You have a large 5-TB AVRO file stored in a Cloud Storage bucket. Your analysts are proficient only in SQL and need access to the data stored in this file. You want to find a cost-effective way to complete their request as soon as possible. What should you do?

A. Load data in Cloud Datastore and run a SQL query against it.
B. Create a BigQuery table and load data in BigQuery. Run a SQL query on this table and drop this table after you complete your request.
C. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.
D. Create a Hadoop cluster and copy the AVRO file to NDFS by compressing it. Load the file in a hive table and provide access to your analysts so that they can run SQL queries.

Your company uses BigQuery for data warehousing. Over time, many different business units in your company have created 1000+ datasets across hundreds of projects. Your CIO wants you to examine all datasets to find tables that contain an employee_ssn column. You want to minimize effort in performing this task.
What should you do?

A. Go to Data Catalog and search for employee_ssn in the search box.
B. Write a shell script that uses the bq command line tool to loop through all the projects in your organization.
C. Write a script that loops through all the projects in your organization and runs a query on INFORMATION_SCHEMA.COLUMNS view to find the employee_ssn column.
D. Write a Cloud Dataflow job that loops through all the projects in your organization and runs a query on INFORMATION_SCHEMA.COLUMNS view to find employee_ssn column.

Your company implemented BigQuery as an enterprise data warehouse. Users from multiple business units run queries on this data warehouse. However, you notice that query costs for BigQuery are very high, and you need to control costs. Which two methods should you use? (Choose two.)

A. Split the users from business units to multiple projects.
B. Apply a user- or project-level custom query quota for BigQuery data warehouse.
C. Create separate copies of your BigQuery data warehouse for each business unit.
D. Split your BigQuery data warehouse into multiple data warehouses for each business unit.
E. Change your BigQuery query model from on-demand to flat rate. Apply the appropriate number of slots to each Project.

You have an application that uses Cloud Spanner as a database backend to keep current state information about users. Cloud Bigtable logs all events triggered by users. You export Cloud Spanner data to Cloud Storage during daily backups. One of your analysts asks you to join data from Cloud Spanner and Cloud
Bigtable for specific users. You want to complete this ad hoc request as efficiently as possible. What should you do?

A. Create a dataflow job that copies data from Cloud Bigtable and Cloud Storage for specific users.
B. Create a dataflow job that copies data from Cloud Bigtable and Cloud Spanner for specific users.
C. Create a Cloud Dataproc cluster that runs a Spark job to extract data from Cloud Bigtable and Cloud Storage for specific users.
D. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

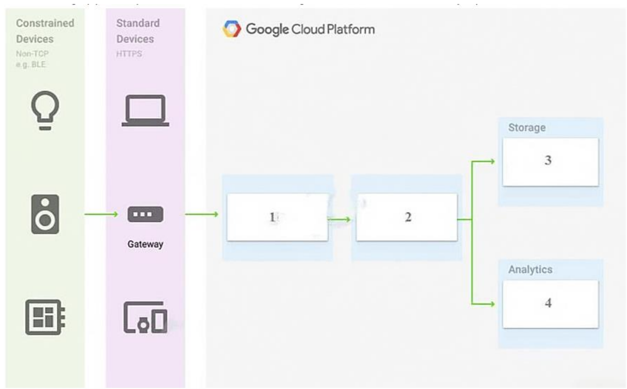
You need to run an important query in BigQuery but expect it to return a lot of records. You want to find out how much it will cost to run the query. You are using on- demand pricing. What should you do?

A. Arrange to switch to Flat-Rate pricing for this query, then move back to on-demand.
B. Use the command line to run a dry run query to estimate the number of bytes read. Then convert that bytes estimate to dollars using the Pricing Calculator.
C. Use the command line to run a dry run query to estimate the number of bytes returned. Then convert that bytes estimate to dollars using the Pricing Calculator.
D. Run a select count (*) to get an idea of how many records your query will look through. Then convert that number of rows to dollars using the Pricing Calculator.

You are analyzing Google Cloud Platform service costs from three separate projects. You want to use this information to create service cost estimates by service type, daily and monthly, for the next six months using standard query syntax. What should you do?

A. Export your bill to a Cloud Storage bucket, and then import into Cloud Bigtable for analysis.
B. Export your bill to a Cloud Storage bucket, and then import into Google Sheets for analysis.
C. Export your transactions to a local file, and perform analysis with a desktop tool.
D. Export your bill to a BigQuery dataset, and then write time window-based SQL queries for analysis.

You are building a pipeline to process time-series data. Which Google Cloud Platform services should you put in boxes 1,2,3, and 4?



A. Cloud Pub/Sub, Cloud Dataflow, Cloud Datastore, BigQuery
B. Firebase Messages, Cloud Pub/Sub, Cloud Spanner, BigQuery
C. Cloud Pub/Sub, Cloud Storage, BigQuery, Cloud Bigtable
D. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery

Auditors visit your teams every 12 months and ask to review all the Google Cloud Identity and Access Management (Cloud IAM) policy changes in the previous 12 months. You want to streamline and expedite the analysis and audit process. What should you do?

A. Enable Logging export to Google Cloud Storage (GCS) bucket and delegate access to the bucket
B. Enable Logging export to Google BigQuery and use ACLs and views to scope the data shared with the auditor
C. Create custom Google Stackdriver alerts and send them to the auditor
D. Use Cloud Functions to transfer log entries to Google Cloud SQL and use ACLs and views to limit an auditor's view

You want to ingest and analyze large volumes of stream data from sensors in real-time, matching the high speeds of IoT data to track normal and abnormal behavior. You want to run it through a data processing pipeline and store the results. Finally, you want to enable customers to build dashboards and drive analytics on their data in real-time. What services should you use for this task?

A. Cloud Pub/Sub, Cloud Dataflow, BigQuery
B. Cloud Pub/Sub, Cloud Dataflow, Cloud Dataprep
C. Stackdriver, Cloud Dataflow, BigQuery
D. Cloud Pub/Sub, Cloud Dataflow, Cloud Dataproc

Your company runs a very successful web platform and has accumulated 3 petabytes of customer activity data in sharded MySQL database located in your datacenter. Due to storage limitations in your on-premise data center, your company has decided to move this data to GCP. The data must be available all through the day. Your business analysts, who have experience of using a SQL Interface, have asked for a seamless transition. How should you store the data so that availability is ensured while optimizing the ease of analysis for the business analysts?

A. Import data into Google Cloud SQL.
B. Import flat files into Google Cloud Storage.
C. Import data into Google Cloud Datastore.
D. Import data into Google BigQuery.

You need to estimate the annual cost of running a BigQuery query that is scheduled to run nightly. What should you do?

A. Use gcloud query --dry_run to determine the number of bytes read by the query. Use this number in the Pricing Calculator.

B. Use bq query -dry_run to determine the number of bytes read by the query. Use this number in the Pricing Calculator.

C. Use gcloud estimate to determine the amount billed for a single query. Multiply this amount by 365.

D. Use bq estimate to determine the amount billed for a single query. Multiply this amount by 365.

You are required to fire a query on large amount of data stored in BigQuery. You know the query is expected to return a large amount of data. How would you estimate the cost for the query?

A. Using Command line, use the --dry_run option on BigQuery to determine the amount of bytes read, and then use the price calculator to determine the cost.
B. Using Command line, use the --dry_run option on BigQuery to determine the amount of bytes returned, and then use the price calculator to determine the cost.
C. Using Command line, use the --dry_run option on BigQuery to determine the amount of time taken, and then use the price calculator to determine the cost.
D. Using Command line, use the -dry_run option on BigQuery to determine the total amount of table data in bytes, as it would be a full scan, and then use the price calculator to determine the cost.

The core business of your company is to rent out construction equipment at large scale. All the equipment that is being rented out has been equipped with multiple sensors that send event information every few seconds. These signals can vary from engine status, distance traveled, fuel level, and more. Customers are billed based on the consumption monitored by these sensors. You expect high throughput â€" up to thousands of events per hour per device â€" and need to retrieve consistent data based on the time of the event. Storing and retrieving individual signals should be atomic. What should you do?

A. Create a file in Cloud Storage per device and append new data to that file.
B. Create a file in Cloud Filestore per device and append new data to that file.
C. Ingest the data into Datastore. Store data in an entity group based on the device.
D. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

You have created a code snippet that should be triggered whenever a new file is uploaded to a Cloud Storage bucket. You want to deploy this code snippet. What should you do?

A. Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub.
B. Use Cloud Functions and configure the bucket as a trigger resource.
C. Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub.
D. Use Dataflow as a batch job, and configure the bucket as a data source.

A company wants to build an application that stores images in a Cloud Storage bucket and wants to generate thumbnails as well as resize the images. They want to use a google managed service that can scale up and scale down to zero automatically with minimal effort. You have been asked to recommend a service. Which GCP service would you suggest?

A. Google Compute Engine
B. Google Kubernetes Engine
C. Cloud Functions
D. Google App Engine

You have a number of applications that have bursty workloads and are heavily dependent on topics to decouple publishing systems from consuming systems. Your company would like to go serverless to enable developers to focus on writing code without worrying about infrastructure. Your solution architect has already identified Cloud Pub/Sub as a suitable alternative for decoupling systems. You have been asked to identify a suitable GCP Serverless service that is easy to use with Cloud Pub/Sub. You want the ability to scale down to zero when there is no traffic in order to minimize costs. You want to follow Google recommended practices. What should you suggest?

A. Cloud Run for Anthos
B. Cloud Functions
C. App Engine Standard
D. Cloud Run

You want to create a new role and grant it to the SME team. The new role should provide your SME team BigQuery Job User and Cloud Bigtable User roles on all projects in the organization.

You want to minimize operational overhead. You want to follow Google recommended practices. How should you create the new role?

A. Execute command gcloud iam combineroles --global to combine the 2 roles into a new custom role and grant them globally to SME team group.

B. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at the organization level.

C. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Use gcloud iam promote-

D. role to promote the role to all other projects and grant the role in each project to the SME team group.

E. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Repeat this step for each project.

You have a Google Cloud Platform account with access to both production and development projects. You need to create an automated process to list all compute instances in development and production projects on a daily basis. What should you do?

A. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

B. Create two configurations using gsutil config. Write a script that sets configurations as active, individually. For each configuration, use gsutil compute instances list to get a list of compute resources.

C. Go to Cloud Shell and export this information to Cloud Storage on a daily basis.

D. Go to GCP Console and export this information to Cloud SQL on a daily basis.

You have downloaded and installed the gcloud command line interface (CLI) and have authenticated with your Google Account. Most of your Compute Engine instances in your project run in the europe-west1-d zone. You want to avoid having to specify this zone with each CLI command when managing these instances.
What should you do?

A. Set the europe-west1-d zone as the default zone using the gcloud config set command.

B. In the Settings page for Compute Engine under Default location, set the zone to europe-west1-d.

C. In the CLI installation directory, create a file called default.conf containing zone=europe-west1-d.

D. Create a Metadata entry on the Compute Engine page with key compute/zone and value europe-west1-d.

You have one GCP account running in your default region and zone and another account running in a non-default region and zone. You want to start a new Compute Engine instance in these two Google Cloud Platform accounts using the command line interface. What should you do?

A. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

B. Create two configurations using gcloud config configurations create [NAME]. Run gcloud configurations list to start the Compute Engine instances.

C. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud config list to start the Compute Engine instances.

D. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud configurations list to start the Compute Engine instances.

In Cloud Shell, your active gcloud configuration is as shown below.

```
$ gcloud config list
[component_manager] disable_update_check = True
 [compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False
 project = gcp-ace-lab-266520
 [metrics]
environment = devshell
```

You want to create two compute instances - one in europe-west2-a and another in europe-west2-b. What should you do? (Select 2)

A. gcloud compute instances create instance1
gcloud compute instances create instance2

**B. gcloud compute instances create instance1
gcloud config set compute/zone europe-west2-b
gcloud compute instances create instance2**

**C. gcloud compute instances create instance1
gcloud compute instances create instance2 -zone=europe-west2-b**

D. gcloud compute instances create instance1
gcloud config set zone europe-west2-b
gcloud compute instances create instance2

E. gcloud compute instances create instance1
gcloud configuration set compute/zone europe-west2-b
gcloud compute instances create instance2

You created a compute instance by running gcloud compute instances create instancel. You intended to create the instance in project gcp-ace-proj-266520 but the instance got created in a different project. Your cloud shell gcloud configuration is as shown.

```
$ gcloud config list
[component_manager]
disable_update_check = True
[compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False project = gcp-ace-lab-266520 [metrics]
environment = devshell
```

What should you do to delete the instance that was created in the wrong project and recreate it in gcp-ace-proj-266520 project?

A. gcloud compute instances delete instance1
   gcloud config set compute/project gcp-ace-proj-266520
   gcloud compute instances create instance1

B. gcloud config set project gcp-ace-proj-266520
   gcloud compute instances recreate instancel -previous-project gcp-ace-lab-266520

C. gcloud compute instances delete instancel
   gcloud compute instances create instancel

D. gcloud compute instances delete instancel
   gcloud config set project gcp-ace-proj-266520
   gcloud compute instances create instancel

You developed an application that reads objects from a cloud storage bucket. You followed GCP documentation and created a service account with just the permissions to read objects from the cloud storage bucket. However, when your application uses this service account, it fails to read objects from the bucket. You suspect this might be an issue with the permissions assigned to the service account. You would like to authenticate a gsutil session with the service account credentials, reproduce the issue yourself and identify the root cause. How can you authenticate gsutil with service account credentials?

A. Create JSON keys for the service account and execute
   gcloud auth activate-service-account -key-file [KEY_FILE]

B. Create JSON keys for the service account and execute
   gcloud auth service-account -key-file [KEY_FILE]

C. Create JSON keys for the service account and execute
   gcloud authenticate service-account -key-file [KEY_FILE]

D. Create JSON keys for the service account and execute
gcloud authenticate activate-service-account -key-file [KEY_FILE]

You ran the following commands to create two compute instances,

```
gcloud compute instances create instancel
gcloud compute instances create instance2
```

Both compute instances were created in europe-west2-a zone but you want to create them in other zones. Your active gcloud configuration is as shown below.

```
$ gcloud config list
 [component_manager]
disable_update_check = True
 [compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False project = gcp-ace-lab-266520 [metrics]
environment = devshell
```

You want to modify the gcloud configuration such that you are prompted for a zone when you execute the create instance commands above. What should you do?

A. gcloud config unset compute/zone

B. gcloud config set zone ""

C. gcloud config set compute/zone ""

D. gcloud config unset zone

You plan to deploy an application on an autoscaled managed instances group. The application uses a tomcat server and runs on port 8080. You want to access the application on **https**://www.example.com. You want to follow Google recommended practices. What services would you use?

A. Google Domains, Cloud DNS private zone, HTTP(S) Load Balancer

B. Google Domains, Cloud DNS private zone, SSL Proxy Load Balancer

C. Google DNS, Google CDN, SSL Proxy Load Balancer

D. Google Domains, Cloud DNS, HTTP(S) Load Balancer

You want to serve files under the URL https://www.my-new-gcp-ace-website.com/static/ from Cloud Storage. In addition, the URL https://www.my-new-gcp-ace- website.com/app/ should be handled by a Compute Engine managed instance group (MIG). You want to follow Google recommended practices. How should you configure load balancing?

A. 1. Deploy HAProxy in a second MIG and configure it to route /app/ to the first MIG and /static/ to your Cloud Storage bucket. 2. Create a network Load Balancer in front of the HAProxy MIG 3. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer
B. 1. Create a HTTPS Load Balancer in front of the MIG 2. In Cloud DNS in the my-new-gcp-ace-website.com zone, create a TXT record for _app_._routes_.www.my-new- gcp-ace-website.com containing the address of the load balancer. 3. Create another TXT record for _static_._routes_.www.my-new-gcp-ace-website.com containing the URL of your Cloud Storage bucket.
C. 1. Configure www.my-new-gcp-ace-website.com as a CNAME pointing to storage.googleapis.com 2. Create a HTTPS Load Balancer in front of the MIG 3. IN the app folder of your Cloud Storage Bucket, add a file called redirect containing the address of the load balancer.
D. 1. Create a HTTPS Load Balancer 2. Create a backend service associated with the MIG and route /app/ to the backend service 3. Create a backend bucket associated with your Cloud Storage Bucket, and route /static/ to the backend bucket 4. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer

You need to deploy an application, which is packaged in a container image, in a new project. The application exposes an HTTP endpoint and receives very few requests per day. You want to minimize costs. What should you do?

A. Deploy the container on Cloud Run.
B. Deploy the container on Cloud Run on GKE.
C. Deploy the container on App Engine Flexible.
D. Deploy the container on GKE with cluster autoscaling and horizontal pod autoscaling enabled.

You have developed a containerized web application that will serve internal colleagues during business hours. You want to ensure that no costs are incurred outside of the hours the application is used. You have just created a new Google Cloud project and want to deploy the application. What should you do?

A. Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero.
B. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.
C. Deploy the container on App Engine flexible environment with autoscaling, and set the value mininstances to zero in the app.yaml.
D. Deploy the container on App Engine flexible environment with manual scaling, and set the value instances to zero in the app.yaml.

Your web application has been running successfully on Cloud Run for Anthos. You want to evaluate an updated version of the application with a specific percentage of your production users (canary deployment). What should you do?

A. Create a new service with the new version of the application. Split traffic between this version and the version that is currently running.
B. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.
C. Create a new service with the new version of the application. Add HTTP Load Balancer in front of both services.
D. Create a new revision with the new version of the application. Add HTTP Load Balancer in front of both revisions.

You have an application running in App Engine standard environment. You want to add a custom C# library to enhance the functionality of this application. However, C# isn't supported by App Engine standard. You want to maintain the serverless aspect of your application. What should you do? Choose 2 answers.

- Containerize your new application and deploy it to a Cloud Run on GKE environment.

O Containerize your new application and deploy it to a Cloud Run environment.

- Containerize your new application and deploy it to a App Engine flexible environment.
- Containerize your new application and deploy it to a Google Kubernetes Engine environment.
- Split your application into different functions. Deploy your application as separate cloud functions in Google Cloud Functions (GCP) environment.

Your company has chosen to go serverless to enable developers to focus on writing code without worrying about infrastructure. You have been asked to identify a GCP Serverless service that does not limit your developers to specific runtimes. In addition, some of the applications need WebSockets support. What should you suggest?

A. Cloud Run
B. Cloud Run for Anthos
C. App Engine Standard
D. Cloud Functions

You are building an application that stores relational data from users. Users across the globe will use this application. Your CTO is concerned about the scaling requirements because the size of the user base is unknown. You need to implement a database solution that can scale with your user growth with minimum configuration changes. Which storage solution should you use?

A. Cloud SQL
B. Cloud Spanner
C. Cloud Firestore

D. Cloud Datastore

You have a developer laptop with the Cloud SDK installed on Ubuntu. The Cloud SDK was installed from the Google Cloud Ubuntu package repository. You want to test your application locally on your laptop with Cloud Datastore. What should you do?

A. Export Cloud Datastore data using gcloud datastore export.
B. Create a Cloud Datastore index using gcloud datastore indexes create.
C. Install the google-cloud-sdk-datastore-emulator component using the apt get install command.
D. Install the cloud-datastore-emulator component using the gcloud components install command.

Your company has an App Engine application that needs to store stateful data in a proper storage service. Your data is non-relational data. You do not expect the database size to grow beyond 10 GB and you need to have the ability to scale down to zero to avoid unnecessary costs. Which storage service should you use?

A. Cloud SQL
B. Cloud Datastore
C. Cloud Bigtable
D. Cloud Dataproc

You are using Deployment Manager to create a Google Kubernetes Engine cluster. Using the same Deployment Manager deployment, you also want to create a DaemonSet in the kube-system namespace of the cluster. You want a solution that uses the fewest possible services. What should you do?

A. Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.
B. Use the Deployment Manager Runtime Configurator to create a new Config resource that contains the DaemonSet definition.
C. With Deployment Manager, create a Compute Engine instance with a startup script that uses kubectl to create the DaemonSet.
D. In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value.

Your team maintains the infrastructure for your organization. The current infrastructure requires changes. You need to share your proposed changes with the rest of the team. You want to follow Google's recommended best practices. What should you do?

A. Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket.
B. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.
C. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.
D. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

Your company wants to standardize the creation and management of multiple Google Cloud resources using Infrastructure as Code. You want to minimize the amount of repetitive code needed to manage the environment. What should you do?

A. Develop templates for the environment using Cloud Deployment Manager.
B. Use curl in a terminal to send a REST request to the relevant Google API for each individual resource.
C. Use the Cloud Console interface to provision and manage all related resources.
D. Create a bash script that contains all requirement steps as gcloud commands.

You need a dynamic way of provisioning VMs on Compute Engine. The exact specifications will be in a dedicated configuration file. You want to follow Google's recommended practices. Which method should you use?

A. Deployment Manager
B. Cloud Composer
C. Managed Instance Group
D. Unmanaged Instance Group

You need to update a deployment in Deployment Manager without any resource downtime in the deployment. Which command should you use?

A. gcloud deployment-manager deployments create -config <deployment-config-path>
B. gcloud deployment-manager deployments update --config <deployment-config-path>
C. gcloud deployment-manager resources create --config <deployment-config-path>
D. gcloud deployment-manager resources update --config <deployment-config-path>

You significantly changed a complex Deployment Manager template and want to confirm that the dependencies of all defined resources are properly met before committing it to the project. You want the most rapid feedback on your changes. What should you do?

A. Use granular logging statements within a Deployment Manager template authored in Python.

B. Monitor activity of the Deployment Manager execution on the Stackdriver Logging page of the GCP Console.
C. Execute the Deployment Manager template against a separate project with the same configuration, and monitor for failures.
D. Execute the Deployment Manager template using the -preview option in the same project, and observe the state of interdependent resources.

You created a cluster.YAML file containing
resources:
- name: cluster
type: container.v1 .cluster
properties:
zone: europe-west1-b cluster:
description: “My GCP ACE cluster” initialNodeCount: 2
You want to use Cloud Deployment Manager to create this cluster in GKE. What should you do?

- **A. gcloud deployment-manager deployments create my-gcp-ace-cluster --config cluster.yaml**
- B. gcloud deployment-manager deployments create my-gcp-ace-cluster --type container.v1 .cluster -config cluster.yaml
- C. gcloud deployment-manager deployments apply my-gcp-ace-cluster --config cluster.yaml
- D. gcloud deployment-manager deployments apply my-gcp-ace-cluster --type container.v1 .cluster --config cluster.yaml

You want to deploy a python application to an autoscaled managed instance group on Compute Engine. You want to use GCP deployment manager to do this. What is the fastest way to get the application onto the instances without introducing undue complexity?

- A. Include a startup script to bootstrap the python application when creating an instance template by running gcloud compute instance-templates create app-template - metadata-from-file startup-script-url=/scripts/install_app.sh
- B. Once the instance starts up, connect over SSH and install the application.
- **C. Include a startup script to bootstrap the python application when creating an instance template by running gcloud compute instance-templates create app-template - metadata-from-file startup-script=/scripts/install_app.sh**
- D. Include a startup script to bootstrap the python application when creating an instance template by running gcloud compute instance-templates create app-template - startup-script=/scripts/install_app.sh

You created a Google Cloud Platform project with an App Engine application inside the project. You initially configured the application to be served from the us- central region. Now you want the application to be served from the asia-northeast1 region. What should you do?

A. Change the default region property setting in the existing GCP project to asia-northeast1.
B. Change the region property setting in the existing App Engine application from us-central to asia-northeast1.
C. Create a second App Engine application in the existing GCP project and specify asia-northeast1 as the region to serve your application.
D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

You recently deployed a new version of an application to App Engine and then discovered a bug in the release. You need to immediately revert to the prior version of the application. What should you do?

A. Run gcloud app restore.
B. On the App Engine page of the GCP Console, select the application that needs to be reverted and click Revert.
C. On the App Engine Versions page of the GCP Console, route 100% of the traffic to the previous version.
D. Deploy the original version as a separate application. Then go to App Engine settings and split traffic between applications so that the original version serves 100% of the requests.

You deployed an App Engine application using gcloud app deploy, but it did not deploy to the intended project. You want to find out why this happened and where the application deployed. What should you do?

A. Check the app.yaml file for your application and check project settings.
B. Check the web-application.xml file for your application and check project settings.
C. Go to Deployment Manager and review settings for deployment of applications.
D. Go to Cloud Shell and run gcloud config list to review the Google Cloud configuration used for deployment.

You have a website hosted on App Engine standard environment. You want 1 % of your users to see a new test version of the website. You want to minimize complexity. What should you do?

A. Deploy the new version in the same application and use the --migrate option.
B. Deploy the new version in the same application and use the --splits option to give a weight of 99 to the current version and a weight of 1 to the new version.
C. Create a new App Engine application in the same project. Deploy the new version in that application. Use the App Engine library to proxy 1 % of the requests to the new version.
D. Create a new App Engine application in the same project. Deploy the new version in that application. Configure your network load balancer to send 1 % of the traffic to that new application.

You are building a new version of an application hosted in an App Engine environment. You want to test the new version with 1 % of users before you completely switch your application over to the new version. What should you do?

A. Deploy a new version of your application in Google Kubernetes Engine instead of App Engine and then use GCP Console to split traffic.
B. Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic.
C. Deploy a new version as a separate app in App Engine. Then configure the App Engine using GCP Console to split traffic between the two apps.
D. Deploy a new version of your application in the App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

You are developing a new web application that will be deployed on Google Cloud Platform. As part of your release cycle, you want to test updates to your application on a small portion of real user traffic. The majority of the users should still be directed towards a stable version of your application. What should you do?

A. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

B. Deploy the application on App Engine. For each update, create a new service. Configure traffic splitting to send a small percentage of traffic to the new service.

C. Deploy the application on Kubernetes Engine. For a new release, update the deployment to use the new version.

D. Deploy the application on Kubernetes Engine. For a new release, create a new deployment for the new version. Update the service to use the new deployment.

You are deploying an application to the App Engine. You want the number of instances to scale based on request rate. You need at least 3 unoccupied instances at all times. Which scaling type should you use?

A. Manual Scaling with 3 instances.
B. Basic Scaling with min_nstances set to 3.
C. Basic Scaling with max_nstances set to 3.
D. Automatic Scaling with min_idle_nstances set to 3.

You have a project for your App Engine application that serves a development environment. The required testing has succeeded and you want to create a new project to serve as your production environment. What should you do?

A. Use gcloud to create the new project, and then deploy your application to the new project.

B. Use gcloud to create the new project and to copy the deployed application to the new project.
C. Create a Deployment Manager configuration file that copies the current App Engine deployment into a new project.
D. Deploy your application again using gcloud and specify the project parameter with the new project name to create the new project.

An engineer from your team accidentally deployed several new versions of NodeJS application on Google App Engine Standard. You are concerned the new versions are serving traffic. You have been asked to produce a list of all the versions of the application that are receiving traffic as well the percent traffic split between them. What should you do?

A. gcloud app versions list --hide-no-traffic
B. gcloud app versions list -show-traffic
C. gcloud app versions list
D. gcloud app versions list -traffic

You deployed a number of services to Google App Engine Standard. The services are designed as microservices with several interdependencies between them. Most services have few version upgrades but some key services have over 20 version upgrades. You identified an issue with the service pt-createOrder and deployed a new version v3 for this service. You are confident this works and want this new version to receive all traffic for the service. You want to minimize effort and ensure the availability of service. What should you do?

A. Execute gcloud app versions stop v2 and gcloud app versions start v3
B. Execute gcloud app versions stop v2 --service="pt-createOrder" and gcloud app versions start v3 --service="pt-createOrder"
C. Execute gcloud app versions migrate v3
D. Execute gcloud app versions migrate v3 -service="pt-createOrder"

You want to migrate an application from Google App Engine Standard to Google App Engine Flex. Your application is currently serving live traffic and you want to ensure everything is working in Google App Engine Flex before migrating all traffic. You want to minimize effort and ensure the availability of service. What should you do?

A. 1. Set env: flex in app.yaml 2. gcloud app deploy -version=[NEW_VERSION] 3. Validate [NEW_VERSION] in App Engine Flex 4. gcloud app versions migrate [NEW_VERSION]
B. 1. Set env: app-engine-flex in app.yaml 2. gcloud app deploy -no-promote -version=[NEW_VERSION] 3. Validate [NEW_VERSION] in App Engine Flex 4. gcloud app versions start [NEW_VERSION]
C. 1. Set env: app-engine-flex in app.yaml 2. gcloud app deploy-version=[NEW_VERSION] 3. Validate [NEW_VERSION] in App Engine Flex 4. gcloud app versions start [NEW_VERSION]

D. 1. Set env: flex in app.yaml 2. gcloud app deploy -no-promote -version=[NEW_VERSION] 3. Validate [NEW_VERSION] in App Engine Flex 4. gcloud app versions migrate [NEW_VERSION]

Your Company is planning to migrate all Java web applications to Google App Engine. However, you still want to continue using your on-premise database. How can you set up the app engine to communicate with your on-premise database while minimizing effort?

A. Setup the application using App Engine Flexible environment with Cloud Router to connect to an on-premise database.

B. Setup the application using App Engine Standard environment with Cloud VPN to connect to an on-premise database.

C. Setup the application using App Engine Standard environment with Cloud Router to connect to an on-premise database.

D. Setup the application using App Engine Flexible environment with Cloud VPN to connect to an on-premise database.

You need to select and configure compute resources for a set of batch processing jobs. These jobs take around 2 hours to complete and are run nightly. You want to minimize service costs. What should you do?

A. Select Google Kubernetes Engine. Use a single-node cluster with a small instance type.

B. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types.

C. Select Compute Engine. Use preemptible VM instances of the appropriate standard machine type.

D. Select Compute Engine. Use VM instance types that support micro bursting.

You have a virtual machine that is currently configured with 2 vCPUs and 4 GB of memory. It is running out of memory. You want to upgrade the virtual machine to have 8 GB of memory. What should you do?

A. Rely on live migration to move the workload to a machine with more memory.

B. Use gcloud to add metadata to the VM. Set the key to required-memory-size and the value to 8 GB.

C. Stop the VM, change the machine type to n1-standard-8, and start the VM.

D. Stop the VM, increase the memory to 8 GB, and start the VM.

You are setting up a Windows VM on Compute Engine and want to make sure you can log in to the VM via RDP. What should you do?

A. After the VM has been created, use your Google Account credentials to log in into the VM.

B. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

C. When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value.
D. After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM.

You want to configure an SSH connection to a single Compute Engine instance for users in the dev1 group. This instance is the only resource in this particular Google Cloud Platform project that the dev1 users should be able to connect to. What should you do?

A. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.
B. Set metadata to enable-oslogin=true for the instance. Set the service account to no service account for that instance. Direct them to use the Cloud Shell to ssh to that instance.
C. Enable block project wide keys for the instance. Generate an SSH key for each user in the dev1 group. Distribute the keys to devl users and direct them to use their third-party tools to connect.
D. Enable block project wide keys for the instance. Generate an SSH key and associate the key with that instance. Distribute the key to dev1 users and direct them to use their third-party tools to connect.

You are migrating a production-critical on-premises application that requires 96 vCPUs to perform its task. You want to make sure the application runs in a similar environment on GCP. What should you do?

A. When creating the VM, use machine type n1-standard-96.
B. When creating the VM, use Intel Skylake as the CPU platform.
C. Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs.
D. Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations.

You need to host an application on a Compute Engine instance in a project shared with other teams. You want to prevent the other teams from accidentally causing downtime on that application. Which feature should you use?

A. Use a Shielded VM.
B. Use a Preemptible VM.
C. Use a sole-tenant node.
D. Enable deletion protection on the instance.

You have a workload running on Compute Engine that is critical to your business. You want to ensure that the data on the boot disk of this workload is backed up regularly. You need to be able to restore a backup as quickly as possible in case of disaster. You also want older backups to be cleaned automatically to save on cost. You want to follow Google-recommended practices. What should you do?

A. Create a Cloud Function to create an instance template.
B. Create a snapshot schedule for the disk using the desired interval.
C. Create a cron job to create a new disk from the disk using gcloud.
D. Create a Cloud Task to create an image and export it to Cloud Storage.

Your company is moving from an on-premises environment to Google Cloud. You have multiple development teams that use Cassandra environments as backend databases. They all need a development environment that is isolated from other Cassandra instances. You want to move to Google Cloud quickly and with minimal support effort. What should you do?

A. 1. Build an instruction guide to install Cassandra on Google Cloud. 2. Make the instruction guide accessible to your developers.
B. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.
C. 1. Build a Cassandra Compute Engine instance and take a snapshot of it. 2. Use the snapshot to create instances for your developers.
D. 1. Build a Cassandra Compute Engine instance and take a snapshot of it. 2. Upload the snapshot to Cloud Storage and make it accessible to your developers. 3. Build instructions to create a Compute Engine instance from the snapshot so that developers can do it themselves.

You have an application on a general-purpose Compute Engine instance that is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk. The application primarily reads large files from disk. The disk size is currently 350 GB. You want to provide the maximum amount of throughput while minimizing costs.
What should you do?

A. Increase the size of the disk to 1 TB.
B. Increase the allocated CPU to the instance.
C. Migrate to use a Local SSD on the instance.
D. Migrate to use a Regional SSD on the instance.

You need to create a copy of a custom Compute Engine virtual machine (VM) to facilitate an expected increase in application traffic due to a business acquisition.
What should you do?

A. Create a Compute Engine snapshot of your base VM. Create your images from that snapshot.
B. Create a Compute Engine snapshot of your base VM. Create your instances from that snapshot.
C. Create a custom Compute Engine image from a snapshot. Create your images from that image.
D. Create a custom Compute Engine image from a snapshot. Create your instances from that image.

Your company runs one batch process in an on-premises server that takes around 30 hours to complete. The task runs monthly, can be performed offline, and must be restarted if interrupted. You want to migrate this workload to the cloud while minimizing cost. What should you do?

A. Migrate the workload to a Compute Engine Preemptible VM.
B. Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.
C. Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.
D. Create an Instance Template with Preemptible VMs On. Create a Managed Instance Group from the template and adjust Target CPU Utilization. Migrate the workload.

You are developing a new application and are looking for a Jenkins installation to build and deploy your source code. You want to automate the installation as quickly and easily as possible. What should you do?

A. Deploy Jenkins through the Google Cloud Marketplace.
B. Create a new Compute Engine instance. Run the Jenkins executable.
C. Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image.
D. Create an instance template with the Jenkins executable. Create a managed instance group with this template.

You have a Compute Engine instance hosting an application used between 9 AM and 6 PM on weekdays. You want to back up this instance daily for disaster recovery purposes. You want to keep the backups for 30 days. You want the Google-recommended solution with the least management overhead and the least number of services. What should you do?

A. 1. Update your instances metadata to add the following value: snapshot schedule: 01 * *
2. Update your instances' metadata to add the following value: snapshot retention: 30
B. 1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk.
2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM to 2:00 AM - Autodelete snapshots after: 30 days
C. 1. Create a Cloud Function that creates a snapshot of your instance's disk.

2. Create a Cloud Function that deletes snapshots that are older than 30 days.
3. Use Cloud Scheduler to trigger both Cloud Functions daily at 1:00 AM.

D. 1. Create a bash script in the instance that copies the content of the disk to Cloud Storage.
2. Create a bash script in the instance that deletes data older than 30 days in the backup Cloud Storage bucket.
3. Configure the instance's crontab to execute these scripts daily at 1:00 AM.

You have a batch workload that runs every night and uses a large number of virtual machines (VMs). It is fault-tolerant and can tolerate some of the VMs being terminated. The current cost of VMs is too high. What should you do?

A. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

B. Run a test using simulated maintenance events. If the test is successful, use N1 Standard VMs when running future jobs.

C. Run a test using a managed instance group. If the test is successful, use N1 Standard VMs in the managed instance group when running future jobs.

D. Run a test using N1 standard VMs instead of N2. If the test is successful, use N1 Standard VMs when running future jobs.

You are deploying a production application on Compute Engine. You want to prevent anyone from accidentally destroying the instance by clicking the wrong button. What should you do?

A. Disable the flag Delete boot disk when instance is deleted.AC

B. Enable delete protection on the instance.

C. Disable Automatic restart on the instance.

D. Enable Preemptibility on the instance.

You are about to deploy a new Enterprise Resource Planning (ERP) system on Google Cloud. The application holds the full database in memory for fast data access, and you need to configure the most appropriate resources on Google Cloud for this application. What should you do?

A. Provision preemptible Compute Engine instances.
B. Provision Compute Engine instances with GPUs attached.
C. Provision Compute Engine instances with local SSDs attached.
D. Provision Compute Engine instances with M1 machine type.

You have deployed multiple Linux instances on Compute Engine. You plan on adding more instances in the coming weeks. You want to be able to access all of these instances through your SSH client over the internet without having to configure specific access on the existing and new instances. You do not want the Compute Engine instances to have a public IP. What should you do?

A. Configure Cloud Identity-Aware Proxy for HTTPS resources.
B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources
C. Create an SSH keypair and store the public key as a project-wide SSH Key.
D. Create an SSH keypair and store the private key as a project-wide SSH Key.

Every employee of your company has a Google account. Your operational team needs to manage a large number of instances on Compute Engine. Each member of this team needs only administrative access to the servers. Your security team wants to ensure that the deployment of credentials is operationally efficient and must be able to determine who accessed a given instance. What should you do?
A. Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key in the metadata of each instance.
B. Ask each member of the team to generate a new SSH key pair and to send you their public key. Use a configuration management tool to deploy those keys on each instance.
C. Ask each member of the team to generate a new SSH key pair and to add the public key to their Google account. Grant the compute.osAdminLogin role to the Google group corresponding to this team.
D. Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key as a project-wide public SSH key in your Cloud Platform project and allow project-wide public SSH keys on each instance.

You have an application that looks for its licensing server on the IP 10.0.3.21. You need to deploy the licensing server on Compute Engine. You do not want to change the configuration of the application and want the application to be able to reach the licensing server. What should you do?
A. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.
B. Reserve the IP 10.0.3.21 as a static public IP address using gcloud and assign it to the licensing server.
C. Use the IP 10.0.3.21 as a custom ephemeral IP address and assign it to the licensing server.
D. Start the licensing server with an automatic ephemeral IP address, and then promote it to a static internal IP address.

Your development team needs a new Jenkins server for their project. You need to deploy the server using the fewest steps possible. What should you do?
A. Download and deploy the Jenkins Java WAR to App Engine Standard.
B. Create a new Compute Engine instance and install Jenkins through the command line interface.
C. Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image.

D. Use GCP Marketplace to launch the Jenkins solution.

You have a Linux VM that must connect to Cloud SQL. You created a service account with the appropriate access rights. You want to make sure that the VM uses this service account instead of the default Compute Engine service account. What should you do?

A. When creating the VM via the web console, specify the service account under the 'Identity and API Access' section.

B. Download a JSON Private Key for the service account. On the Project Metadata, add that JSON as the value for the key compute-engine-service- account.

C. Download a JSON Private Key for the service account. On the Custom Metadata of the VM, add that JSON as the value for the key compute-engine- service- account.

D. Download a JSON Private Key for the service account. After creating the VM, ssh into the VM and save the JSON under ~/.gcloud/compute-engine-service- account.json.

You created an instance of SQL Server 2017 on Compute Engine to test features in the new version. You want to connect to this instance using the fewest number of steps. What should you do?

A. Install a RDP client on your desktop. Verify that a firewall rule for port 3389 exists.

B. Install a RDP client in your desktop. Set a Windows username and password in the GCP Console. Use the credentials to log in to the instance.

C. Set a Windows password in the GCP Console. Verify that a firewall rule for port 22 exists. Click the RDP button in the GCP Console and supply the credentials to log in.

D. Set a Windows username and password in the GCP Console. Verify that a firewall rule for port 3389 exists. Click the RDP button in the GCP Console, and supply the credentials to log in.

You have a number of compute instances belonging to an unmanaged instances group. You need to SSH to one of the Compute Engine instances to run an ad hoc script. You've already authenticated gcloud, however, you don't have an SSH key deployed yet. In the fewest steps possible, what’s the easiest way to SSH to the instance?

A. Create a key with the ssh-keygen command. Upload the key to the instance. Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.
B. Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.
C. Create a key with the ssh-keygen command. Then use the gcloud compute ssh command.
D. Use the gcloud compute ssh command.

You want to ensure the boot disk of a preemptible instance is persisted for re-use. How should you provision the gcloud compute instance to ensure your requirement is met.

A. **gcloud compute instances create [INSTANCE_NAME] -preemptible -no-boot-disk-auto-delete**
B. gcloud compute instances create [INSTANCE_NAME] -preemptible -boot-disk-auto-delete=no
C. gcloud compute instances create [INSTANCE_NAME] -no-auto-delete
D. gcloud compute instances create [INSTANCE_NAME] -preemptible. The flag -boot-disk-auto-delete is disabled by default.

You want to find a list of regions and the prebuilt images offered by Google Compute Engine. Which commands should you execute to retrieve this information?

A. gcloud compute regions list gcloud images list
B. **gcloud compute regions list gcloud compute images list**
C. gcloud regions list gcloud images list
D. gcloud regions list gcloud compute images list

You want to list all the compute instances in zones us-central1-b and europe-west1-d. Which of the commands below should you run to retrieve this information?

A. gcloud compute instances list -filter="zone:(us-central1-b)" and gcloud compute instances list -filter="zone:(europe-west1-d)" and combine the results.
B. gcloud compute instances get-filter="zone:(us-central1-b)" and gcloud compute instances list —filter="zone:(europe-west1-d)" and combine the results.
C. gcloud compute instances get -filter="zone:(us-central1-b europe-west1-d)"
D. **gcloud compute instances list-filter="zone:(us-central1-b europe-west1-d)"**

You want to list all the internal and external IP addresses of all compute instances. Which of the commands below should you run to retrieve this information?

A. **gcloud compute instances list.**
B. gcloud compute networks list-ip.
C. gcloud compute networks list.
D. gcloud compute instances list-ip.

You have 32 GB of data in a single file that you need to upload to a Nearline Storage bucket. The WAN connection you are using is rated at 1 Gbps, and you are the only one on the connection. You want to use as much of the rated 1 Gbps as possible to transfer the file rapidly. How should you upload the file?

A. Use the GCP Console to transfer the file instead of gsutil.
B. **Enable parallel composite uploads using gsutil on the file transfer.**
C. Decrease the TCP window size on the machine initiating the transfer.
D. Change the storage class of the bucket from Nearline to Multi-Regional.

You host a static website on Cloud Storage. Recently, you began to include links to PDF files on this site. Currently, when users click on the links to these PDF files, their browsers prompt them to save the file onto their local system. Instead, you want the clicked PDF files to be displayed within the browser window directly, without prompting the user to save the file locally. What should you do?

A. Enable Cloud CDN on the website frontend.
B. Enable 'Share publicly' on the PDF file objects.
C. Set Content-Type metadata to application/pdf on the PDF file objects.
D. Add a label to the storage bucket with a key of Content-Type and value of application/pdf.

You want to configure a solution for archiving data in a Cloud Storage bucket. The solution must be cost-effective. Data with multiple versions should be archived after 30 days. Previous versions are accessed once a month for reporting. This archive data is also occasionally updated at month-end. What should you do?

A. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Coldline Storage.
B. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.
C. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Coldiine Storage.
D. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Nearline Storage.

You want to select and configure a solution for storing and archiving data on Google Cloud Platform. You need to support compliance objectives for data from one geographic location. This data is archived after 30 days and needs to be accessed annually. What should you do?

A. Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.
B. Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage.
C. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage.
D. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

You are building an archival solution for your data warehouse and have selected Cloud Storage to archive your data. Your users need to be able to access this archived data once a quarter for some regulatory requirements. You want to select a cost-efficient option. Which storage option should you use?

A. Cold Storage(*not typo. If Coldline. This is the answer*)
B. Nearline Storage
C. Regional Storage
D. Multi-Regional Storage

Your company has a large quantity of unstructured data in different file formats. You want to perform ETL transformations on the data. You need to make the data accessible on Google Cloud so it can be processed by a Dataflow job. What should you do?

A. Upload the data to BigQuery using the bq command line tool.
B. Upload the data to Cloud Storage using the gsutil command line tool.
C. Upload the data into Cloud SQL using the import function in the console.
D. Upload the data into Cloud Spanner using the import function in the console.

You need to manage multiple Google Cloud projects in the fewest steps possible. You want to configure the Google Cloud SDK command line interface (CLI) so that you can easily manage multiple projects. What should you do?

A. 1. Create a configuration for each project you need to manage.
2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

B. 1. Create a configuration for each project you need to manage.
2. Use gcloud init to update the configuration values when you need to work with a non-default project

C. 1. Use the default configuration for one project you need to manage.
2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

D. 1. Use the default configuration for one project you need to manage.
2. Use gcloud init to update the configuration values when you need to work with a non-default project.

You have been asked to set up Object Lifecycle Management for objects stored in storage buckets. The objects are written once and accessed frequently for 30 days. After 30 days, the objects are not read again unless there is a special need. The objects should be kept for three years, and you need to minimize cost.
What should you do?

A. Set up a policy that uses Nearline storage for 30 days and then moves to Archive storage for three years.

B. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

C. Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years.

D. Set up a policy that uses Standard storage for 30 days, then moves to Coldline for one year, and then moves to Archive storage for two years.

You are storing sensitive information in a Cloud Storage bucket. For legal reasons, you need to be able to record all requests that read any of the stored data. You want to make sure you comply with these requirements. What should you do?

A. Enable the Identity Aware Proxy API on the project.

B. Scan the bucket using the Data Loss Prevention API.

C. Allow only a single Service Account access to read the data.

D. Enable Data Access audit logs for the Cloud Storage API.

You are building an application that processes data files uploaded from thousands of suppliers. Your primary goals for the application are
data security and the expiration of aged data. You need to design the application to:

- Restrict access so that suppliers can access only their own data.
- Give suppliers write access to data only for 30 minutes.
- Delete data that is over 45 days old.

You have a very short development cycle, and you need to make sure that the application requires minimal maintenance. Which two strategies should you use?
(Choose two.)

A. Build a lifecycle policy to delete Cloud Storage objects after 45 days.
B. Use signed URLs to allow suppliers limited time access to store their objects.
C. Set up an SFTP server for your application, and create a separate user for each supplier.
D. Build a Cloud function that triggers a timer of 45 days to delete objects that have expired.
E. Develop a script that loops through all Cloud Storage buckets and deletes any buckets that are older than 45 days.

You are working for a hospital that stores its medical images in an on-premises data room. The hospital wants to use Cloud Storage for archival storage of these images. The hospital wants an automated process to upload any new medical images to Cloud Storage. You need to design and implement a solution. What should you do?

A. Create a Pub/Sub topic, and enable a Cloud Storage trigger for the Pub/Sub topic. Create an application that sends all medical images to the Pub/Sub topic.

B. Deploy a Dataflow job from the batch template, aCDatastore to Cloud Storage.^ Schedule the batch job on the desired interval.

C. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

D. In the Cloud Console, go to Cloud Storage. Upload the relevant images to the appropriate bucket.

You need to configure optimal data storage for files stored in Cloud Storage for minimal cost. The files are used in a mission-critical analytics pipeline that is used continually The users are in Boston, MA (United States). What should you do?

A. Configure regional storage for the region closest to the users. Configure a Nearline storage class.

B. Configure regional storage for the region closest to the users. Configure a Standard storage class.

C. Configure dual-regional storage for the dual region closest to the users. Configure a Nearline storage class.

D. Configure dual-regional storage for the dual region closest to the users. Configure a Standard storage class.

Your company uses Cloud Storage to store application backup files for disaster recovery purposes. You want to follow Google's recommended practices. Which storage option should you use?

A. Multi-Regional Storage

B. Regional Storage

C. Nearline Storage

D. Coldline Storage

You need to set up a policy so that videos stored in a specific Cloud Storage Regional bucket are moved to Coldline after 90 days, and then deleted after one year from their creation. How should you set up the policy?

A. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 275 days (365-90)

B. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days.

C. Use gsutil rewrite and set the Delete action to 275 days (365-90).

D. Use gsutil rewrite and set the Delete action to 365 days.

You have an object in a Cloud Storage bucket that you want to share with an external company. The object contains sensitive data. You want access to the content to be removed after four hours. The external company does not have a Google account to which you can grant specific user-based access privileges. You want to use the most secure method that requires the fewest steps. What should you do?

A. Create a signed URL with a four-hour expiration and share the URL with the company.

B. Set object access to 'public' and use object lifecycle management to remove the object after four hours.

C. Configure the storage bucket as a static website and furnish the object's URL to the company. Delete the object from the storage bucket after four hours.

D. Create a new Cloud Storage bucket specifically for the external company to access. Copy the object to that bucket. Delete the bucket after four hours have passed.

In Regional Storage buckets with object versioning enabled, what is the effect of deleting the live version of an object and deleting a noncurrent version of an object?

- **A. 1. The live version becomes a noncurrent version.**
  2. The noncurrent version is deleted permanently.
- B. 1. The live version becomes a noncurrent version and a lifecycle rule is applied to delete after 30 days.
  2. A lifecycle rule is applied on the noncurrent version to delete after 30 days.
- C. 1. The live version becomes a noncurrent version and a lifecycle rule is applied to transition to Nearline Storage after 30 days.
  2. A lifecycle rule is applied on the noncurrent version to transition to Nearline Storage after 30 days.
- D. 1. The live version is deleted permanently.
  2. The noncurrent version is deleted permanently.

The storage costs for your application logs have far exceeded the project budget. The logs are currently being retained indefinitely in the Cloud Storage bucket myapp-gcp-ace- logs. You have been asked to remove logs older than 90 days from your Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend. What should you do?

- A. Write a script that runs gsutil ls -l gs://myapp-gcp-ace-logs/** to find and remove items older than 90 days. Schedule the script with cron.
- B. Write a script that runs gsutil ls -lr gs://myapp-gcp-ace-logs/** to find and remove items older than 90 days. Repeat this process every morning.
- C. Write a lifecycle management rule in XML and push it to the bucket with gsutil lifecycle set config-xml-file.
- **D. Write a lifecycle management rule in JSON and push it to the bucket with gsutil lifecycle set config-json-file.**

You are designing an application that lets users upload and share photos. You expect your application to grow really fast and you are targeting a worldwide audience. You want to delete uploaded photos after 30 days. You want to minimize costs while ensuring your application is highly available. Which GCP storage solution should you choose?

A. Persistent SSD on VM instances.
B. Cloud Filestore.
C. Multiregional Cloud Storage bucket.
D. Cloud Datastore database.

You have a collection of audio/video files over 80GB each that you need to migrate to Google Cloud Storage. The files are in your on-premises data center. What migration method can you use to help speed up the transfer process?

A. Use parallel uploads to break the file into smaller chunks then transfer it simultaneously.
B. Use multithreaded uploads using the -m option.
C. Use the Cloud Transfer Service to transfer.
D. Start a recursive upload.

You have asked your supplier to send you a purchase order and you want to enable them to upload the file to a cloud storage bucket within the next 4 hours. Your supplier does not have a Google account. You want to follow Google recommended practices. What should you do?

A. Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -m PUT -d 4h gs:///**.
B. Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl - httpMethod PUT -d 4h gs:///**.
C. Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m PUT -d 4h gs:///po.pdf.
D. Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 4h gs:///.

You have files in a Cloud Storage bucket that you need to share with your suppliers. You want to restrict the time that the files are available to your suppliers to 1 hour. You want to follow Google recommended practices. What should you do?

A. Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -p 60m gs:///.
B. Create a service account with just the permissions to access files in the bucket Create a JSON key for the service account Execute the command gsutil signurl -d 1h gs:///.**

C. Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -t 60m gs:///*.* .
D. Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m 1 h gs:///*.

You want to create a Google Cloud Storage regional bucket logs-archive in the Los Angeles region (us-west2). You want to use Coldline storage class to minimize costs and you want to retain files for 10 years. Which of the following commands should you run to create this bucket?

A. gsutil mb -l us-west2 -s nearline -retention 10y gs://logs-archive
B. gsutil mb -l los-angeles -s coldline -retention 10m gs://logs-archive
C. gsutil mb -l us-west2 -s coldline -retention 10m gs://logs-archive
D. gsutil mb -l us-west2 -s coldline -retention 10y gs://logs-archive

You want to use Google Cloud Storage to host a static website on http://www.example.com for your staff. You created a bucket example-static-website and uploaded index.html and css files to it. You turned on static website hosting on the bucket and set up a CNAME record on http://www.example.com to point to c.storage.googleapis.com. You access the static website by navigating to http://www.example.com in the browser but your index page is not displayed. What should you do?

A. In example.com zone, delete the existing CNAME record and set up an A record instead to point to c.storage.googleapis.com.
B. In example.com zone, modify the CNAME record to c.storage.googleapis.com/example-static-website.
C. Reload the Cloud Storage static website server to load the objects.
D. Delete the existing bucket, create a new bucket with the name www.example.com and upload the html/css files.

Your company plans to store sensitive PII data in a cloud storage bucket. Your compliance department doesn't like encrypting sensitive PII data with Google-managed keys and has asked you to ensure the new objects uploaded to this bucket are encrypted by customer-managed encryption keys. What should you do? (Select Three)

A. In the bucket advanced settings, select the Customer-supplied key and then select a Cloud KMS encryption key.
B. Use gsutil with --encryption-key=[ENCRYPTION_KEYj when uploading objects to the bucket.
C. Use gsutil with -o "GSUtil:encryption_key=[KEY_RESOURCE]" when uploading objects to the bucket.
D. In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key.
E. Modify .boto configuration to include encryption_key = [KEY_RESOURCE] when uploading objects to bucket.

Your company plans to store sensitive PIl data in a cloud storage bucket. Your compliance department has asked you to ensure the objects in this bucket are encrypted by customer-managed encryption keys. What should you do?

A. In the bucket advanced settings, select Google-managed key and then select a Cloud KMS encryption key.
B. Recreate the bucket to use a Customer-managed key. Encryption can only be specified at the time of bucket creation.
C. In the bucket advanced settings, select Customer-supplied key and then select a Cloud KMS encryption key.
D. In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key.

Your company stores sensitive PI I data in a cloud storage bucket. The objects are currently encrypted by Google-managed keys. Your compliance department has asked you to ensure all current and future objects in this bucket are encrypted by customer-managed encryption keys. You want to minimize effort. What should you do?

A. 1. In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key. 2. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key.
B. 1. In the bucket advanced settings, select the customer-supplied key and then select a Cloud KMS encryption key. 2. Delete all existing objects and upload them again so they use the new customer-supplied key for encryption.
C. 1. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key. 2. In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key.
D. 1. In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key. 2. Existing objects encrypted by Google-managed keys can still be decrypted by the new Customer-managed key.

Your company wants to move all documents from a secure internal NAS drive to a Google Cloud Storage (GCS) bucket. The data contains personally identifiable information (PIl) and sensitive customer information. Your company tax auditors need access to some of these documents. What security strategy would you recommend on GCS?

A. Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.
B. Grant IAM read-only access to users, and use default ACLs on the bucket.
C. Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.
D. Use signed URLs to generate time-bound access to objects.

You create a new Google Kubernetes Engine (GKE) cluster and want to make sure that it always runs a supported and stable version of Kubernetes. What should you do?

A. Enable the Node Auto-Repair feature for your GKE cluster.

B. Enable the Node Auto-Upgrades feature for your GKE cluster.

C. Select the latest available cluster version for your GKE cluster.

D. Select Container-Optimized OS (cos) as a node image for your GKE cluster.

You've deployed a microservice called myappl to a Google Kubernetes Engine cluster using the YAML file specified below:

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: rayappl-deployment
 matchLabels:
  app: myappl
replicas: 2
template:
 metadata :
  labels:
  app: myapp1
 spec:
  containers :
  - name: mam-container
   image : gcr.ro/my-company-repo/myappl: 1.4
   env:
    name: DB_PASSWORD
    vàlue: "t0ugh2guess!"
  ports:
  -containerPort: 8080
```

You need to refactor this configuration so that the database password is not stored in plain text. You want to follow Google-recommended practices. What should you do?

A. Store the database password inside the Docker image of the container, not in the YAML file.

B. Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.

C. Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.

D. Store the database password in a file inside a Kubernetes persistent volume, and use a persistent volume claim to mount the volume to the container.

Your projects incurred more costs than you expected last month. Your research reveals that a development GKE container emitted a huge number of logs, which resulted in higher costs. You want to disable the logs quickly using the minimum number of steps. What should you do?

A. 1.Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

B. 1.Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE Cluster Operations resource.

C. 1.Go to the GKE console, and delete existing clusters.
2. Recreate a new cluster.

3. Clear the option to enable legacy Stackdriver Logging.

D. 1.Go to the GKE console, and delete existing clusters.
   2. Recreate a new cluster.
   3. Clear the option to enable legacy Stackdriver Monitoring.

You have an application running in Google Kubernetes Engine (GKE) with cluster autoscaling enabled. The application exposes a TCP endpoint. There are several replicas of this application. You have a Compute Engine instance in the same region, but in another Virtual Private Cloud (VPC), called gee-network, that has no overlapping IP ranges with the first VPC. This instance needs to connect to the application on GKE. You want to minimize effort. What should you do?

A. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.
   2. Set the service's externalTrafficPolicy to Cluster.
   3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

B. 1. In GKE, create a Service of type NodePort that uses the application's Pods as backend.
   2. Create a Compute Engine instance called proxy with 2 network interfaces, one in each VPC.
   3. Use iptables on this instance to forward traffic from gee-network to the GKE nodes.
   4. Configure the Compute Engine instance to use the address of proxy in gee-network as endpoint.

C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.
   2. Add an annotation to this service: cloud.google.com/load- balancer-type: Internal
   3. Peer the two VPCs together.
   4. Configure the Compute Engine instance to use the address of the load balancer that has been created.

D. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.
   2. Add a Cloud Armor Security Policy to the load balancer that whitelists the internal IPs of the MiG's instances.
   3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

You are using Container Registry to centrally store your company's container images in a separate project. In another project, you want to create a Google Kubernetes Engine (GKE) cluster. You want to ensure that Kubernetes can download images from Container Registry. What should you do?

A. **In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.**
B. When you create the GKE cluster, choose the Allow full access to all Cloud APIs option under 'Access scopes'.
C. Create a service account, and give it access to Cloud Storage. Create a PI 2 key for this service account and use it as an imagePullSecrets in Kubernetes.
D. Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account.

You deployed a new application inside your Google Kubernetes Engine cluster using the YAML file specified below.

```
apiVersion: apps/vl
kind: Deployment
metadata :
  name : myapp-deployment
spec:
  selector :
  matchLabels: app: myapp
replicas : 2
template :
  metadata :
    labels :
      app: myapp
  spec :
    containers:
     - name : myapp
       image: myapp: 1.1
       ports :
       - containerPort :80
```

```
apiVersion : v1
kind: Service
metadata :
name: myapp-service
spec:
  ports :
  - port :i8000
    targetPort: 80 :
    protocol: TCP
  selector : app: myapp
```

You check the status of the deployed pods and notice that one of them is still in PENDING status:

kubectl get pods -l app=myapp

```
NAME                                   READY   STATUS   RESTART       AGE
myapp-deployment-58ddbbb 995-lp86m      0/1    Pending     0          9m
myapp-deployment-58ddbbb995-qjpkg      1/1     Running     0          9m
```

You want to find out why the pod is stuck in pending status. What should you do?

A. Review details of the myapp-service Service object and check for error messages.
B. Review details of the myapp-deployment Deployment object and check for error messages.
C. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.
D. View logs of the container in myapp-deployment-58ddbbb995-lp86m pod and check for warning messages.

You are using Google Kubernetes Engine with autoscaling enabled to host a new application. You want to expose this new application to the public, using HTTPS on a public IP address. What should you do?

A. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

B. Create a Kubernetes Service of type ClusterIP for your application. Configure the public DNS name of your application using the IP of this Service.

C. Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluster. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing.

D. Create a HAProxy pod in the cluster to load-balance the traffic to all the pods of the application. Forward the public traffic to HAProxy with an iptable rule. Configure the DNS name of your application using the public IP of the node HAProxy is running on.

You are operating a Google Kubernetes Engine (GKE) cluster for your company where different teams can run non-production workloads. Your Machine Learning (ML) team needs access to Nvidia Tesla P100 GPUs to train their models. You want to minimize effort and cost. What should you do?

A. Ask your ML team to add the accelerator: gpu annotation to their pod specification.
B. Recreate all the nodes of the GKE cluster to enable GPUs on all of them.
C. Create your own Kubernetes cluster on top of Compute Engine with nodes that have GPUs. Dedicate this cluster to your ML team.
**D. Add a new, GPU-enabled, node pool to the GKE cluster.
Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesia-p100 nodeSelector to their pod specification.**

You create a Deployment with 2 replicas in a Google Kubernetes Engine cluster that has a single preemptible node pool. After a few minutes, you use kubectl to examine the status of your Pod and observe that one of them is still in Pending status:

```
kubectl get pods -l app=myapp
NAME                                      READY   STATUS   RESTART        AGE
myapp-deployment-58ddbbb 995-lp86m         0/1    Pending     0           9m
myapp-deployment-58ddbbb995-qjpkg         1/1     Running     0           9m
```

What is the most likely cause?

A. The pending Pod's resource requests are too large to fit on a single node of the cluster.
B. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.
C. The node pool is configured with a service account that does not have permission to pull the container image used by the pending Pod.
D. The pending Pod was originally scheduled on a node that has been preempted between the creation of the Deployment and your verification of the Pods' status. It is currently being rescheduled on a new node.

You are building a product on top of Google Kubernetes Engine (GKE). You have a single GKE cluster. For each of your customers, a Pod is running in that cluster, and your customers can run arbitrary code inside their Pod. You want to maximize the isolation between your customers' Pods. What should you do?

A. Use Binary Authorization and whitelist only the container images used by your customers' Pods.
B. Use the Container Analysis API to detect vulnerabilities in the containers used by your customers' Pods.
C. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.
D. Use the cos_containerd image for your GKE nodes. Add a nodeSeiector with the value cloud.google.com/gke-os-distribution: cos_containerd to the specification of your customers' Pods.

A team of data scientists infrequently needs to use a Google Kubernetes Engine (GKE) cluster that you manage. They require GPUs for some long-running, non- restartable jobs. You want to minimize cost. What should you do?

A. Enable node auto-provisioning on the GKE cluster.
B. Create a VerticalPodAutoscaler for those workloads.
C. Create a node pool with preemptible VMs and GPUs attached to those VMs.
D. Create a node pool of instances with GPUs, and enable autoscaling on this node pool with a minimum size of 1.

Your existing application running in Google Kubernetes Engine (GKE) consists of multiple pods running on four GKE n1-standard-2 nodes. You need to deploy additional pods requiring n2-highmem-16 nodes without any downtime. What should you do?

A. Use gcloud container clusters upgrade. Deploy the new services.
B. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.
C. Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.
D. Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

You are runni*963.ng multiple VPC-native Google Kubernetes Engine clusters in the same subnet. The IPs available for the nodes are exhausted, and you want to ensure that the clusters can grow in nodes when needed. What should you do?

A. Create a new subnet in the same region as the subnet being used.
B. Add an alias IP range to the subnet used by the GKE clusters.
C. Create a new VPC, and set up VPC peering with the existing VPC.
D. Expand the CIDR range of the relevant subnet for the cluster.

You have developed an application that consists of multiple microservices, with each microservice packaged in its own Docker container image. You want to deploy the entire application on Google Kubernetes Engine so that each microservice can be scaled individually. What should you do?

A. Create and deploy a Custom Resource Definition per microservice.
B. Create and deploy a Docker Compose File.
C. Create and deploy a Job per microservice.
D. Create and deploy a Deployment per microservice.

You are creating an application that will run on Google Kubernetes Engine. You have identified MongoDB as the most suitable database system for your application and want to deploy a managed MongoDB environment that provides a support SLA. What should you do?

A. Create a Cloud Bigtable cluster, and use the HBase API.
B. Deploy MongoDB Atlas from the Google Cloud Marketplace.
C. Download a MongoDB installation package, and run it on Compute Engine instances.dsa
D. Download a MongoDB installation package, and run it on a Managed Instance Group.

You are assigned to maintain a Google Kubernetes Engine (GKE) cluster named 'dev' that was deployed on Google Cloud. You want to manage the GKE configuration using the command line interface (CLI). You have just downloaded and installed the Cloud SDK. You want to ensure that future CLI commands by default address this specific cluster What should you do?

A. Use the command gcloud config set container/cluster dev.

B. Use the command gcloud container clusters update dev.

C. Create a file called gke.default in the ~/.gcloud folder that contains the cluster name.

D. Create a file called defaults.json in the ~/.gcloud folder that contains the cluster name.

You have created an application that is packaged into a Docker image. You want to deploy the Docker image as a workload on Google Kubernetes Engine. What should you do?

A. Upload the image to Cloud Storage and create a Kubernetes Service referencing the image.

B. Upload the image to Cloud Storage and create a Kubernetes Deployment referencing the image.

C. Upload the image to Container Registry and create a Kubernetes Service referencing the image.

D. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

You are using multiple configurations for gcloud. You want to review the configured Kubernetes Engine cluster of an inactive configuration using the fewest possible steps. What should you do?

A. Use gcloud config configurations describe to review the output.

B. Use gcloud config configurations activate and gcloud config list to review the output.

C. Use kubectl config get-contexts to review the output.

D. Use kubectl config use-context and kubectl config view to review the output.

You have a Dockerfile that you need to deploy on Kubernetes Engine. What should you do?

A. Use kubectl app deploy <dockerfilename>.

B. Use gcloud app deploy <dockerfilename>.

C. Create a docker image from the Dockerfile and upload it to Container Registry. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

D. Create a docker image from the Dockerfile and upload it to Cloud Storage. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

You are creating a Google Kubernetes Engine (GKE) cluster with a cluster autoscaler feature enabled. You need to make sure that each node of the cluster will run a monitoring pod that sends container metrics to a third-party monitoring solution. What should you do?

A. Deploy the monitoring pod in a StatefulSet object.
B. Deploy the monitoring pod in a DaemonSet object.
C. Reference the monitoring pod in a Deployment object.
D. Reference the monitoring pod in a cluster initializer at the GKE cluster creation time.

You created a Kubernetes deployment by running
kubectl run nginx -image=nginx -labels=vapp=prod,
Your Kubernetes cluster is also used by a number of other deployments. How can you find the identifier of the pods for this nginx deployment?

A. kubectl get deployments --output=pods
B. gcloud get pods --selector="app=prod"
C. gcloud list gke-deployments --filter={ pod }
D. kubectl get pods -l "app=prod"

You created a Kubernetes deployment by running kubectl run nginx -image=nginx -replicas=1. After a few days, you decided you no longer want this deployment. You identified the pod and deleted it by running kubectl delete pod. You noticed the pod got recreated.

```
$ kubectl get pods
NAME                          READY  STATUS   RESTARTS AGE
nginx-84748895c4-nqqmt        1/1    Running     0        9m41s
$ kubectl delete pod nginx-84748895c4-nqqmt
pod "nginx-84748895c4-nqqmt” deleted
$ kubectl get pods
NAME                          READY STATUS RESTARTS AGE
nginx-84748895c4-k6bzl         1/1    Running    0      25s
```

What should you do to delete the deployment and avoid pod getting recreated?

A. kubectl delete nginx
B. kubectl delete -deployment=nginx
C. kubectl delete pod nginx-84748895c4-k6bzl --no-restart
D. kubectl delete deployment nginx

You deployed a workload to your GKE cluster by running the command kubectl apply -f app.yaml. You also enabled a LoadBalancer service to expose the deployment by running kubectl apply -f service.yaml. Your pods are struggling due to increased load so you decided to enable horizontal pod autoscaler by running kubectl autoscale deployment [YOUR DEPLOYMENT] -cpu-percent=50 -min=1 -max=10. You noticed the autoscaler has launched several new pods but the new pods have failed with the message “Insufficient cpu”. What should you do to resolve this issue?

A. Use "gcloud container clusters resize" to add more nodes to the node pool.
B. Use "kubectl container clusters resize" to add more nodes to the node pool.
C. Edit the managed instance group of the cluster and enable autoscaling.
D. Edit the managed instance group of the cluster and increase the number of VMs by 1.

You deployed your application to a default node pool on the GKE cluster and you want to configure cluster autoscaling for this GKE cluster. For your application to be profitable, you must limit the number of Kubernetes nodes to 10. You want to start small and scale up as traffic increases and scale down when the traffic goes down. What should you do?

A. Update existing GKE cluster to enable autoscaling by running the command gcloud container clusters update [CLUSTER_NAME] --enable-autoscaling -min-nodes=1 - max-nodes=10
B. Create a new GKE cluster by running the command gcloud container clusters create [CLUSTER_NAME] --enable-autoscaling --min-nodes=1 --max-nodes=10. Redeploy your application
C. To enable autoscaling, add a tag to the instances in the cluster by running the command gcloud compute instances add-tags [INSTANCE] ~tags=enable-autoscaling,min-nodes=1,max-nodes=10
D. Set up a stack driver alert to detect slowness in the application. When the alert is triggered, increase nodes in the cluster by running the command gcloud container clusters resize CLUSTER Name --size .

You have an application deployed in a GKE Cluster as a Kubernetes workload with Daemon Sets. Your application has become very popular and is now struggling to cope up with increased traffic. You want to add more pods to your workload and want to ensure your cluster scales up and scales down automatically based on volume. What should you do?

A. Perform a rolling update to modify machine type from n1-standard-2 to n1 -standard-4.
B. Enable autoscaling on Kubernetes Engine.
C. Enable Horizontal Pod Autoscaling for the Kubernetes deployment.
D. Create another identical Kubernetes workload and split traffic between the two workloads.

You have been asked to create a new Kubernetes Cluster on Google Kubernetes Engine that can autoscale the number of worker nodes as well as pods. What should you do? (Select 2)

A. Create a GKE cluster and enable autoscaling on Kubernetes Engine.

B. Create Compute Engine instances for the workers and the master and install Kubernetes. Rely on Kubernetes to create additional Compute Engine instances when needed.
C. Create a GKE cluster and enable autoscaling on the instance group of the cluster.
D. Configure a Compute Engine instance as a worker and add it to an unmanaged instance group. Add a load balancer to the instance group and rely on the load balancer to create additional Compute Engine instances when needed.
E. Enable Horizontal Pod Autoscaling for the Kubernetes deployment.

You have been asked to migrate a docker application from datacenter to cloud. Your solution architect has suggested uploading docker images to GCR in one project and running an application in a GKE cluster in a separate project. You want to store images in the project img-278322 and run the application in the project prod-278986. You want to tag the image as acme_track_n_trace:v1. You want to follow Google-recommended practices. What should you do?

A. Run gcloud builds submit -tag gcr.io/img-278322/acme_track_n_trace
B. Run gcloud builds submit -tag gcr.io/img-278322/acme_track_n_trace:v1
C. Run gcloud builds submit -tag gcr.io/prod-278986/acme_track_n_trace
D. Run gcloud builds submit -tag gcr.io/prod-278986/acme_track_n_trace:v1

You have two Kubernetes resource configuration files.
deployments.yaml - creates a deployment
service.yaml - sets up a LoadBalancer service to expose the pods.
You don't have a GKE cluster in the development project and you need to provision one. Which of the commands fail with an error in Cloud Shell when you are attempting to create a GKE cluster and deploy the YAML configuration files to create a deployment and service. (Select Two)

A. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl apply -f [deployment.yaml,service.yaml]
B. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl apply -f deployment.yaml&&service.yaml
C. gcloud config set compute/zone us-central1-a gcloud container clusters create cluster-1 gcloud container clusters get-credentials cluster-1 -zone=us-central1-a kubectl apply -f deployment.yaml kubectl apply -f service.yaml
D. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl apply -f deployment.yaml kubectl apply -f service.yaml

E. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl apply -f deployment.yaml,service.yaml

You have two workloads on GKE (Google Kubernetes Engine) - create-order and dispatch-order, create-order handles the creation of customer orders, and dispatch-order handles dispatching orders to your shipping partner. Both create-order and dispatch-order workloads have cluster autoscaling enabled. The create-order deployment needs to access (i.e. invoke web service of dispatch-order deployment, dispatch-order deployment cannot be exposed publicly. How should you define the services?

A. Create a Service of type NodePort for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address.
B. Create a Service of type LoadBalancer for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address.
C. Create a Service of type LoadBalancer for dispatch-order. Have create-order use the Service IP address.
D. **Create a Service of type ClusterIP for dispatch-order. Have create-order use the Service IP address.**

You have two Kubernetes resource configuration files.
deployments.yaml - creates a deployment
service.YAML - sets up a LoadBalancer service to expose the pods.
You don't have a GKE cluster in the development project and you need to provision one. Which of the commands below would you run in Cloud Shell to create a GKE cluster and deploy the YAML configuration files to create a deployment and service?

A. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl create -f deployment.yaml kubectl create -f service.yaml
B. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a kubectl apply -f deployment.yaml kubectl apply -f service.yaml
C. gcloud container clusters create cluster-1 -zone=us-central1-a gcloud container clusters get-credentials cluster-1 --zone=us-central1-a gcloud gke apply -f deployment.yaml gcloud gke apply -f service.yaml
D. **kubectl container clusters create cluster-1 -zone=us-central1-a kubectl container clusters get-credentials cluster-1 -zone=us-central1-a kubectl apply -f deployment.yaml kubectl apply -f service.yaml**

Your company owns a web application that lets users post travel stories. You began noticing errors in logs for a specific Deployment. The deployment is responsible for translating a post from one language to another. You've narrowed the issue down to a specific container named “msg-translator-22” that is throwing the errors. You are unable to reproduce the error in any other environment and none of the other containers serving the deployment have this issue. You would like to connect to this container to figure out the root cause. What steps would allow you to run commands against the msg-translator-22?

A. Use the kubectl run msg-translator-22 /bin/ bash command to run a shell on that container.

B. Use the kubectl exec -it -- /bin/bash command to run a shell on that container.

C. Use the kubectl run command to run a shell on that container.

D. Use the kubectl exec -it msg-translator-22 - /bin/bash command to run a shell on that container.

Your company recently migrated all infrastructure to Google Cloud Platform (GCP) and you want to use Google Cloud Build to build all container images. You want to store the build logs in Google Cloud Storage. You also have a requirement to push the images to Google Container Registry. You wrote a cloud build YAML configuration file with the following contents, steps:

```
- name: ‘gcr.io/cloud-builders/docker’
args: [‘build*, ‘-t\ ‘gcr.io/[PROJECT_ID]/[IMAGE_NAME]’, V]
images: |‘gcr.io/[PROJECT_ID]/[IMAGE_NAME]*]
```

How should you execute Cloud build to satisfy these requirements?

A. Execute gcloud builds run -config=[CONFIG_FILE_PATH] -gcs-log-dir=[GCS_LOG_DIR] [SOURCE]

B. Execute gcloud builds submit --config=[CONFIG_FILE_PATH] -gcs-log-dir=[GCS_LOG_DIR] [SOURCE]

C. Execute gcloud builds submit --config=[CONFIG_FILE_PATH] [SOURCE]

D. Execute gcloud builds push --config=[CONFIG_FILE_PATH] [SOURCE]

You want to select and configure a cost-effective solution for relational data on Google Cloud Platform. You are working with a small set of operational data in one geographic location. You need to support point-in-time recovery. What should you do?

A. Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.

B. Select Cloud SQL (MySQL). Select the create failover replicas option.

C. Select Cloud Spanner. Set up your instance with 2 nodes.

D. Select Cloud Spanner. Set up your instance as multi-regional.

You are working with a Cloud SQL MySQL database at your company. You need to retain a month-end copy of the database for three years for audit purposes.
What should you do?

A. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

B. Save the automatic first-of-the-month backup for three years. Store the backup file in an Archive class Cloud Storage bucket.
C. Set up an on-demand backup for the first of the month. Write the backup to an Archive class Cloud Storage bucket.
D. Convert the automatic first-of-the-month backup to an export file. Write the export file to a Coldline class Cloud Storage bucket.

Your company has an internal application for managing transactional orders. The application is used exclusively by employees in a single physical location. The application requires strong consistency, fast queries, and ACID guarantees for multi-table transactional updates. The first version of the application is implemented in PostgreSQL, and you want to display it to the cloud with minimal code changes. Which database is most appropriate for this application?

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

You developed an application to serve production users and you plan to use Cloud SQL to host user state data which is very critical for the application flow. You want to protect your user state data from zone failures. What should you do?

A. Create a Read replica in the same region but in a different zone.
B. Create a Read replica in the same region but in a different zone.
C. Configure High Availability (HA) for Cloud SQL and Create a Failover replica in the same region but in a different zone.
D. Configure High Availability (HA) for Cloud SQL and Create a Failover replica in a different region

You want to verify the IAM users and roles assigned within a GCP project named my-project. What should you do?

A. Run gcloud iam roles list. Review the output section.
B. Run gcloud iam service-accounts list. Review the output section.
C. Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles.
D. Navigate to the project and then to the Roles section in the GCP Console. Review the roles and status.

You need to create a new billing account and then link it with an existing Google Cloud Platform project. What should you do?

A. Verify that you are Project Billing Manager for the GCP project. Update the existing project to link it to the existing billing account.
B. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

You have one project called proj-sa where you manage all your service accounts. You want to be able to use a service account from this project to take snapshots of VMs running in another project called proj-vm. What should you do?

A. Download the private key from the service account, and add it to each VMs custom metadata.
B. Download the private key from the service account, and add the private key to each VM's SSH keys.
C. Grant the service account the IAM Role of Compute Storage Admin in the project called proj-vm.
D. When creating the VMs, set the service account's API scope for Compute Engine to read/write.

You need to grant access for three users so that they can view and edit table data on a Cloud Spanner instance. What should you do?

A. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to the role.
B. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.
C. Run gcloud iam roles describe roles/spanner.viewer --project my-project. Add the users to the role.
D. Run gcloud iam roles describe roles/spanner.viewer --project my-project. Add the users to a new group. Add the group to the role.

Your company has a Google Cloud Platform project that uses BigQuery for data warehousing. Your data science team changes frequently and has few members.
You need to allow members of this team to perform queries. You want to follow Google-recommended practices. What should you do?

A. 1. Create an IAM entry for each data scientist's user account.
2. Assign the BigQuery jobUser role to the group.
B. 1. Create an IAM entry for each data scientist's user account.
2. Assign the BigQuery dataViewer user role to the group.
C. 1.Create a dedicated Google group in Cloud Identity.
2. Add each data scientist's user account to the group.
3. Assign the BigQuery jobUser role to the group.
D. 1.Create a dedicated Google group in Cloud Identity.
2. Add each data scientist's user account to the group.
3. Assign the BigQuery dataViewer user role to the group.

You are the organization and billing administrator for your company. The engineering team has the Project Creator role on the organization. You do not want the engineering team to be able to link projects to the billing account. Only the finance team should be able to link a project to a billing account, but they should not be able to make any other changes to projects. What should you do?

A. Assign the finance team only the Billing Account User role on the billing account.
B. Assign the engineering team only the Billing Account User role on the billing account.
C. Assign the finance team the Billing Account User role on the billing account and the Project Billing Manager role on the organization.
D. Assign the engineering team the Billing Account User role on the billing account and the Project Billing Manager role on the organization.

Your company has an existing GCP organization with hundreds of projects and a billing account. Your company recently acquired another company that also has hundreds of projects and its own billing account. You would like to consolidate all GCP costs of both GCP organizations onto a single invoice. You would like to consolidate all costs as of tomorrow. What should you do?

A. Link the acquired company's projects to your company's billing account.
B. Configure the acquired company's billing account and your company's billing account to export the billing data into the same BigQuery dataset.
C. Migrate the acquired company's projects into your company's GCP organization. Link the migrated projects to your company's billing account.
D. Create a new GCP organization and a new billing account. Migrate the acquired company's projects and your company's projects into the new GCP organization and link the projects to the new billing account.

You built an application on Google Cloud that uses Cloud Spanner. Your support team needs to monitor the environment but should not have access to table data. You need a streamlined solution to grant the correct permissions to your support team, and you want to follow Google-recommended practices. What should you do?

A. Add the support team group to the roles/monitoring.viewer role
B. Add the support team group to the roles/spanner.databaseUser role.
C. Add the support team group to the roles/spanner.databaseReader role.
D. Add the support team group to the roles/stackdriver.accounts.viewer role.

You are building an application that will run in your data center. The application will use Google Cloud Platform (GCP) services like AutoML. You created a service account that has appropriate access to AutoML. You need to enable authentication to the APIs from your on-premises environment. What should you do?

A. Use service account credentials in your on-premises application.
B. Use gcloud to create a key file for the service account that has appropriate permissions.
C. Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.

D. Go to the IAM & admin console, grant a user account permissions similar to the service account permissions, and use this user account for authentication from your data center.

You need to produce a list of the enabled Google Cloud Platform APIs for a GCP project using the gcloud command line in the Cloud Shell. The project name is my- project. What should you do?

A. Run gcloud projects list to get the project ID, and then run gcloud services list --project <project ID>.
B. Run gcloud init to set the current project to my-project, and then run gcloud services list -available.
C. Run gcloud info to view the account value, and then run gcloud services list -account <Account>.
D. Run gcloud projects describe <project ID> to verify the project value, and then run gcloud services list -available.

You want to add a new auditor to a Google Cloud Platform project. The auditor should be allowed to read, but not modify, all project items.
How should you configure the auditor's permissions?

A. Create a custom role with view-only project permissions. Add the user's account to the custom role.
B. Create a custom role with view-only service permissions. Add the user's account to the custom role.
C. Select the built-in IAM project Viewer role. Add the user's account to this role.
D. Select the built-in IAM service Viewer role. Add the user's account to this role.

Your organization uses G Suite for communication and collaboration. All users in your organization have a G Suite account. You want to grant some G Suite users access to your Cloud Platform project. What should you do?

A. Enable Cloud Identity in the GCP Console for your domain.
B. Grant them the required IAM roles using their G Suite email address.
C. Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.
D. In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group.

Your finance team wants to view the billing report for your projects. You want to make sure that the finance team does not get additional permissions to the project. What should you do?

A. Add the group for the finance team to roles/billing user role.
B. Add the group for the finance team to roles/billing admin role.
C. Add the group for the finance team to roles/billing viewer role.

D. Add the group for the finance team to roles/billing project/Manager role.

Your organization has strict requirements to control access to Google Cloud projects. You need to enable your Site Reliability Engineers (SREs) to approve requests from the Google Cloud support team when an SRE opens a support case. You want to follow Google-recommended practices. What should you do?

A. Add your SREs to roles/iam.roleAdmin role.
B. Add your SREs to roles/accessapproval.approver role.
C. Add your SREs to a group and then add this group to roles/iam.roleAdmin.role.
D. Add your SREs to a group and then add this group to roles/accessapproval.approver role.

Your organization needs to grant users access to query datasets in BigQuery but prevent them from accidentally deleting the datasets. You want a solution that follows Google-recommended practices. What should you do?

A. Add users to roles/bigquery user role only, instead of roles/bigquery dataOwner.
B. Add users to roles/bigquery dataEditor role only, instead of roles/bigquery dataOwner.
C. Create a custom role by removing delete permissions, and add users to that role only.
D. Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role.

Your company set up a complex organizational structure on Google Cloud. The structure includes hundreds of folders and projects. Only a few team members should be able to view the hierarchical structure. You need to assign minimum permissions to these team members, and you want to follow Google-recommended practices. What should you do?

A. Add the users to roles/browser role.
B. Add the users to roles/iam.roleViewer role.
C. Add the users to a group, and add this group to roles/browser.
D. Add the users to a group, and add this group to roies/iam.roieViewer role.

Your company has a single sign-on (SSO) identity provider that supports Security Assertion Markup Language (SAML) integration with service providers. Your company has users in Cloud Identity. You would like users to authenticate using your company's SSO provider. What should you do?

A. In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps.
B. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.
C. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps.

D. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications.

Your organization has a dedicated person who creates and manages all service accounts for Google Cloud projects. You need to assign this person the minimum role for projects. What should you do?

A. Add the user to roles/iam.roleAdmin role.
B. Add the user to roles/iam.securityAdmin role.
C. Add the user to roles/iam.serviceAccountUser role.
D. Add the user to roles/iam.serviceAccountAdmin role.

Your organization has user identities in Active Directory. Your organization wants to use Active Directory as their source of truth for identities. Your organization wants to have full control over the Google accounts used by employees for all Google services, including your Google Cloud Platform (GCP) organization. What should you do?

A. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.
B. Use the cloud Identity APIs and write a script to synchronize users to Cloud Identity.
C. Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console.
D. Ask each employee to create a Google account using self signup. Require that each employee use their company email address and password.

You have successfully created a development environment in a project for an application. This application uses Compute Engine and Cloud SQL. Now you need to create a production environment for this application. The security team has forbidden the existence of network routes between these 2 environments and has asked you to follow Google-recommended practices. What should you do?

A. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.
B. Create a new production subnet in the existing VPC and a new production Cloud SQL instance in your existing project, and deploy your application using those resources.
C. Create a new project, modify your existing VPC to be a Shared VPC, share that VPC with your new project, and replicate the setup you have in the development environment in that new project in the Shared VPC.
D. Ask the security team to grant you the Project Editor role in an existing production project used by another division of your company. Once they grant you that role, replicate the setup you have in the development environment in that project.

Your management has asked an external auditor to review all the resources in a specific project. The security team has enabled the Organization Policy called
Domain Restricted Sharing on the organization node by specifying only your Cloud Identity domain. You want the auditor to only be able to view, but not modify, the resources in that project. What should you do?

A. Ask the auditor for their Google account, and give them the Viewer role on the project.
B. Ask the auditor for their Google account, and give them the Security Reviewer role on the project.
C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.
D. Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project.

You need to assign a Cloud Identity and Access Management (Cloud IAM) role to an external auditor. The auditor needs to have permissions to review your
Google Cloud Platform (GCP) Audit Logs and also to review your Data Access logs. What should you do?

A. Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage.
B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.
C. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Perform the export of logs to Cloud Storage.
D. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

You need to reduce GCP service costs for a division of your company using the fewest possible steps. You need to turn off all configured services in an existing GCP project. What should you do?

A. 1. Verify that you are assigned the Project Owners IAM role for this project.
2. Locate the project in the GCP console, click Shut down and then enter the project ID.
B. 1. Verify that you are assigned the Project Owners IAM role for this project.
2. Switch to the project in the GCP console, locate the resources and delete them.
C. 1. Verify that you are assigned the Organizational Administrator IAM role for this project.
2. Locate the project in the GCP console, enter the project ID and then click Shut down.
D. 1. Verify that you are assigned the Organizational Administrators IAM role for this project.
2. Switch to the project in the GCP console, locate the resources and delete them.

You are configuring service accounts for an application that spans multiple projects. Virtual machines (VMs) running in the web-applications project need access to BigQuery datasets in crm-databases- proj. You want to follow Google-recommended practices to give access to the service account in the web-applications project. What should you do?

A. Give project owner for web-applications appropriate roles to crm-databases-proj.
B. Give project owner role to crm-databases-proj and the web-applications project.
C. Give project owner role to crm-databases-proj and bigquery.dataViewer role to web-applications.
D. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

You need to create a custom IAM role for use with a GCP service. All permissions in the role must be suitable for production use. You also want to clearly share with your organization the status of the custom role. This will be the first version of the custom role. What should you do?

A. **Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.**

B. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to BETA while testing the role permissions.

C. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

D. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to BETA while testing the role permissions.

You manage an App Engine Service that aggregates and visualizes data from BigQuery. The application is deployed with the default App Engine Service account.
The data that needs to be visualized resides in a different project managed by another team. You do not have access to this project, but you want your application to be able to read data from the BigQuery dataset. What should you do?

A. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

B. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.

C. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.

D. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

An application generates daily reports in a Compute Engine virtual machine (VM). The VM is in the project corp-iot-insights. Your team operates only in the project corp-aggregate-reports and needs a copy of the daily exports in the bucket corp-aggregate-reports-storage. You want to configure access so that the daily reports from the VM are available in the bucket corp-aggregate-reports-storage and use as few steps as possible while following Google-recommended practices. What should you do?

A. Move both projects under the same folder.
B. **Grant the VM Service Account the role Storage Object Creator on corp-aggregate-reports-storage**.
C. Create a Shared VPC network between both projects. Grant the VM Service Account the role Storage Object Creator on corp-iot- insights.
D. Make corp-aggregate-reports-storage public and create a folder with a pseudo-randomized suffix name. Share the folder with the IoT team.

You built an application on your development laptop that uses Google Cloud services. Your application uses Application Default Credentials for authentication and works fine on your development laptop. You want to migrate this application to a Compute Engine virtual machine (VM) and set up authentication using Google- recommended practices and minimal changes. What should you do?

A. Assign appropriate access for Google services to the service account used by the Compute Engine VM.
B. Create a service account with appropriate access for Google services, and configure the application to use this account.
C. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.
D. Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application.

A colleague handed over a Google Cloud Platform project for you to maintain. As part of a security checkup, you want to review who has been granted the Project Owner role. What should you do?

A. In the console, validate which SSH keys have been stored as project-wide keys.
B. Navigate to Identity-Aware Proxy and check the permissions for these resources.
C. Enable Audit Logs on the IAM & admin page for all resources, and validate the results.
D. Use the command gcloud projects get-iam-policy to view the current role assignments.

Your company uses a large number of Google Cloud services centralized in a single project. All teams have specific projects for testing and development. The
DevOps team needs access to all of the production services in order to perform their job. You want to prevent Google Cloud product changes from broadening their permissions in the future. You want to follow Google-recommended practice
s. What should you do?

A. Grant all members of the DevOps team the role of Project Editor on the organization level.
B. Grant all members of the DevOps team the role of Project Editor on the production project.
C. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.
D. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the organization level.

You are performing a monthly security check of your Google Cloud environment and want to know who has access to view data stored in your Google Cloud
Project. What should you do?

A. Enable Audit Logs for all APIs that are related to data storage.
B. Review the IAM permissions for any role that allows for data access.
C. Review the Identity-Aware Proxy settings for each resource.
D. Create a Data Loss Prevention job.

You are running a data warehouse on BigQuery. A partner company is offering a recommendation engine based on the data in your data warehouse. The partner company is also running their application on Google Cloud. They manage the resources in their own project, but they need access to the BigQuery dataset in your project. You want to provide the partner company with access to the dataset. What should you do?

A. Create a Service Account in your own project, and grant this Service Account access to BigQuery in your project.
B. Create a Service Account in your own project, and ask the partner to grant this Service Account access to BigQuery in their project.
C. Ask the partner to create a Service Account in their project, and have them give the Service Account access to BigQuery in their project.
D. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

You received a JSON file that contained a private key of a Service Account in order to get access to several resources in a Google Cloud project. You downloaded and installed the Cloud SDK and want to use this private key for authentication and authorization when performing gcloud commands. What should you do?

A. Use the command gcloud auth login and point it to the private key.

B. Use the command gcloud auth activate-service-account and point it to the private key.

C. Place the private key file in the installation directory of the Cloud SDK and rename it to credentials.json.

D. Place the private key file in your home directory and rename it to GOOGLE_APPLICATION_CREDENTIALS

You will have several applications running on different Compute Engine instances in the same project. You want to specify at a more granular level the service account each instance uses when calling Google Cloud APIs. What should you do?

A. When creating the instances, specify a Service Account for each instance.

B. When creating the instances, assign the name of each Service Account as instance metadata.

C. After starting the instances, use gcloud compute instances update to specify a Service Account for each instance.

D. After starting the instances, use gcloud compute instances update to assign the name of the relevant Service Account as instance metadata.

You are managing a project for the Business Intelligence (BI) department in your company. A data pipeline ingests data into BigQuery via streaming. You want the users in the BI department to be able to run the custom SQL queries against the latest data in BigQuery. What should you do?

A. Create a Data Studio dashboard that uses the related BigQuery tables as a source and give the BI team view access to the Data Studio dashboard.

B. Create a Service Account for the BI team and distribute a new private key to each member of the BI team.

C. Use Cloud Scheduler to schedule a batch Dataflow job to copy the data from BigQuery to the BI team's internal data warehouse.

D. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

You have created a new project in Google Cloud through the gcloud command line interface (CLI) and linked a billing account. You need to create a new Compute

Engine instance using the CLI. You need to perform the prerequisite steps. What should you do?

A. Create a Cloud Monitoring Workspace.

B. Create a VPC network in the project.

C. Enable the compute googleapis.com API.

D. Grant yourself the IAM role of Computer Admin.

You need to manage a third-party application that will run on a Compute Engine instance. Other Compute Engine instances are already running with default configuration. Application installation files are hosted on Cloud Storage. You need to access these files from the new instance without allowing other virtual machines (VMs) to access these files. What should you do?

A. Create the instance with the default Compute Engine service account. Grant the service account permissions on Cloud Storage.

B. Create the instance with the default Compute Engine service account Add metadata to the objects on Cloud Storage that matches the metadata on the new instance.

C. Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

D. Create a new service account and assign this service account to the new instance. Add metadata to the objects on Cloud Storage that matches the metadata on the new instance.

You need to add a group of new users to Cloud Identity. Some of the users already have existing Google accounts. You want to follow one of Google's recommended practices and avoid conflicting accounts. What should you do?

A. Invite the user to transfer their existing account.

B. Invite the user to use an email alias to resolve the conflict.

C. Tell the user that they must delete their existing account.

D. Tell the user to remove all personal email from the existing account.

The sales team has a project named Sales Data Digest that has the ID acme-data-digest. You need to set up similar Google Cloud resources for the marketing team but their resources must be organized independently of the sales team. What should you do?

A. Grant the Project Editor role to the Marketing team for acme-data-digest.

B. Create a Project Lien on acme-data-digest and then grant the Project Editor role to the Marketing team.

C. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

D. Create a new project named Marketing Data Digest and use the ID acme-data-digest. Grant the Project Editor role to the Marketing team.

You have a development project with appropriate IAM roles defined. You are creating a production project and want to have the same IAM roles on the new project, using the fewest possible steps. What should you do?

A. Use gcloud iam roles copy and specify the production project as the destination project.

B. Use gcloud iam roles copy and specify your organization as the destination organization.

C. In the Google Cloud Platform Console, use the 'create role from role' functionality.

D. In the Google Cloud Platform Console, use the 'create role' functionality and select all applicable permissions.

You need to configure IAM access audit logging in BigQuery for external auditors. You want to follow Google-recommended practices. What should you do?

A. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

B. Add the auditors group to two new custom IAM roles.

C. Add the auditor user accounts to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

D. Add the auditor user accounts to two new custom IAM roles.

You need to set up permissions for a set of Compute Engine instances to enable them to write data into a particular Cloud Storage bucket. You want to follow Google-recommended practices. What should you do?

A. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/devstorage.write_only'.

B. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/cloud-platform1.

C. Create a service account and add it to the IAM role 'storage.objectCreator' for that bucket.

D. Create a service account and add it to the IAM role 'storage.objectAdmin' for that bucket.

You are the project owner of a GCP project and want to delegate control to colleagues to manage buckets and files in Cloud Storage. You want to follow Google- recommended practices. Which IAM roles should you grant your colleagues?

A. Project Editor

B. Storage Admin
C. Storage Object Admin
D. Storage Object Creator

An intern joined your team recently and needs access to Google Compute Engine in your sandbox project to explore various settings and spin up compute instances to test features. You have been asked to facilitate this. How should you give your intern access to compute engine without giving more permissions than is necessary?

A. Grant Project Editor IAM role for sandbox project.
B. Grant Compute Engine Admin Role for sandbox project.
C. Create a shared VPC to enable the intern access Compute resources.
D. Grant Compute Engine Instance Admin Role for the sandbox project.

You developed an application that lets users upload statistical files and subsequently run analytics on this data. You chose to use Google Cloud Storage and BigQuery respectively for these requirements as they are highly available and scalable. You have a docker image for your application code, and you plan to deploy on your on-premises Kubernetes clusters. Your on-prem Kubernetes cluster needs to connect to Google Cloud Storage and BigQuery and you want to do this in a secure way following Google recommended practices. What should you do?

A. Create a new service account, with editor permissions, generate and download a key. Use the key to authenticate inside the application.
B. Use the default service account for App Engine, which already has the required permissions.
C. Use the default service account for Compute Engine, which already has the required permissions.
D. Create a new service account, grant it the least viable privileges to the required services, generate and download a JSON key. Use the JSON key to authenticate inside the application.

You have one project called ptech-sa where you manage all your service accounts. You want to be able to use a service account from this project to take snapshots of VMs running in another project called ptech-vm. What should you do?

A. When creating the VMs, set the service account's API scope for Compute Engine to read/write.
B. Grant the service account the IAM Role of Compute Storage Admin in the project called ptech-vm.

C. Download the private key from the service account, and add it to each VMs custom metadata.
D. Download the private key from the service account, and add the private key to each VM's SSH keys.

You want to find out when users were added to Cloud Spanner Identity Access Management (IAM) roles on your Google Cloud Platform (GCP) project. What should you do in the GCP Console?

A. Open the Cloud Spanner console to review configurations.
B. Open the IAM & admin console to review IAM policies for Cloud Spanner roles.
C. Go to the Stackdriver Monitoring console and review information for Cloud Spanner.
D. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.
bucket

Your company has a number of GCP projects that are managed by the respective project teams. Your expenditure of all GCP projects combined has exceeded your operational expenditure budget. At a review meeting, it has been agreed that your finance team should be able to set budgets and view the current charges for all projects in the organization but not view the project resources; and your developers should be able to see the Google Cloud Platform billing charges for only their own projects as well as view resources within the project. You want to follow Google recommended practices to set up 1AM roles and permissions. What should you do?

A. Add the finance team to the Viewer role for the Project. Add the developers to the Security Reviewer role for each of the billing accounts.
B. Add the developers and finance managers to the Viewer role for the Project.
C. Add the finance team to the Billing Account Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the
Project.
D. Add the finance team to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only.

Your company procured a license for a third-party cloud-based document signing system for the procurement team. All members of the procurement team need to sign in with
the same service account. Your security team prohibits sharing service account passwords. You have been asked to recommend a solution that lets the procurement team
login as the service account in the document signing system but without the team knowing the service account password. What should you do?

A. Ask the third-party provider to enable SAML for the application and set the credentials to the service account credentials.
B. Ask the third-party provider to enable OAuth 2.0 for the application and set the credentials to the service account credentials.
C. Have a single person from the procurement team access document signing system with the service account credentials.
D. Register the application as a password vaulted app and set the credentials to the service account credentials.

Your company stores customer PII data in Cloud Storage buckets. A subset of this data is regularly imported into a BigQuery dataset to carry out analytics. You want to make sure the access to this bucket is strictly controlled. Your analytics team needs read access on the bucket so that they can import data in BigQuery. Your operations team needs read/write access to both the bucket and BigQuery dataset to add Customer PII data of new customers on an ongoing basis. Your Data Vigilance officers need Administrator access to the Storage bucket and BigQuery dataset. You want to follow Google recommended practices. What should you do?

A. Create 3 custom IAM roles with appropriate permissions for the access levels needed for Cloud Storage and BigQuery. Add your users to the appropriate roles.
B. At the Project level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.
C. At the Organization level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.
D. Use the appropriate predefined IAM roles for each of the access levels needed for Cloud Storage and BigQuery. Add your users to those roles for each of the services.

Your company uses a legacy application that still relies on the legacy LDAP protocol to authenticate. Your company plans to migrate this application to cloud and is looking for a cost effective solution while minimizing any developer effort. What should you do?

A. Modify the legacy application to use SAML and ask users to sign in through Gmail.
B. Modify the legacy application to use OAuth 2.0 and ask users to sign in through Gmail.
C. Use secure LDAP to authenticate the legacy application and ask users to sign in through Gmail.
D. Synchronize data within your LDAP server with Google Cloud Directory Sync.

You work in a small company where everyone should be able to view all resources of a specific project. You want to grant them access following Google's recommended practices. What should you do?

A. Create a script that uses gcloud projects add-iam-policy-binding for all users' email addresses and the Project Viewer role.

B. Create a script that uses gcloud iam roles create for all users' email addresses and the Project Viewer role.
C. Create a new Google Group and add all users to the group. Use gcloud projects add-iam-policy-binding with the Project Viewer role and Group email address.
D. Create a new Google Group and add all members to the group. Use gcloud iam roles create with the Project Viewer role andGroupemail address.

You are deploying an application to a Compute Engine VM in a managed instance group. The application must be running at all times, but only a single instance of the VM should run per GCP project. How should you configure the instance group?

A. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
B. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
C. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 2.
D. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 2.

You are running an application on multiple virtual machines within a managed instance group and have autoscaling enabled. The autoscaling policy is configured so that additional instances are added to the group if the CPU utilization of instances goes above 80%. VMs are added until the instance group reaches its maximum limit of five VMs or until CPU utilization of instances lowers to 80%. The initial delay for HTTP health checks against the instances is set to 30 seconds.
The virtual machine instances take around three minutes to become available for users. You observe that when the instance group autoscales, it adds more instances than necessary to support the levels of end-user traffic. You want to properly maintain instance group sizes when autoscaling. What should you do?

A. Set the maximum number of instances to 1.
B. Decrease the maximum number of instances to 3.
C. Use a TCP health check instead of an HTTP health check.
D. Increase the initial delay of the HTTP health check to 200 seconds.

You want to configure 10 Compute Engine instances for availability when maintenance occurs. Your requirements state that these instances should attempt to automatically restart if they crash. Also, the instances should be highly available including during system maintenance. What should you do?

A. **Create an instance template for the instances. Set the Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.**
B. Create an instance template for the instances. Set 'Automatic Restart' to off. Set 'On-host maintenance' to Terminate VM instances. Add the instance template to an instance group.
C. Create an instance group for the instances. Set the 'Autohealing' health check to healthy (HTTP).
D. Create an instance group for the instance. Verify that the 'Advanced creation options' setting for 'do not retry machine creation' is set to off.

You need to create an autoscaling managed instance group for an HTTPS web application. You want to make sure that unhealthy VMs are recreated. What should you do?

A. **Create a health check on port 443 and use that when creating the Managed Instance Group.**
B. Select Multi-Zone instead of Single-Zone when creating the Managed Instance Group.
C. In the Instance Template, add the label 'health-check'.
D. In the Instance Template, add a startup script that sends a heartbeat to the metadata server.

You have a web application deployed as a managed instance group. You have a new version of the application to gradually deploy. Your web application is currently receiving live web traffic. You want to ensure that the available capacity does not decrease during the deployment. What should you do?

A. Perform a rolling-action start-update with maxSurge set to 0 and maxUnavailable set to 1.
B. **Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.**
C. Create a new managed instance group with an updated instance template. Add the group to the backend service for the load balancer. When all instances in the new managed instance group are healthy, delete the old managed instance group.
D. Create a new instance template with the new application version. Update the existing managed instance group with the new instance template. Delete the instances in the managed instance group to allow the managed instance group to recreate the instance using the new instance template.

Your managed instance group raised an alert stating that new instance creation has failed to create new instances. You need to maintain the number of running instances specified by the template to be able to process expected application traffic. What should you do?

A. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

B. Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

C. Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template.

D. Delete the current instance template and replace it with a new instance template. Verify that the instance name and persistent disk name values are not the same in the template. Set the disks.autoDelete property to true in the instance template.

You want to configure autohealing for network load balancing for a group of Compute Engine instances that run in multiple zones, using the fewest possible steps. You need to configure re-creation of VMs if they are unresponsive after 3 attempts of 10 seconds each. What should you do?

A. Create an HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP)

B. Create an HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10.

C. Create a managed instance group. Set the Autohealing health check to healthy (HTTP)

D. Create a managed instance group. Verify that the autoscaling setting is on.

You have a single binary application that you want to run on Google Cloud Platform. You decided to automatically scale the application based on underlying infrastructure CPU usage. Your organizational policies require you to use virtual machines directly. You need to ensure that the application scaling is operationally efficient and completed as quickly as possible. What should you do?

A. Create a Google Kubernetes Engine cluster, and use horizontal pod autoscaling to scale the application.

B. Create an instance template, and use the template in a managed instance group with autoscaling configured.

C. Create an instance template, and use the template in a managed instance group that scales up and down based on the time of day.

D. Use a set of third-party tools to build automation around scaling the application up and down, based on Stackdriver CPU usage monitoring.

You defined an instance template for a Python web application. When you deploy this application in Google Compute Engine, you want to ensure the service scales up and scales down automatically based on the number of HTTP requests. What should you do?

A. 1. Create the necessary number of instances based on the instance template to handle peak user traffic.
   2. Group the instances together in an unmanaged instance group.
   3. Configure the instance group as the Backend Service of an External HTTP(S) load balancer.
B. 1. Create an instance from the instance template.
   2. Create an image from the instance's disk and export it to Cloud Storage.
   3. Create an External HTTP(s) load balancer and add the Cloud Storage bucket as its backend service.
C. 1. Create an unmanaged instance group from the instance template.
   2. Configure autoscaling on the unmanaged instance group with a scaling policy based on HTTP traffic.
   3. Configure the unmanaged instance group as the backend service of an Internal HTTP(S) load balancer.
D. 1. Deploy your Python web application instance template to Google Cloud App Engine.
   2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.
E. 1. Create a managed instance group from the instance template.
   2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.
   3. Configure the instance group as the backend service of an External HTTP(S) load balancer.

You have a web application deployed as a managed instance group based on an instance template. You modified the startup script used in the instance template and would like the existing instances to pick up changes from the new startup scripts. Your web application is currently serving live web traffic. You want to propagate the startup script changes to all instances in the managed instances group while minimizing effort, minimizing cost and ensuring that the available capacity does not decrease. What would you do?

A. Delete instances in the managed instance group (MIG) one at a time and rely on auto-healing to provision an additional instance.
B. Perform a rolling-action replace with max-unavailable set to 0 and max-surge set to 1
C. Create a new managed instance group (MIG) based on a new template. Add the group to the backend service for the load balancer. When all instances in the new managed instance group are healthy, delete the old managed instance group
D. Perform a rolling-action start-update with max-unavailable set to 1 and max-surge set to 0

You have a web application deployed as a managed instance group. You noticed some of the compute instances are running low on memory. You suspect this is due to JVM memory leak and you want to restart the compute instances to reclaim the leaked memory. Your web application is currently serving live web traffic. You want to ensure that the available capacity does not go below 80% at any time during the restarts and you want to do this at the earliest. What would you do?

A. Stop instances in the managed instance group (MIG) one at a time and rely on autohealing to bring them back up.
B. Perform a rolling-action replace with max-unavailable set to 20%.
C. Perform a rolling-action restart with max-unavailable set to 20%.
D. Perform a rolling-action reboot with max-surge set to 20%.

You host a production application in Google Compute Engine in the us-central1-a zone. Your application needs to be available 24*7 all through the year. The application suffered an outage recently due to a Compute Engine outage in the zone hosting your application. Your application is also susceptible to slowness during peak usage. You have been asked for a recommendation on how to modify the infrastructure to implement a cost-effective and scalable solution that can withstand zone failures. What would you recommend?

A. Use Managed instance groups with instances in a single zone. Enable Autoscaling on the Managed instance group.
B. Use Managed instance groups with preemptible instances across multiple zones. Enable Autoscaling on the Managed instance group.
C. Use Managed instance groups across multiple zones. Enable Autoscaling on the Managed instance group.
D. Use Unmanaged instance groups across multiple zones. Enable Autoscaling on the Unmanaged instance group.

You have an instance group that you want to load balance. You want the load balancer to terminate the client SSL session. The instance group is used to serve a public web application over HTTPS. You want to follow Google-recommended practices. What should you do?

A. Configure an HTTP(S) load balancer.
B. Configure an internal TCP load balancer.
C. Configure an external SSL proxy load balancer.
D. Configure an external TCP proxy load balancer.

You have an application that receives SSL-encrypted TCP traffic on port 443. Clients for this application are located all over the world. You want to minimize latency for the clients. Which load balancing option should you use?

A. HTTPS Load Balancer
B. Network Load Balancer
C. SSL Proxy Load Balancer
D. Internal TCP/UDP Load Balancer. Add a firewall rule allowing ingress traffic from 0.0.0.0/0 on the target instances.

You are hosting an application from Compute Engine virtual machines (VMs) in us-central1-a.
You want to adjust your design to support the failure of a single
Compute Engine zone, eliminate downtime, and minimize cost. What should you do?

- **A. Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.**
- B. Create a Managed Instance Group and specify us-central1-aa as the zone. Configure the Health Check with a short Health Interval.
- C. Create an HTTP(S) Load Balancer. Create one or more global forwarding rules to direct traffic to your VMs.
- D. Perform regular backups of your application. Create a Cloud Monitoring Alert and be notified if your application becomes unavailable. Restore from backups when notified.

Your company developed a mobile game that is deployed on Google Cloud. Gamers are connecting to the game with their personal phones over the Internet. The game sends UDP packets to update the servers about the gamers' actions while they are playing in multiplayer mode. Your game backend can scale over multiple virtual machines (VMs), and you want to expose the VMs over a single IP address. What should you do?

- A. Configure an SSL Proxy load balancer in front of the application servers.
- B. Configure an Internal UDP load balancer in front of the application servers.
- C. Configure an External HTTP(s) load balancer in front of the application servers.
- **D. Configure an External Network load balancer in front of the application servers.**

You are designing an application that uses WebSockets and HTTP sessions that are not distributed across the web servers. You want to ensure the application runs properly on Google Cloud Platform. What should you do?

- **A. Meet with the cloud enablement team to discuss load balancer options.**
- B. Redesign the application to use a distributed user session service that does not rely on WebSockets and HTTP sessions.
- C. Review the encryption requirements for WebSocket connections with the security team.
- D. Convert the WebSocket code to use HTTP streaming.

You want to run a single caching HTTP reverse proxy on GCP for a latency-sensitive website. This specific reverse proxy consumes almost no CPU. You want to have a 30- GB in-memory cache, and need an additional 2 GB of memory for the rest of the processes. You want to minimize cost. How should you run this reverse proxy?

A. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

B. Run it on Compute Engine, and choose a custom instance type with 6 vCPUs and 32 GB of memory.

C. Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes.

D. Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

Your organization is a financial company that needs to store audit log files for 3 years. Your organization has hundreds of Google Cloud projects. You need to implement a cost-effective approach for log file retention. What should you do?

A. Create an export to the sink that saves logs from Cloud Audit to BigQuery.
B. Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket.
C. Write a custom script that uses logging API to copy the logs from Stackdriver logs to BigQuery.
D. Export these logs to Cloud Pub/Sub and write a Cloud Dataflow pipeline to store logs to Cloud SQL.

For analysis purposes, you need to send all the logs from all of your Compute Engine instances to a BigQuery dataset called platform-logs. You have already installed the Cloud Logging agent on all the instances. You want to minimize cost. What should you do?

A. 1. Give the BigQuery Data Editor role on the platform-logs dataset to the service accounts used by your instances. 2. Update your instances' metadata to add the following value: logs-destination: bq://platform-logs.
B. 1. In Cloud Logging, create a logs export with a Cloud Pub/Sub topic called logs as a sink. 2. Create a Cloud Function that is triggered by messages in the logs topic. 3. Configure that Cloud Function to drop logs that are not from Compute Engine and to insert Compute Engine logs in the platform-logs dataset.
C. 1. In Cloud Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the platform-logs dataset as Sink Destination.
D. 1. Create a Cloud Function that has the BigQuery User role on the platform-logs dataset. 2. Configure this Cloud Function to create a BigQuery Job that executes this query: INSERT INTO dataset.platform-logs (timestamp, log) SELECT timestamp, log FROM compute.logs WHERE timestamp > DATE_SUB(CURRENT_DATE(), INTERVAL 1 DAY) 3. Use Cloud Scheduler to trigger this Cloud Function once a day.

You need to verify that a Google Cloud Platform service account was created at a particular time. What should you do?

A. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.
B. Filter the Activity log to view the Configuration category. Filter the Resource type to Google Project.
C. Filter the Activity log to view the Data Access category. Filter the Resource type to Service Account.

D. Filter the Activity log to view the Data Access category. Filter the Resource type to Google Project.

You want to find out when users were added to Cloud Spanner Identity Access Management (IAM) roles on your Google Cloud Platform (GCP) project. What should you do in the GCP Console?

A. Open the Cloud Spanner console to review configurations.
B. Open the IAM & admin console to review IAM policies for Cloud Spanner roles.
C. Go to the Stackdriver Monitoring console and review information for Cloud Spanner.
D. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

You are managing several Google Cloud Platform (GCP) projects and need access to all logs for the past 60 days. You want to be able to explore and quickly analyze the log contents. You want to follow Google-recommended practices to obtain the combined logs for all projects. What should you do?

A. Navigate to Stackdriver Logging and select resource.labels.projectjd-'*"
B. Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.
C. Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days.
D. Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days.

An employee was terminated, but their access to Google Cloud was not removed until 2 weeks later. You need to find out this employee accessed any sensitive customer information after their termination. What should you do?

A. View System Event Logs in Cloud Logging. Search for the user's email as the principal.
B. View System Event Logs in Cloud Logging. Search for the service account associated with the user.
C. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.
D. View the Admin Activity log in Cloud Logging. Search for the service account associated with the user.

You have deployed an application on a single Compute Engine instance. The application writes logs to disk. Users start reporting errors with the application. You want to diagnose the problem. What should you do?

A. Navigate to Cloud Logging and view the application logs.

B. Connect to the instance's serial console and read the application logs.

C. Configure a Health Check on the instance and set a Low Healthy Threshold value.

D. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

You are asked to set up application performance monitoring on Google Cloud projects A, B, and C as a single pane of glass. You want to monitor CPU, memory, and disk. What should you do?

A. Enable API and then share charts from project A, B, and C.
B. Enable API and then give the metrics.reader role to projects A, B, and C.
C. Enable API and then use default dashboards to view all projects in sequence.
D. Enable API, create a workspace under project A, and then add projects B and C.

Your auditor wants to view your organization's use of data in Google Cloud. The auditor is most interested in auditing who accessed data in Cloud Storage buckets. You need to help the auditor access the data they need. What should you do?

A. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.
B. Assign the appropriate permissions, and then create a Data Studio report on Admin Activity Audit Logs.
C. Assign the appropriate permissions, and then use Cloud Monitoring to review metrics.
D. Use the export logs API to provide the Admin Activity Audit Logs in the format they want.

You are monitoring an application and receive user feedback that a specific error is spiking. You notice that the error is caused by a Service Account having insufficient permissions. You are able to solve the problem but want to be notified if the problem recurs. What should you do?

A. In the Log Viewer, filter the logs on severity 'Error' and the name of the Service Account.
B. Create a sink to BigQuery to export all the logs. Create a Data Studio dashboard on the exported logs.
C. Create a custom log-based metric for the specific error to be used in an Alerting Policy.
D. Grant Project Owner access to the Service Account.

You have sensitive data stored in three Cloud Storage buckets and have enabled data access logging. You want to verify activities for a particular user for these buckets, using the fewest possible steps. You need to verify the addition of metadata labels and which files have been viewed from those buckets. What should you do?

A. Using the GCP Console, filter the Activity log to view the information.

B. Using the GCP Console, filter the Stackdriver log to view the information.

C. View the bucket in the Storage section of the GCP Console.

D. Create a trace in Stackdriver to view the information.

You need to monitor resources that are distributed over different projects in Google Cloud Platform. You want to consolidate reporting under the same Stackdriver Monitoring dashboard. What should you do?

A. Use Shared VPC to connect all projects, and link Stackdriver to one of the projects.

B. For each project, create a Stackdriver account. In each project, create a service account for that project and grant it the role of Stackdriver Account Editor in all other projects.

C. Configure a single Stackdriver account, and link all projects to the same account.

D. Configure a single Stackdriver account for one of the projects. In Stackdriver, create a Group and add the other project names as criteria for that Group.

You developed a web application that lets users upload and share images. You deployed this application in Google Compute Engine and you have configured Stackdriver Logging. Your application sometimes times out while uploading large images, and your application generates relevant error log entries that are ingested to Stackdriver Logging. You would now like to create alerts based on these metrics. You intend to add more compute resources manually when the number of failures exceeds a threshold. What should you do in order to alert based on these metrics with minimal effort?

A. In Stackdriver logging, create a new logging metric with the required filters, edit the application code to set the metric value when needed, and create an alert in Stackdriver based on the new metric.

B. Create a custom monitoring metric in code, edit the application code to set the metric value when needed, create an alert in Stackdriver based on the new metric.

C. In Stackdriver Logging, create a custom monitoring metric from log data and create an alert in Stackdriver based on the new metric.

D. Add the Stackdriver monitoring and logging agent to the instances running the code.

You have a compute engine instance running a production application. You want to receive an email when the instance consumes more than 90% of its CPU resources for more than 15 minutes. You want to use Google services. What should you do?

A. 1. Create a Stackdriver Workspace and associate your GCP project with it.
2. Write a script that monitors the CPU usage and sends it as a custom metric to Stackdriver

3 Create an uptime check for the instance in Stackdriver.

B. 1. Create a consumer Gmail Account
2. Write a script that monitors the CPU usage.
3. When the CPU usage exceeds the threshold, have the script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.

C. 1. Create a Stackdriver Workspace and associate your Google Cloud Platform (GCP) project with it
2. Create an Alerting Policy in Stackdriver that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

D. 1. In Stackdriver logging, create a logs based metric to extract the CPU usage by using a regular expression.
2. In Stackdriver Monitoring, create an Alerting Policy based on this metric
3. Configure your email address in the notification channel.

You have annual audits every year and you need to provide external auditors access to the last 10 years of audit logs. You want to minimize the cost and operational overhead while following Google recommended practices. What should you do? (Select Three)

A. Grant external auditors Storage Object Viewer role on the logs storage bucket.

B. Set a custom retention of 10 years in Stackdriver logging and provide external auditors view access to Stackdriver Logs.

C. Export audit logs to Cloud Storage via an audit log export sink.

D. Export audit logs to BigQuery via an audit log export sink.

E. Export audit logs to Cloud Filestore via a Pub/Sub export sink.

F. Configure a lifecycle management policy on the logs bucket to delete objects older than 10 years

You need to provide a cost estimate for a Kubernetes cluster using the GCP pricing calculator for Kubernetes. Your workload requires high IOPs, and you will also be using disk snapshots. You start by entering the number of nodes, average hours, and average days. What should you do next?

A. Fill in local SSD. Fill in persistent disk storage and snapshot storage.

B. Fill in local SSD. Add estimated cost for cluster management.

C. Select Add GPUs. Fill in persistent disk storage and snapshot storage.

D. Select Add GPUs. Add estimated cost for cluster management.

You need to set a budget alert for use of Compute Engineer services on one of the three Google Cloud Platform projects that you manage. All three projects are linked to a single billing account. What should you do?

A. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

B. Verify that you are the project billing administrator. Select the associated billing account and create a budget and a custom alert.

C. Verify that you are the project administrator. Select the associated billing account and create a budget for the appropriate project.

D. Verify that you are project administrator. Select the associated billing account and create a budget and a custom alert.

Your company publishes large files on an Apache web server that runs on a Compute Engine instance. The Apache web server is not the only application running in the project. You want to receive an email when the egress network costs for the server exceed 100 dollars for the current month as measured by Google Cloud.

What should you do?

A. Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of email

B. Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of email

C. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

D. Use the Cloud Logging Agent to export the Apache web server logs to Cloud Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Cloud Logging for the current month and sends an email if the size of all HTTP responses, multiplied by current Google Cloud egress prices, totals over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

You have designed a solution on Google Cloud that uses multiple Google Cloud products. Your company has asked you to estimate the costs of the solution. You need to provide estimates for the monthly total cost. What should you do?

A. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

B. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Create a Google Sheet that summarizes the expected monthly costs for each product.

C. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Navigate to the Billing Report page in the Cloud Console. Multiply the 1 week cost to determine the monthly costs.

D. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Use Cloud Monitoring to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

You created several resources in multiple Google Cloud projects. All projects are linked to different billing accounts. To better estimate future charges, you want to have a single visual representation of all costs incurred. You want to include new cost data as soon as possible. What should you do?

A. **Configure Billing Data Export to BigQuery and visualize the data in Data Studio.**
B. Visit the Cost Table page to get a CSV export and visualize it using Data Studio.
C. Fill all resources in the Pricing Calculator to get an estimate of the monthly cost.
D. Use the Reports view in the Cloud Billing Console to view the desired cost information.

You are the team lead of a group of 10 developers. You provided each developer with an individual Google Cloud Project that they can use as their personal sandbox to experiment with different Google Cloud solutions. You want to be notified if any of the developers are spending above $500 per month on their sandbox environment. What should you do?
A. Create a single budget for all projects and configure budget alerts on this budget.
B. Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account.
C. Create a budget per project and configure budget alerts on all of these budgets.
D. Create a single billing account for all sandbox projects and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per project.

You have experimented with Google Cloud using your own credit card and expensed the costs to your company. Your company wants to streamline the billing process and charge the costs of your projects to their monthly invoice. What should you do?
A. Grant the financial team the IAM role of Billing Account User on the billing account linked to your credit card.
B. Set up BigQuery billing export and grant your financial department IAM access to query the data.
C. Create a ticket with Google Billing Support to ask them to send the invoice to your company.
D. Change the billing account of your projects to the billing account of your company.

Several employees at your company have been creating projects with Cloud Platform and paying for it with their personal credit cards, which the company reimburses. The company wants to centralize all these projects under a single, new billing account. What should you do?
A. Contact cloud-billing@google.com with your bank account details and request a corporate billing account for your company.

B. Create a ticket with Google Support and wait for their call to share your credit card details over the phone.
C. In the Google Platform Console, go to the Resource Manage and move all projects to the root Organization.
D. In the Google Cloud Platform Console, create a new billing account and set up a payment method.

You want to deploy an application on Cloud Run that processes messages from a Cloud Pub/Sub topic. You want to follow Google-recommended practices. What should you do?

A. 1. Create a Cloud Function that uses a Cloud Pub/Sub trigger on that topic. 2. Call your application on Cloud Run from the Cloud Function for every message.
B. 1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run. 2. Create a Cloud Pub/Sub subscription for that topic. 3. Make your application pull messages from that subscription.
C. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.
D. 1. Deploy your application on Cloud Run on GKE with the connectivity set to Internal. 2. Create a Cloud Pub/Sub subscription for that topic. 3. In the same Google Kubernetes Engine cluster as your application, deploy a container that takes the messages and sends them to your application.

You want to send and consume Cloud Pub/Sub messages from your App Engine application. The Cloud Pub/Sub API is currently disabled. You will use a service account to authenticate your application to the API. You want to make sure your application can use Cloud Pub/Sub. What should you do?

A. Enable the Cloud Pub/Sub API in the API Library on the GCP Console.
B. Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it.
C. Use Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed.
D. Grant the App Engine Default service account the role of Cloud Pub/Sub Admin. Have your application enable the API on the first connection to Cloud Pub/ Sub.

Your customer has implemented a solution that uses Cloud Spanner and notices some read latency-related performance issues on one table. This table is accessed only by their users using a primary key. The table schema is shown below.

```
CREATE TABLE Persons (
  person_id INT64 NOT NULL,  // sequential number based on number of registration
```

```
 account_creation_date DATE, // system date
 birthdate DATE, // customer birthdate
 firstname STRING (255), // first name
 lastname STRING (255), // last name
 profile_picture BYTES (255) // profile picture
) PRIMARY KEY (person_id)
```

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

A. Remove the profile_picture field from the table.
B. Add a secondary index on the personid column.
C. Change the primary key to not have monotonically increasing values.
D. Create a secondary index using the following Data Definition Language (DDL)

```
CREATE INDEX person_id_ix ON Persons (
 person_id,
 firstname,
 lastname
) STORING (
  profile_picture
)
```

You have an application that uses Cloud Spanner as a backend database. The application has a very predictable traffic pattern. You want to automatically scale up or down the number of Spanner nodes depending on traffic. What should you do?

A. Create a cron job that runs on a scheduled basis to review Cloud Monitoring metrics, and then resize the Spanner instance accordingly.
B. Create a Cloud Monitoring alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly.
C. Create a Cloud Monitoring alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.
D. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

You are developing a financial trading application that will be used globally. Data is stored and queried using a relational structure, and clients from all over the world should get the exact identical state of the data. The application will be deployed in multiple regions to provide the lowest latency to end users. You need to select a storage option for the application data while minimizing latency. What should you do?

A. Use Cloud Bigtable for data storage.
B. Use Cloud SQL for data storage.
C. Use Cloud Spanner for data storage.
D. Use Firestore for data storage.

You have just created a new project which will be used to deploy a globally distributed application. You will use Cloud Spanner for data storage. You want to create a Cloud Spanner instance. You want to perform the first step in preparation of creating the instance. What should you do?

A. Enable the Cloud Spanner API.

B. Configure your Cloud Spanner instance to be multi-regional.

C. Create a new VPC network with subnetworks in all desired regions.

D. Grant yourself the IAM role of Cloud Spanner Admin.

You need to manage a Cloud Spanner instance for best query performance. Your instance in production runs in a single Google Cloud region. You need to improve performance in the shortest amount of time. You want to follow Google best practices for service configuration. What should you do?

A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 45%. If you exceed this threshold, add nodes to your instance.

B. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 45%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

C. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

D. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

You have an application that uses Cloud Spanner as a backend database. The application has a very predictable traffic pattern. You want to automatically scale up or down the number of Spanner nodes depending on traffic. What should you do?

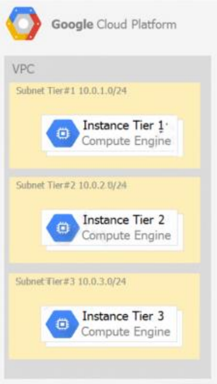
A. Create a cron job that runs on a scheduled basis to review stackdriver monitoring metrics, and then resize the Spanner instance accordingly.

B. Create a Stackdriver alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly.
C. Create a Stackdriver alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.
D. Create a Stackdriver alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

You have production and test workloads that you want to deploy on Compute Engine. Production VMs need to be in a different subnet than the test VMs. All the
VMs must be able to reach each other over Internal IP without creating additional routes. You need to set up VPC and the 2 subnets. Which configuration meets these requirements?

A. Create a single custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range.
B. Create a single custom VPC with 2 subnets. Create each subnet in the same region and with the same CIDR range.
C. Create 2 custom VPCs, each with a single subnet. Create each subnet in a different region and with a different CIDR range.
D. Create 2 custom VPCs, each with a single subnet. Create each subnet in the same region and with the same CIDR range.

Your company has a 3-tier solution running on Compute Engine. The configuration of the current infrastructure is shown below.



Each tier has a service account that is associated with all instances within it. You need to enable communication on TCP port 8080 between tiers as follows:

a. Instances in tier #1 must communicate with tier #2.
b. Instances in tier #2 must communicate with tier #3.

What should you do?

A. 1. Create an ingress firewall rule with the following settings:
Targets: all instances

Source filter: IP ranges (with the range set to 10.0.2.0/24)
Protocols: allow all
2. Create an ingress firewall rule with the following settings:
Targets: all instances
Source filter: IP ranges (with the range set to 10.0.1.0/24)
Protocols: allow all

B. **1. Create an ingress firewall rule with the following settings:**
Targets: all instances with tier #2 service account
Source filter: all instances with tier #1 service account
Protocols: allow TCP:8080
2. Create an ingress firewall rule with the following settings:
Targets: all instances with tier #3 service account
Source filter: all instances with tier #2 service account
Protocols: allow TCP: 8080

C. 1. Create an ingress firewall rule with the following settings:
Targets: all instances with tier #2 service account
Source filter: all instances with tier #1 service account
Protocols: allow all
2. Create an ingress firewall rule with the following settings:
Targets: all instances with tier #3 service account
Source filter: all instances with tier #2 service account
Protocols: allow all

D. 1. Create an egress firewall rule with the following settings:
Targets: all instances
Source filter: IP ranges (with the range set to 10.0.2.0/24)
Protocols: allow TCP: 8080
2. Create an egress firewall rule with the following settings:
Targets: all instances
Source filter: IP ranges (with the range set to 10.0.1.0/24)
Protocols: allow TCP: 8080

You are given a project with a single Virtual Private Cloud (VPC) and a single subnetwork in the us-central1 region. There is a Compute Engine instance hosting an application in this subnetwork. You need to deploy a new instance in the same project in the europe-west1 region. This new instance needs access to the application. You want to follow Google-recommended practices. What should you do?

A. **1. Create a subnetwork in the same VPC, in europe-west1.**
2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

B. 1. Create a VPC and a subnetwork in europe-west1.
2. Expose the application with an internal load balancer.
3. Create the new instance in the new subnetwork and use the load balancer's address as the endpoint.

C. 1. Create a subnetwork in the same VPC, in europe-west1.
   2. Use Cloud VPN to connect the two subnetworks.
   3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.
D. 1. Create a VPC and a subnetwork in europe-west1.
   2. Peer the 2 VPCs.
   3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

You are hosting an application on bare-metal servers in your own data center. The application needs access to Cloud Storage. However, security policies prevent the servers hosting the application from having public IP addresses or access to the internet. You want to follow Google-recommended practices to provide the application with access to Cloud Storage. What should you do?

A. 1. Use nslookup to get the IP address for storage.googleapis.com. 2. Negotiate with the security team to be able to give a public IP address to the servers. 3. Only allow egress traffic from those servers to the IP addresses for storage.googleapis.com.
B. 1. Using Cloud VPN, create a VPN tunnel to a Virtual Private Cloud (VPC) in Google Cloud. 2. In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance. 3. Configure your servers to use that instance as a proxy to access Cloud Storage.
C. 1. Use Migrate for Compute Engine (formerly known as Velostrata) to migrate those servers to Compute Engine. 2. Create an internal load balancer (ILB) that uses storage.googleapis.com as backend. 3. Configure your new instances to use this ILB as proxy.
D. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in Google Cloud. 2. Use Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel. 3. In your on-premises network, configure your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com.

You need to enable traffic between multiple groups of Compute Engine instances that are currently running two different GCP projects. Each group of Compute Engine instances is running in its own VPC. What should you do?

A. Verify that both projects are in a GCP Organization. Create a new VPC and add all instances.
B. Verify that both projects are in a GCP Organization. Share the VPC from one project and reguest that the Compute Engine instances in the other project use this shared VPC.

C. Verify that you are the Project Administrator of both projects. Create two new VPCs and add all instances.
D. Verify that you are the Project Administrator of both projects. Create a new VPC and add all instances.

Your VMs are running in a subnet that has a subnet mask of 255.255.255.240. The current subnet has no more free IP addresses and you require an additional
10 IP addresses for new VMs. The existing and new VMs should all be able to reach each other without additional routes. What should you do?

A. Use gcloud to expand the IP range of the current subnet.
B. Delete the subnet, and recreate it using a wider range of IP addresses.
C. Create a new project. Use Shared VPC to share the current network with the new project.
D. Create a new subnet with the same starting IP but a wider range to overwrite the current subnet.

You deployed an LDAP server on Compute Engine that is reachable via TLS through port 636 using UDP You want to make sure it is reachable by clients over that port. What should you do?

A. Add the network tag allow-udp-636 to the VM instance running the LDAP server.
B. Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server.
C. Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.
D. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag.

Your company's infrastructure is on-premises, but all machines are running at maximum capacity. You want to burst to Google Cloud. The workloads on Google
Cloud must be able to directly communicate to the workloads on-premises using a private IP range. What should you do?

A. In Google Cloud, configure the VPC as a host for Shared VPC.
B. In Google Cloud, configure the VPC for VPC Network Peering.
C. Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses.
D. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Your Dataproc cluster runs in a single Virtual Private Cloud (VPC) network in a single subnet with range 172.16.20.128/25. There are no private IP addresses available in the VPC network. You want to add new VMs to communicate with your cluster using the minimum number of steps. What should you do?

A. Modify the existing subnet range to 172.16.20.0/24.

B. Create a new Secondary IP Range in the VPC and configure the VMs to use that range.
C. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.
D. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

Your company has workloads running on Compute Engine and on-premises. The Google Cloud Virtual Private Cloud (VPC) is connected to your WAN over a
Virtual Private Network (VPN). You need to deploy a new Compute Engine instance and ensure that no public Internet traffic can be routed to it. What should you do?

A. **Create the instance without a public IP address.**
B. Create the instance with Private Google Access enabled.
C. Create a deny-all egress firewall rule on the VPC network.
D. Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

You are working with a user to set up an application in a new VPC behind a firewall. The user is concerned about data egress. You want to configure the fewest open egress ports. What should you do?
A. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.
B. Set up a high-priority (1000) rule that pairs both ingress and egress ports.
C. Set up a high-priority (1000) rule that blocks all egress and a low-priority (65534) rule that allows only the appropriate ports.
D. Set up a high-priority (1000) rule to allow the appropriate ports.

Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google
Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling. What should you do?
A. **Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.**
B. Tag all the instances with the same network tag. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.
C. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.

D. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

Your company has embraced a hybrid cloud strategy where some of the applications are deployed on Google Cloud. A Virtual Private Network (VPN) tunnel connects your Virtual Private Cloud (VPC) in Google Cloud with your company's on-premises network. Multiple applications in Google Cloud need to connect to an on-premises database server, and you want to avoid having to change the IP configuration in all of your applications when the IP of the database changes.
What should you do?

A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances.

B. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

C. Configure the IP of the database as custom metadata for each instance, and query the metadata server.

D. Query the Compute Engine internal DNS from the applications to retrieve the IP of the database.

Your company is moving its entire workload to Compute Engine. Some servers should be accessible through the Internet, and other servers should only be accessible over the internal network. All servers need to be able to talk to each other over specific ports and protocols. The current on-premises network relies on a demilitarized zone (DMZ) for the public servers and a Local Area Network (LAN) for the private servers. You need to design the networking infrastructure on Google Cloud to match these requirements. What should you do?

A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN.
2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

B. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN.
2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public egress traffic for the DMZ.

C. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN.
2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

D. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN.
2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public egress traffic for the DMZ.

You need to create a custom VPC with a single subnet. The subnet's range must be as large as possible. Which range should you use?

A. 0.0.0.0/0

B. 10.0.0.0/8

C. 172.16.0.0/12

D. 192.168.0.0/16

For service discovery, you need to associate each of the Compute Engine instances of your VPC with an internal (DNS) record in a custom zone. You want to follow Google recommended practices. What should you do?

A. Create a new VPC, block all external traffic with a firewall rule and create 2 Cloud DNS zones - a first zone in the new VPC and a second zone in the main VPC that is forwarding requests to the first Cloud DNS zone. Create records for each instance in the first zone.

B. Deploy the BIND DNS server in the VPC, and create a Cloud DNS forwarding zone to forward the DNS requests to BIND. Create records for each instance in the BIND DNS server.

C. Create a Cloud DNS zone, set its visibility to private and associate it with your VPC. Create records for each instance in that zone.

D. Create your Compute Engine instances with custom hostnames.

You have two compute instances in the same VPC but in different regions. You can SSH from one instance to another instance using their external IP address but not their internal IP address. What could be the reason for SSH failing on the internal IP address?

A. The internal IP address is disabled.

B. The combination of compute instance network tags and VPC firewall rules allow SSH from 0.0.0.0 but denies SSH from the VPC subnets IP range.

C. The compute instances are not using the right cross-region SSH IAM permissions

D. The compute instances have a static IP for their internal IP.

You have two compute instances in the same VPC but in different regions. You can SSH from one instance to another instance using their internal IP address but not their external IP address. What could be the reason for SSH failing on external IP address?

A. The combination of compute instance network tags and VPC firewall rules only allow SSH from the subnets IP range.

B. The external IP address is disabled.

C. The compute instances have a static IP for their external IP.

D. The compute instances are not using the right cross-region SSH IAM permissions

Your company has migrated most of the data center VMs to Google Compute Engine. The remaining VMs in the data center host legacy applications that are due to be decommissioned soon and your company has decided to retain them in the datacenter. Due to a change in the business operational model, you need to introduce changes to one of the legacy applications to read files from Google Cloud Storage. However, your data center does not have access to the internet and your company doesn't want to invest in setting up internet access as the data center is due to be turned off soon. Your data center has a partner interconnect to GCP. You wish to route traffic from your datacenter to Google Storage through partner interconnect. What should you do?

A. 1. In on-premises DNS configuration, map storage.cloud.google.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30. 2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel. 3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway. 4. Created a Cloud DNS managed private zone for storage.cloud.google.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

B. 1. In on-premises DNS configuration, map storage.cloud.google.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30. 2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel. 3. Created a Cloud DNS managed public zone for storage.cloud.google.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

C. 1. In on-premises DNS configuration, map *.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30. 2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel. 3. Created a Cloud DNS managed public zone for *.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

D. 1. In on-premises DNS configuration, map *.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30. 2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel. 3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway. 4. Created a Cloud DNS managed private zone for *.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network