',
    'gs://webphotos-prod' ]
  waitFor: [ '*' ]
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: C**

Explanation:

<https://cloud.google.com/storage/docs/gsutil/commands/cp>

### Question: 108

You are developing a web application that will be accessible over both HTTP and HTTPS and will run on Compute Engine instances. On occasion, you will need to SSH from your remote laptop into one of the Compute Engine instances to conduct maintenance on the app. How should you configure the instances while following Google-recommended best practices?

- A. Set up a backend with Compute Engine web server instances with a private IP address behind a TCP proxy load balancer.
- B. Configure the firewall rules to allow all ingress traffic to connect to the Compute Engine web servers, with each server having a unique external IP address.
- C. Configure Cloud Identity-Aware Proxy API for SSH access. Then configure the Compute Engine servers with private IP addresses behind an HTTP(s) load balancer for the application web traffic.
- D. Set up a backend with Compute Engine web server instances with a private IP address behind an HTTP(S) load balancer. Set up a bastion host with a public IP address and open firewall ports. Connect to the web instances using the bastion host.

**Answer: C**

Explanation:

Reference: [https://cloud.google.com/compute/docs/instances/connecting-advanced#cloud\\_iap](https://cloud.google.com/compute/docs/instances/connecting-advanced#cloud_iap)  
[https://cloud.google.com/solutions/connecting-securely#storing\\_host\\_keys\\_by\\_enabling\\_guest\\_attributes](https://cloud.google.com/solutions/connecting-securely#storing_host_keys_by_enabling_guest_attributes)

### Question: 109

You have a mixture of packaged and internally developed applications hosted on a Compute Engine instance that is running Linux. These applications write log records as text in local files. You want the logs to be written to Cloud Logging. What should you do?

- A. Pipe the content of the files to the Linux Syslog daemon.
- B. Install a Google version of fluentd on the Compute Engine instance.
- C. Install a Google version of collectd on the Compute Engine instance.
- D. Using cron, schedule a job to copy the log files to Cloud Storage once a day.

**Answer: B**

Explanation:

Reference: <https://cloud.google.com/logging/docs/agent/logging/configuration>

### Question: 110

You want to create “fully baked” or “golden” Compute Engine images for your application. You need to bootstrap your application to connect to the appropriate database according to the environment the application is running on (test, staging, production). What should you do?

- A. Embed the appropriate database connection string in the image. Create a different image for each environment.
- B. When creating the Compute Engine instance, add a tag with the name of the database to be connected. In your application, query the Compute Engine API to pull the tags for the current instance, and use the tag to construct the appropriate database connection string.
- C. When creating the Compute Engine instance, create a metadata item with a key of “DATABASE” and a value for the appropriate database connection string. In your application, read the “DATABASE” environment variable, and use the value to connect to the appropriate database.
- D. When creating the Compute Engine instance, create a metadata item with a key of “DATABASE” and a value for the appropriate database connection string. In your application, query the metadata server for the “DATABASE” value, and use the value to connect to the appropriate database.

**Answer: D**

Explanation:

### Question: 111

You are developing a microservice-based application that will be deployed on a Google Kubernetes Engine cluster. The application needs to read and write to a Spanner database. You want to follow security best practices while minimizing code changes. How should you configure your application to retrieve Spanner credentials?

- A. Configure the appropriate service accounts, and use Workload Identity to run the pods.
- B. Store the application credentials as Kubernetes Secrets, and expose them as environment variables.
- C. Configure the appropriate routing rules, and use a VPC-native cluster to directly connect to the

database.

- D. Store the application credentials using Cloud Key Management Service, and retrieve them whenever a database connection is made.

**Answer: A**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity>

### Question: 112

You are deploying your application on a Compute Engine instance that communicates with Cloud SQL. You will use Cloud SQL 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 Google- recommended best practice of providing minimum access 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.

**Answer: C**

Explanation:

Reference: <https://cloud.google.com/sql/docs/mysql/sql-proxy>

### Question: 113

Your team develops stateless services that run on Google Kubernetes Engine (GKE). You need to deploy a new service that will only be accessed by other services running in the GKE cluster. The service will need to scale as quickly as possible to respond to changing load. What should you do?

- A. Use a Vertical Pod Autoscaler to scale the containers, and expose them via a ClusterIP Service.
- B. Use a Vertical Pod Autoscaler to scale the containers, and expose them via a NodePort Service.
- C. Use a Horizontal Pod Autoscaler to scale the containers, and expose them via a ClusterIP Service.
- D. Use a Horizontal Pod Autoscaler to scale the containers, and expose them via a NodePort Service.

**Answer: C**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/service>

### Question: 114

You recently migrated a monolithic application to Google Cloud by breaking it down into microservices. One of the microservices is deployed using Cloud Functions. As you modernize the application, you make a change to the API of the service that is backward-incompatible. You need to support both existing callers who use the original API and new callers who use the new API. What should you do?

- A. Leave the original Cloud Function as-is and deploy a second Cloud Function with the new API. Use a load balancer to distribute calls between the versions.
- B. Leave the original Cloud Function as-is and deploy a second Cloud Function that includes only the changed API. Calls are automatically routed to the correct function.
- C. Leave the original Cloud Function as-is and deploy a second Cloud Function with the new API. Use Cloud Endpoints to provide an API gateway that exposes a versioned API.
- D. Re-deploy the Cloud Function after making code changes to support the new API. Requests for both versions of the API are fulfilled based on a version identifier included in the call.

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/endpoints/docs/openapi/versioning-an-api>

### Question: 115

You are developing an application that will allow users to read and post comments on news articles.

You want to configure your application to store and display user-submitted comments using Firestore. How should you design the schema to support an unknown number of comments and articles?

- A. Store each comment in a subcollection of the article.
- B. Add each comment to an array property on the article.
- C. Store each comment in a document, and add the comment's key to an array property on the article.
- D. Store each comment in a document, and add the comment's key to an array property on the user profile.

**Answer: D**

Explanation:

### Question: 116

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

**Answer: D**

Explanation:

<https://cloud.google.com/vpc/docs/private-google-access>

### Question: 117

You are a developer working with the CI/CD team to troubleshoot a new feature that your team introduced. The CI/CD team used HashiCorp Packer to create a new Compute Engine image from your development branch. The image was successfully built, but is not booting up. You need to investigate the issue with the CI/CD team. What should you do?

- A. Create a new feature branch, and ask the build team to rebuild the image.
- B. Shut down the deployed virtual machine, export the disk, and then mount the disk locally to access the boot logs.
- C. Install Packer locally, build the Compute Engine image locally, and then run it in your personal Google Cloud project.
- D. Check Compute Engine OS logs using the serial port, and check the Cloud Logging logs to confirm access to the serial port.

**Answer: D**

Explanation:

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console>

### Question: 118

You manage an application that runs in a Compute Engine instance. You also have multiple backend services executing in stand-alone Docker containers running in Compute Engine instances. The Compute Engine instances supporting the backend services are scaled by managed instance groups in multiple regions. You want your calling application to be loosely coupled. You need to be able to invoke distinct service implementations that are chosen based on the value of an HTTP header found in the request. Which Google Cloud feature should you use to invoke the backend services?

- A. Traffic Director
- B. Service Directory
- C. Anthos Service Mesh
- D. Internal HTTP(S) Load Balancing

**Answer: D**

Explanation:

### Question: 119

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 saved. How should you store users' session and shopping cart information while following Google-recommended best practices?

- A. Store the session information in Pub/Sub, and store the shopping cart information in Cloud SQL.
- B. Store the shopping cart information in a file on Cloud Storage where the filename is the SESSION ID.
- C. Store the session and shopping cart information in a MySQL database running on multiple Compute Engine instances.

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

**Answer: D**

Explanation:

### Question: 120

You are designing a resource-sharing policy for applications used by different teams in a Google Kubernetes Engine cluster. You need to ensure that all applications can access the resources needed to run. What should you do? (Choose two.)

- A. Specify the resource limits and requests in the object specifications.
- B. Create a namespace for each team, and attach resource quotas to each namespace.
- C. Create a LimitRange to specify the default compute resource requirements for each namespace.
- D. Create a Kubernetes service account (KSA) for each application, and assign each KSA to the namespace.
- E. Use the Anthos Policy Controller to enforce label annotations on all namespaces. Use taints and tolerations to allow resource sharing for namespaces.

**Answer: BC**

Explanation:

<https://kubernetes.io/docs/concepts/policy/resource-quotas/>

<https://kubernetes.io/docs/concepts/policy/limit-range/>

<https://cloud.google.com/blog/products/containers-kubernetes/kubernetes-best-practices-resource-requests-and-limits>

### Question: 121

You are developing a new application that has the following design requirements:

Creation and changes to the application infrastructure are versioned and auditable.

The application and deployment infrastructure uses Google-managed services as much as possible.

The application runs on a serverless compute platform.

How should you design the application's architecture?

A.

1. Store the application and infrastructure source code in a Git repository.
2. Use Cloud Build to deploy the application infrastructure with Terraform.
3. Deploy the application to a Cloud Function as a pipeline step.

B.

1. Deploy Jenkins from the Google Cloud Marketplace, and define a continuous integration pipeline in Jenkins.
2. Configure a pipeline step to pull the application source code from a Git repository.
3. Deploy the application source code to App Engine as a pipeline step.

C.

1. Create a continuous integration pipeline on Cloud Build, and configure the pipeline to deploy the application infrastructure using Deployment Manager templates.
2. Configure a pipeline step to create a container with the latest application source code.
3. Deploy the container to a Compute Engine instance as a pipeline step.

D.

1. Deploy the application infrastructure using gcloud commands.
2. Use Cloud Build to define a continuous integration pipeline for changes to the application source code.
3. Configure a pipeline step to pull the application source code from a Git repository, and create a containerized application.
4. Deploy the new container on Cloud Run as a pipeline step.

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/docs/ci-cd>

### Question: 122

You are creating and running containers across different projects in Google Cloud. The application you are developing needs to access Google Cloud services from within Google Kubernetes Engine (GKE).

What should you do?

- A. Assign a Google service account to the GKE nodes.
- B. Use a Google service account to run the Pod with Workload Identity.
- C. Store the Google service account credentials as a Kubernetes Secret.
- D. Use a Google service account with GKE role-based access control (RBAC).

**Answer: B**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity>

### Question: 123

You have containerized a legacy application that stores its configuration on an NFS share. You need to deploy this application to Google Kubernetes Engine (GKE) and do not want the application serving traffic until after the configuration has been retrieved. What should you do?

- A. Use the gsutil utility to copy files from within the Docker container at startup, and start the service using an ENTRYPOINT script.
- B. Create a PersistentVolumeClaim on the GKE cluster. Access the configuration files from the volume, and start the service using an ENTRYPOINT script.
- C. Use the COPY statement in the Dockerfile to load the configuration into the container image. Verify that the configuration is available, and start the service using an ENTRYPOINT script.
- D. Add a startup script to the GKE instance group to mount the NFS share at node startup. Copy the configuration files into the container, and start the service using an ENTRYPOINT script.

## Answer: B

Explanation:

Reference: <https://cloud.google.com/compute/docs/instances/startup-scripts/linux>

### Question: 124

Your team is developing a new application using a PostgreSQL database and Cloud Run. You are responsible for ensuring that all traffic is kept private on Google Cloud. You want to use managed services and follow Google-recommended best practices. What should you do?

A.

1. Enable Cloud SQL and Cloud Run in the same project.
2. Configure a private IP address for Cloud SQL. Enable private services access.
3. Create a Serverless VPC Access connector.
4. Configure Cloud Run to use the connector to connect to Cloud SQL.

B.

1. Install PostgreSQL on a Compute Engine virtual machine (VM), and enable Cloud Run in the same project.
2. Configure a private IP address for the VM. Enable private services access.
3. Create a Serverless VPC Access connector.
4. Configure Cloud Run to use the connector to connect to the VM hosting PostgreSQL.

C.

1. Use Cloud SQL and Cloud Run in different projects.
2. Configure a private IP address for Cloud SQL. Enable private services access.
3. Create a Serverless VPC Access connector.
4. Set up a VPN connection between the two projects. Configure Cloud Run to use the connector to connect to Cloud SQL.

D.

1. Install PostgreSQL on a Compute Engine VM, and enable Cloud Run in different projects.
2. Configure a private IP address for the VM. Enable private services access.
3. Create a Serverless VPC Access connector.
4. Set up a VPN connection between the two projects. Configure Cloud Run to use the connector to access the VM hosting PostgreSQL.

## Answer: A

Explanation:

<https://cloud.google.com/sql/docs/postgres/connect-run#private-ip>

### Question: 125

You are developing an application that will allow clients to download a file from your website for a specific period of time. How should you design the application to complete this task while following Google-recommended best practices?

- A. Configure the application to send the file to the client as an email attachment.
- B. Generate and assign a Cloud Storage-signed URL for the file. Make the URL available for the client to download.
- C. Create a temporary Cloud Storage bucket with time expiration specified, and give download permissions to the bucket. Copy the file, and send it to the client.

D. Generate the HTTP cookies with time expiration specified. If the time is valid, copy the file from the Cloud Storage bucket, and make the file available for the client to download.

**Answer: B**

Explanation:

### Question: 126

Your development team has been asked to refactor an existing monolithic application into a set of composable microservices. Which design aspects should you implement for the new application? (Choose two.)

- A. Develop the microservice code in the same programming language used by the microservice caller.
- B. Create an API contract agreement between the microservice implementation and microservice caller.
- C. Require asynchronous communications between all microservice implementations and microservice callers.
- D. Ensure that sufficient instances of the microservice are running to accommodate the performance requirements.
- E. Implement a versioning scheme to permit future changes that could be incompatible with the current interface.

**Answer: BE**

Explanation:

### Question: 127

You deployed a new application to Google Kubernetes Engine and are experiencing some performance degradation. Your logs are being written to Cloud Logging, and you are using a Prometheus sidecar model for capturing metrics. You need to correlate the metrics and data from the logs to troubleshoot the performance issue and send real-time alerts while minimizing costs.

What should you do?

- A. Create custom metrics from the Cloud Logging logs, and use Prometheus to import the results using the Cloud Monitoring REST API.
- B. Export the Cloud Logging logs and the Prometheus metrics to Cloud Bigtable. Run a query to join the results, and analyze in Google Data Studio.
- C. Export the Cloud Logging logs and stream the Prometheus metrics to BigQuery. Run a recurring query to join the results, and send notifications using Cloud Tasks.
- D. Export the Prometheus metrics and use Cloud Monitoring to view them as external metrics. Configure Cloud Monitoring to create log-based metrics from the logs, and correlate them with the Prometheus data.

**Answer: D**

Explanation:

Reference: <https://cloud.google.com/blog/products/operations/troubleshoot-gke-faster-with-monitoring-data-in-your-logs>

### Question: 128

You have been tasked with planning the migration of your company's application from on-premises to Google Cloud. Your company's monolithic application is an ecommerce website. The application will be migrated to microservices deployed on Google Cloud in stages. The majority of your company's revenue is generated through online sales, so it is important to minimize risk during the migration. You need to prioritize features and select the first functionality to migrate. What should you do?

- A. Migrate the Product catalog, which has integrations to the frontend and product database.
- B. Migrate Payment processing, which has integrations to the frontend, order database, and third-party payment vendor.
- C. Migrate Order fulfillment, which has integrations to the order database, inventory system, and third-party shipping vendor.
- D. Migrate the Shopping cart, which has integrations to the frontend, cart database, inventory system, and payment processing system.

**Answer: A**

Explanation:

### Question: 129

Your team develops services that run on Google Kubernetes Engine. Your team's code is stored in Cloud Source Repositories. You need to quickly identify bugs in the code before it is deployed to production. You want to invest in automation to improve developer feedback and make the process as efficient as possible. What should you do?

- A. Use Spinnaker to automate building container images from code based on Git tags.
- B. Use Cloud Build to automate building container images from code based on Git tags.
- C. Use Spinnaker to automate deploying container images to the production environment.
- D. Use Cloud Build to automate building container images from code based on forked versions.

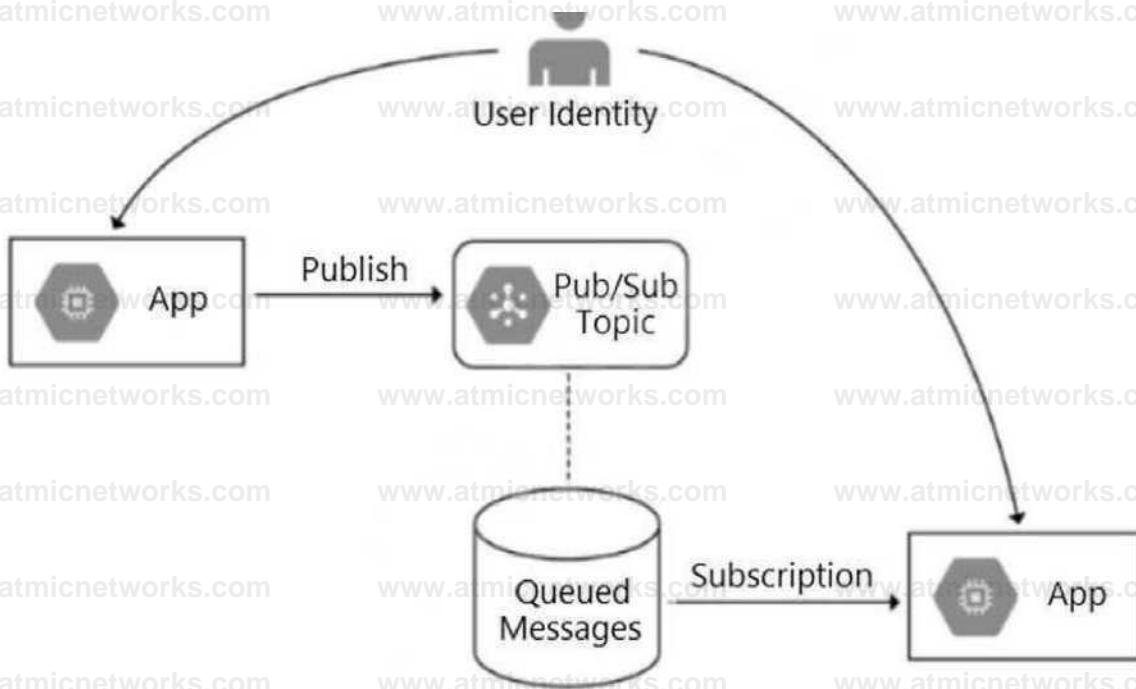
**Answer: A**

Explanation:

Reference: <https://spinnaker.io/docs/guides/tutorials/codelabs/kubernetes-v2-source-to-prod/>

### Question: 130

Your team is developing an application in Google Cloud that executes with user identities maintained by Cloud Identity. Each of your application's users will have an associated Pub/Sub topic to which messages are published, and a Pub/Sub subscription where the same user will retrieve published messages. You need to ensure that only authorized users can publish and subscribe to their own specific Pub/Sub topic and subscription. What should you do?



- A. Bind the user identity to the pubsub.publisher and pubsub.subscriber roles at the resource level.
- B. Grant the user identity the pubsub.publisher and pubsub.subscriber roles at the project level.
- C. Grant the user identity a custom role that contains the pubsub.topics.create and pubsub.subscriptions.create permissions.
- D. Configure the application to run as a service account that has the pubsub.publisher and pubsub.subscriber roles.

**Answer: C**

Explanation:

### Question: 131

You are evaluating developer tools to help drive Google Kubernetes Engine adoption and integration with your development environment, which includes VS Code and IntelliJ. What should you do?

- A. Use Cloud Code to develop applications.
- B. Use the Cloud Shell integrated Code Editor to edit code and configuration files.
- C. Use a Cloud Notebook instance to ingest and process data and deploy models.
- D. Use Cloud Shell to manage your infrastructure and applications from the command line.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/code>

### Question: 132

You are developing an ecommerce web application that uses App Engine standard environment 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 App Engine instance.
- C. The firewall rule allowing a connection between App Engine 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 availability zone than your App Engine instance.

**Answer: A**

Explanation:

Reference: <https://cloud.google.com/endpoints/docs/openapi/troubleshoot-response-errors>

### Question: 133

Your team develops services that run on Google Cloud. You need to build a data processing service and will use Cloud Functions. The data to be processed by the function is sensitive. You need to ensure that invocations can only happen from authorized services and follow Google-recommended best practices for securing functions. What should you do?

- A. Enable Identity-Aware Proxy in your project. Secure function access using its permissions.
- B. Create a service account with the Cloud Functions Viewer role. Use that service account to invoke the function.
- C. Create a service account with the Cloud Functions Invoker role. Use that service account to invoke the function.
- D. Create an OAuth 2.0 client ID for your calling service in the same project as the function you want to secure. Use those credentials to invoke the function.

**Answer: C**

Explanation:

Reference: <https://medium.com/google-cloud/how-to-securely-invoke-a-cloud-function-from-google-kubernetes-engine-running-on-another-gcp-79797ec2b2c6>

### Question: 134

You are deploying your applications on Compute Engine. One of your Compute Engine instances failed to launch. What should you do? (Choose two.)

- A. Determine whether your file system is corrupted.
- B. Access Compute Engine as a different SSH user.
- C. Troubleshoot firewall rules or routes on an instance.
- D. Check whether your instance boot disk is completely full.
- E. Check whether network traffic to or from your instance is being dropped.

## Answer: AD

Explanation:

<https://cloud.google.com/compute/docs/troubleshooting/vm-startup>

### Question: 135

Your web application is deployed to the corporate intranet. You need to migrate the web application to Google Cloud. The web application must be available only to company employees and accessible to employees as they travel. You need to ensure the security and accessibility of the web application while minimizing application changes. What should you do?

- A. Configure the application to check authentication credentials for each HTTP(S) request to the application.
- B. Configure Identity-Aware Proxy to allow employees to access the application through its public IP address.
- C. Configure a Compute Engine instance that requests users to log in to their corporate account. Change the web application DNS to point to the proxy Compute Engine instance. After authenticating, the Compute Engine instance forwards requests to and from the web application.
- D. Configure a Compute Engine instance that requests users to log in to their corporate account. Change the web application DNS to point to the proxy Compute Engine instance. After authenticating, the Compute Engine issues an HTTP redirect to a public IP address hosting the web application.

## Answer: B

Explanation:

### Question: 136

You have an application that uses an HTTP Cloud Function to process user activity from both desktop browser and mobile application clients. This function will serve as the endpoint for all metric submissions using HTTP POST.

Due to legacy restrictions, the function must be mapped to a domain that is separate from the domain requested by users on web or mobile sessions. The domain for the Cloud Function is `https://fn.example.com`. Desktop and mobile clients use the domain `https://www.example.com`. You need to add a header to the function's HTTP response so that only those browser and mobile sessions can submit metrics to the Cloud Function. Which response header should you add?

- A. Access-Control-Allow-Origin: \*
- B. Access-Control-Allow-Origin: `https://*.example.com`
- C. Access-Control-Allow-Origin: `https://fn.example.com`
- D. Access-Control-Allow-origin: `https://www.example.com`

## Answer: D

Explanation:

### Question: 137

You have an HTTP Cloud Function that is called via POST. Each submission's request body has a flat, unnested JSON structure containing numeric and text data.

a. After the Cloud Function completes, the collected data should be immediately available for ongoing and complex analytics by many users in parallel. How should you persist the submissions?

- A. Directly persist each POST request's JSON data into Datastore.
- B. Transform the POST request's JSON data, and stream it into BigQuery.
- C. Transform the POST request's JSON data, and store it in a regional Cloud SQL cluster.
- D. Persist each POST request's JSON data as an individual file within Cloud Storage, with the file name containing the request identifier.

**Answer: D**

Explanation:

### Question: 138

Your security team is auditing all deployed applications running in Google Kubernetes Engine. After completing the audit, your team discovers that some of the applications send traffic within the cluster in clear text. You need to ensure that all application traffic is encrypted as quickly as possible while minimizing changes to your applications and maintaining support from Google. What should you do?

- A. Use Network Policies to block traffic between applications.
- B. Install Istio, enable proxy injection on your application namespace, and then enable mTLS.
- C. Define Trusted Network ranges within the application, and configure the applications to allow traffic only from those networks.
- D. Use an automated process to request SSL Certificates for your applications from Let's Encrypt and add them to your applications.

**Answer: D**

Explanation:

### Question: 139

You migrated some of your applications to Google Cloud. You are using a legacy monitoring platform deployed on-premises for both on-premises and cloud-deployed applications. You discover that your notification system is responding slowly to time-critical problems in the cloud applications. What should you do?

- A. Replace your monitoring platform with Cloud Monitoring.
- B. Install the Cloud Monitoring agent on your Compute Engine instances.
- C. Migrate some traffic back to your old platform. Perform A/B testing on the two platforms concurrently.
- D. Use Cloud Logging and Cloud Monitoring to capture logs, monitor, and send alerts. Send them to your existing platform.

**Answer: D**

Explanation:

### Question: 140

You recently deployed your application in Google Kubernetes Engine, and now need to release a new version of your application. You need the ability to instantly roll back to the previous version in case there are issues with the new version. Which deployment model should you use?

- A. Perform a rolling deployment, and test your new application after the deployment is complete.
- B. Perform A/B testing, and test your application periodically after the new tests are implemented.
- C. Perform a blue/green deployment, and test your new application after the deployment is complete.
- D. Perform a canary deployment, and test your new application periodically after the new version is deployed.

**Answer: C**

Explanation:

### Question: 141

You developed a JavaScript web application that needs to access Google Drive's API and obtain permission from users to store files in their Google Drives. You need to select an authorization approach for your application. What should you do?

- A. Create an API key.
- B. Create a SAML token.
- C. Create a service account.
- D. Create an OAuth Client ID.

**Answer: D**

Explanation:

Reference: <https://developers.google.com/drive/api/v3/about-auth>

### Question: 142

You manage an ecommerce application that processes purchases from customers who can subsequently cancel or change those purchases. You discover that order volumes are highly variable and the backend order-processing system can only process one request at a time. You want to ensure seamless performance for customers regardless of usage volume. It is crucial that customers' order update requests are performed in the sequence in which they were generated. What should you do?

- A. Send the purchase and change requests over WebSockets to the backend.
- B. Send the purchase and change requests as REST requests to the backend.
- C. Use a Pub/Sub subscriber in pull mode and use a data store to manage ordering.
- D. Use a Pub/Sub subscriber in push mode and use a data store to manage ordering.

**Answer: C**

Explanation:

<https://cloud.google.com/pubsub/docs/pull>

### Question: 143

Your company needs a database solution that stores customer purchase history and meets the following requirements:

Customers can query their purchase immediately after submission.

Purchases can be sorted on a variety of fields.

Distinct record formats can be stored at the same time.

Which storage option satisfies these requirements?

- A. Firestore in Native mode
- B. Cloud Storage using an object read
- C. Cloud SQL using a SQL SELECT statement
- D. Firestore in Datastore mode using a global query

**Answer: A**

Explanation:

### Question: 144

You recently developed a new service on Cloud Run. The new service authenticates using a custom service and then writes transactional information to a Cloud Spanner database. You need to verify that your application can support up to 5,000 read and 1,000 write transactions per second while identifying any bottlenecks that occur. Your test infrastructure must be able to autoscale. What should you do?

- A. Build a test harness to generate requests and deploy it to Cloud Run. Analyze the VPC Flow Logs using Cloud Logging.
- B. Create a Google Kubernetes Engine cluster running the Locust or JMeter images to dynamically generate load tests. Analyze the results using Cloud Trace.
- C. Create a Cloud Task to generate a test load. Use Cloud Scheduler to run 60,000 Cloud Task transactions per minute for 10 minutes. Analyze the results using Cloud Monitoring.
- D. Create a Compute Engine instance that uses a LAMP stack image from the Marketplace, and use Apache Bench to generate load tests against the service. Analyze the results using Cloud Trace.

**Answer: B**

Explanation:

<https://cloud.google.com/architecture/distributed-load-testing-using-gke>

### Question: 145

You are using Cloud Build for your CI/CD pipeline to complete several tasks, including copying certain files to Compute Engine virtual machines. Your pipeline requires a flat file that is generated in one builder in the pipeline to be accessible by subsequent builders in the same pipeline. How should you store the file so that all the builders in the pipeline can access it?

- A. Store and retrieve the file contents using Compute Engine instance metadata.
- B. Output the file contents to a file in /workspace. Read from the same /workspace file in the subsequent build step.
- C. Use gsutil to output the file contents to a Cloud Storage object. Read from the same object in the subsequent build step.
- D. Add a build argument that runs an HTTP POST via curl to a separate web server to persist the value in one builder. Use an HTTP GET via curl from the subsequent build step to read the value.

**Answer: B**

Explanation:

<https://cloud.google.com/build/docs/build-config-file-schema>

### Question: 146

Your company's development teams want to use various open source operating systems in their Docker builds. When images are created in published containers in your company's environment, 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 Vulnerability scanning setting in the Container Registry.
- B. Create a Cloud Function 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.

**Answer: A**

Explanation:

<https://cloud.google.com/container-analysis/docs/os-overview>

### Question: 147

You are configuring a continuous integration pipeline using Cloud Build to automate the deployment of new container images to Google Kubernetes Engine (GKE). The pipeline builds the application from its source code, runs unit and integration tests in separate steps, and pushes the container to Container Registry. The application runs on a Python web server.

The Dockerfile 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 Docker image for subsequent builds using the --cache-from argument in your build config file.
- D. Change the base image in the Dockerfile 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.

**Answer: AC**

Explanation:

<https://cloud.google.com/build/docs/optimize-builds/increase-vcpu-for-builds>

By default, Cloud Build runs your builds on a standard virtual machine (VM). In addition to the standard VM, Cloud Build provides several high-CPU VM types to run builds. To increase the speed of your build, select a machine with a higher vCPU to run builds. Keep in mind that although selecting a high vCPU machine increases your build speed, it may also increase the startup time of your build as Cloud Build only starts non-standard machines on demand.

[https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using\\_a\\_cached\\_docker\\_image](https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using_a_cached_docker_image)

The easiest way to increase the speed of your Docker image build is by specifying a cached image that can be used for subsequent builds. You can specify the cached image by adding the --cache-from argument in your build config file, which will instruct Docker to build using that image as a cache SOURCE.

## Question: 148

You are building a CI/CD pipeline that consists of a version control system, Cloud Build, and Container Registry. Each time a new tag is pushed to the repository, a Cloud Build job is triggered, which runs unit tests on the new code builds a new Docker container image, and pushes it into Container Registry. The last step of your pipeline should deploy the new container to your production Google Kubernetes Engine (GKE) cluster. You need to select a tool and deployment strategy that meets the

following requirements:

- Zero downtime is incurred
- Testing is fully automated
- Allows for testing before being rolled out to users
- Can quickly rollback if needed

What should you do?

- A. Trigger a Spinnaker pipeline configured as an A/B test of your new code and, if it is successful, deploy the container to production.
- B. Trigger a Spinnaker pipeline configured as a canary test of your new code and, if it is successful, deploy the container to production.

- C. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a canary test.
- D. Trigger another Cloud Build job that uses the Kubernetes CLI tools to deploy your new container to your GKE cluster, where you can perform a shadow test.

**Answer: D**

Explanation:

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform\\_a\\_shadow\\_test](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform_a_shadow_test) With a shadow test, you test the new version of your application by mirroring user traffic from the current application version without impacting the user requests.

### Question: 149

Your operations team has asked you to create a script that lists the Cloud Bigtable, Memorystore, and Cloud SQL databases running within a project. The script should allow users to submit a filter expression to limit the results presented. How should you retrieve the data?

- A. Use the HBase API, Redis API, and MySQL connection to retrieve database lists. Combine the results, and then apply the filter to display the results
- B. Use the HBase API, Redis API, and MySQL connection to retrieve database lists. Filter the results individually, and then combine them to display the results
- C. Run `gcloud bigtable instances list`, `gcloud redis instances list`, and `gcloud sql databases list`. Use a filter within the application, and then display the results
- D. Run `gcloud bigtable instances list`, `gcloud redis instances list`, and `gcloud sql databases list`. Use `-filter` flag with each command, and then display the results

**Answer: D**

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/topic/filters>

Most `gcloud` commands return a list of resources on success. By default they are pretty-printed on the standard output. The `--format=NAME[ATTRIBUTES](PROJECTION)` and `--filter=EXPRESSION` flags along with projections can be used to format and change the default output to a more meaningful result. Use the `--format` flag to change the default output format of a command. For details run `$ gcloud topic formats`.

### Question: 150

You need to deploy a new European version of a website hosted on Google Kubernetes Engine. The current and new websites must be accessed via the same HTTP(S) load balancer's external IP address, but have different domain names. What should you do?

- A. Define a new Ingress resource with a host rule matching the new domain

- B. Modify the existing Ingress resource with a host rule matching the new domain
- C. Create a new Service of type LoadBalancer specifying the existing IP address as the loadBalancerIP
- D. Generate a new Ingress resource and specify the existing IP address as the kubernetes.io/ingress.global-static-ip-name annotation value

**Answer: B**

Explanation:

<https://kubernetes.io/docs/concepts/services-networking/ingress/#name-based-virtual-hosting> Name-based virtual hosts support routing HTTP traffic to multiple host names at the same IP address.

### Question: 151

You are developing a single-player mobile game backend that has unpredictable traffic patterns as users interact with the game throughout the day and night. You want to optimize costs by ensuring that you have enough resources to handle requests, but minimize over-provisioning. You also want the system to handle traffic spikes efficiently. Which compute platform should you use?

- A. Cloud Run
- B. Compute Engine with managed instance groups
- C. Compute Engine with unmanaged instance groups
- D. Google Kubernetes Engine using cluster autoscaling

**Answer: A**

Explanation:

### Question: 152

The development teams in your company want to manage resources from their local environments. You have been asked to enable developer access to each team's Google Cloud projects. You want to maximize efficiency while following Google-recommended best practices. What should you do?

- A. Add the users to their projects, assign the relevant roles to the users, and then provide the users with each relevant Project ID.
- B. Add the users to their projects, assign the relevant roles to the users, and then provide the users with each relevant Project Number.
- C. Create groups, add the users to their groups, assign the relevant roles to the groups, and then provide the users with each relevant Project ID.
- D. Create groups, add the users to their groups, assign the relevant roles to the groups, and then provide the users with each relevant Project Number.

**Answer: C**

Explanation:

### Question: 153

Your company's product team has a new requirement based on customer demand to autoscale your stateless and distributed service running in a Google Kubernetes Engine (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.

**Answer: C**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/horizontalpodautoscaler>

The Horizontal Pod Autoscaler changes the shape of your Kubernetes workload by automatically increasing or decreasing the number of Pods in response to the workload's CPU or memory consumption, or in response to custom metrics reported from within Kubernetes or external metrics from sources outside of your cluster.

### Question: 154

Your application is composed of a set of loosely coupled services orchestrated by code executed on Compute Engine. You want your application to easily bring up new Compute Engine instances that find and use a specific version of a service. How should this be configured?

- A. Define your service endpoint information as metadata that is retrieved at runtime and used to connect to the desired service.
- B. Define your service endpoint information as label data that is retrieved at runtime and used to connect to the desired service.
- C. Define your service endpoint information to be retrieved from an environment variable at runtime and used to connect to the desired service.
- D. Define your service to use a fixed hostname and port to connect to the desired service. Replace the service at the endpoint with your new version.

**Answer: A**

Explanation:

<https://cloud.google.com/service-infrastructure/docs/service-metadata/reference/rest#service-endpoint>

### Question: 155

You are developing a microservice-based application that will run on Google Kubernetes Engine (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 in the cluster via the gcloud command-line tool.
- C. Access the Google service account keys from a secret management service.
- D. Store the Google service account keys in a central secret management service.
- E. Use gcloud to bind the Kubernetes service account and the Google service account using roles/iam.workloadIdentity.

**Answer: BE**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/how-to/workload-identity>

### Question: 156

Your development team has been tasked with maintaining a .NET legacy application. The application incurs occasional changes and was recently updated. Your goal is to ensure that the application provides consistent results while moving through the CI/CD pipeline from environment to environment. You want to minimize the cost of deployment while making sure that external factors and dependencies between hosting environments are not problematic. Containers are not yet approved in your organization. What should you do?

- A. Rewrite the application using .NET Core, and deploy to Cloud Run. Use revisions to separate the environments.
- B. Use Cloud Build to deploy the application as a new Compute Engine image for each build. Use this image in each environment.
- C. Deploy the application using MS Web Deploy, and make sure to always use the latest, patched MS Windows Server base image in Compute Engine.
- D. Use Cloud Build to package the application, and deploy to a Google Kubernetes Engine cluster. Use namespaces to separate the environments.

**Answer: B**

Explanation:

[https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#phase\\_1\\_rehost\\_in\\_the\\_cloud](https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud#phase_1_rehost_in_the_cloud)

<https://cloud.google.com/architecture/modernization-path-dotnet-applications-google-cloud>

### Question: 157

The new version of your containerized application has been tested and is ready to deploy to production on Google Kubernetes Engine. You were not able to fully load-test the new version in preproduction environments, and you need to make sure that it does not have performance problems once deployed. Your deployment must be automated. What should you do?

- www.atmicnetworks.com
- A. Use Cloud Load Balancing to slowly ramp up traffic between versions. Use Cloud Monitoring to look for performance issues.
  - B. Deploy the application via a continuous delivery pipeline using canary deployments. Use Cloud Monitoring to look for performance issues. and ramp up traffic as the metrics support it.
  - C. Deploy the application via a continuous delivery pipeline using blue/green deployments. Use Cloud Monitoring to look for performance issues, and launch fully when the metrics support it.
  - D. Deploy the application using kubectl and set the spec.updateStrategy.type to RollingUpdate. Use Cloud Monitoring to look for performance issues, and run the kubectl rollback command if there are any issues.

**Answer: C**

Explanation:

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform a bluegreen deployment](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#perform_a_bluegreen_deployment)

### Question: 158

Users are complaining that your Cloud Run-hosted website responds too slowly during traffic spikes. You want to provide a better user experience during traffic peaks. What should you do?

- A. Read application configuration and static data from the database on application startup.
- B. Package application configuration and static data into the application image during build time.
- C. Perform as much work as possible in the background after the response has been returned to the user.
- D. Ensure that timeout exceptions and errors cause the Cloud Run instance to exit quickly so a replacement instance can be started.

**Answer: C**

Explanation:

### Question: 159

You are a developer working on an internal application for payroll processing. You are building a component of the application that allows an employee to submit a timesheet, which then initiates several steps:

- An email is sent to the employee and manager, notifying them that the timesheet was submitted.
- A timesheet is sent to payroll processing for the vendor's API.
- A timesheet is sent to the data warehouse for headcount planning.

These steps are not dependent on each other and can be completed in any order. New steps are being considered and will be implemented by different development teams. Each development team will implement the error handling specific to their step. What should you do?

- A. Deploy a Cloud Function for each step that calls the corresponding downstream system to complete the required action.
- B. Create a Pub/Sub topic for each step. Create a subscription for each downstream development team to subscribe

to their step's topic.

C. Create a Pub/Sub topic for timesheet submissions. Create a subscription for each downstream development team to subscribe to the topic.

D. Create a timesheet microservice deployed to Google Kubernetes Engine. The microservice calls each downstream step and waits for a successful response before calling the next step.

**Answer: C**

Explanation:

### Question: 160

You are designing an application that uses a microservices architecture. You are planning to deploy the application in the cloud and on-premises. You want to make sure the application can scale up on demand and also use managed services as much as possible. What should you do?

- A. Deploy open source Istio in a multi-cluster deployment on multiple Google Kubernetes Engine (GKE) clusters managed by Anthos.
- B. Create a GKE cluster in each environment with Anthos, and use Cloud Run for Anthos to deploy your application to each cluster.
- C. Install a GKE cluster in each environment with Anthos, and use Cloud Build to create a Deployment for your application in each cluster.
- D. Create a GKE cluster in the cloud and install open-source Kubernetes on-premises. Use an external load balancer service to distribute traffic across the two environments.

**Answer: B**

Explanation:

<https://cloud.google.com/anthos/run>

Integrated with Anthos, Cloud Run for Anthos provides a flexible serverless development platform for hybrid and multicloud environments. Cloud Run for Anthos is Google's managed and fully supported Knative offering, an open source project that enables serverless workloads on Kubernetes.

### Question: 161

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. Google Kubernetes Engine
- D. App Engine flexible environment

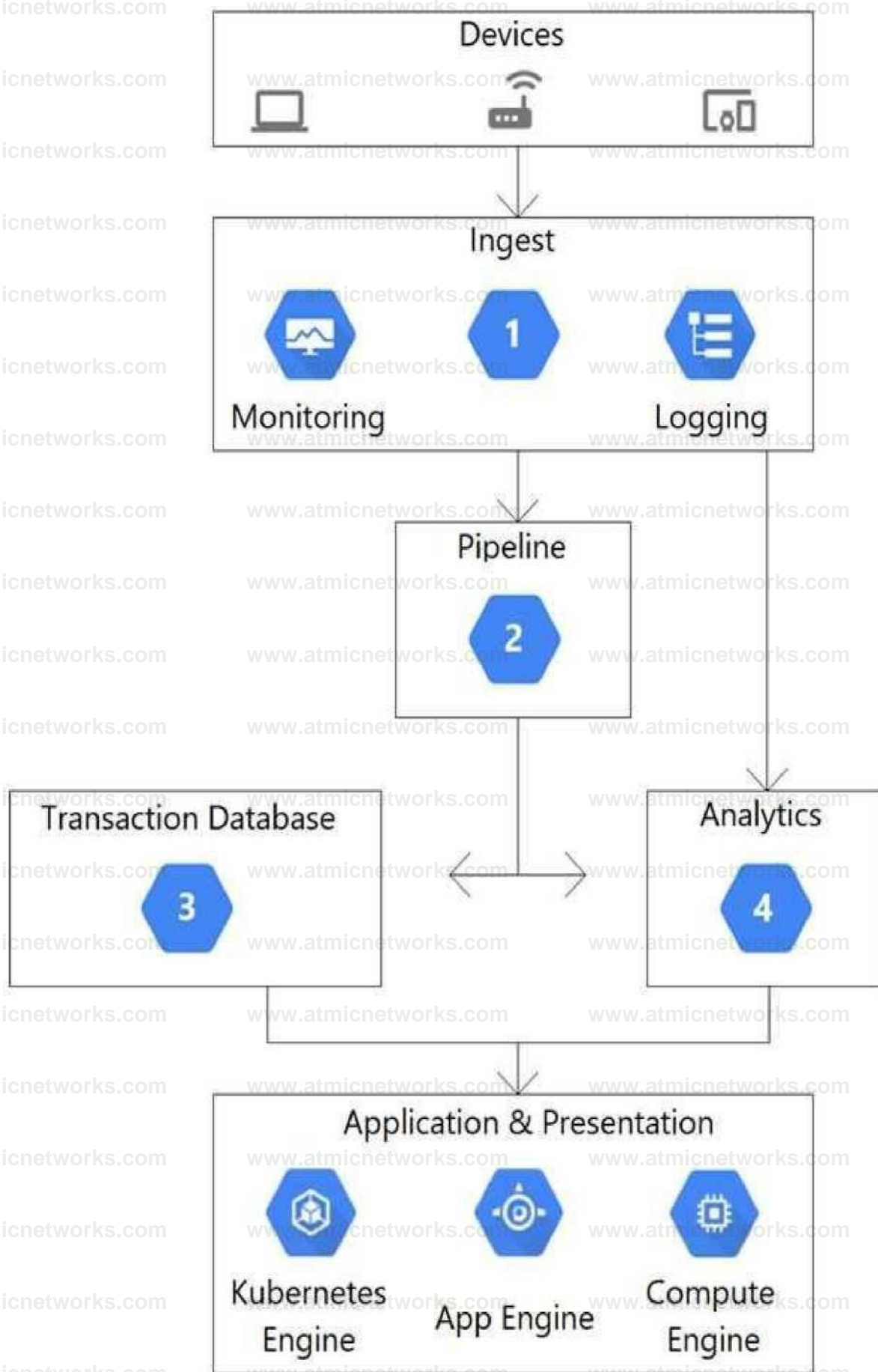
**Answer: A**

Explanation:

<https://cloud.google.com/blog/products/serverless/knative-based-cloud-run-services-are-ga>

**Question: 162**

This architectural diagram depicts a system that streams data from thousands of devices. You want to ingest data into a pipeline, store the data, and analyze the data using SQL statements. Which Google Cloud services should you use for steps 1, 2, 3, and 4?



A. 1) App Engine

- 2) Pub/Sub
- 3) BigQuery
- 4) Firestore
- 8) 1) Dataflow
- 2) Pub/Sub
- 3) Firestore
- 4) BigQuery C. 1) Pub/Sub 2) Dataflow
- 3) BigQuery
- 4) Firestore D. 1) Pub/Sub 2) Dataflow
- 3) Firestore
- 4) BigQuery

**Answer: D**

Explanation:

### Question: 163

Your company just experienced a Google Kubernetes Engine (GKE) API outage due to a zone failure. You want to deploy a highly available GKE architecture that minimizes service interruption to users in the event of a future zone failure. What should you do?

- A. Deploy Zonal clusters
- B. Deploy Regional clusters
- C. Deploy Multi-Zone clusters
- D. Deploy GKE on-premises clusters

**Answer: B**

Explanation:

[https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional\\_clusters](https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters#regional_clusters)

A regional cluster has multiple replicas of the control plane, running in multiple zones within a given region. Nodes in a regional cluster can run in multiple zones or a single zone depending on the configured node locations. By default, GKE replicates each node pool across three zones of the control plane's region. When you create a cluster or when you add a new node pool, you can change the default configuration by specifying the zone(s) in which the cluster's nodes run. All zones must be within the same region as the control plane.

### Question: 164

Your team develops services that run on Google Cloud. You want to process messages sent to a Pub/Sub topic, and then store them. Each message must be processed exactly once to avoid duplication of data and any data conflicts. You need to use the cheapest and most simple solution. What should you do?

- A. Process the messages with a Dataproc job, and write the output to storage.
- B. Process the messages with a Dataflow streaming pipeline using Apache Beam's PubSubIO package, and write the output to storage.
- C. Process the messages with a Cloud Function, and write the results to a BigQuery location where you can run a job to deduplicate the data.
- D. Retrieve the messages with a Dataflow streaming pipeline, store them in Cloud Bigtable, and use another Dataflow streaming pipeline to deduplicate messages.

**Answer: B**

Explanation:

<https://cloud.google.com/dataflow/docs/concepts/streaming-with-cloud-pubsub>

### Question: 165

You are running a containerized application on Google Kubernetes Engine. Your container images are stored in Container Registry. Your team uses CI/CD practices. You need to prevent the deployment of containers with known critical vulnerabilities. What should you do?

- A.
  - Use Web Security Scanner to automatically crawl your application
  - Review your application logs for scan results, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- B.
  - Use Web Security Scanner to automatically crawl your application
  - Review the scan results in the scan details page in the Cloud Console, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- C.
  - Enable the Container Scanning API to perform vulnerability scanning
  - Review vulnerability reporting in Container Registry in the Cloud Console, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed
- D.
  - Enable the Container Scanning API to perform vulnerability scanning
  - Programmatically review vulnerability reporting through the Container Scanning API, and provide an attestation that the container is free of known critical vulnerabilities
  - Use Binary Authorization to implement a policy that forces the attestation to be provided before the container is deployed

**Answer: D**

Explanation:

<https://cloud.google.com/binary-authorization/docs/creating-attestations-kritis>  
<https://cloud.google.com/container-analysis/docs/os-overview>

### Question: 166

You have an on-premises application that authenticates to the Cloud Storage API using a user-managed service account with a user-managed key. The application connects to Cloud Storage using Private Google Access over a Dedicated Interconnect link. You discover that requests from the application to access objects in the Cloud Storage bucket are failing with a 403 Permission Denied error code. What is the likely cause of this issue?

- A. The folder structure inside the bucket and object paths have changed.
- B. The permissions of the service account's predefined role have changed.
- C. The service account key has been rotated but not updated on the application server.
- D. The Interconnect link from the on-premises data center to Google Cloud is experiencing a temporary outage.

**Answer: C**

Explanation:

### Question: 167

You are using the Cloud Client Library to upload an image in your application to Cloud Storage. Users of the application report that occasionally the upload does not complete and the client library reports an HTTP 504 Gateway Timeout error. You want to make the application more resilient to errors. What changes to the application should you make?

- A. Write an exponential backoff process around the client library call.
- B. Write a one-second wait time backoff process around the client library call.
- C. Design a retry button in the application and ask users to click if the error occurs.
- D. Create a queue for the object and inform the users that the application will try again in 10 minutes.

**Answer: A**

Explanation:

### Question: 168

You are building a mobile application that will store hierarchical data structures in a database. The application will enable users working offline to sync changes when they are back online. A backend service will enrich the data in the database using a service account. The application is expected to be very popular and needs to scale seamlessly and securely. Which database and IAM role should you use?

- A. Use Cloud SQL, and assign the roles/cloudsql.editor role to the service account.
- B. Use Bigtable, and assign the roles/bigtable.viewer role to the service account.
- C. Use Firestore in Native mode and assign the roles/datastore.user role to the service account.

D. Use Firestore in Datastore mode and assign the roles/datastore.viewer role to the service account.

**Answer: C**

Explanation:

<https://firebase.google.com/docs/firestore/manage-data/enable-offline>

Cloud Firestore supports offline data persistence. This feature caches a copy of the Cloud Firestore data that your app is actively using, so your app can access the data when the device is offline. You can write, read, listen to, and query the cached data. When the device comes back online, Cloud Firestore synchronizes any local changes made by your app to the Cloud Firestore backend.

**Question: 169**

Your application is deployed on hundreds of Compute Engine instances in a managed instance group (MIG) in multiple zones. You need to deploy a new instance template to fix a critical vulnerability immediately but must avoid impact to your service. What setting should be made to the MIG after updating the instance template?

- A. Set the Max Surge to 100%.
- B. Set the Update mode to Opportunistic.
- C. Set the Maximum Unavailable to 100%.
- D. Set the Minimum Wait time to 0 seconds.

**Answer: B**

Explanation:

<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#type> Alternatively, if an automated update is potentially too disruptive, you can choose to perform an opportunistic update. The MIG applies an opportunistic update only when you manually initiate the update on selected instances or when new instances are created. New instances can be created when you or another service, such as an autoscaler, resizes the MIG. Compute Engine does not actively initiate requests to apply opportunistic updates on existing instances.

**Question: 170**

You made a typo in a low-level Linux configuration file that prevents your Compute Engine instance from booting to a normal run level. You just created the Compute Engine instance today and have

done no other maintenance on it, other than tweaking files. How should you correct this error?

- A. Download the file using scp, change the file, and then upload the modified version.
- B. Configure and log in to the Compute Engine instance through SSH, and change the file.
- C. Configure and log in to the Compute Engine instance through the serial port, and change the file.
- D. Configure and log in to the Compute Engine instance using a remote desktop client, and change the file.

**Answer: C**

Explanation:

<https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-using-serial-console>

### Question: 171

You are developing an application that needs to store files belonging to users in Cloud Storage. You want each user to have their own subdirectory in Cloud Storage. When a new user is created, the corresponding empty subdirectory should also be created. What should you do?

- A. Create an object with the name of the subdirectory ending with a trailing slash ('/') that is zero bytes in length.
- B. Create an object with the name of the subdirectory, and then immediately delete the object within that subdirectory.
- C. Create an object with the name of the subdirectory that is zero bytes in length and has WRITER access control list permission.
- D. Create an object with the name of the subdirectory that is zero bytes in length. Set the ContentType metadata to CLOUDSTORAGE\_FOLDER.

**Answer: A**

Explanation:

<https://cloud.google.com/storage/docs/folders>

If you create an empty folder using the Google Cloud console, Cloud Storage creates a zero-byte object as a placeholder. For example, if you create a folder called folder in a bucket called my-bucket, a zero-byte object called gs://my-bucket/folder/ is created. This placeholder is discoverable by other tools when listing the objects in the bucket, for example when using the gsutil ls command.

### Question: 172

Your company's corporate policy states that there must be a copyright comment at the very beginning of all source files. You want to write a custom step in Cloud Build that is triggered by each source commit. You need the trigger to validate that the source contains a copyright and add one for subsequent steps if not there. What should you do?

- A. Build a new Docker container that examines the files in /workspace and then checks and adds a copyright for each source file. Changed files are explicitly committed back to the source repository.
- B. Build a new Docker container that examines the files in /workspace and then checks and adds a copyright for each source file. Changed files do not need to

be committed back to the source repository.

C. Build a new Docker container that examines the files in a Cloud Storage bucket and then checks and adds a copyright for each source file. Changed files are written back to the Cloud Storage bucket. D. Build a new Docker container that examines the files in a Cloud Storage bucket and then checks and adds a copyright for each source file. Changed files are explicitly committed back to the source repository.

**Answer: A**

Explanation:

[https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing\\_data\\_using\\_workspaces](https://cloud.google.com/build/docs/configuring-builds/pass-data-between-steps#passing_data_using_workspaces)

To pass data between build steps, store the assets produced by the build step in /workspace and these assets will be available to any subsequent build steps.

### Question: 173

One of your deployed applications in Google Kubernetes Engine (GKE) is having intermittent performance issues. Your team uses a third-party logging solution. You want to install this solution on each node in your GKE cluster so you can view the logs. What should you do?

- A. Deploy the third-party solution as a DaemonSet
- B. Modify your container image to include the monitoring software
- C. Use SSH to connect to the GKE node, and install the software manually
- D. Deploy the third-party solution using Terraform and deploy the logging Pod as a Kubernetes Deployment

**Answer: A**

Explanation:

[https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage\\_patterns](https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage_patterns)

DaemonSets are useful for deploying ongoing background tasks that you need to run on all or certain nodes, and which do not require user intervention. Examples of such tasks include storage daemons like ceph, log collection daemons like fluent-bit, and node monitoring daemons like collectd.

### Question: 174

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 this migration. What should you do?

- A. Modernize and deploy the code on App Engine flexible environment.
- B. Modernize and deploy the code on App Engine standard environment.
- C. Deploy the modernized application to an n1-standard-1 Compute Engine instance.
- D. Ask the development team to re-write the application to run as a Docker container on Google Kubernetes Engine.

**Answer: B**

Explanation:

<https://cloud.google.com/appengine/docs/standard>

### Question: 175

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

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

**Answer: D**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets>

By default, Google Kubernetes Engine (GKE) encrypts customer content stored at rest, including Secrets. GKE handles and manages this default encryption for you without any additional action on your part.

Application-layer secrets encryption provides an additional layer of security for sensitive data, such as Secrets, stored in etcd. Using this functionality, you can use a key managed with Cloud KMS to encrypt data at the application layer. This encryption protects against attackers who gain access to an offline copy of etcd.

### Question: 176

You manage your company's ecommerce platform's payment system, which runs on Google Cloud. Your company must retain user logs for 1 year for internal auditing purposes and for 3 years to meet compliance requirements. You need to store new user logs on Google Cloud to minimize on-premises storage usage and ensure that they are easily searchable.

You want to minimize effort while ensuring that the logs are stored correctly. What should you do?

- A. Store the logs in a Cloud Storage bucket with bucket lock turned on.
- B. Store the logs in a Cloud Storage bucket with a 3-year retention period.
- C. Store the logs in Cloud Logging as custom logs with a custom retention period.
- D. Store the logs in a Cloud Storage bucket with a 1-year retention period. After 1 year, move the logs to another bucket with a 2-year retention period.

**Answer: C**

Explanation:

<https://cloud.google.com/logging/docs/buckets#custom-retention>

### Question: 177

Your company has a new security initiative that requires all data stored in Google Cloud to be encrypted by customer-managed encryption keys. You plan to use Cloud Key Management Service (KMS) to configure access to the keys. You need to follow the "separation of duties" principle and Google-recommended best practices. What should you do? (Choose two.)

- A. Provision Cloud KMS in its own project.
- B. Do not assign an owner to the Cloud KMS project.
- C. Provision Cloud KMS in the project where the keys are being used.
- D. Grant the roles/cloudkms.admin role to the owner of the project where the keys from Cloud KMS are being used.
- E. Grant an owner role for the Cloud KMS project to a different user than the owner of the project where the keys from Cloud KMS are being used.

**Answer: AB**

Explanation:

[https://cloud.google.com/kms/docs/separation-of-duties#using\\_separate\\_project](https://cloud.google.com/kms/docs/separation-of-duties#using_separate_project)

### Question: 178

You need to migrate a standalone Java application running in an on-premises Linux virtual machine (VM) to Google Cloud in a cost-effective manner. You decide not to take the lift-and-shift approach, and instead you plan to modernize the application by converting it to a container. How should you accomplish this task?

- A. Use Migrate for Anthos to migrate the VM to your Google Kubernetes Engine (GKE) cluster as a container.
- B. Export the VM as a raw disk and import it as an image. Create a Compute Engine instance from the Imported image.
- C. Use Migrate for Compute Engine to migrate the VM to a Compute Engine instance, and use Cloud Build to convert it to a container.
- D. Use Jib to build a Docker image from your source code, and upload it to Artifact Registry. Deploy the application in a GKE cluster, and test the application.

**Answer: D**

Explanation:

<https://cloud.google.com/blog/products/application-development/introducing-jib-build-java-docker-images-better>

### Question: 179

Your organization has recently begun an initiative to replatform their legacy applications onto Google Kubernetes Engine. 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.

**Answer: D**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/configmap>

ConfigMaps bind non-sensitive configuration artifacts such as configuration files, command-line arguments, and environment variables to your Pod containers and system components at runtime.

A ConfigMap separates your configurations from your Pod and components, which helps keep your workloads portable. This makes their configurations easier to change and manage, and prevents **hardcoding** configuration data to Pod specifications.

### Question: 180

Your development team has built several Cloud Functions using Java along with corresponding integration and service tests. You are building and deploying the functions and launching the tests using Cloud Build. Your Cloud Build job is reporting deployment failures immediately after successfully validating the code. What should you do?

- A. Check the maximum number of Cloud Function instances.
- B. Verify that your Cloud Build trigger has the correct build parameters.
- C. Retry the tests using the truncated exponential backoff polling strategy.
- D. Verify that the Cloud Build service account is assigned the Cloud Functions Developer role.

**Answer: D**

Explanation:

<https://cloud.google.com/build/docs/securing-builds/configure-access-for-cloud-build-service-account>

### Question: 181

You manage a microservices application on Google Kubernetes Engine (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 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 Authorization Policy 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.

**Answer: C**

Explanation:

### Question: 182

You recently migrated an on-premises monolithic application to a microservices application on Google Kubernetes Engine (GKE). The application has dependencies on backend services on-premises, including a CRM system and a MySQL database that contains personally identifiable information (PII). The backend services must remain on-premises to meet regulatory requirements.

You established a Cloud VPN connection between your on-premises data center and Google Cloud. You notice that some requests from your microservices application on GKE to the backend services are failing due to latency issues caused by fluctuating bandwidth, which is causing the application to crash. How should you address the latency issues?

- A. Use Memorystore to cache frequently accessed PII data from the on-premises MySQL database
- B. Use Istio to create a service mesh that includes the microservices on GKE and the on-premises services
- C. Increase the number of Cloud VPN tunnels for the connection between Google Cloud and the on-premises services
- D. Decrease the network layer packet size by decreasing the Maximum Transmission Unit (MTU) value from its default value on Cloud VPN

**Answer: C**

Explanation:

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing#route-alignment>

### Question: 183

Your company has deployed a new API to a Compute Engine instance. During testing, the API is not behaving as expected. You want to monitor the application over 12 hours to diagnose the problem within the application code without redeploying the application. Which tool should you use?

- A. Cloud Trace
- B. Cloud Monitoring
- C. Cloud Debugger logpoints
- D. Cloud Debugger snapshots

**Answer: C**

Explanation:

<https://cloud.google.com/debugger/docs/using/logpoints>

Logpoints allow you to inject logging into running services without restarting or interfering with the normal function of the service

### Question: 184

You are designing an application that consists of several microservices. Each microservice has its own RESTful API and will be deployed as a separate Kubernetes Service. You want to ensure that the consumers of these APIs aren't impacted when there is a change to your API, and also ensure that third-party systems aren't interrupted when new versions of the API are released. How should you

configure the connection to the application following Google-recommended best practices?

- A. Use an Ingress that uses the API's URL to route requests to the appropriate backend.
- B. Leverage a Service Discovery system, and connect to the backend specified by the request.
- C. Use multiple clusters, and use DNS entries to route requests to separate versioned backends.
- D. Combine multiple versions in the same service, and then specify the API version in the POST request.

**Answer: D**

Explanation:

### Question: 185

Your team is building an application for a financial institution. The application's frontend runs on Compute Engine, and the data resides in Cloud SQL and one Cloud Storage bucket. The application will collect data containing PII, which will be stored in the Cloud SQL database and the Cloud Storage bucket. You need to secure the PII data. What should you do?

- A. 1) Create the relevant firewall rules to allow only the frontend to communicate with the Cloud SQL database  
2) Using IAM, allow only the frontend service account to access the Cloud Storage bucket
- B. 1) Create the relevant firewall rules to allow only the frontend to communicate with the Cloud SQL database  
2) Enable private access to allow the frontend to access the Cloud Storage bucket privately
- C. 1) Configure a private IP address for Cloud SQL  
2) Use VPC-SC to create a service perimeter  
3) Add the Cloud SQL database and the Cloud Storage bucket to the same service perimeter
- D. 1) Configure a private IP address for Cloud SQL

- 2) Use VPC-SC to create a service perimeter
- 3) Add the Cloud SQL database and the Cloud Storage bucket to different service perimeters

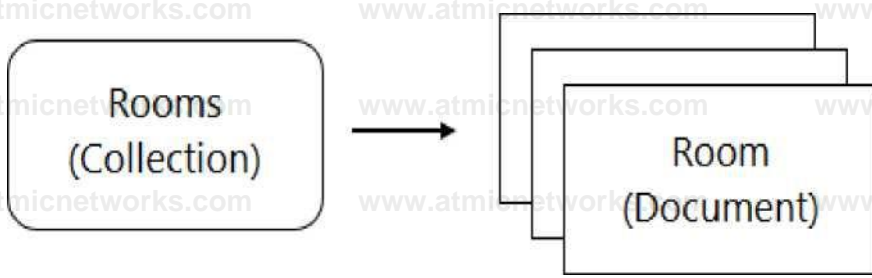
**Answer: C**

Explanation:

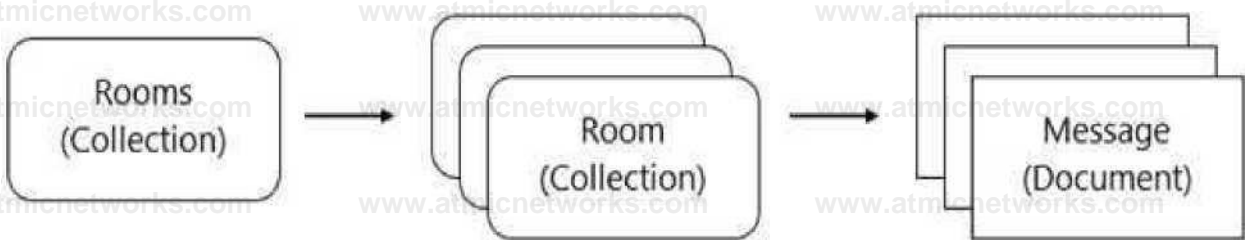
**Question: 186**

You are designing a chat room application that will host multiple rooms and retain the message history for each room. You have selected Firestore as your database. How should you represent the data in Firestore?

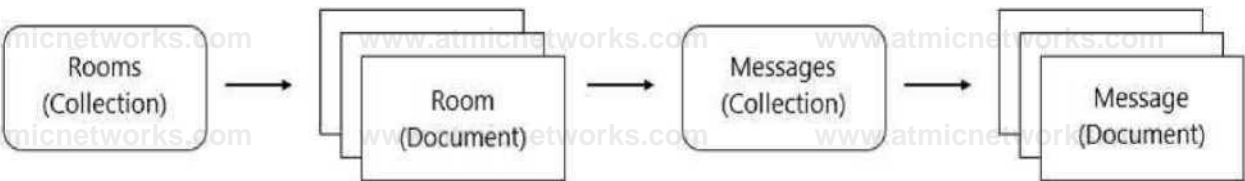
- A. Create a collection for the rooms. For each room, create a document that lists the contents of the messages



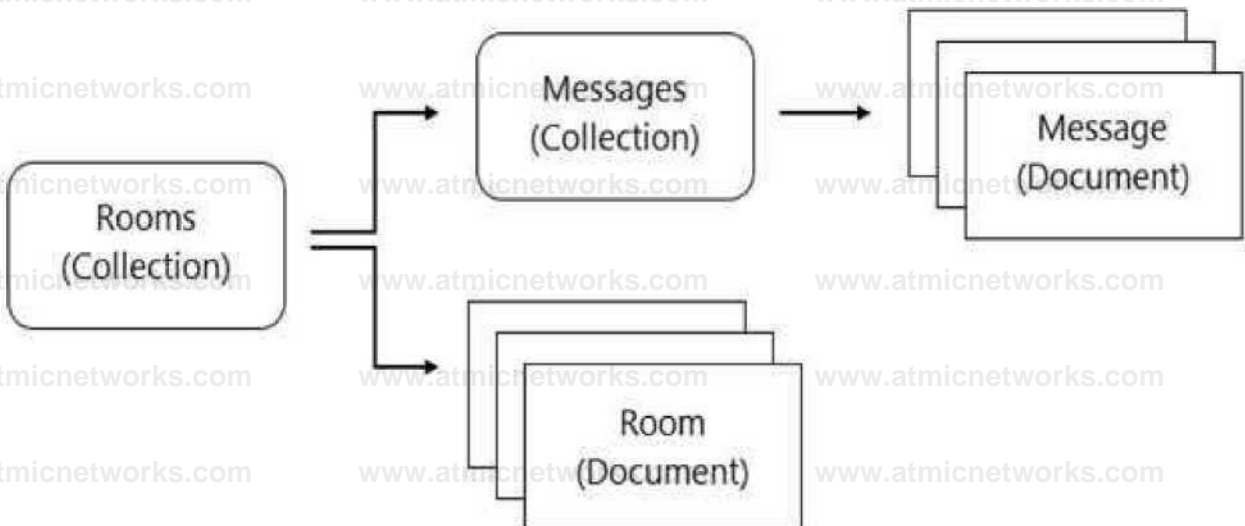
B. Create a collection for the rooms. For each room, create a collection that contains a document for each message



C. Create a collection for the rooms. For each room, create a document that contains a collection for documents, each of which contains a message.



D. Create a collection for the rooms, and create a document for each room. Create a separate collection for messages, with one document per message. Each room's document contains a list of references to the messages.



**Answer:**

**C**

Explanation:

<https://firebase.google.com/docs/firestore/data-model#hierarchical-data>

**Question:**

**187**

You are developing an application that will handle requests from end users. You need to secure a Cloud Function called by the application to allow authorized end users to authenticate to the function via the application while restricting access to unauthorized users. You will integrate Google Sign-In as part of the solution and want to follow Google-recommended best practices. What should you do?

- A. Deploy from a source code repository and grant users the roles/cloudfunctions.viewer role.
- B. Deploy from a source code repository and grant users the roles/cloudfunctions.invoker role
- C. Deploy from your local machine using gcloud and grant users the roles/cloudfunctions.admin role
- D. Deploy from your local machine using gcloud and grant users the roles/cloudfunctions.developer role

**Answer: C**

Explanation:

### Question: 188

You are running a web application on Google Kubernetes Engine that you inherited. You want to determine whether the application is using libraries with known vulnerabilities or is vulnerable to XSS attacks. Which service should you use?

- A. Google Cloud Armor
- B. Debugger
- C. Web Security Scanner
- D. Error Reporting

**Answer: C**

Explanation:

<https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview> Web Security Scanner identifies security vulnerabilities in your App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications. It crawls your application, following all links within the scope of your starting URLs, and attempts to exercise as many user inputs and event handlers as possible.

### Question: 189

You are building a highly available and globally accessible application that will serve static content to users. You need to configure the storage and serving components. You want to minimize management overhead and latency while maximizing reliability for users. What should you do?

- A. 1) Create a managed instance group. Replicate the static content across the virtual machines (VMs)  
2) Create an external HTTP(S) load balancer.

- 3) Enable Cloud CDN, and send traffic to the managed instance group.
- B. 1) Create an unmanaged instance group. Replicate the static content across the VMs.  
2) Create an external HTTP(S) load balancer  
3) Enable Cloud CDN, and send traffic to the unmanaged instance group.
- C. 1) Create a Standard storage class, regional Cloud Storage bucket. Put the static content in the bucket  
2) Reserve an external IP address, and create an external HTTP(S) load balancer  
3) Enable Cloud CDN, and send traffic to your backend bucket
- D. 1) Create a Standard storage class, multi-regional Cloud Storage bucket. Put the static content in the bucket.  
2) Reserve an external IP address, and create an external HTTP(S) load balancer.  
3) Enable Cloud CDN, and send traffic to your backend bucket.

**Answer: D**

Explanation:

### Question: 190

You are writing from a Go application to a Cloud Spanner database. You want to optimize your application's performance using Google-recommended best practices. What should you do?

- A. Write to Cloud Spanner using Cloud Client Libraries.
- B. Write to Cloud Spanner using Google API Client Libraries
- C. Write to Cloud Spanner using a custom gRPC client library.
- D. Write to Cloud Spanner using a third-party HTTP client library.

**Answer: A**

Explanation:

<https://cloud.google.com/apis/docs/cloud-client-libraries>

"Cloud Client Libraries are the recommended option for accessing Cloud APIs programmatically, where available. Cloud Client Libraries use the latest client library models"

<https://cloud.google.com/apis/docs/client-libraries-explained>

<https://cloud.google.com/go/docs/reference>

### Question: 191

You have an application deployed in Google Kubernetes Engine (GKE). You need to update the application to make authorized requests to Google Cloud managed services. You want this to be a one-time setup, and you need to follow security best practices of auto-rotating your security keys

and storing them in an encrypted store. You already created a service account with appropriate access to the Google Cloud service. What should you do next?

- A. Assign the GoogleCloud service account to your GKE Pod using Workload Identity.
- B. Export the GoogleCloud serviceaccount, and share it with the Pod as a Kubernetes Secret.
- C. Export the GoogleCloud serviceaccount, and embed it in the source code of the application.
- D. Export the GoogleCloud serviceaccount, and upload it to HashiCorp Vault to generate a dynamic service account for your application.

**Answer: A**

Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity>

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

### Question: 192

You are planning to deploy hundreds of microservices in your Google Kubernetes Engine (GKE) cluster. How should you secure communication between the microservices on GKE using a managed service?

- A. Use global HTTP(S) Load Balancing with managed SSL certificates to protect your services
- B. Deploy open source Istio in your GKE cluster, and enable mTLS in your Service Mesh
- C. Install cert-manager on GKE to automatically renew the SSL certificates.
- D. Install Anthos Service Mesh, and enable mTLS in your Service Mesh.

**Answer: D**

Explanation:

[https://cloud.google.com/service-mesh/docs/overview#security\\_benefits](https://cloud.google.com/service-mesh/docs/overview#security_benefits)

- Ensures encryption in transit. Using mTLS for authentication also ensures that all TCP communications are encrypted in transit.

### Question: 193

You are developing an application that will store and access sensitive unstructured data objects in a Cloud Storage bucket. To comply with regulatory requirements, you need to ensure that all data 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. Use IAM Conditions to provide access to objects 7 years after 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.

**Answer: AD**

**Explanation:**

<https://cloud.google.com/storage/docs/bucket-lock>

This page discusses the Bucket Lock feature, which allows you to configure a data retention policy for a Cloud Storage bucket that governs how long objects in the bucket must be retained. The feature also allows you to lock the data retention policy, permanently preventing the policy from being reduced or removed.

<https://cloud.google.com/storage/docs/storage-classes#archive>

Archive storage is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Unlike the "coldest" storage services offered by other Cloud providers, your data is available within milliseconds, not hours or days.

Archive storage is the best choice for data that you plan to access less than once a year.

## Question: 194

You are developing an application using different microservices that should remain internal to the cluster. You want to be able to configure each microservice with a specific number of replicas. You also want to be able to address a specific microservice from any other microservice in a uniform way, regardless of the number of replicas the microservice scales to. You need to implement this solution on Google Kubernetes Engine.

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 name to address the Pod from other microservices within the cluster.

**Answer: A**

Explanation:

### Question: 195

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. Add a public IP address to the instance. 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.

**Answer: D**

Explanation:

<https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs>

### Question: 196

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. Implement a mocking framework.
- B. Create a topic and subscription for each tester.
- C. Add a filter by tester to the subscription.
- D. Use the Pub/Sub emulator.

**Answer: D**

Explanation:

<https://cloud.google.com/pubsub/docs/emulator>, "Testing apps locally with the emulator".

### Question: 197

You have an application deployed in Google Kubernetes Engine (GKE) that reads and processes Pub/Sub messages. Each Pod handles a fixed number of messages per minute. The rate at which messages are published to the Pub/Sub topic varies considerably throughout the day and week, including occasional large batches of messages published at a single moment.

You want to scale your GKE Deployment to be able to process messages in a timely manner. What GKE feature should you use to automatically adapt your workload?

- A. Vertical Pod Autoscaler in Auto mode
- B. Vertical Pod Autoscaler in Recommendation mode
- C. Horizontal Pod Autoscaler based on an external metric
- D. Horizontal Pod Autoscaler based on resources utilization

**Answer: C**

Explanation:

<https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/>

### Question: 198

You are using Cloud Run to host a web application. You need to securely obtain the application project ID and region where the application is running and display this information to users. You want to use the most performant approach. What should you do?

- A. Use HTTP requests to query the available metadata server at the `http://metadata.google.internal/` endpoint with the `Metadata-Flavor: Google` header.
- B. In the Google Cloud console, navigate to the Project Dashboard and gather configuration details. Navigate to the Cloud Run "Variables & Secrets" tab, and add the desired environment variables in `Key:Value` format.
- C. In the Google Cloud console, navigate to the Project Dashboard and gather configuration details. Write the application configuration information to Cloud Run's in-memory container filesystem.
- D. Make an API call to the Cloud Asset Inventory API from the application and format the request to include instance metadata.

**Answer: B**

Explanation:

### Question: 199

You need to deploy resources from your laptop to Google Cloud using Terraform. Resources in your Google Cloud environment must be created using a service account. Your Cloud Identity has the

roles/`iam.serviceAccountTokenCreator` Identity and Access Management (IAM) role and the necessary permissions to deploy the resources using Terraform. You want to set up your development environment to deploy the desired resources following Google-recommended best practices. What should you do?

- A. 1) Download the service account's key file in JSON format, and store it locally on your laptop.
- 2) Set the `GOOGLE_APPLICATION_CREDENTIALS` environment variable to the path of your downloaded key file.

- B. 1) Run the following command from a command line: `gcloud config set auth/impersonate_service_account service-account-name@project.iam.gserviceaccount.com`.
- 2) Set the `GOOGLE_OAUTH_ACCESS_TOKEN` environment variable to the value that is returned by the `gcloud auth print-access-token` command.
- C. 1) Run the following command from a command line: `gcloud auth application-default login`.
- 2) In the browser window that opens, authenticate using your personal credentials.
- D. 1) Store the service account's key file in JSON format in Hashicorp Vault.
- 2) Integrate Terraform with Vault to retrieve the key file dynamically, and authenticate to Vault using a short-lived access token.

### Answer: D

Explanation:

<https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys#file-system>

Whenever possible, avoid storing service account keys on a file system. If you can't avoid storing keys on disk, make sure to restrict access to the key file, configure file access auditing, and encrypt the underlying disk.

<https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys#software-keystore>

In situations where using a hardware-based key store isn't viable, use a software-based key store to manage service account keys. Similar to hardware-based options, a software-based key store lets users or applications use service account keys without revealing the private key. Software-based key store solutions can help you control key access in a fine-grained manner and can also ensure that each key access is logged.

### Question: 200

Your company uses Cloud Logging to manage large volumes of log data.

- a. You need to build a real-time log analysis architecture that pushes logs to a third-party application for processing. What should you do?
- A. Create a Cloud Logging log export to Pub/Sub.
- B. Create a Cloud Logging log export to BigQuery.
- C. Create a Cloud Logging log export to Cloud Storage.
- D. Create a Cloud Function to read Cloud Logging log entries and send them to the third-party application.

### Answer: A

Explanation:

### Question: 201

You are developing a new public-facing application that needs to retrieve specific properties in the metadata of users' objects in their respective Cloud Storage buckets. Due to privacy and data residency requirements, you must retrieve only the metadata and not the object data. You want to maximize the performance of the retrieval process. How should you retrieve the metadata?

- A. Use the patch method.
- B. Use the compose method.
- C. Use the copy method.
- D. Use the fields request parameter.

**Answer: D**

Explanation:

[https://cloud.google.com/storage/docs/json\\_api/v1/objects/get](https://cloud.google.com/storage/docs/json_api/v1/objects/get)

### Question: 202

You are deploying a microservices application to Google Kubernetes Engine (GKE) that will broadcast livestreams. You expect unpredictable traffic patterns and large variations in the number of concurrent users. Your application must meet the following requirements:

- Scales automatically during popular events and maintains high availability
- Is resilient in the event of hardware failures

How should you configure the deployment parameters? (Choose two.)

- A. Distribute your workload evenly using a multi-zonal node pool.
- B. Distribute your workload evenly using multiple zonal node pools.
- C. Use cluster autoscaler to resize the number of nodes in the node pool, and use a Horizontal Pod Autoscaler to scale the workload.
- D. Create a managed instance group for Compute Engine with the cluster nodes. Configure autoscaling rules for the managed instance group.
- E. Create alerting policies in Cloud Monitoring based on GKE CPU and memory utilization. Ask an on-duty engineer to scale the workload by executing a script when CPU and memory usage exceed predefined thresholds.

**Answer: AC**

Explanation:

### Question: 203

You work at a rapidly growing financial technology startup. You manage the payment processing application written in Go and hosted on Cloud Run in the Singapore region (asia-southeast1). The payment processing application processes data stored in a Cloud Storage bucket that is also located in the Singapore region.

The startup plans to expand further into the Asia Pacific region. You plan to deploy the Payment Gateway in Jakarta, Hong Kong, and Taiwan over the next six months. Each location has data residency requirements that require customer data to reside in the country where the transaction was made. You want to minimize the cost of these deployments. What should you do?

- A. Create a Cloud Storage bucket in each region, and create a Cloud Run service of the payment processing

application in each region.

- B. Create a Cloud Storage bucket in each region, and create three Cloud Run services of the payment processing application in the Singapore region.
- C. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run services of the payment processing application in the Singapore region.
- D. Create three Cloud Storage buckets in the Asia multi-region, and create three Cloud Run revisions of the payment processing application in the Singapore region.

**Answer: A**

Explanation:

### Question: 204

You recently joined a new team that has a Cloud Spanner database instance running in production. Your manager has asked you to optimize the Spanner instance to reduce cost while maintaining high reliability and availability of the database. What should you do?

- A. Use Cloud Logging to check for error logs, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- B. Use Cloud Trace to monitor the requests per sec of incoming requests to Spanner, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- C. Use Cloud Monitoring to monitor the CPU utilization, and reduce Spanner processing units by small increments until you find the minimum capacity required.
- D. Use Snapshot Debugger to check for application errors, and reduce Spanner processing units by small increments until you find the minimum capacity required.

**Answer: C**

Explanation:

[https://cloud.google.com/spanner/docs/compute-capacity#increasing\\_and\\_decreasing\\_compute\\_capacity](https://cloud.google.com/spanner/docs/compute-capacity#increasing_and_decreasing_compute_capacity)

### Question: 205

You recently deployed a Go application on Google Kubernetes Engine (GKE). The operations team has noticed that the application's CPU usage is high even when there is low production traffic. The operations team has asked you to optimize your application's CPU resource consumption. You want to determine which Go functions consume the largest amount of CPU. What should you do?

- A. Deploy a Fluent Bit daemonset on the GKE cluster to log data in Cloud Logging. Analyze the logs to get insights into your application code's performance.
- B. Create a custom dashboard in Cloud Monitoring to evaluate the CPU performance metrics of your application.
- C. Connect to your GKE nodes using SSH. Run the top command on the shell to extract the CPU utilization of your application.

D. Modify your Go application to capture profiling data. Analyze the CPU metrics of your application in flame graphs in Profiler.

**Answer: D**

Explanation:

<https://cloud.google.com/profiler/docs/about-profiler>

Cloud Profiler is a statistical, low-overhead profiler that continuously gathers CPU usage and memory-allocation information from your production applications. It attributes that information to the source code that generated it, helping you identify the parts of your application that are consuming the most resources, and otherwise illuminating your applications performance characteristics.

<https://cloud.google.com/profiler/docs>

### Question: 206

Your team manages a Google Kubernetes Engine (GKE) cluster where an application is running. A different team is planning to integrate with this application. Before they start the integration, you need to ensure that the other team cannot make changes to your application, but they can deploy the integration on GKE. What should you do?

- A. Using Identity and Access Management (IAM), grant the Viewer IAM role on the cluster project to the other team.
- B. Create a new GKE cluster. Using Identity and Access Management (IAM), grant the Editor role on the cluster project to the other team.
- C. Create a new namespace in the existing cluster. Using Identity and Access Management (IAM), grant the Editor role on the cluster project to the other team.
- D. Create a new namespace in the existing cluster. Using Kubernetes role-based access control (RBAC), grant the Admin role on the new namespace to the other team.

**Answer: D**

Explanation:

### Question: 207

You have recently instrumented a new application with OpenTelemetry, and you want to check the latency of your application requests in Trace. You want to ensure that a specific request is always traced. What should you do?

- A. Wait 10 minutes, then verify that Trace captures those types of requests automatically.
- B. Write a custom script that sends this type of request repeatedly from your dev project.
- C. Use the Trace API to apply custom attributes to the trace.
- D. Add the X-Cloud-Trace-Context header to the request with the appropriate parameters.

**Answer: D**

Explanation:

<https://cloud.google.com/trace/docs/setup#force-trace>

Cloud Trace doesn't sample every request. To force a specific request to be traced, add an X-Cloud-Trace-Context header to the request.

### **Question: 208**

You are trying to connect to your Google Kubernetes Engine (GKE) cluster using kubectl from Cloud Shell. You have deployed your GKE cluster with a public endpoint. From Cloud Shell, you run the following command:

geloud

```
container clusters get-credentials <cluster-name> \  
-zone <zone> -project <project-name> \
```

You notice that the kubectl commands time out without returning an error message. What is the most likely cause of this issue?

- A. Your user account does not have privileges to interact with the cluster using kubectl.
- B. Your Cloud Shell external IP address is not part of the authorized networks of the cluster.
- C. The Cloud Shell is not part of the same VPC as the GKE cluster.
- D. A VPC firewall is blocking access to the cluster's endpoint.

**Answer: B**

Explanation:

[https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#cloud\\_shell](https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#cloud_shell)

If you want to use Cloud Shell to access the cluster, you must add the public IP address of your Cloud Shell to the cluster's list of authorized networks.

## Question: 209

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. 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.
- B. Grant the Storage Object Viewer IAM role to allUsers. Allow users to access the bucket after authenticating through your web application.
- C. Configure Identity-Aware Proxy (IAP) to authenticate users into the web application. Allow users to access the bucket after authenticating through IAP.
- D. Generate a signed URL that grants read access to the bucket. Allow users to access the URL after authenticating through your web application.

**Answer: D**

Explanation:

<https://cloud.google.com/storage/docs/access-control/signed-urls#should-you-use>

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 typical 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. You specify an expiration time when you create the signed URL. Anyone who knows the URL can access the resource until the expiration time for the URL is reached or the key used to sign the URL is rotated.

## Question: 210

You need to configure a Deployment on Google Kubernetes Engine (GKE). You want to include a check that verifies that the containers can connect to the database. If the Pod is failing to connect, you want a script on the container to run to complete a graceful shutdown. How should you configure the Deployment?

- A. Create two jobs: one that checks whether the container can connect to the database, and another that runs the shutdown script if the Pod is failing.
- B. Create the Deployment with a livenessProbe for the container that will fail if the container can't connect to the database. Configure a PreStop lifecycle handler that runs the shutdown script if the container is failing.
- C. Create the Deployment with a PostStart lifecycle handler that checks the service availability. Configure a PreStop lifecycle handler that runs the shutdown script if the container is failing.
- D. Create the Deployment with an initContainer that checks the service availability. Configure a PreStop lifecycle handler that runs the shutdown script if the Pod is failing.

**Answer: B**

Explanation:

<https://cloud.google.com/architecture/best-practices-for-running-cost-effective-kubernetes-applications-on-gke#make-sure-your-applications-are-shutting-down-in-accordance-with-kubernetes-expectations>

## Question: 211

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 one Cloud Function as a backend service exposed using an HTTPS load balancer.
- B. Create three Cloud Functions exposed directly.
- C. Create one Cloud Function exposed directly.
- D. Create three Cloud Functions as three backend services exposed using an HTTPS load balancer.

**Answer: D**

Explanation:

<https://cloud.google.com/load-balancing/docs/https/setup-global-ext-https-serverless>

## Question: 212

You are deploying a microservices application to Google Kubernetes Engine (GKE). The application will receive daily updates. You expect to deploy a large number of distinct containers that will run on the Linux operating system (OS). You want to be alerted to any known OS vulnerabilities in the new containers. You want to follow Google-recommended best practices. What should you do?

- A. Use the gcloud CLI to call Container Analysis to scan new container images. Review the vulnerability results before each deployment.
- B. Enable Container Analysis, and upload new container images to Artifact Registry. Review the vulnerability results before each deployment.
- C. Enable Container Analysis, and upload new container images to Artifact Registry. Review the critical vulnerability results before each deployment.
- D. Use the Container Analysis REST API to call Container Analysis to scan new container images. Review the vulnerability results before each deployment.

**Answer: D**

Explanation:

<https://cloud.google.com/container-analysis/docs/automated-scanning-howto>

<https://cloud.google.com/container-analysis/docs/os-overview> says: The Container Scanning API allows you to automate OS vulnerability detection, scanning each time you push an image to Container Registry or Artifact Registry. Enabling this API also triggers language package scans for Go and Java vulnerabilities (Preview).

### Question: 213

You are a developer at a large organization. You have an application written in Go running in a production Google Kubernetes Engine (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.

**Answer: D**

Explanation:

[https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what\\_is](https://cloud.google.com/kubernetes-engine/docs/concepts/workload-identity#what_is)

Applications running on GKE might need access to Google Cloud APIs such as Compute Engine API, BigQuery Storage API, or Machine Learning APIs.

Workload Identity allows a Kubernetes service account in your GKE cluster to act as an IAM service account. Pods that use the configured Kubernetes service account automatically authenticate as the IAM service account when accessing Google Cloud APIs. Using Workload Identity allows you to assign distinct, fine-grained identities and authorization for each application in your cluster.

### Question: 214

You have an application written in Python running in production on Cloud Run. Your application needs to read/write data stored in a Cloud Storage bucket in the same project. You want to grant access to your application following the principle of least privilege. What should you do?

- A. Create a user-managed service account with a custom Identity and Access Management (IAM) role.
- B. Create a user-managed service account with the Storage Admin Identity and Access Management (IAM) role.
- C. Create a user-managed service account with the Project Editor Identity and Access Management (IAM) role.

D. Use the default service account linked to the Cloud Run revision in production.

**Answer: A**

Explanation:

<https://cloud.google.com/iam/docs/understanding-roles#storage.admin>

### Question: 215

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.

**Answer: D**

Explanation:

### Question: 216

Your team detected a spike of errors in an application running on Cloud Run in your production project. The application is configured to read messages from Pub/Sub topic A, process the messages, and write the messages to topic B. You want to conduct tests to identify the cause of the errors. You can use a set of mock messages for testing. What should you do?

- A. Deploy the Pub/Sub and Cloud Run emulators on your local machine. Deploy the application locally, and change the logging level in the application to DEBUG or INFO. Write mock messages to topic A, and then analyze the logs.
- B. Use the gcloud CLI to write mock messages to topic A. Change the logging level in the application to DEBUG or INFO, and then analyze the logs.
- C. Deploy the Pub/Sub emulator on your local machine. Point the production application to your local Pub/Sub topics. Write mock messages to topic A, and then analyze the logs.
- D. Use the Google Cloud console to write mock messages to topic A. Change the logging level in the application to DEBUG or INFO, and then analyze the logs.

## Answer: B

Explanation:

### Question: 217

You are developing a Java Web Server that needs to interact with Google Cloud services via the Google Cloud API on the user's behalf. Users should be able to authenticate to the Google Cloud API using their Google Cloud 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 Google Cloud 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 Cloud 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 Google Cloud API.
- C. 1) When a user arrives at your application, route them to a Google Cloud 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 Google Cloud API using the authorization code in the cookie.
- D. 1) When a user arrives at your application, route them to a Google Cloud 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 Google Cloud API.

## Answer: D

Explanation:

<https://developers.google.com/identity/protocols/oauth2#webserver>

The Google OAuth 2.0 endpoint supports web server applications that use languages and frameworks such as PHP, Java, Python, Ruby, and ASP.NET. The authorization sequence begins when your application redirects a browser to a Google URL; the URL includes query parameters that indicate the type of access being requested. Google handles the user authentication, session selection, and user consent. The result is an authorization code, which the application can exchange for an access token and a refresh token.

### Question: 218

You recently developed a new application. You want to deploy the application on Cloud Run without a Dockerfile. Your organization requires that all container images are pushed to a centrally managed container repository. How should you build your container using Google Cloud services? (Choose two.)

- A. Push your source code to Artifact Registry.
- B. Submit a Cloud Build job to push the image.
- C. Use the pack build command with pack CLI.
- D. Include the --source flag with the gcloud run deploy CLI command.
- E. Include the --platform=kubernetes flag with the gcloud run deploy CLI command.

**Answer: AC**

Explanation:

<https://cloud.google.com/run/docs/deploying#images>

<https://cloud.google.com/blog/products/containers-kubernetes/google-cloud-now-supports-buildpacks>

### Question: 219

You work for an organization that manages an online ecommerce website. Your company plans to expand across the world; however, the estore currently serves one specific region. You need to select a SQL database and configure a schema that will scale as your organization grows. You want to create a table that stores all customer transactions and ensure that the customer (CustomerId) and the transaction (TransactionId) are unique. What should you do?

- A. Create a Cloud SQL table that has TransactionId and CustomerId configured as primary keys. Use an incremental number for the TransactionId.
- B. Create a Cloud SQL table that has TransactionId and CustomerId configured as primary keys. Use a random string (UUID) for the TransactionId.
- C. Create a Cloud Spanner table that has TransactionId and CustomerId configured as primary keys. Use a random string (UUID) for the TransactionId.
- D. Create a Cloud Spanner table that has TransactionId and CustomerId configured as primary keys. Use an incremental number for the TransactionId.

**Answer: C**

Explanation:

### Question: 220

You are monitoring a web application that is written in Go and deployed in Google Kubernetes Engine. You notice an increase in CPU and memory utilization. You need to determine which source code is consuming the most CPU and memory resources. What should you do?

- A. Download, install, and start the Snapshot Debugger agent in your VM. Take debug snapshots of the functions that take the longest time. Review the call stack frame, and identify the local variables at that level in the stack.
- B. Import the Cloud Profiler package into your application, and initialize the Profiler agent. Review the generated flame graph in the Google Cloud console to identify time-intensive functions.
- C. Import OpenTelemetry and Trace export packages into your application, and create the trace provider. Review the latency data for your application on the Trace overview page, and identify where bottlenecks are occurring.
- D. Create a Cloud Logging query that gathers the web application's logs. Write a Python script that calculates the difference between the timestamps from the beginning and the end of the application's longest functions to identify time-intensive functions.

**Answer: B**

Explanation:

### Question: 221

You have a container deployed on Google Kubernetes Engine. The container can sometimes be slow to launch, so you have implemented a liveness probe. You notice that the liveness probe occasionally fails on launch. What should you do?

- A. Add a startup probe.
- B. Increase the initial delay for the liveness probe.
- C. Increase the CPU limit for the container.
- D. Add a readiness probe.

**Answer: B**

Explanation:

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes>

### Question: 222

You work for an organization that manages an ecommerce site. Your application is deployed behind a global HTTP(S) load balancer. You need to test a new product recommendation algorithm. You plan to use A/B testing to determine the new algorithm's effect on sales in a randomized way. How should you test this feature?

- A. Split traffic between versions using weights.
- B. Enable the new recommendation feature flag on a single instance.
- C. Mirror traffic to the new version of your application.
- D. Use HTTP header-based routing.

**Answer: C**

Explanation:

[https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic\\_actions\\_weight-based\\_traffic\\_splitting](https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic_actions_weight-based_traffic_splitting)

Deploying a new version of an existing production service generally incurs some risk. Even if your tests pass in staging, you probably don't want to subject 100% of your users to the new version immediately. With traffic management, you can define percentage-based traffic splits across multiple backend services.

For example, you can send 95% of the traffic to the previous version of your service and 5% to the new version of your service. After you've validated that the new production version works as expected, you can gradually shift the percentages until 100% of the traffic reaches the new version of your service. Traffic splitting is typically used for deploying new versions, A/B testing, service migration, and similar processes.

[https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based\\_traffic\\_splitting\\_for\\_safer\\_deployments](https://cloud.google.com/traffic-director/docs/advanced-traffic-management#weight-based_traffic_splitting_for_safer_deployments)

[https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#split\\_the\\_traffic\\_2](https://cloud.google.com/architecture/implementing-deployment-and-testing-strategies-on-gke#split_the_traffic_2)

[https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic\\_actions\\_weight-based\\_traffic\\_splitting](https://cloud.google.com/load-balancing/docs/https/traffic-management-global#traffic_actions_weight-based_traffic_splitting)

## Question: 223

You plan to deploy a new application revision with a Deployment resource to Google Kubernetes Engine (GKE) in production. The container might not work correctly. You want to minimize risk in case there are issues after deploying the revision. You want to follow Google-recommended best practices. What should you do?

- A. Perform a rolling update with a PodDisruptionBudget of 80%.
- B. Perform a rolling update with a HorizontalPodAutoscaler scale-down policy value of 0.
- C. Convert the Deployment to a StatefulSet, and perform a rolling update with a PodDisruptionBudget of 80%.
- D. Convert the Deployment to a StatefulSet, and perform a rolling update with a HorizontalPodAutoscaler scale-down policy value of 0.

**Answer: A**

Explanation:

<https://cloud.google.com/blog/products/containers-kubernetes/ensuring-reliability-and-uptime-for-your-gke-cluster>

Setting PodDisruptionBudget ensures that your workloads have a sufficient number of replicas, even during maintenance. Using the PDB, you can define a number (or percentage) of pods that can be terminated, even if terminating them brings the current replica count below the desired value. With PDB configured, Kubernetes will drain a node following the configured disruption schedule. New pods will be deployed on other available nodes. This approach ensures Kubernetes schedules workloads in an optimal way while controlling the disruption based on the PDB configuration.

<https://blog.knoldus.com/how-to-avoid-outages-in-your-kubernetes-cluster-using-pdb/>

## Question: 224

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 Google Kubernetes Engine with Anthos Service Mesh. Use traffic splitting to direct a subset of user traffic to the new version based on the user-agent header.
- C. 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.
- D. Deploy your application on Compute Engine. Use Traffic Director to direct a subset of user traffic to the new version based on predefined weights.

**Answer: B**

Explanation:

## Question: 225

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. Compute Engine
- B. Google Kubernetes Engine cluster in Standard mode

- C. Cloud Functions
- D. Cloud Run

**Answer: D**

**Explanation:**

This page shows Cloud Run-specific details for developers who want to use gRPC to connect a Cloud Run service with other services, for example, to provide simple, high performance communication between internal microservices. You can use all gRPC types, streaming or unary, with Cloud Run.

Possible use cases include:

Communication between internal microservices.

High loads of data (gRPC uses protocol buffers, which are up to seven times faster than REST calls).

Only a simple service definition is needed, you don't want to write a full client library.

Use streaming gRPCs in your gRPC server to build more responsive applications and APIs.

<https://cloud.google.com/run/docs/tutorials/secure-services#:~:text=The%20backend%20service%20is%20private,Google%20Cloud%20except%20where%20necessary.>

**Question: 226**

You are developing an application hosted on Google Cloud that uses a MySQL relational database schema

a. The application will have a large volume of reads and writes to the database and will require backups and ongoing capacity planning. Your team does not have time to fully manage the database but can take on small administrative tasks. How should you host the database?

- A. Configure Cloud SQL to host the database, and import the schema into Cloud SQL.
- B. Deploy MySQL from the Google Cloud Marketplace to the database using a client, and import the schema.
- C. Configure Bigtable to host the database, and import the data into Bigtable.
- D. Configure Cloud Spanner to host the database, and import the schema into Cloud Spanner.
- E. Configure Firestore to host the database, and import the data into Firestore.

**Answer: A**

**Explanation:**

<https://cloud.google.com/spanner/docs/migrating-mysql-to-spanner#migration-process>

Cloud SQL: Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully-managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.

<https://cloud.google.com/sql/docs/mysql> Cloud SQL for MySQL is a fully-managed database service that helps you set up, maintain, manage, and administer your MySQL relational databases on Google Cloud Platform.

## Question: 227

You are developing a new web application using Cloud Run and committing code to Cloud Source Repositories. You want to deploy new code in the most efficient way possible. You have already created a Cloud Build YAML file that builds a container and runs the following command: `gcloud run deploy`. What should you do next?

- A. Create a Pub/Sub topic to be notified when code is pushed to the repository. Create a Pub/Sub trigger that runs the build file when an event is published to the topic.
- B. Create a build trigger that runs the build file in response to a repository code being pushed to the development branch.
- C. Create a webhook build trigger that runs the build file in response to HTTP POST calls to the webhook URL.
- D. Create a Cron job that runs the following command every 24 hours: `gcloud builds submit`.

**Answer: B**

Explanation:

<https://cloud.google.com/build/docs/triggers>

Cloud Build uses build triggers to enable CI/CD automation. You can configure triggers to listen for incoming events, such as when a new commit is pushed to a repository or when a pull request is initiated, and then automatically execute a build when new events come in. You can also configure triggers to build code on any changes to your source repository or only on changes that match certain criteria.

## Question: 228

Your team has created an application that is hosted on a Google Kubernetes Engine (GKE) cluster. You need to connect the application to a legacy REST service that is deployed in two GKE clusters in two different regions. You want to connect your application to the legacy service in a way that is resilient and requires the fewest number of steps. You also want to be able to run probe-based health checks on the legacy service on a separate port. How should you set up the connection?

- A. Use Traffic Director with a sidecar proxy to connect the application to the service.
- B. Use a proxyless Traffic Director configuration to connect the application to the service.
- C. Configure the legacy service's firewall to allow health checks originating from the proxy.
- D. Configure the legacy service's firewall to allow health checks originating from the application.
- E. Configure the legacy service's firewall to allow health checks originating from the Traffic Director control plane.

**Answer: A, C**

Explanation:

<https://cloud.google.com/traffic-director/docs/advanced-setup#routing-rule-maps>

<https://cloud.google.com/traffic-director/docs/advanced-setup>

A) Using Traffic Director with a sidecar proxy can provide resilience for your application by allowing for failover

to the secondary region in the event of an outage. The sidecar proxy can route traffic to the legacy service in either of the two GKE clusters, ensuring high availability. C. Configuring the legacy service's firewall to allow health checks originating from the proxy allows the proxy to periodically check the health of the legacy service and ensure that it is functioning properly. This helps to ensure that traffic is only routed to healthy instances of the legacy service, further improving the resilience of the setup.

### Question: 229

You work for a financial services company that has a container-first approach. Your team develops microservices applications. You have a Cloud Build pipeline that creates a container image, runs regression tests, and publishes the image to Artifact Registry. You need to ensure that only containers that have passed the regression tests are deployed to Google Kubernetes Engine (GKE) clusters. You have already enabled Binary Authorization on the GKE clusters. What should you do next?

- A. Deploy Voucher Server and Voucher Client Components. After a container image has passed the regression tests, run Voucher Client as a step in the Cloud Build pipeline.
- B. Set the Pod Security Standard level to Restricted for the relevant namespaces. Digitally sign the container images that have passed the regression tests as a step in the Cloud Build pipeline.
- C. Create an attestor and a policy. Create an attestation for the container images that have passed the regression tests as a step in the Cloud Build pipeline.
- D. Create an attestor and a policy. Run a vulnerability scan to create an attestation for the container image as a step in the Cloud Build pipeline.

**Answer: C**

Explanation:

### Question: 230

You have an ecommerce application hosted in Google Kubernetes Engine (GKE) that receives external requests and forwards them to third-party APIs external to Google Cloud. The third-party APIs are responsible for credit card processing, shipping, and inventory management using the process shown.

in the diagram.

Your customers are reporting that the ecommerce application is running slowly at unpredictable times. The application doesn't report any metrics. You need to determine the cause of the inconsistent performance. What should you do?



- A. Install the Ops Agent inside your container and configure it to gather application metrics.
- B. Install the OpenTelemetry library for your respective language, and instrument your application.
- C. Modify your application to read and forward the x-Cloud-Trace-context header when it calls the downstream services
- D. Enable Managed Service for Prometheus on the GKE cluster to gather application metrics.

**Answer: B**

Explanation:

### Question: 231

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/S{PROJECT_ID}/_REPO_NAME/myimage:${SHORT_SHA};
- name: 'gcr.io/cloud-builders/docker'
  args: ['push', 'us-central1-
docker.pkg.dev/S{PROJECT_ID}/_REPO_NAME/my image :S{SHORT_SHA}^1.]
- name: google/cloud-sdk
  args: ['gcloud' > 'run', 'deploy', 'the!LowerId=${SHORT_SHA}', '--image=us-central1-
docker.pkg.dev/S{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. Remove the step that pushes the container to Artifact Registry.
- B. Add the `--cache-from` argument to the Docker build step in your build config file.
- C. Store image artifacts in a Cloud Storage bucket in the same region as the Cloud Run instance.
- D. Deploy a new Docker registry in a VPC and use Cloud Build worker pools inside the VPC to run the build pipeline.

**Answer: B**

Explanation:

[https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using\\_a\\_cached\\_docker\\_image](https://cloud.google.com/build/docs/optimize-builds/speeding-up-builds#using_a_cached_docker_image)

### Question: 232

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 invoke the Cloud Function. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it.
- B. Deploy your code on Cloud Functions. Use a Pub/Sub trigger to handle new messages in the topic.
- C. Deploy the application on Google Kubernetes Engine. Use the Pub/Sub API to create a pull subscription to the Pub/Sub topic and read messages from it
- D. Deploy the application on Compute Engine. Use a Pub/Sub push subscription to process new messages in the topic.

**Answer: B**

Explanation:

<https://cloud.google.com/functions/docs/calling/pubsub>

### Question: 233

You are a developer at a large organization. Your team uses Git for source code management (SCM). You want to ensure that your team follows Google-recommended best practices to manage code to drive higher rates of software delivery. Which SCM process should your team use?

- A. Each developer commits their code to the main branch before each product release, conducts testing, and rolls back if integration issues are detected.
- B. Each group of developers copies the repository, commits their changes to their repository, and merges their code into the main repository before each product release.
- C. Each developer creates a branch for their own work, commits their changes to their branch, and merges their code into the main branch daily.
- D. Each group of developers creates a feature branch from the main branch for their work, commits their changes to their branch, and merges their code into the main branch after the change advisory board approves it.

**Answer: D**

Explanation:

Use a centralized repository. A centralized repository is a single location where all of your team's code is stored. This makes it easy for everyone to access the latest code, and it also helps to prevent conflicts. Use branches. Branches are a way to create a separate version of the code for development purposes. This allows developers to work on new features or bug fixes without affecting the main branch of the code.

### Question: 234

You recently developed an application that monitors a large number of stock prices. You need to configure Pub/Sub to receive a high volume of messages and update the current stock price in a single large in-memory database. The downstream service needs only the most up-to-date prices in the in-memory database to perform stock trading transactions. Each message contains three pieces of information:

- Stock symbol
- Stock price
- Timestamp for the update

How should you set up your Pub/Sub subscription?

- A. Create a pull subscription with both ordering and exactly-once delivery turned off
- B. Create a pull subscription with exactly-once delivery enabled
- C. Create a push subscription with exactly-once delivery enabled
- D. Create a push subscription with both ordering and exactly-once delivery turned off

**Answer: C**

Explanation:

### Question: 235

You are a developer at a large corporation You manage three Google Kubernetes Engine clusters.

Your team's developers need to switch from one cluster to another regularly without losing access to their preferred development tools. You want to configure access to these clusters using the fewest number of steps while following Google-recommended best practices. What should you do?

- A. Ask the developers to use Cloud Shell and run `gcloud container clusters get-credentials` to switch to another cluster.
- B. Ask the developers to open three terminals on their workstation and use `kubectrl config` to configure access to each cluster.
- C. Ask the developers to install the `gcloud` CLI on their workstation and run `gcloud container clusters get-credentials` to switch to another cluster
- D. In a configuration file, define the clusters users, and contexts Email the file to the developers and ask them to use `kubectrl config` to add cluster, user and context details.

**Answer: D**

Explanation:

<https://kubernetes.io/docs/tasks/access-application-cluster/configure-access-multiple-clusters/>

### Question: 236

You have a web application that publishes messages to Pub/Sub. You plan to build new versions of the application locally and need to quickly test Pub/Sub integration for each new build. How should you configure local testing?

- A. Run the `gcloud config set api_endpoint_overrides/pubsub https://pubsubemulator.googleapis.com` command to change the Pub/Sub endpoint prior to starting the application
- B. In the Google Cloud console, navigate to the API Library and enable the Pub/Sub API When developing locally, configure your application to call `pubsub.googleapis.com`
- C. Install Cloud Code on the integrated development environment (IDE) Navigate to Cloud APIs, and enable Pub/Sub against a valid Google Project ID. When developing locally, configure your application to call `pubsub.googleapis.com`
- D. Install the Pub/Sub emulator using `gcloud` and start the emulator with a valid Google Project ID. When developing locally, configure your application to use the local emulator by exporting the `FUHSUB` emulator Host variable

**Answer: C**

Explanation:

### Question: 237

You are supporting a business-critical application in production deployed on Cloud Run. The application is reporting HTTP 500 errors that are affecting the usability of the application. You want to be alerted when the number of errors exceeds 15% of the requests within a specific time window. What should you do?

- A. Navigate to the Cloud Run page in the Google Cloud console, and select the service from the services list. Use the Metrics tab to visualize the number of errors for that revision and refresh the page daily.
- B. Create a Cloud Function that consumes the Cloud Monitoring API Use Cloud Composer to trigger the Cloud Function daily and alert you if the number of errors is above the defined threshold.
- C. Create an alerting policy in Cloud Monitoring that alerts you if the number of errors is above the defined threshold.
- D. Create a Cloud Function that consumes the Cloud Monitoring API Use Cloud Scheduler to trigger the Cloud Function daily and alert you if the number of errors is above the defined threshold

**Answer: B**

Explanation:

### Question: 238

You have an application running in a production Google Kubernetes Engine (GKE) cluster. You use Cloud Deploy to automatically deploy your application to your production GKE cluster. As part of your development process: you are planning to make frequent changes to the applications source code and need to select the tools to test the changes before pushing them to your remote source code repository. Your toolset must meet the following requirements:

- Test frequent local changes automatically.
- Local deployment emulates production deployment.

Which tools should you use to test building and running a container on your laptop using minimal resources'?

- A. Terraform and kubeadm
- B. Docker Compose and dockerd
- C. Minikube and Skaffold
- D. kaniko and Tekton

**Answer: B**

Explanation:

### Question: 239

You have an application running on Google Kubernetes Engine (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. Change your application s logging library to the Cloud Logging library and configure your application to

export logs to Cloud Logging

- B. Update your application to output logs in CSV format, and add the necessary metadata to the CSV.
- 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 JSON format, and add the necessary metadata to the JSON

**Answer: B**

Explanation:

### Question: 240

You are a developer at a large organization. You are deploying a web application to Google Kubernetes Engine (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
  - 3 Create a Cloud Build trigger that listens to SUCCEEDED Pub/Sub messages from the cloud-builds topic
  - 4 Configure this pipeline to run a deployment step to the Test cluster

**Answer: B**

Explanation:

### Question: 241

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 Compute Engine, and configure Cloud Endpoints for your application.
- B. Host the application on Google Kubernetes Engine and use Identity-Aware Proxy (IAP) with Cloud Load Balancing and Google-managed certificates.
- C. Host the application on Google Kubernetes Engine, and deploy an NGINX Ingress Controller to handle authentication.
- D. Host the application on Google Kubernetes Engine, and deploy cert-manager to manage SSL certificates.

**Answer: B**

Explanation:

### Question: 242

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 BigQuery tables
- D. Store user data in a Cloud Storage bucket

**Answer: B**

Explanation:

### Question: 243

You need to load-test a set of REST API endpoints that are deployed to Cloud Run. The API responds to HTTP POST requests Your load tests must meet the following requirements:

- Load is initiated from multiple parallel threads
- User traffic to the API originates from multiple source IP addresses.
- Load can be scaled up using additional test instances

You want to follow Google-recommended best practices How should you configure the load testing'?

- A. Create an image that has cURL installed and configure cURL to run a test plan Deploy the image in a managed instance group, and run one instance of the image for each VM.
- B. Create an image that has cURL installed and configure cURL to run a test plan Deploy the image in an unmanaged instance group, and run one instance of the image for each VM.
- C. Deploy a distributed load testing framework on a private Google Kubernetes Engine Cluster Deploy additional Pods as needed to initiate more traffic and support the number of concurrent users.
- D. Download the container image of a distributed load testing framework on Cloud Shell Sequentially start several instances of the container on Cloud Shell to increase the load on the API.

**Answer: C**

Explanation:

### Question: 244

You are a lead developer working on a new retail system that runs on Cloud Run and Firestore. A web UI requirement is for the user to be able to browse through all products. A few months after go-live, you notice that Cloud Run instances are terminated with HTTP 500: Container instances are exceeding memory limits errors during busy times

This error coincides with spikes in the number of Firestore queries

You need to prevent Cloud Run from crashing and decrease the number of Firestore queries. You want to use a solution that optimizes system performance. What should you do?

- A. Create a custom index over the products
- B. Modify the query that returns the product list using cursors with limits
- C. Modify the Cloud Run configuration to increase the memory limits
- D. Modify the query that returns the product list using integer offsets

**Answer: B**

Explanation:

### Question: 245

You are using Cloud Run to host a global ecommerce web application. Your company's design team is creating a new color scheme for the web app. You have been tasked with determining whether the new color scheme will increase sales. You want to conduct testing on live production traffic. How should you design the study?

- A. Use an external HTTP(S) load balancer to route a predetermined percentage of traffic to two different color schemes of your application. Analyze the results to determine whether there is a statistically significant difference in sales.
- B. Use an external HTTP(S) load balancer to route traffic to the original color scheme while the new deployment is created and tested. After testing is complete, reroute all traffic to the new color scheme. Analyze the results to determine whether there is a statistically significant difference in sales.
- C. Enable a feature flag that displays the new color scheme to half of all users. Monitor sales to see whether they increase for this group of users.
- D. Use an external HTTP(S) load balancer to mirror traffic to the new version of your application. Analyze the results to determine whether there is a statistically significant difference in sales.

**Answer: A**

Explanation:

### Question: 246

Your team is setting up a build pipeline for an application that will run in Google Kubernetes Engine (GKE). For security reasons, you only want images produced by the pipeline to be deployed to your GKE cluster. Which combination of Google Cloud services should you use?

- A. Google Cloud Deploy, Artifact Registry, and Google Cloud Armor
- B. Google Cloud Deploy, Cloud Storage, and Google Cloud Armor
- C. Cloud Build, Cloud Storage, and Binary Authorization
- D. Cloud Build, Artifact Registry, and Binary Authorization

**Answer: A**

Explanation:

### Question: 247

You are developing an online gaming platform as a microservices application on Google Kubernetes Engine (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. 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.
- C. 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.
- D. 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.

**Answer: B**

Explanation:

### Question: 248

You are working on a new application that is deployed on Cloud Run and uses Cloud Functions. Each time new features are added, new Cloud Functions and Cloud Run services are deployed. You use ENV variables to keep track of the services and enable interservice communication, but the maintenance of the ENV variables has become difficult. You want to implement dynamic discovery in a scalable way. What should you do?

- A. Create a Service Directory Namespace. Use API calls to register the services during deployment, and query during runtime.
- B. Configure your microservices to use the Cloud Run Admin and Cloud Functions APIs to query for deployed Cloud Run services and Cloud Functions in the Google Cloud project.
- C. Deploy Hashicorp Consul on a single Compute Engine Instance. Register the services with Consul during deployment and query during runtime.
- D. Rename the Cloud Functions and Cloud Run services endpoints using a well-documented naming convention.

**Answer: B**

Explanation:

### Question: 249

You have deployed a Java application to Cloud Run. Your application requires access to a database hosted on Cloud SQL. Due to regulatory requirements, your connection to the Cloud SQL instance must use its internal IP address. How should you configure the connectivity while following Google-recommended best practices?

- A. Configure your Cloud Run service with a Cloud SQL connection.
- B. Configure your Cloud Run service to use a Serverless VPC Access connector
- C. Configure your application to use the Cloud SQL Java connector
- D. Configure your application to connect to an instance of the Cloud SQL Auth proxy

**Answer: A**

Explanation:

### Question: 250

Your team is developing a Cloud Function triggered by Cloud Storage Events. You want to accelerate testing and development of your Cloud Function while following Google-recommended best practices. What should you do?

- A. Install the Functions Framework library, and configure the Cloud Function on localhost. Make a copy of the function, and make edits to the new version Test the new version using curl.
- B. Make a copy of the Cloud Function, and rewrite the code to be HTTP-triggered Edit and test the new version by triggering the HTTP endpoint. Send mock requests to the new function to evaluate the functionality.
- C. Make a copy of the Cloud Function in the Google Cloud Console Use the Cloud console's in-line editor to make source code changes to the new function Modify your web application to call the new function and test the new version in production.
- D. Create a new Cloud Function that is triggered when Cloud Audit Logs detects the cloudfunctions. functions. sourceCodeSet operation in the original Cloud Function Send mock requests to the new function to evaluate the functionality.

**Answer: A**

Explanation:

### Question: 251

Your team recently deployed an application on Google Kubernetes Engine (GKE). You are monitoring your application and want to be alerted when the average memory consumption of your containers is under 20% or above 80% How should you configure the alerts?

- A. Create a Cloud Function that consumes the Monitoring API. Create a schedule to trigger the Cloud Function hourly and alert you if the average memory consumption is outside the defined range
- B. In Cloud Monitoring, create an alerting policy to notify you if the average memory consumption is outside the defined range
- C. Create a Cloud Function that runs on a schedule, executes kubectl top on all the workloads on the cluster, and sends an email alert if the average memory consumption is outside the defined range
- D. Write a script that pulls the memory consumption of the instance at the OS level and sends an email alert if the average memory consumption is outside the defined range

**Answer: B**

Explanation:

**Question: 252**

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. Create an Eventarc trigger that monitors your Cloud Storage bucket for a specific filename, and set the target as Cloud Run.
- B. 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.
- C. Configure a Firebase function that executes your application and is triggered when an object is updated in Cloud Storage.
- D. Configure a Cloud Function that executes your application and is triggered when an object is updated in Cloud Storage.

**Answer: C**

Explanation:

## Question: 253

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.

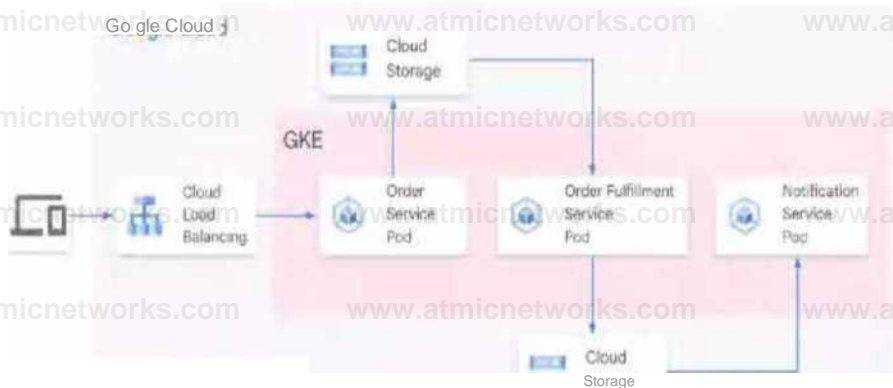
i Order request -> Order Service -> Order Fulfillment Service — Notification Service

Go gle Cloud



B.

Order request -> Order Service -> Cloud Storage bucket -> Order Fulfillment Service -> Cloud Storage bucket -> Notification Service



C.

Order request -> Order Service — Firestore database — Order Fulfillment Service — Firestore database — Notification Service



D.

Order request — Order Service — Pub/Sub queue — Order Fulfillment Service — Firestore database — Pub/Sub queue — Notification Service



**Answer: A**

Explanation:

### Question: 254

You need to deploy an internet-facing microservices application to Google Kubernetes Engine (GKE).

You want to validate new features using the A/B testing method. You have the following requirements for deploying new container image releases

- There is no downtime when new container images are deployed.
- New production releases are tested and verified using a subset of production users.

What should you do?

- .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.

8.1 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.

**Answer: C**

Explanation:

### Question: 255

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 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.
- D. Configure the sender application to retry the execution of the Cloud Function every one second if a request fails.

**Answer: B**

Explanation:

This is a robust and scalable approach. By decoupling the email sending process using Pub/Sub, you introduce a queueing mechanism. This ensures that even if the Cloud Function encounters an issue, the email messages are not lost but remain in the queue. Additionally, Pub/Sub can handle high throughput and provides retry mechanisms.

### Question: 256

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 new project with a random name for every build. Load the required data. Delete the project after the test is run.

- B. Create a new Cloud Spanner instance for every build. Load the required data. Delete the Cloud Spanner instance after the test is run.
- C. 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 run.
- D. Start the Cloud Spanner emulator locally. Load the required data. Shut down the emulator after the test is run.

**Answer: B**

**Explanation:**

Since the testing needs to accommodate scenarios where multiple commits are made simultaneously, and hence multiple tests might run concurrently, the testing environment should support isolated and independent testing instances to avoid interference among tests. Given these requirements, using the Cloud Spanner emulator would not be the best choice for this scenario. The emulator is primarily suited for local development, unit, and integration testing, and is not built for production-scale performance testing. It may not accurately replicate performance characteristics at scale or under load, which are crucial aspects in this case.

**Question: 257**

You are monitoring a web application that is written in Go and deployed in Google Kubernetes Engine. You notice an increase in CPU and memory utilization. You need to determine which function is consuming the most CPU and memory resources. What should you do?

- A. Import the Cloud Profiler package into your application, and initialize the Profiler agent. Review the generated flame graph in the Google Cloud console to identify time-intensive functions.
- B. Create a Cloud Logging query that gathers the web application's logs. Write a Python script that calculates the difference between the timestamps from the beginning and the end of the application's longest functions to identify time-intensive functions.
- C. Import OpenTelemetry and Trace export packages into your application, and create the trace provider. Review the latency data for your application on the Trace overview page, and identify which functions cause the most latency.
- D. Add print commands to the application source code to log when each function is called, and redeploy the application.

**Answer: A**

**Explanation:**

Google Cloud Profiler efficiently analyzes cloud-based applications, like those on GKE, using minimal code changes and flame graphs for in-depth insights into CPU and memory usage, thus identifying performance bottlenecks with ease. For more information, visit: [https://dev.to/billcchung/profiling-](https://dev.to/billcchung/profiling-go-grpc-service-with-google-cloud-profiler-1k8l)

[go-grpc-service-with-google-cloud-profiler-1k8l](https://www.cncf.io/blog/2020/03/27/continuous-profiling-go-application-running-in-kubernetes/) and <https://www.cncf.io/blog/2020/03/27/continuous-profiling-go-application-running-in-kubernetes/>

## Question: 258

You are a developer at a large organization. Your team uses Git for source code management (SCM). You want to ensure that your team follows Google-recommended best practices to manage code to drive higher rates of software delivery. Which SCM process should your team use?

- A. Each group of developers creates a feature branch from the main branch for their work, commits their changes to their branch, and merges their code into the main branch before each major release.
- B. Each developer commits their code to the main branch before each product release, conducts testing, and rolls back if integration issues are detected.
- C. Each group of developers copies the repository, commits their changes to their repository, and merges their code into the main repository before each product release.
- D. Each developer creates a branch for their own work, commits their changes to their branch, and merges their code into the main branch after peer review.

**Answer: D**

Explanation:

## Question: 259

A governmental regulation was recently passed that affects your application. For compliance purposes, you are now required to send a duplicate of specific application logs from your application's project to a project that is restricted to the security team. What should you do?

- A. Modify the `_Default` log bucket sink rules to reroute the logs into the security team's log bucket.
- B. Create user-defined log buckets in the security team's project. Configure a Cloud Logging sink to route your application's logs to log buckets in the security team's project.
- C. Create a job that copies the System Event logs from the `_Required` log bucket into the security team's log bucket in their project.
- D. Create a job that copies the logs from the `_Required` log bucket into the security team's log bucket in their project.

**Answer: B**

Explanation:

## Question: 260

Your application stores customers' content in a Cloud Storage bucket, with each object being encrypted with the customer's encryption key. The key for each object in Cloud Storage is entered into your application by the customer. You discover that your application is receiving an HTTP 4xx error when reading the object from Cloud Storage. What is a possible cause of this error?

- A. You attempted the read operation without the base64-encoded SHA256 hash of the encryption key.
- B. You entered the same encryption algorithm specified by the customer when attempting the read operation.

- C. You attempted the read operation on the object with the base64-encoded SHA256 hash of the customer's key.
- D. You attempted the read operation on the object with the customer's base64-encoded key.

**Answer: D**

Explanation:

### Question: 261

You are reviewing and updating your Cloud Build steps to adhere to Google-recommended practices.

Currently, your build steps include:

1. Pull the source code from a source repository.
2. Build a container image
3. Upload the built image to Artifact Registry.

You need to add a step to perform a vulnerability scan of the built container image, and you want the results of the scan to be available to your deployment pipeline running in Google Cloud. You want to minimize changes that could disrupt other teams' processes. What should you do?

- A. Enable Binary Authorization, and configure it to attest that no vulnerabilities exist in a container image.
- B. Enable the Container Scanning API in Artifact Registry, and scan the built container images for vulnerabilities.
- C. Upload the built container images to your Docker Hub instance, and scan them for vulnerabilities.
- D. Add Artifact Registry to your Aqua Security instance, and scan the built container images for vulnerabilities.

**Answer: B**

Explanation:

### Question: 262

You are tasked with using C++ to build and deploy a microservice for an application hosted on Google Cloud. The code needs to be containerized and use several custom software libraries that your team has built. You do not want to maintain the underlying infrastructure of the application. How should you deploy the microservice?

- A. Use Cloud Functions to deploy the microservice.
- B. Use Cloud Build to create the container, and deploy it on Cloud Run.
- C. Use Cloud Shell to containerize your microservice, and deploy it on GKE Standard.
- D. Use Cloud Shell to containerize your microservice, and deploy it on a Container-Optimized OS Compute Engine instance.

**Answer: B**

Explanation:

### Question: 263

Your team is creating a serverless web application on Cloud Run. The application needs to access images stored

in a private Cloud Storage bucket. You want to give the application Identity and Access Management (IAM) permission to access the images in the bucket, while also securing the services using Google-recommended best practices. What should you do?

- A. Enforce signed URLs for the desired bucket. Grant the Storage Object Viewer IAM role on the bucket to the Compute Engine default service account.
- B. Enforce public access prevention for the desired bucket. Grant the Storage Object Viewer IAM role on the bucket to the Compute Engine default service account.
- C. Enforce signed URLs for the desired bucket. Create and update the Cloud Run service to use a user-managed service account. Grant the Storage Object Viewer IAM role on the bucket to the service account.
- D. Enforce public access prevention for the desired bucket. Create and update the Cloud Run service to use a user-managed service account. Grant the Storage Object Viewer IAM role on the bucket to the service account.

**Answer: B**

Explanation:

### Question: 264

You are developing an online gaming platform as a microservices application on Google Kubernetes Engine (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. 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.
- B. 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.
- C. Instrument your microservices by installing the Open Telemetry 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.
- D. 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.

**Answer: D**

Explanation:

### Question: 265

You are a developer at a social media company. The company runs their social media website on-premises and uses MySQL as a backend to store user profiles and user posts. Your company plans to migrate to Google Cloud, and your team will migrate user profile information to Firestore. You are tasked with designing the Firestore collections. What should you do?

- A. Create one root collection for user profiles, and store each user's post as a nested list in the user profile document.
- B. Create one root collection for user profiles, and create one root collection for user posts.
- C. Create one root collection for user profiles, and create one subcollection for each user's posts.
- D. Create one root collection for user posts, and create one subcollection for each user's profile

**Answer: C**

**Explanation:**