1. Question

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?

- gsutil mb -l us-west2 -s nearline --retention 10y gs://logs-archive
- gsutil mb -l los-angeles -s coldline --retention 10m gs://logs-archive
- gsutil mb -l us-west2 -s coldline --retention 10m gs://logs-archive
- **gsutil mb -l us-west2 -s coldline --retention 10y gs://logs-archive**

Unattempted

gsutil mb -l us-west2 -s nearline –retention 10y gs://logs-archive. is not right.
This command creates a bucket that uses nearline storage class whereas we want to use Coldline storage class.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

gsutil mb -l los-angeles -s coldline –retention 10m gs://logs-archive. is not right.
This command uses los-angeles as the location but los-angeles is not a supported region name. The region name for Los Angeles is us-west-2.
Ref: https://cloud.google.com/storage/docs/locations

gsutil mb -l us-west2 -s coldline –retention 10m gs://logs-archive. is not right.
This command creates a bucket with retention set to 10 months whereas we want to retain the objects for 10 years.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

gsutil mb -l us-west2 -s coldline –retention 10y gs://logs-archive. is the right answer.
This command correctly creates a bucket in Los Angeles, uses Coldline storage class and retains objects for 10 years.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

2. Question

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?

- Execute command gcloud iam combineroles --global to combine the 2 roles into a new custom role and grant them globally to SME team group.
- **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.**
- 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-role to promote the role to all other projects and grant the role in each project to the SME team group.
- 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.

Unattempted

We want to create a new role and grant it to a team. Since you want to minimize operational overhead, we need to grant it to a group – so that new users who join the team just need to be added to the group and they inherit all the permissions. Also, this team needs to have the role for all projects in the organization. And since we want to minimize the operational overhead, we need to grant it at the organization level so that all current projects, as well as future projects, have the role granted to them.

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. is not right.
Repeating the step for all projects is a manual, error-prone and time-consuming task. Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead.

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-role to promote the role to all other projects and grant the role in each project to the SME team group. is not right.
Repeating the step for all projects is a manual, error-prone and time-consuming task. Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead.

Execute command gcloud iam combine-roles –global to combine the 2 roles into a new custom role and grant them globally to all. is not right.
There are several issues with this. gcloud iam command doesn't support the action combine-roles. Secondly, we don't want to grant the roles globally. We want to grant them to the SME team and no one else.

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. is the right answer.
This correctly creates the role and assigns the role to the group at the organization. When any new users join the team, the only additional task is to add them to the group. Also, when a new project is created under the organization, no additional human intervention is needed. Since the role is granted at the organization level, it automatically is granted to all the current and future projects belonging to the organization.

.

3. Question

.

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?

.

- 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
- Once the instance starts up, connect over SSH and install the application.
- **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**
- 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

Unattempted

Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template –startup-script=/scripts/install_app.sh. is not right.
gcloud compute instance-templates create command does not accept a flag called –startup-script. While creating compute engine images, the startup script can be provided through a special metadata key called startup-script which specifies a script that will be executed by the instances once they start running. For convenience, –metadata-from-file can be used to pull the value from a file.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instance-templates/create

Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template –metadata-from-file startup-script-url=/scripts/install_app.sh. is not right.
startup-script-url is to be used when contents of the script need to be pulled from a publicly-accessible location on the web. But in this scenario, we are passing the location of the script on the filesystem which doesn't work and the command errors out.
$ gcloud compute instance-templates create app-template –metadata-from-file startup-script-url=/scripts/install_app.sh
ERROR: (gcloud.compute.instance-templates.create) Unable to read file [/scripts/install_app.sh]: [Errno 2] No such file or directory: '/scripts/install_app.sh'

Once the instance starts up, connect over SSH and install the application. is not right.
The managed instances group has auto-scaling enabled. If we are to connect over SSH and install the application, we have to repeat this task on all current instances and on future instances the autoscaler adds to the group. This process is manual, error-prone, time consuming and should be avoided.

Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template –metadata-from-file startup-script=/scripts/install_app.sh. is the right answer.
This command correctly provides the startup script using the flag metadata-from-file and providing a valid startup-script value. When creating compute engine images, the startup script can be provided through a special metadata key called startup-script which specifies a script that will be executed by the instances once they start running. For convenience, –metadata-from-file can be used to pull the value from a file.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instance-templates/create

.

4. Question

.

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?

.

- 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.
- 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.
- **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.**
- 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.

Unattempted

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. is not right.
Both Cloud functions and Cloud Run are serverless offerings from GCP and they are both capable of integrating with Cloud Pub/Sub. It is pointless to invoking Cloud Function from Cloud Run.

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. is not right.
You need to provide Cloud Run Invoker role to that service account for your Cloud Run application.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub

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. is not right.
Like above, you need cloud Run Invoker role on the service account.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub
Also, our question states the application on Cloud Run processes messages from a Cloud Pub/Sub topic; whereas in this option, we are utilizing a separate container to process messages from the topic. So this doesn't satisfy our requirements.

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. is the right answer.
This exact process is described in
https://cloud.google.com/run/docs/tutorials/pubsub
You create a service account.
gcloud iam service-accounts create cloud-run-pubsub-invoker \
–display-name "Cloud Run Pub/Sub Invoker"
You then give the invoker service account permission to invoke your service:
gcloud run services add-iam-policy-binding pubsub-tutorial \
–member=serviceAccount:cloud-run-pubsub-invoker@PROJECT_ID.iam.gserviceaccount.com \
–role=roles/run.invoker
And finally, you create a Pub/Sub subscription with the service account:
gcloud pubsub subscriptions create myRunSubscription –topic myRunTopic \
–push-endpoint=SERVICE-URL/ \
–push-auth-service-account=cloud-run-pubsub-invoker@PROJECT_ID.iam.gserviceaccount

.

5. Question

.

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.

.

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

Unattempted

gcloud compute instances create [INSTANCE_NAME] –preemptible –boot-disk-auto-delete=no. is not right.
gcloud compute instances create doesn't provide a parameter called boot-disk-auto-delete. It does have a flag by the same name. –boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use –no-boot-disk-auto-delete to disable.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

gcloud compute instances create [INSTANCE_NAME] –preemptible. –boot-disk-auto-delete flag is disabled by default. is not right.
–boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use –no-boot-disk-auto-delete to disable.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

gcloud compute instances create [INSTANCE_ NAME] –no-auto-delete. is not right.
gcloud compute instances create doesn't provide a flag called no-auto-delete
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

gcloud compute instances create [INSTANCE_NAME] –preemptible –no-boot-disk-auto-delete. is the right answer.
Use –no-boot-disk-auto-delete to disable automatic deletion of boot disks when the instances are deleted. –boot-disk-auto-delete flag is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. In order to prevent automatic deletion, we have to specify –no-boot-disk-auto-delete flag.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

6. Question

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?

- gcloud compute regions list gcloud images list
- **gcloud compute regions list gcloud compute images list**
- gcloud regions list gcloud images list
- gcloud regions list gcloud compute images list

Unattempted

gcloud regions list.
gcloud images list. is not right.
The correct command to list compute regions is gcloud compute regions list.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/regions/list
The correct command to list compute images is gcloud compute images list.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/images/list

gcloud compute regions list
gcloud images list. is not right.
The correct command to list compute images is gcloud compute images list.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/images/list

gcloud regions list
gcloud compute images list. is not right.
The correct command to list compute regions is gcloud compute regions list.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/regions/list

gcloud compute regions list
gcloud compute images list. is the right answer.
Both the commands correctly retrieve images and regions offered by Google Compute Engine
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/regions/list
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/images/list

7. Question

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?

.

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

Unattempted

Go to the Stackdriver Monitoring console and review information for Cloud Spanner. is not right.
Monitoring collects metrics, events, and metadata from Google Cloud and lets you generate insights via dashboards, charts, and alerts. It can't provide information on when a role has been granted to a user.
Ref: https://cloud.google.com/monitoring/docs

Open the IAM & admin console to review IAM policies for Cloud Spanner roles. is not right.
You can't find the role bindings and the timestamps in the policies.
https://cloud.google.com/iam/docs/overview

Open the Cloud Spanner console to review configurations. is not right.
You manage cloud spanner instances in the console but you can't check when a role has been granted to a user.
Ref: https://cloud.google.com/spanner/docs/quickstart-console

Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles. is the right answer.
Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions. Admin Activity audit logs are always written; you can't configure or disable them. There is no charge for your Admin Activity audit logs.
Ref: https://cloud.google.com/logging/docs/audit#admin-activity
See below a screenshot from GCP console showing this in action.
Among other things, the payload contains
{
action: "ADD"
role: "roles/spanner.admin"
member: "user:testuser@gmail.com"
}

.

8. Question

.

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?

.

- **Cloud Pub/Sub, Cloud Dataflow, BigQuery**
- Cloud Pub/Sub, Cloud Dataflow, Cloud Dataprep
- Stackdriver, Cloud Dataflow, BigQuery
- Cloud Pub/Sub, Cloud Dataflow, Cloud Dataproc

Unattempted

You want to ingest large volumes of streaming data at high speeds. So you need to use Cloud Pub/Sub. Cloud Pub/Sub provides a simple and reliable staging location for your event data on its journey towards processing, storage, and analysis. Cloud Pub/Sub is serverless and you can ingest events at any scale.
Ref: https://cloud.google.com/pubsub

Next, you want to analyze this data. Cloud Dataflow is a fully managed streaming analytics service that minimizes latency, processing time, and cost through autoscaling and batch processing. Dataflow enables fast, simplified streaming data pipeline development with lower data latency.
Ref: https://cloud.google.com/dataflow

Next, you want to store these results. BigQuery is an ideal place to store these results as BigQuery supports the querying of streaming data in real-time. This assists in real-time predictive analytics.
Ref: https://cloud.google.com/bigquery

Therefore the correct answer is Cloud Pub/Sub, Cloud Dataflow, BigQuery

Here's more information from Google docs about the Stream analytics use case. Google recommends we use Dataflow along with Pub/Sub and BigQuery.
https://cloud.google.com/dataflow#section-6
Google's stream analytics makes data more organized, useful, and accessible from the instant it's generated. Built on Dataflow along with Pub/Sub and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights. This abstracted provisioning reduces complexity and makes stream analytics accessible to both data analysts and data engineers.
and
https://cloud.google.com/solutions/stream-analytics
Ingest, process, and analyze event streams in real time. Stream analytics from Google Cloud makes data more organized, useful, and accessible from the instant it's generated. Built on the autoscaling infrastructure of Pub/Sub, Dataflow, and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights.

.

9. Question

.

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?

.

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

Unattempted

gcloud compute instances get –filter="zone:(us-central1-b europe-west1-d)". is not right.
gcloud compute instances command does not support get action.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances

gcloud compute instances get –filter="zone:(us-central1-b)" and gcloud compute instances list –filter="zone:(europe-west1-d)" and combine the results. is not right.

gcloud compute instances command does not support get action.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances

gcloud compute instances list –filter="zone:(us-central1-b)" and gcloud compute instances list –filter="zone:(europe-west1-d)" and combine the results. is not right.
The first command retrieves compute instances from us-central1-b and the second command retrieves compute instances from europe-west1-d. The output from the two statements can be combined to create a full list of instances from us-central1-b and europe-west1-d, however, this is not efficient as it is a manual activity. Moreover, gcloud already provides the ability to list and filter on multiple zones in a single command.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

gcloud compute instances list –filter="zone:(us-central1-b europe-west1-d)". is the right answer.
gcloud compute instances list – lists Google Compute Engine instances. The output includes internal as well as external IP addresses. The filter expression –filter="zone:(us-central1-b europe-west1-d)" is used to filter instances from zones us-central1-b and europe-west1-d.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
Here's a sample output of the command.
$gcloud compute instances list
NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS
gke-cluster-1-default-pool-8c599c87-16g9 us-central1-a n1-standard-1 10.128.0.8 35.184.212.227 RUNNING
gke-cluster-1-default-pool-8c599c87-36xh us-central1-b n1-standard-1 10.129.0.2 34.68.254.220 RUNNING
gke-cluster-1-default-pool-8c599c87-lprq us-central1-c n1-standard-1 10.130.0.13 35.224.96.151 RUNNING

$gcloud compute instances list –filter="zone:(us-central1-b europe-west1-d)"
NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS
gke-cluster-1-default-pool-8c599c87-36xhus-central1-bn1-standard-110.129.0.234.68.254.220RUNNING

.

10. Question

.

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?

.

- **gcloud compute instances list.**
- gcloud compute networks list-ip.
- gcloud compute networks list.
- gcloud compute instances list-ip.

Unattempted

gcloud compute instances list-ip. is not right.
"gcloud compute instances" doesn't support the action list-ip.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

gcloud compute networks list-ip. is not right.
"gcloud compute networks" doesn't support the action list-ip.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/networks/list

gcloud compute networks list. is not right.
"gcloud compute networks list" doesn't list the IP addresses. It is used for listing Google Compute Engine networks (i.e. VPCs)
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/networks/list
Here's a sample output of the command.

$ gcloud compute networks list
NAME SUBNET_MODE BGP_ROUTING_MODE IPV4_RANGE GATEWAY_IPV4
default AUTO REGIONAL
test-vpc CUSTOM REGIONAL

gcloud compute instances list. is the right answer
gcloud compute instances list – lists Google Compute Engine instances. The output includes internal as well as external IP addresses.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
Here's a sample output of the command.
$ gcloud compute instances list
NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS
gke-cluster-1-default-pool-8c599c87-16g9 us-central1-a n1-standard-1 10.128.0.8 35.184.212.227 RUNNING
gke-cluster-1-default-pool-8c599c87-36xh us-central1-a n1-standard-1 10.128.0.6 34.68.254.220 RUNNING
gke-cluster-1-default-pool-8c599c87-lprq us-central1-a n1-standard-1 10.128.0.7 35.224.96.151 RUNNING

.

11. Question

.

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?

.

- 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]
- 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]
- 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]
- **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]**

Unattempted

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]. is not right.
Executing gcloud app deploy –version=[NEW_VERSION] without –no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

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] is not right.
env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex. Also, Executing gcloud app deploy –version=[NEW_VERSION] without –no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

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] is not right.
env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

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] is the right answer.
These commands together achieve the end goal while satisfying our requirements. Setting env: flex in app.yaml and executing gcloud app deploy –no-promote –version=[NEW_VERSION] results in a new version deployed to flex engine. but the new version is not configured to serve traffic. We take the opportunity to review this version before migrating it to serve live traffic by running gcloud app versions migrate [NEW_VERSION]
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate
Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy

.

12. Question

.

You want to persist logs for 10 years to comply with regulatory requirements. You want to follow Google recommended practices. Which Google Cloud Storage class should you use?

.

- **Archive storage class**
- Nearline storage class
- Coldline storage class
- Standard storage class

Unattempted

In April 2019, Google introduced a new storage class “Archive storage class” is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Google previously recommended you use Coldline storage class but the recommendation has since been updated to “Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Note, however, that for data being kept entirely for backup or archiving purposes, Archive Storage is more cost-effective, as it offers the lowest storage costs.”

Ref: https://cloud.google.com/storage/docs/storage-classes#archive
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

So the correct answer is Archive storage class.

.

13. Question

.

You want to reduce storage costs for infrequently accessed data. The data will still be accessed approximately once a month and data older than 2 years is no longer needed. What should you do to reduce storage costs? (Select 2)

.

- **Store infrequently accessed data in a Nearline bucket.**
- **Set an Object Lifecycle Management policy to delete data older than 2 years.**

- Set an Object Lifecycle Management policy to change the storage class to Coldline for data older than 2 years.
- Store infrequently accessed data in a Multi-Regional bucket.
- Set an Object Lifecycle Management policy to change the storage class to Archive for data older than 2 years.

Unattempted

Set an Object Lifecycle Management policy to change the storage class to Coldline for data older than 2 years. is not right.
Data older than 2 years is not needed so there is no point in transitioning the data to Coldline. The data needs to be deleted.

Set an Object Lifecycle Management policy to change the storage class to Archive for data older than 2 years. is not right.
Data older than 2 years is not needed so there is no point in transitioning the data to Archive. The data needs to be deleted.

Store infrequently accessed data in a Multi-Regional bucket. is not right.
While infrequently accessed data can be stored in Multi-Regional bucket, there are several other storage classes offered by Google Cloud Storage that are primarily aimed at storing infrequently accessed data and cost less. Multi-Region buckets are primarily used for achieving geo-redundancy.
Ref: https://cloud.google.com/storage/docs/locations

Set an Object Lifecycle Management policy to delete data older than 2 years. is the right answer.
Since you don't need data older than 2 years, deleting such data is the right approach. You can set a lifecycle policy to automatically delete objects older than 2 years. The policy is valid on current as well as future objects and doesn't need any human intervention.
Ref: https://cloud.google.com/storage/docs/lifecycle

Store infrequently accessed data in a Nearline bucket. is the right answer.
Nearline Storage is a low-cost, highly durable storage service for storing infrequently accessed data. Nearline Storage is ideal for data you plan to read or modify on average once per month or less.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

.

14. Question

.

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 costs. How should you run this reverse proxy?

.

- **Create a Cloud Memorystore for Redis instance with 32-GB capacity.**
- Run it on Compute Engine and choose a custom instance type with 6 vCPUs and 32 GB of memory.
- Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes.
- Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

Unattempted

Requirements
1. latency sensitive
2. 30 GB in-memory cache

3. 2 GB for rest of processes
4. Cost-effective

Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB. is not right.
Fetching data from disk is slower compared to fetching from in-memory. Our requirements state we need 30GB in-memory cache for a latency-sensitive website and a compute engine with disk can't provide in-memory cache.

Run it on Compute Engine and choose a custom instance type with 6 vCPUs and 32 GB of memory. is not right.
While this option provides us with 32 GB of memory, a part of it used by the compute engine operating system as well as the reverse proxy process leaving us with less than 32GB which does not satisfy our requirements. In addition, the reverse proxy consumes almost no CPU so having 6vCPUs is a waste of resources and money.

Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes. is not right.
Without going into details of the feasibility of this option, let's assume for now that this option is possible. But this option is quite expensive. At the time of writing, just the compute cost for a n1-standard-32 instance is $1.5200 per hour in the Iowa region.
Ref: https://cloud.google.com/compute/all-pricing
In comparison, the cost of GCP Cloud Memorystore which is $0.023 per GB-hr which is $0.736 for 32GB per hour. Ref: https://cloud.google.com/memorystore

Create a Cloud Memorystore for Redis instance with 32-GB capacity. is the right answer.
This is the only option that fits the requirements. Cloud Memorystore is a fully managed in-memory data store service for Redis built on scalable, secure, and highly available infrastructure managed by Google. Use Memorystore to build application caches that provide sub-millisecond data access.
Ref: https://cloud.google.com/memorystore
Memorystore for Redis instance pricing is charged per GB-hour and you can scale as needed. You can also specify eviction (maxmemory) policies to restrict the rest of processes to 2GB or the reverse proxy to 30GB or both; you can select a suitable maxmemory policy to handle scenarios when memory is full.
Ref: https://cloud.google.com/memorystore/docs/reference/redis-configs#maxmemory_policies

15. Question

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?

- Select Cloud Spanner. Set up your instance with 2 nodes.
- **Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.**
- Select Cloud SQL (MySQL). Select the create failover replicas option.
- Select Cloud Spanner. Set up your instance as multi-regional.

Unattempted

Requirements
1. Cost effective
2. Relational Data
3. Small set of data
4. One location
5. Point in time recovery

Select Cloud Spanner. Set up your instance with 2 nodes. is not right.
Cloud spanner is a massively scalable, fully managed, relational database service for regional and global application data. Cloud spanner is expensive compared to Cloud SQL. We have a small set of data and we want to be cost-effective, so Cloud Spanner doesn't fit these requirements. Furthermore, Cloud Spanner does not offer a "Point in time" recovery feature.
Ref: https://cloud.google.com/spanner

Select Cloud Spanner. Set up your instance as multi-regional. is not right.
Cloud spanner is a massively scalable, fully managed, relational database service for regional and global application data. Cloud spanner is expensive compared to Cloud SQL. We don't have a requirement for more than "one geographic location" and we also have a small set of data and we want to be cost-effective, so Cloud Spanner doesn't fit these requirements. Furthermore, Cloud Spanner does not offer a "Point in time" recovery feature.
Ref: https://cloud.google.com/spanner

Select Cloud SQL (MySQL). Select the create failover replicas option. is not right.
Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. But This option does not enable point in time recovery so our requirement to support point-in-time recovery is not met.
Ref: https://cloud.google.com/sql/docs/mysql

Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected. is the right answer
Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. And by enabling binary logging, we can enable point-in-time recovery which fits our requirement.
You must enable binary logging to use point-in-time recovery. Point-in-time recovery helps you recover an instance to a specific point in time. For example, if an error causes a loss of data, you can recover a database to its state before the error occurred.
Ref: https://cloud.google.com/sql/docs/mysql/backup-recovery/backups#tips-pitr

.

16. Question

.

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?

.

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

Unattempted

Our requirements are one region, archival after 30 days and data to be accessed annually.

Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage. is not right.
When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region, moreover, this is expensive compared to standard Regional storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard

Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage. is not right.
When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region, moreover, this is expensive compared to standard Regional storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard

Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage. is not right.
While selecting Regional Storage is the right choice, archiving to Nearline is not the most optimal. We have a requirement to access data annually whereas Nearline Storage is ideal for data you plan to read or modify on average once per month or less. Nearline storage is more expensive than Coldline Storage which is more suitable for our requirements.
https://cloud.google.com/storage/docs/storage-classes#nearline

Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage. is the right answer.
Regional Storage is the right fit for our requirements (one geographic region) and archiving to Coldline storage is the most cost-efficient solution. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Since we have a requirement to access data once a quarter and want to go with the most cost-efficient option, we should select Coldline Storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

.

17. Question

.

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?

.

- Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it.
- **Enable the Cloud Pub/Sub API in the API Library on the GCP Console.**
- 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.
- Use the Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed.

Unattempted

Requirements
1. We need to enable Cloud Pub/Sub API
2. Get our application to use the service account.

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. is not right.
APIs are not automatically enabled on the first connection to the service (Cloud Pub/Sub in this scenario). APIs can be enabled through Google Cloud Console, gcloud command-line and REST API.
See https://cloud.google.com/service-usage/docs/enable-disable for more information.

Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it. is not right.
There is no such thing as automatic enablement of the APIs when the service (Cloud Pub/Sub in this scenario) is

accessed. APIs can be enabled through Google Cloud Console, gcloud command-line and REST API.
See https://cloud.google.com/service-usage/docs/enable-disable for more information.

Use the Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed. is not right.
There is no such thing as automatic enablement of the APIs (Cloud Pub/Sub in this scenario) is accessed. APIs can be enabled through Google Cloud Console, gcloud command-line and REST API.
See https://cloud.google.com/service-usage/docs/enable-disable for more information.

Enable the Cloud Pub/Sub API in the API Library on the GCP Console. is the right answer.
For most operational use cases, the simplest way to enable and disable services is to use the Google Cloud Console. you need to create scripts, you can also use the gcloud command-line interface. If you need to program against the Service Usage API, we recommend that you use one of our provided client libraries
Ref: https://cloud.google.com/service-usage/docs/enable-disable
Secondly, after you create an App Engine application, the App Engine default service account is created and used as the identity of the App Engine service. The App Engine default service account is associated with your Cloud project and executes tasks on behalf of your apps running in App Engine. By default, the App Engine default service account has the Editor role in the project so this already has the permissions to push/pull/receive messages from Cloud Pub/Sub

.

18. Question

.

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?

.

- 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
- 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.
- 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.
- **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.**

Unattempted

Our requirement here is to serve content from two backends while following Google recommended practices.

Let's look at each of the options

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. is not right.
We can create a CNAME www.my-new-gcp-ace-website.com pointing to storage.googleapis.com, however, the

cloud storage bucket does not support routing requests to a load balancer based on routing information in a file in the app folder. So this option doesn't work.

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 is not right.
This could possibly work, but we want to follow Google recommended practices and why deploy and manage HAProxy when there might be some other Google product that does exactly the same with minimal configuration (there is !!)?

1. Create a HTTPS Load Balancer in front of the MIG
2. In Cloud DNS in the example.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. is not right.
TXT records are used to verify the domain and TXT records can also hold any arbitrary text but the DNS providers don't use the text in these TXT records for routing.
Ref: https://cloud.google.com/dns/records
Ref: https://support.google.com/cloudidentity/answer/183895?hl=en

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. is the right answer.
Since we need to send requests to multiple backends, Cloud DNS can't alone help us. We need Cloud HTTPS Load Balancer – it's URL maps (a fancy name for path-based routing) helps distribute traffic to backends based on the path information. Ref https://cloud.google.com/load-balancing/docs/url-map
Traffic received by Cloud HTTPS Load Balancer can be configured to send all requests on /app path to the MIG group; and requests on /static/ path to the bucket.
Ref Adding MIG as backend service- https://cloud.google.com/load-balancing/docs/backend-service#backend_services_and_autoscaled_managed_instance_groups.
Ref Adding a backend bucket(s) – https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers
The Load Balancer has a public IP address. But we want to instead access on www.my-new-gcp-ace-website.com, so we configure this as an A Record in our DNS provider. So this option is the right answer.
Ref: https://cloud.google.com/dns/records.

19. Question

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?

- In example.com zone, delete the existing CNAME record and set up an A record instead to point to c.storage.googleapis.com.
- In example.com zone, modify the CNAME record to c.storage.googleapis.com/example-static-website.
- Reload the Cloud Storage static website server to load the objects.

- **Delete the existing bucket, create a new bucket with the name www.example.com and upload the html/css files.**

Unattempted

In example.com zone, modify the CNAME record to c.storage.googleapis.com/example-static-website. is not right.
CNAME records cannot contain paths. There is nothing wrong with the current CNAME record.

In example.com zone, delete the existing CNAME record and set up an A record instead to point to c.storage.googleapis.com. is not right.
A records cannot use hostnames. A records use IP Addresses.

Reload the Cloud Storage static website server to load the objects. is not right.
There is no such thing as a Cloud Storage static website server. All infrastructure that underpins the static websites is handled by Google Cloud Platform.

Delete the existing bucket, create a new bucket with the name http://www.example.com and upload the html/css files. is the right answer.
We need to create a bucket whose name matches the CNAME you created for your domain. For example, if you added a CNAME record pointing http://www.example.com to c.storage.googleapis.com., then create a bucket with the name "www.example.com".A CNAME record is a type of DNS record. It directs traffic that requests a URL from your domain to the resources you want to serve, in this case, objects in your Cloud Storage buckets.
For http://www.example.com, the CNAME record might contain the following information:

NAME TYPE DATA
http://www.example.com CNAME c.storage.googleapis.com.
Ref: https://cloud.google.com/storage/docs/hosting-static-website

.

20. Question

.

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

.

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

Unattempted

Requirements – verify users (i.e. IAM members) and roles.

Run gcloud iam roles list. Review the output section. is not right.
gcloud iam roles list lists the roles but does not list the users (i.e. IAM members)

Run gcloud iam service-accounts list. Review the output section. is not right.
gcloud iam service-accounts list lists the service accounts which are users (i.e. IAM members) but it ignores other users that are not service accounts e.g. users in GSuite domain, or groups etc.

Navigate to the project and then to the Roles section in the GCP Console. Review the roles and status. is not right.
This allows us to review the roles but not users. See the screenshot below.

Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles. is the right answer.
This is the only option that lets us view roles as well as users (members).
Ref: https://cloud.google.com/iam/docs/overview
See the screenshot below.
A member can be a Google Account (for end-users), a service account (for apps and virtual machines), a Google group, or a G Suite or Cloud Identity domain that can access a resource. The identity of a member is an email address associated with a user, service account, or Google group; or a domain name associated with G Suite or Cloud Identity domains

.

21. Question

.

You've deployed a microservice called myapp1 to a Google Kubernetes Engine cluster using the YAML file specified below:
Larger image
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?

.

- 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.
- Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.
- Store the database password inside the Docker image of the container, not in the YAML file.
- **Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.**

Unattempted

Store the database password inside the Docker image of the container, not in the YAML file. is not right.
Baking passwords into Docker images is a very bad idea. Anyone who spins up a container from this image has access to the password.

Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap. is not right.
ConfigMaps are useful for storing and sharing non-sensitive, unencrypted configuration information. To use sensitive information in your clusters, you must use Secrets.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/configmap

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. is not right.
Persistent volumes should not be used for storing sensitive information. PersistentVolume resources are used to manage durable storage in a cluster and PersistentVolumeClaim is a request for and claim to a PersistentVolume resource.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/persistent-volumes

Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret. is the right answer.
In GKE, you can create a secret to hold the password; and then use the secret as an environment variable in the YAML file.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/secret
You can create a secret using kubectl create secret generic passwords –from-literal

myapp1 db password=t0ugh2guess!
And you can then modify the YAML file to reference this secret as shown below.

22. Question

Your company collects and stores CCTV footage videos in raw format in Google Cloud Storage. Within the first 30 days, the footage is processed regularly for detecting patterns such as threat/object/face detection and suspicious behavior detection. You want to minimize the cost of storing all the data in Google Cloud. How should you store the videos?

- Use Google Cloud Nearline Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage.
- **Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage.**
- Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Nearline Storage.
- Use Google Cloud Regional Storage for the first 30 days, and then move videos to Google Persistent Disk.

Unattempted

Footage is processed regularly within the first 30 days and is rarely used after that. So we need to store the videos for the first 30 days in a storage class that supports economic retrieval (for processing) or at no cost, and then transition the videos to a cheaper storage after 30 days.

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Nearline Storage. is not right.
Transitioning the data to Nearline Storage is a good idea as Nearline Storage costs less than standard storage, is highly durable for storing infrequently accessed data and a better choice than Standard Storage in scenarios where slightly lower availability is an acceptable trade-off for lower at-rest storage costs.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline
However, we do not have a requirement to access the data after 30 days; and there are storage classes that are cheaper than nearline storage, so it is not a suitable option.
Ref: https://cloud.google.com/storage/pricing#storage-pricing

Use Google Cloud Regional Storage for the first 30 days, and then move videos to Google Persistent Disk. is not right.
Persistent disk pricing is almost double that of standard storage class in Google Cloud Storage service. Plus the persistent disk can only be accessed when attached to another service such as compute engine, GKE, etc making this option very expensive.
Ref: https://cloud.google.com/storage/pricing#storage-pricing
Ref: https://cloud.google.com/compute/disks-image-pricing#persistentdisk

Use Google Cloud Nearline Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage. is not right.
Nearline storage class is suitable for storing infrequently accessed data and has costs associated with retrieval. Since the footage is processed regularly within the first 30 days, data retrieval costs may far outweigh the savings made by using nearline storage over standard storage class.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline
Ref: https://cloud.google.com/storage/pricing#archival-pricing

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage. is the right answer.
We save the videos initially in Regional Storage (Standard) which does not have retrieval charges so we do not pay

for accessing data within the first 30 days during which the videos are accessed frequently. We only pay for the standard storage costs. After 30 days, we transition the CCTV footage videos to Coldline storage which is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline storage class is cheaper than Nearline storage class.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

.

23. Question

.

Your company has a 3-tier solution running on Compute Engine. The configuration of the current infrastructure is shown below.
Larger image
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:
– Instances in tier #1 must communicate with tier #2.
– Instances in tier #2 must communicate with tier #3.
What should you do?

.

- **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**
- 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
- 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
- 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

Unattempted

This resembles a standard 3 tier architecture – web, application, and database; where the web tier can talk to just the application tier; and the application tier can talk to both the web and database tier. The database tier only accepts requests from the application tier and not the web tier.

We want to ensure that Tier 1 can communicate with Tier 2, and Tier 2 can communicate with Tier 3.

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.

is not right.
We are creating egress rules here which allow outbound communication but not ingress rules which are for inbound traffic.

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.

is not right.
If we create an ingress firewall rule with the settings
– Targets: all instances
– Source filter: IP ranges (with the range set to 10.0.1.0/24)
– Protocols: allow all.
then, we are allowing Tier 1 (10.0.1.0/24) access to all instances – including Tier 3 (10.0.3.0/24) which is not desirable.

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.

is not right.
The first firewall rule ensures that all instances with tier #2 service account i.e. all instances in Subnet Tier #2 (10.0.2.0/24) can be reached from all instances with tier #1 service account i.e. all instances in Subnet Tier #1 (10.0.1.0/24), on all ports. Similarly, the second firewall rule ensures that all instances with tier #3 service account i.e. all instances in Subnet Tier #3 (10.0.3.0/24) can be reached from all instances with tier #2 service account i.e. all instances in Subnet Tier #2 (10.0.2.0/24), on all ports. Though this matches our requirements, we are opening all ports instead of port 8080 which is our requirement. While this solution works, it is not as secure as the other option (see below)

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.

is the right answer.
The first firewall rule ensures that all instances with tier #2 service account i.e. all instances in Subnet Tier #2 (10.0.2.0/24) can be reached from all instances with tier #1 service account i.e. all instances in Subnet Tier #1 (10.0.1.0/24), on port 8080. Similarly, the second firewall rule ensures that all instances with tier #3 service account i.e. all instances in Subnet Tier #3 (10.0.3.0/24) can be reached from all instances with tier #2 service account i.e. all instances in Subnet Tier #2 (10.0.2.0/24), on port 8080. This matches our requirements.

.

24. Question

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?

- **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.**
- 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.
- 1. Create an IAM entry for each data scientist's user account. 2. Assign the BigQuery jobUser role to the group.
- 1. Create an IAM entry for each data scientist's user account. 2. Assign the BigQuery dataViewer user role to the group.

Unattempted

1. Create an IAM entry for each data scientist's user account.
2. Assign the BigQuery dataViewer user role to the group. is not right.
dataViewer provides permissions to Read the dataset's metadata and to list tables in the dataset, and read data and metadata from the dataset's tables. But it does not provide permissions to run jobs, including queries within the project.
Ref: https://cloud.google.com/bigquery/docs/access-control

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. is not right.
dataViewer provides permissions to Read the dataset's metadata and to list tables in the dataset, and read data and metadata from the dataset's tables. But it does not provide permissions to run jobs, including queries within the project.
Ref: https://cloud.google.com/bigquery/docs/access-control

1. Create an IAM entry for each data scientist's user account.
2. Assign the BigQuery jobUser role to the group. is not right.
jobUser is the right role. It provides permissions to run jobs, including queries, within the project. But given that our data science team changes frequently, we do not want to go through this lengthy provisioning and de-provisioning process. Instead, we should be using groups so that provisioning and de-provisioning is as simple as adding/removing the user to/from the group. Google Groups are a convenient way to apply an access policy to a collection of users
Ref: https://cloud.google.com/bigquery/docs/access-control
Ref: https://cloud.google.com/iam/docs/overview#google_group

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. is the right answer.
This is the only option that follows Google recommended practices and meets our requirements. jobUser is the right role. It provides permissions to run jobs, including queries, within the project.
And we want to use a group and grant the group all the necessary roles so that whenever a user joins or leaves, they can be provided access to run big query jobs by simply adding them to the group or removing from the group respectively. Google Groups are a convenient way to apply an access policy to a collection of users
Ref: https://cloud.google.com/bigquery/docs/access-control
Ref: https://cloud.google.com/iam/docs/overview#google_group

25. Question

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?

- Upload the data to BigQuery using the bq command line tool.
- **Upload the data to Cloud Storage using the gsutil command line tool.**
- Upload the data into Cloud SQL using the import function in the console.
- Upload the data into Cloud Spanner using the import function in the console.

Unattempted

The key to answering this question is "unstructured data".

Upload the data to BigQuery using the bq command line tool. is not right.
The bq load command is used to load data in BigQuery from a local data source i.e. local file but the data has to be in a structured format.
bq –location=LOCATION load \
–source_format=FORMAT \
PROJECT_ID:DATASET.TABLE \
PATH_TO_SOURCE \
SCHEMA
where
schema: a valid schema. The schema can be a local JSON file, or it can be typed inline as part of the command. You can also use the –autodetect flag instead of supplying a schema definition.
Ref: https://cloud.google.com/bigquery/docs/loading-data-local#bq

Upload the data into Cloud SQL using the import function in the console. is not right.
Fully managed relational database service for MySQL, PostgreSQL, and SQL Server. As this is relational database, it is for structured data and not fit for unstructured data.
Ref: https://cloud.google.com/sql

Upload the data into Cloud Spanner using the import function in the console. is not right.
Cloud Spanner is the first scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with non-relational horizontal scale. Although Google claims Cloud Spanner is the best of the relational and non-relational worlds, it also says "With Cloud Spanner, you get the best of relational database structure and non-relational database scale and performance with external strong consistency across rows, regions, and continents.". Cloud spanner is for structured data and not fit for unstructured data.
Ref: https://cloud.google.com/spanner

Upload the data to Cloud Storage using the gsutil command line tool. is the right answer.
Cloud storage imposes no such restrictions, you can store large quantities of unstructured data in different file formats. Cloud Storage provides globally unified, scalable, and highly durable object storage for developers and enterprises. In addition, Dataflow can query Cloud Storage filesets as described in this article
Ref: https://cloud.google.com/dataflow/docs/guides/sql/data-sources-destinations#querying-gcs-filesets

26. Question

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 IAM roles and permissions. What should you do?

.

- 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.
- Add the developers and finance managers to the Viewer role for the Project.
- **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.**
- 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.

Unattempted

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. is not right.
Granting your finance team the default IAM role provides them permissions to manage roles and permissions for a project and subsequently use that to assign them the permissions to view/edit resources in all projects. This is against our requirements. Also, you can write a custom role that lets developers view their project spend but they are missing permissions to view project resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

Add the developers and finance managers to the Viewer role for the Project. is not right.
Granting your finance team the Project viewer role lets them view resources in all projects and doesn't let them set budgets – both are against our requirements.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

Add the finance team to the Viewer role on all projects. Add the developers to the Security Reviewer role for each of the billing accounts. is not right.
Granting your finance team the Project viewer role lets them view resources in all projects which is against our requirements. Also, the security Reviewer role enables the developers to view custom roles but doesn't let them view the project's costs or project resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

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. is the right answer.
Billing Account Administrator role is an owner role for a billing account. It provides permissions to manage payment instruments, configure billing exports, view cost information, set budgets, link and unlink projects and manage other user roles on the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access
Project viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data; including viewing the billing charges for the project.
https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

.

27. Question

.

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

.

- In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps.

- **In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.**
- Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps.
- Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications.

Unattempted

In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps. is not right.
The question states that you want to use the company's existing Identity provider for SSO, not Google. Moreover, your users are in Cloud Identity and not in a GSuite domain so they don't have GSuite Gmail accounts and therefore can not sign in through Google.
Ref: https://cloud.google.com/identity/solutions/enable-sso

Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps. is not right.
OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow. See https://oauth.net/2/ for more information about OAuth 2.0 which is quite a popular protocol for SSO. When you sign in to a 3rd party website using Facebook/Twitter/Google, it uses OAuth 2.0 behind the scenes.
Ref: https://cloud.google.com/identity/solutions/enable-sso

Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications. is not right.
OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow. See https://oauth.net/2/ for more information about OAuth 2.0 which is quite a popular protocol for SSO. When you sign in to a 3rd party website using Facebook/Twitter/Google, it uses OAuth 2.0 behind the scenes.
Ref: https://cloud.google.com/identity/solutions/enable-sso

In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider. is the right answer.
This is the only possible option. You configure applications (service providers) to accept SAML assertions from the company's existing identity provider and users in Cloud Identity can sign in to various applications through the third-party single sign-on (SSO) identity provider. It is important to note that user authentication occurs in the third-party IdP so the absence of a Gmail login is not an issue for signing in.
Ref: https://cloud.google.com/identity/solutions/enable-sso
If you have a third-party IdP, you can still configure SSO for third-party apps in the Cloud Identity catalog. User authentication occurs in the third-party IdP, and Cloud Identity manages the cloud apps.
To use Cloud Identity for SSO, your users need Cloud Identity accounts. They sign in through your third-party IdP or using a password on their Cloud Identity accounts.

.

28. Question

.

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?

.

- Cloud SQL
- **Cloud Datastore**
- Cloud Bigtable
- Cloud Dataproc

Unattempted

Cloud SQL. is not right.
Cloud SQL is not suitable for non-relational data. Cloud SQL is a fully-managed database service that makes it easy to set up, maintain, manage, and administer your relational databases on Google Cloud Platform
Ref: https://cloud.google.com/sql/docs

Cloud Dataproc. is not right.
Cloud Dataproc is a fast, easy-to-use, fully managed cloud service for running Apache Spark and Apache Hadoop clusters in a simple, cost-efficient way. It is not a database.
Ref: https://cloud.google.com/dataproc

Cloud Bigtable. is not right.
Bigtable is a petabyte-scale, massively scalable, fully managed NoSQL database service for large analytical and operational workloads. Cloud Bigtable is overkill for our database which is just 10 GB. Also, Cloud Bigtable can't be scaled down to 0, as there is always a cost with the node, SSD/HDD storage etc.
Ref: https://cloud.google.com/bigtable

Cloud Datastore. is the right answer.
Cloud Datastore is a highly-scalable NoSQL database. Cloud Datastore scales seamlessly and automatically with your data, allowing applications to maintain high performance as they receive more traffic; automatically scales back when the traffic reduces.
Ref: https://cloud.google.com/datastore/

.

29. Question

.

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 and you would like to do this as soon as possible. What should you do?

.

- **Link the acquired company's projects to your company's billing account.**
- Configure the acquired company's billing account and your company's billing account to export the billing data into the same BigQuery dataset.
- Migrate the acquired company's projects into your company's GCP organization. Link the migrated projects to your company's billing account.
- 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.

Unattempted

Configure the acquired company's billing account and your company's billing account to export the billing data into the same BigQuery dataset. is not right.
Cloud Billing export to BigQuery enables you to export detailed Google Cloud billing data (such as usage and cost estimate data) automatically throughout the day to a BigQuery dataset that you specify. Then you can access your Cloud Billing data from BigQuery for detailed analysis or use a tool like Google Data Studio to visualize your data. Exporting billing data from both the GCP organizations into a single BigQuery dataset can help you have a single view of the billing information, but it doesn't result in a consolidated invoice, which is our requirement.

Migrate the acquired company's projects into your company's GCP organization. Link the migrated projects to your company's billing account. is not right.
While the result is what we need, migrating projects from the acquired company into your company's GCP organization is not straightforward and takes a lot of time. Our requirements state we would like to do this as soon as possible but this option isn't quick.

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. is not right.
While the result is what we need, migrating projects from both organizations into a new single organization is not straightforward and takes a lot of time. Our requirements state we would like to do this as soon as possible but this option isn't quick.

Link the acquired company's projects to your company's billing account. is the right answer.
This option is the quickest that lets us achieve our end requirement of having all GCP billing in a single invoice.
Linking the acquired company's projects to your company's billing account can be very quick and can be scripted using gcloud.
Ref: https://cloud.google.com/logging/docs/reference/tools/gcloud-logging

30. Question

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?

- Cloud Run
- **Cloud Run for Anthos**
- App Engine Standard
- Cloud Functions

Unattempted

App Engine Standard. is not right.
Google App Engine Standard offers a limited number of runtimes – Java, Node.js, Python, Go, PHP and Ruby; and at the same time doesn't offer support for Websockets.
Ref: https://cloud.google.com/appengine/docs/standard

Cloud Functions. is not right.
Like Google App Engine Standard, Cloud functions offer a limited number of runtimes – Node.js, Python, Go and Java; and doesn't offer support for Websockets.
Ref: https://cloud.google.com/blog/products/application-development/your-favorite-runtimes-now-generally-available-on-cloud-functions

Cloud Run. is not right.
Cloud Run lets you run stateless containers in a fully managed environment. As this is container-based, we are not limited to specific runtimes. Developers can write code using their favorite languages (Go, Python, Java, C#, PHP, Ruby, Node.js, Shell, and others). However, Cloud Run does not support Websockets.
Ref: https://cloud.google.com/run

Cloud Run for Anthos. is the right answer.
Cloud Run for Anthos leverage Kubernetes and serverless together using Cloud Run integrated with Anthos. As this is container-based, we are not limited to specific runtimes. Developers can write code using their favorite languages (Go, Python, Java, C#, PHP, Ruby, Node.js, Shell, and others). Cloud Run for Anthos is the only serverless GCP offering that supports WebSockets.
https://cloud.google.com/serverless-options

31. Question

.

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?

.

- 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
- 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
- 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
- **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**

Unattempted

While Google APIs are accessible on *.googleapis.com, to restrict Private Google Access within a service perimeter to only VPC Service Controls supported Google APIs and services, hosts must send their requests to the restricted.googleapis.com domain name instead of *.googleapis.com. The restricted.googleapis.com domain resolves to a VIP (virtual IP address) range 199.36.153.4/30. This IP address range is not announced to the Internet. If you require access to other Google APIs and services that aren't supported by VPC Service Controls, you can use 199.36.153.8/30 (private.googleapis.com). However, we recommend that you use restricted.googleapis.com, which integrates with VPC Service Controls and mitigates data exfiltration risks. In either case, VPC Service Controls service perimeters are always enforced on APIs and services that support VPC Service Controls.
Ref: https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity

This rules out the two options that map storage.cloud.google.com to restricted.googleapis.com.

The main differences between the remaining two options are
1. Static route in the VPC network.
2. Public/Private zone.

According to Google's guide on setting up private connectivity, in order to configure a route to restricted.googleapis.com within the VPC, we need to create a static route whose destination is 199.36.153.4/30 and whose next hop is the default Internet gateway.

So, the right answer is
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

Here's more information about how to set up private connectivity to Google's services through VPC.
Ref: https://cloud.google.com/vpc/docs/private-access-options#private-vips

In the following example, the on-premises network is connected to a VPC network through a Cloud VPN tunnel. Traffic from on-premises hosts to Google APIs travels through the tunnel to the VPC network. After traffic reaches the VPC network, it is sent through a route that uses the default internet gateway as its next hop. The next hop allows traffic to leave the VPC network and be delivered to restricted.googleapis.com (199.36.153.4/30).

? The on-premises DNS configuration maps *.googleapis.com requests to restricted.googleapis.com, which resolves to the 199.36.153.4/30.
? Cloud Router has been configured to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel by using a custom route advertisement. Traffic going to Google APIs is routed through the tunnel to the VPC network.
? A custom static route was added to the VPC network that directs traffic with the destination 199.36.153.4/30 to the default internet gateway (as the next hop). Google then routes traffic to the appropriate API or service.
If you created a Cloud DNS managed private zone for *.googleapis.com that maps to 199.36.153.4/30 and have authorized that zone for use by your VPC network, requests to anything in the googleapis.com domain are sent to the IP addresses that are used by restricted.googleapis.com

.

32. Question

.

Your company hosts a number of applications in Google Cloud and requires that log messages from all applications be archived for 10 years to comply with local regulatory requirements. Which approach should you use?

.

- **1. Enable Stackdriver Logging API 2. Configure web applications to send logs to Stackdriver 3. Export logs to Google Cloud Storage**
- Grant the security team access to the logs in each Project
- 1. Enable Stackdriver Logging API 2. Configure web applications to send logs to Stackdriver 3. Export logs to BigQuery
- 1. Enable Stackdriver Logging API 2. Configure web applications to send logs to Stackdriver

Unattempted

Grant the security team access to the logs in each Project. is not right.
Granting the security team access to the logs in each Project doesn't guarantee log retention. If the security team is to come up with a manual process to copy all the logs files into another archival source, the ongoing operational costs can be huge.

1. Enable Stackdriver Logging API
2. Configure web applications to send logs to Stackdriver. is not right.
In Stackdriver, application logs are retained by default for just 30 days after which they are purged.
Ref: https://cloud.google.com/logging/quotas
While it is possible to configure a custom retention period of 10 years, storing logs in Stackdriver is very expensive compared to Cloud Storage. Stackdriver charges $.01 per GB per month, whereas something like Cloud Storage Coldline Storage costs $0.007 per GB per month (30% cheaper) and Cloud Storage Archive Storage costs 0.004 per GB per month (60% cheaper than Stackdriver)
Ref: https://cloud.google.com/logging/docs/storage#pricing
Ref: https://cloud.google.com/storage/pricing

The difference between the remaining two options is whether we store the logs in BigQuery or Google Cloud Storage.

1. Enable Stackdriver Logging API
2. Configure web applications to send logs to Stackdriver
3. Export logs to BigQuery. is not right.
While enabling Stackdriver Logging API and having the applications send logs to stack driver is a good start, exporting and storing logs in BigQuery is fairly expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

1. Enable Stackdriver Logging API
2. Configure web applications to send logs to Stackdriver
3. Export logs to Google Cloud Storage. is the right answer.
Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.
Ref: https://cloud.google.com/storage/pricing

.

33. Question

.

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.)

.

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

Unattempted

Once your data is loaded into BigQuery, you are charged for storing it. Storage pricing is based on the amount of data stored in your tables when it is uncompressed. BigQuery doesn't charge for the query execution based on the output of the query (i.e. bytes returned) but on the number of bytes processed (also referred to as bytes read or bytes scanned) in order to arrive at the output of the query. You are charged for the number of bytes processed whether the data is stored in BigQuery or in an external data source such as Cloud Storage, Google Drive, or Cloud Bigtable. On-demand pricing is based solely on usage. You are charged for the bytes scanned even if your query itself doesn't return any data.
Ref: https://cloud.google.com/bigquery/pricing

Split the users from business units to multiple projects. is not right.
The bytes scanned is not expected to go down by splitting the users into multiple projects so this wouldn't reduce/control the costs.
Ref: https://cloud.google.com/bigquery/pricing

Split your BigQuery data warehouse into multiple data warehouses for each business unit. is not right.
The bytes scanned is not expected to go down by splitting the BigQuery warehouse into two so this wouldn't

reduce/control the costs either.
Ref: https://cloud.google.com/bigquery/pricing

Create separate copies of your BigQuery data warehouse for each business unit. is not right.
Creating separate copies of the BigQuery data warehouse for each business unit is going to increase your costs. Not only is this expected to reduce the bytes scanned, but this is also going to increase the storage costs as we are now storing double the amount of data.
Ref: https://cloud.google.com/bigquery/pricing

Apply a user- or project-level custom query quota for BigQuery data warehouse. is the right answer.
BigQuery limits the maximum rate of incoming requests and enforces appropriate quotas on a per-project basis. You can set various limits to control costs such as Concurrent rate limit for interactive queries, Concurrent rate limit for interactive queries against Bigtable external data sources, Concurrent rate limit for legacy SQL queries that contain UDFs, Cross-region federated querying, Daily query size limit, etc.
https://cloud.google.com/bigquery/quotas

Change your BigQuery query model from on-demand to flat rate. Apply the appropriate number of slots to each Project. is the right answer.
This pricing option is best for customers who desire cost predictability. Flat-rate customers purchase dedicated resources for query processing and are not charged for individual queries. BigQuery offers flat-rate pricing for customers who prefer a stable cost for queries rather than paying the on-demand price per TB of data processed. You can choose to use flat-rate pricing using BigQuery Reservations. When you enroll in flat-rate pricing, you purchase slot commitments – dedicated query processing capacity, measured in BigQuery slots. Your queries consume this capacity, and you are not billed for bytes processed. If your capacity demands exceed your committed capacity, BigQuery will queue up slots, and you will not be charged additional fees.
Ref: https://cloud.google.com/bigquery/pricing#flat_rate_pricing

.

34. Question

.

Your company is moving all corporate applications to Google Cloud Platform. The security team wants detailed visibility of all GCP projects in the organization. You provision the Google Cloud Resource Manager and set up yourself as the org admin. What Google Cloud Identity and Access Management (Cloud IAM) roles should you give to the security team?

.

- **Grant roles/resourcemanager.organizationViewer and roles/viewer.**
- Grant roles/resourcemanager.organizationViewer and roles/owner.
- Grant roles/owner, roles/networkmanagement.admin.
- Grant roles/resourcemanager.organizationAdmin and roles/browser.

Unattempted

The security team needs detailed visibility of all GCP projects in the organization so they should be able to view all the projects in the organization as well as view all resources within these projects.

Grant roles/resourcemanager.organizationViewer and roles/owner. is not right.
roles/resourcemanager.organizationViewer role provides permissions to see the organization in the Cloud Console without having access to view all resources in the organization.
roles/owner provides permissions to manage roles and permissions for a project and all resources within the project and set up billing for a project.
Neither of the roles give the security team visibility of the projects in the organization.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

Grant roles/resourcemanager.organizationAdmin and roles/browser. is not right.
roles/resourcemanager.organizationAdmin provides access to administer all resources belonging to the organization. This doesn't follow the least privilege principle. Our security team needs detailed visibility i.e. read-only access but should not be able to administer resources..
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

Grant roles/owner, roles/networkmanagement.admin. is not right.
roles/owner provides permissions to manage roles and permissions for a project and all resources within the project and set up billing for a project.
roles/networkmanagement.admin provides full access to Cloud Network Management resources.
Neither of the roles give the security team visibility of the projects in the organization.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

Grant roles/resourcemanager.organizationViewer and roles/viewer. is the right answer.
roles/viewer provides permissions to view existing resources or data.
roles/resourcemanager.organizationViewer provides access to view an organization.
With the two roles, the security team can view the organization including all the projects and folders; as well as view all the resources within the projects.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

.

35. Question

.

Your company is moving from an on-premises environment to Google Cloud Platform (GCP). 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 GCP quickly and with minimal support effort. What should you do?

.

- 1. Build an instruction guide to install Cassandra on GCP. 2. Make the instruction guide accessible to your developers.
- **1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.**
- 1. Build a Cassandra Compute Engine instance and take a snapshot of it. 2. Use the snapshot to create instances for your developers.
- 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.

Unattempted

1. Build an instruction guide to install Cassandra on GCP.
2. Make the instruction guide accessible to your developers. is not right.
There is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to come up with an installation guide and ask your developers to do it.
Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud
Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

1. Build a Cassandra Compute Engine instance and take a snapshot of it.
2. Use the snapshot to create instances for your developers. is not right.
Like above, there is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.
Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

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. is not right.
Like above, there is a very simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.
Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud
Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

1. Advise your developers to go to Cloud Marketplace.
2. Ask the developers to launch a Cassandra image for their development work. is the right answer.
You can deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. Not only do you get a unified bill for all GCP services, your Developers can now create Cassandra clusters on Google Cloud in minutes and build applications with Cassandra as a database as a service without the operational overhead of managing Cassandra. Each instance is deployed to a separate set of VM instances (at the time of writing this, 3 x VM instance: 4 vCPUs + 26 GB memory (n1-highmem-4) + 10-GB Boot Disk) which are all isolated from the VM instances for other Cassandra deployments.
Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud
Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

.

36. Question

.

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?

.

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

Unattempted

Setup the application using App Engine Standard environment with Cloud Router to connect to an on-premise database. is not right.
Cloud router by itself is not sufficient to connect VPC to an on-premise network. Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP).
Ref: https://cloud.google.com/router

Setup the application using App Engine Flexible environment with Cloud Router to connect to an on-premise database. is not right.
Cloud router by itself is not sufficient to connect VPC to an on-premise network. Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP).
Ref: https://cloud.google.com/router

Setup the application using App Engine Flexible environment with Cloud VPN to connect to an on-premise database. is not right.
You need Cloud VPN to connect VPC to an on-premise network.
Ref: https://cloud.google.com/vpn/docs/concepts/overview
However, we don't have a requirement to run docker containers and App Engine Standard already supports the requirements of our existing web applications, we should avoid using App Engine Flexible. Converting to a container model involves effort and we want to minimize effort.

Setup the application using App Engine Standard environment with Cloud VPN to connect to an on-premise database. is the right answer.
You need Cloud VPN to connect VPC to an on-premise network.
Ref: https://cloud.google.com/vpn/docs/concepts/overview
And since we don't have a requirement to run docker containers, App Engine Standard already supports the requirements of our existing web applications – Java runtime environment, so we should use App Engine Standard

.

37. Question

.

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?

.

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

Unattempted

Use the kubectl run command to run a shell on that container. is not right.
kubectl run creates and runs a deployment. It creates a deployment or a job to manage the created container(s). It is not possible to use kubectl run to connect to an existing container.
https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#run

Use the kubectl run msg-translator-22 /bin/ bash command to run a shell on that container. is not right.
kubectl run creates and runs a deployment. It creates a deployment or a job to manage the created container(s). It is not possible to use kubectl run to connect to an existing container.
https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#run

Use the kubectl exec -it — /bin/bash command to run a shell on that container. is not right.
While kubectl exec is used to execute a command in a container, the command above doesn't quite work because we haven't passed to it the identifier of the container.
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#exec

Use the kubectl exec -it msg-translator-22 — /bin/bash command to run a shell on that container. is the right answer.
kubectl exec is used to execute a command in a container. We pass the container name msg-translator-22 so kubectl exec knows which container to connect to. And we pass the command /bin/bash to it, so it starts a shell on the container and we can then run custom commands and identify the root cause of the issue.
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#exec

38. Question

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)

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

Unattempted

In the bucket advanced settings, select the Customer-supplied key and then select a Cloud KMS encryption key. is not right.
The customer-supplied key is not an option when selecting the encryption method in the console.

Use gsutil with –encryption-key=[ENCRYPTION_KEY] when uploading objects to the bucket. is not right.
gsutil doesn't accept the flag –encryption-key. gsutil can be set up to use an encryption key by modifying boto configuration or by specifying a top-level -o flag but neither of these is included in this option.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key. is the right answer.
Our compliance department wants us to use customer-managed encryption keys. We can select Customer-Managed radio and provide a cloud KMS encryption key to encrypt objects with the customer-managed key. This fit our requirements.

Use gsutil with -o "GSUtil:encryption_key=[KEY_RESOURCE]" when uploading objects to the bucket. is the right answer.
We can have gsutil use an encryption key by using the -o top-level flag: -o "GSUtil:encryption_key=[KEY_RESOURCE]".
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

Modify .boto configuration to include encryption_key = [KEY_RESOURCE] when uploading objects to bucket. is the right answer.
As an alternative to the -o top-level flag, gsutil can also use an encryption key if .boto configuration is modified to specify the encryption key.
encryption_key = [KEY_RESOURCE]
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

39. Question

Your company plans to store sensitive PII 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?

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

Unattempted

In the bucket advanced settings, select Customer-supplied key and then select a Cloud KMS encryption key. is not right.
Customer-Supplied key is not an option when selecting the encryption method in the console. Moreover, we want to use customer managed encryption keys and not customer supplied encryption keys. This does not fit our requirements.

In the bucket advanced settings, select Google-managed key and then select a Cloud KMS encryption key. is not right.
While Google-managed key is an option when selecting the encryption method in console, we want to use customer managed encryption keys and not Google Managed encryption keys. This does not fit our requirements.

Recreate the bucket to use a Customer-managed key. Encryption can only be specified at the time of bucket creation. is not right.
Bucket encryption can be changed at any time. The bucket doesn't have to be recreated to change encryption.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key. is the right answer.
This option correctly selects the Customer-managed key and then the key to use which satisfies our requirement.
See the screenshot below for reference.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

40. Question

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?

- Ask the third-party provider to enable SAML for the application and set the credentials to the service account credentials.
- Ask the third-party provider to enable OAuth 2.0 for the application and set the credentials to the service account credentials.
- Have a single person from the procurement team access document signing system with the service account credentials.

- **Register the application as a password vaulted app and set the credentials to the service account credentials.**

Unattempted

Ask the third-party provider to enable SAML for the application and set the credentials to always use service account credentials. is not right.
The application may or may not support SAML. Moreover, you can't set the credentials in SAML integration to always use a particular account. The authentication is carried out by IdP such as GSuite or a third-party identity provider. Since users are prohibited from sharing the service account credentials, they wouldn't be able to sign in through the IdP with the service account credentials.

Ask the third-party provider to enable OAuth 2.0 for the application and set the credentials to always use service account credentials. is not right.
The application may or may not support OAuth 2.0. Moreover, you can't set the credentials in SAML integration to always use a particular account. The authentication is carried out by IdP such as GSuite or a third-party identity provider. Since users are prohibited from sharing the service account credentials, they wouldn't be able to sign in through the IdP with the service account credentials.

Have a single person from the procurement team access document signing system with the service account credentials. is not right.
While this would prevent password reuse, it goes against our requirements and results in a single person dependency.

Register the application as a password vaulted app and set the credentials to the service account credentials. is the right answer.
As a G Suite or Cloud Identity administrator, the password vaulted apps service enables you to manage access to some of the apps that don't support federation and that are available to users on the User Dashboard. The password vaulted apps service saves login credential sets for applications and assigns those credential sets to users through group association. When a user has access to one of these applications through a group, they can sign in to the application through the user dashboard, or they can sign in directly from the specific application. This functionality is possible by leveraging Chrome or Firefox extensions/plugins. When adding an app to the password vaulted apps service, you can search and choose from the available web-based applications in the app library, or you can add a custom app. You can then manage usernames and passwords safely while providing users in your organization with quick one-click access to all of the apps they already use.
Ref: https://support.google.com/cloudidentity/answer/9178974?hl=en

.

41. Question

.

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 Platform (GCP). What should you do?

.

- Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of email.
- Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of email.
- **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.**
- Use the Stackdriver Logging Agent to export the Apache web server logs to Stackdriver Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Stackdriver for the current month and sends an email if the size of all HTTP responses, multiplied by current GCP egress prices, totals over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

Unattempted

Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of email. is not right.
This budget alert is defined for the project which means it includes all costs and not just the egress network costs – which goes against our requirements; and it also contains costs across all applications and not just the Compute Engine instance containing the Apache web server. While it is possible to set budget scope to include the Product (i.e. Google Compute Engine) and a label that uniquely identifies the specific compute engine instance, the option doesn't mention this.
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of email. is not right.
Like above, but worse as this budget alert includes costs from all projects linked to the billing account. And like above, while it is possible to scope an alert down to Project/Product/Labels, the option doesn't mention this.
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

Use the Stackdriver Logging Agent to export the Apache web server logs to Stackdriver Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Stackdriver for the current month and sends an email if the size of all HTTP responses, multiplied by current GCP egress prices, totals over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly. is not right.
You can't arrive at the exact egress costs with this approach. You can configure apache logs to include the response object size.
Ref: https://httpd.apache.org/docs/1.3/logs.html#common
And you can then do what this option says to arrive at the combined size of all the responses but this is not 100% accurate as it does not include header sizes. Even if we assume the header size is insignificant compare to the large files published on apache web server, our question asks us to do this the Google way "as measured by Google Cloud Platform (GCP)". GCP does not look at the response sizes in the Apache log files to determine the egress costs. The GCP egress calculator takes into consideration the source and destination (source = the region that hosts the Compute Engine instance running Apache Web Server; and the destination is the destination region of the packet). The egress cost is different for different destinations as shown in this pricing reference.
Ref: https://cloud.google.com/vpc/network-pricing#internet_egress
The Apache logs do not give you the destination information and without this information, you can't accurately calculate the egress costs.

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. is the right answer.
This is the only option that satisfies our requirement. We do it the Google way by (re)using the Billing Data that GCP uses. And we scope down the costs to just egress network costs for the apache web server. Finally, we schedule this to run hourly and send an email if the costs exceed 100 dollars.

42. Question

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]', '.']
images: ['gcr.io/[PROJECT_ID]/[IMAGE_NAME]']
How should you execute Cloud build to satisfy these requirements?

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

- **Execute gcloud builds submit --config=[CONFIG_FILE_PATH] --gcs-log-dir=[GCS_LOG_DIR] [SOURCE]**
- Execute gcloud builds submit --config=[CONFIG_FILE_PATH] [SOURCE]
- Execute gcloud builds push --config=[CONFIG_FILE_PATH] [SOURCE]

Unattempted

Execute gcloud builds push –config=[CONFIG_FILE_PATH] [SOURCE]. is not right.
gcloud builds command does not support push operation. The correct operation to build images and push them to gcr is submit.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Execute gcloud builds run –config=[CONFIG_FILE_PATH] –gcs-log-dir=[GCS_LOG_DIR] [SOURCE]. is not right.
gcloud builds command does not support run operation. The correct operation to build images and push them to gcr is submit.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Execute gcloud builds submit –config=[CONFIG_FILE_PATH] [SOURCE]. is not right.
This command correctly builds the container image and pushes the image to GCR (Google Container Registry) but doesn't upload the build logs to Google Cloud Storage which is one of our requirements.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit
Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

Execute gcloud builds submit –config=[CONFIG_FILE_PATH] –gcs-log-dir=[GCS_LOG_DIR] [SOURCE]. is the right answer.
This command correctly builds the container image, pushes the image to GCR (Google Container Registry) and uploads the build logs to Google Cloud Storage.

–config flag specifies the YAML or JSON file to use as the build configuration file.
–gcs-log-dir specifies the directory in Google Cloud Storage to hold build logs.
[SOURCE] is the location of the source to build. The location can be a directory on a local disk or a gzipped archive file (.tar.gz) in Google Cloud Storage.

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit
Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

.

43. Question

.

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?

.

- Import data into Google Cloud SQL.
- Import flat files into Google Cloud Storage.
- Import data into Google Cloud Datastore.
- **Import data into Google BigQuery.**

Unattempted

Import data into Google Cloud SQL. is not right.
Cloud SQL is a fully-managed relational database service. It supports MySQL so the migration of data from your data center to cloud can be straightforward but Google Cloud SQL cannot handle petabyte-scale data. The current second-generation instances limit the storage to approximately 30TB.
Ref: https://cloud.google.com/sql#overview
Ref: https://cloud.google.com/sql/docs/quotas

Import flat files into Google Cloud Storage. is not right.
Cloud Storage is a service for storing objects in Google Cloud. You store objects in containers called buckets. You could export the MySQL data into files and import them into Google Cloud Storage, but it doesn't offer an SQL Interface to run queries/reports.
Ref: https://cloud.google.com/storage/docs/introduction

Import data into Google Cloud Datastore. is not right.
Your business analysts are already familiar with SQL Interface so we need a service that supports SQL. However, Cloud Datastore is a NoSQL document database. Cloud Datastore doesn't support SQL (it supports GQL which is similar to SQL, but not identical).
Ref: https://cloud.google.com/datastore/docs/reference/gql_reference
Ref: https://cloud.google.com/datastore/docs/concepts/overview

Import data into Google BigQuery. is the right answer.
Bigquery is a petabyte-scale serverless, highly scalable, and cost-effective cloud data warehouse that offers blazing-fast speeds, and with zero operational overhead. BigQuery supports a standard SQL dialect that is ANSI:2011 compliant, which reduces the impact and enables a seamless transition for your business analysts.
Ref: https://cloud.google.com/bigquery

.

44. Question

.

Your company set up a complex organizational structure on Google Could Platform. 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?

.

- Add the users to roles/browser role.
- Add the users to roles/iam.roleViewer role.
- **Add the users to a group and add this group to roles/browser role.**
- Add the users to a group and add this group to roles/iam.roleViewer role.

Unattempted

Add the users to roles/iam.roleViewer role. is not right.
roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.
Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to a group and add this group to roles/iam.roleViewer role. is not right.
roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.
Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to roles/browser role. is not right.
roles/browser provides read access to browse the hierarchy for a project, including the folder, organization, and Cloud IAM policy. This role doesn't include permission to view resources in the project. Although this is the role we require, you want to follow Google recommended practices which means we should instead add a group to the role and add users to the group instead of granting the role individually to users.
Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to a group and add this group to roles/browser role. is the right answer.
roles/browser Read access to browse the hierarchy for a project, including the folder, organization, and Cloud IAM policy. This role doesn't include permission to view resources in the project. And you follow Google recommended practices by adding users to the group and group to the role. Groups are a convenient way to apply an access policy to a collection of users. You can grant and change access controls for a whole group at once instead of granting or changing access controls one at a time for individual users or service accounts. You can also easily add members to and remove members from a Google group instead of updating a Cloud IAM policy to add or remove users.
Ref: https://cloud.google.com/iam/docs/understanding-roles
Ref: https://cloud.google.com/iam/docs/overview

.

45. Question

.

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?

.

- 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.
- 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.
- 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.
- **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.**

Unattempted

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. is not right.
Google recommends we apply the security principle of least privilege, where we grant only necessary permissions to access specific resources.
Ref: https://cloud.google.com/iam/docs/overview
Providing these primitive roles at the organization levels grants them permissions on all resources in all projects under the organization which violates the security principle of least privilege.
Ref: https://cloud.google.com/iam/docs/understanding-roles

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. is not right.
Google recommends we apply the security principle of least privilege, where we grant only necessary permissions to access specific resources.
Ref: https://cloud.google.com/iam/docs/overview
Providing these primitive roles at the project level grants them permissions on all resources in the project which violates the security principle of least privilege.
Ref: https://cloud.google.com/iam/docs/understanding-roles

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. is not right.
While this has the intended outcome, it is not very efficient particularly when there are predefined roles that can be used. Secondly, if Google adds/modifies permissions for these services in the future, we would have to update our roles to reflect the modifications. This results in operational overhead and increases costs.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles#primitive-roles-intrinsic
Ref: https://cloud.google.com/bigquery/docs/access-control

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. is the right answer.
For Google Cloud Storage service, Google provides predefined roles roles/owner, roles/editor, roles/viewer that match the access levels we need.
Similarly, Google provides the roles roles/bigquery.dataViewer, roles/bigquery.dataOwner, roles/bigquery.admin that match the access levels we need.
We can assign these predefined IAM roles to the respective users. Should Google add/modify permissions for these services in the future, we don't need to modify the roles above as Google does this for us; and this helps future proof our solution.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles#primitive-roles-intrinsic
Ref: https://cloud.google.com/bigquery/docs/access-control

.

46. Question

.

Your company stores sensitive PII 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?

.

- **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.**
- 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.
- 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.
- 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.

Unattempted

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. is not right.
While changing the bucket encryption to use the Customer-managed key ensures all new objects use this key, existing objects are still encrypted by the Google-managed key. This doesn't satisfy our compliance requirements. Moreover, the customer managed key can't decrypt objects created by Google-managed keys.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

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. is not right.
The customer-supplied key is not an option when selecting the encryption method in the console. Moreover, we want to use customer-managed encryption keys and not customer-supplied encryption keys. This does not fit our requirements.

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. is not right.
While changing the bucket encryption to use the Customer-managed key ensures all new objects use this key, rewriting existing objects before changing the bucket encryption would result in the objects being encrypted by the encryption method in use at that point – which is still Google-managed.

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. is the right answer.
Changing the bucket encryption to use the Customer-managed key ensures all new objects use this key. Now that bucket encryption is changed to use the Customer-managed key, rewrite all existing objects using gsutil rewrite results in objects being encrypted by the new Customer-managed key. This is the only option that satisfies our requirements.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

.

47. Question

.

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?

.

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

Unattempted

Modify the legacy application to use SAML and ask users to sign in through Gmail. is not right.
Modifying a legacy application to use SAML can be quite challenging. In any case, this is a time consuming and error-prone task and is very expensive.

Modify the legacy application to use OAuth 2.0 and ask users to sign in through Gmail. is not right.
Modifying a legacy application to use OAuth 2.0 can be quite challenging. In any case, this is a time consuming and error-prone task and is very expensive.

Synchronize data within your LDAP server with Google Cloud Directory Sync. is not right.
This can be done but this isn't going to help with the legacy LDAP protocol authentication unless the application is modified to work with either Cloud Identity or GSuite. And your company is looking for a cost-effective solution while minimizing developer effort so this isn't suitable.

Use secure LDAP to authenticate the legacy application and ask users to sign in through Gmail. is the right answer.
Secure LDAP enables authentication, authorization, and user/group lookups for LDAP-based apps and IT infrastructure. Secure LDAP uses the same user directory for both SaaS and LDAP-based applications, so people can use the same Cloud Identity credentials they use to log in to services like G Suite and other SaaS apps as they do to log into traditional applications. Applications and IT infrastructure that use LDAP can be simply configured to leverage Cloud Identity's secure LDAP service instead of an existing legacy identity system—end-users don't have to change how they access their apps.
Ref: https://cloud.google.com/blog/products/identity-security/cloud-identity-now-provides-access-to-traditional-apps-with-secure-ldap

48. Question

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?

- **Go to Data Catalog and search for employee_ssn in the search box.**
- Write a shell script that uses the bq command line tool to loop through all the projects in your organization.
- 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.
- 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.

Unattempted

Go to Data Catalog and search for employee_ssn in the search box. is the right answer.
Data Catalog is a fully managed and scalable metadata management service that empowers organizations to quickly discover, understand, and manage all their data. It offers a simple and easy-to-use search interface for data discovery, a flexible and powerful cataloging system for capturing both technical and business metadata, and a strong security and compliance foundation with Cloud Data Loss Prevention (DLP) and Cloud Identity and Access Management (IAM) integrations. The service automatically ingests technical metadata for BigQuery and Cloud Pub/Sub and allows customers to capture business metadata in schematized format via tags, custom APIs, and the UI, offering a simple and efficient way to catalog their data assets. You can perform a search for data assets from the Data Catalog home page in the Google Cloud Console.
See https://cloud.google.com/data-catalog/docs/how-to/search for example.

All other options are manual, error-prone, time-consuming, and should be avoided.

49. Question

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

- **Coldline Storage**
- Multi-Regional Storage
- Regional Storage
- Nearline Storage

Unattempted

The ideal answer to this would have been Archive Storage but that is not one of the options.
Archive Storage is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Your data is available within milliseconds, not hours or days.
https://cloud.google.com/storage/docs/storage-classes#archive

In the absence of Archive Storage, the next best option for storing backups is Coldline Storage.
Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest

storage costs. Coldline Storage is ideal for data you plan to read or modify at most once a quarter.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

Although Nearline, Regional and Multi-Regional can also be used to store the backups, they are expensive in comparison and Google recommends we use Coldline for backups.
More information about Nearline: https://cloud.google.com/storage/docs/storage-classes#nearline
More information about Standard/Regional: https://cloud.google.com/storage/docs/storage-classes#standard
More information about Standard/Multi-Regional: https://cloud.google.com/storage/docs/storage-classes#standard

.

50. Question

.

Your company wants to move 200 TB of your website clickstream logs from your on-premise data center to Google Cloud Platform. These logs need to be retained in GCP for compliance requirements. Your business analysts also want to run analytics on these logs to understand user click behavior on your website. Which of the below would enable you to meet these requirements? (Select Two)

.

- **Load logs into Google BigQuery.**
- Load logs into Google Cloud SQL.
- Import logs into Google Stackdriver.
- Insert logs into Google Cloud Bigtable.
- **Upload log files into Google Cloud Storage.**

Unattempted

Load logs into Google Cloud SQL. is not right.
Cloud SQL is a fully-managed relational database service. Storing logs in Google Cloud SQL is very expensive. Cloud SQL doesn't help us with analytics. Moreover, Google Cloud Platform offers several storage classes in Google Cloud Storage that are more apt for storing logs at a much cheaper cost.
Ref: https://cloud.google.com/sql/docs
Ref: https://cloud.google.com/sql/pricing#sql-storage-networking-prices
Ref: https://cloud.google.com/storage/pricing

Import logs into Google Stackdriver. is not right.
You can push custom logs to Stackdriver and set custom retention periods to store the logs for longer durations. However, Stackdriver doesn't help us with analytics. You could create a sink and export data into Cloud BigQuery for analytics but that is more work. Moreover, Google Cloud Platform offers several storage classes in Google Cloud Storage that are more apt for storing logs at a much cheaper cost.
Ref: https://cloud.google.com/logging
Ref: https://cloud.google.com/storage/pricing

Insert logs into Google Cloud Bigtable. is not right.
Cloud Bigtable is a petabyte-scale, fully managed NoSQL database service for large analytical and operational workloads. Cloud Bigtable can not run analytics by itself. (But when combined with other services to ingest, process, analyze and present, it can help drive analytics) – see the diagram below. So this option is not right.
Ref: https://cloud.google.com/bigtable/

Upload log files into Google Cloud Storage. is the right answer.
Google Cloud Platform offers several storage classes in Google Cloud Storage that are suitable for storing/archiving logs at a reasonable cost.
GCP recommends you use
1. Standard storage class if you need to access objects frequently
2. Nearline storage class if you access infrequently i.e. once a month
3. Coldline storage class if you access even less frequently e.g. once a quarter

4. Archive storage for logs archival.
Ref: https://cloud.google.com/storage/docs/storage-classes

Load logs into Google BigQuery. is the right answer.
By loading logs into Google BigQuery, you can securely run and share analytical insights in your organization with a few clicks. BigQuery's high-speed streaming insertion API provides a powerful foundation for real-time analytics, making your latest business data immediately available for analysis.
Ref: https://cloud.google.com/bigquery#marketing-analytics

51. Question

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 (PII) and sensitive customer information. Your company tax auditors need access to some of these documents. What security strategy would you recommend on GCS?

- **Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.**
- Grant IAM read-only access to users, and use default ACLs on the bucket.
- 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.
- Use signed URLs to generate time-bound access to objects.

Unattempted

Use signed URLs to generate time-bound access to objects. is not right.
When dealing with sensitive customer information such as PII, using signed URLs is not a great idea as anyone with access to the URL has access to PII data. Signed URLs provide time-limited resource access to anyone in possession of the URL, regardless of whether they have a Google account. With PII Data, we want to be sure who has access and signed URLs don't guarantee that.
Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

Grant IAM read-only access to users, and use default ACLs on the bucket. is not right.
We do not need to grant all IAM read-only access to this sensitive data. Just the users who need access to sensitive/PII data should be provided access to this data.

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. is not right.
Enabling public access to the buckets and objects makes them visible to everyone. There are a number of scanning tools out in the market with the sole purpose of identifying buckets/objects that can be reached publicly. Should one of these tools be used by a bad actor to find out our public bucket/objects, it would result in a security breach.

Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket. is the right answer.
We start with no explicit access to any of the IAM users, and the bucket ACLs can then control which users can access what objects. This is the most secure way of ensuring just the people who require access to the bucket are provided with access. We block everyone from accessing the bucket and explicitly provided access to specific users through ACLs.

52. Question

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?

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

Unattempted

In Google Cloud, configure the VPC as a host for Shared VPC. is not right.
Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. This in no way helps us connect to our on-premises network.
Ref: https://cloud.google.com/vpc/docs/shared-vpc

In Google Cloud, configure the VPC for VPC Network Peering. is not right.
Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization. VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally. Traffic stays within Google's network and doesn't traverse the public internet. This doesn't help us connect to our on-premises network.
Ref: https://cloud.google.com/vpc/docs/vpc-peering

Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses. is not right.
Bastion hosts provide an external facing point of entry into a network containing private network instances. Bastion hosts are primarily for end users so they can connect to an instance that does not have an external IP address through a bastion host.
Ref: https://cloud.google.com/compute/docs/instances/connecting-advanced

Set up Cloud VPN between the infrastructure on-premises and Google Cloud. is the right answer.
Cloud VPN securely connects your on-premises network to your Google Cloud (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection.
Ref: https://cloud.google.com/vpn/docs/concepts/overview

53. Question

Your company's test suite is a custom C++ application that runs tests each day on Linux virtual machines. The full test suite takes several hours to complete, running on a limited number of on-premises servers reserved for testing. Your company wants to move the testing infrastructure to Google Cloud Platform. Your company wants to reduce the amount of time it takes to fully test a change to the system while changing the tests as little as possible. Your project manager has asked you to suggest suitable services in Google Cloud and you want to follow Google recommended practices. What should you do?

- Use Google App Engine and Google Stackdriver for logging.
- Use Google Compute Engine unmanaged instance groups with a Network Load Balancer.

- **Use Google Compute Engine managed instance groups and autoscaling.**
- Use Google Cloud Dataproc and run Apache Hadoop jobs to process each test.

Unattempted

Use Google Compute Engine unmanaged instance groups with a Network Load Balancer. is not right.
An unmanaged instance group is a collection of virtual machines (VMs) that reside in a single zone, VPC network, and subnet. An unmanaged instance group is useful for grouping together VMs that require individual configuration settings or tuning. Unmanaged instance group does not autoscale, so it does not help reduce the amount of time it takes to fully test a change to the system.
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

Use Google App Engine and Google Stackdriver for logging. is not right.
App Engine supports many popular languages like Java, PHP, Node.js, Python, C#, .Net, Ruby, and Go. However, C++ isn't supported by App Engine.
Ref: https://cloud.google.com/appengine

Use Google Cloud Dataproc and run Apache Hadoop jobs to process each test. is not right.
Cloud Dataproc is a fast, easy-to-use, fully managed cloud service for running Apache Spark and Apache Hadoop clusters in a simpler, more cost-efficient way. While Dataproc is very efficient at processing ETL and Big Data pipelines, it is not as suitable for running a ruby application that runs tests each day.
Ref: https://cloud.google.com/dataproc

Use Google Compute Engine managed instance groups and autoscaling. is the right answer.
A managed instance group (MIG) contains identical virtual machine (VM) instances that are based on an instance template. MIGs support auto-healing, load balancing, autoscaling, and auto-updating. Managed instance groups offer auto-scaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load. Autoscaling helps your apps gracefully handle increases in traffic and reduce costs when the need for resources is lower. Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).
Ref: https://cloud.google.com/compute/docs/autoscaler/

.

54. Question

.

Your compliance team requested all audit logs are stored for 10 years and to allow access for external auditors to view. You want to follow Google recommended practices. What should you do? (Choose two)

.

- Create an account for auditors to have view access to Stackdriver Logging.
- **Export audit logs to Cloud Storage via an export sink.**
- Export audit logs to BigQuery via an export sink.
- **Generate a signed URL to the Stackdriver export destination for auditors to access.**
- Export audit logs to Splunk via a Pub/Sub export sink.

Unattempted

Create an account for auditors to have view access to Stackdriver Logging. is not right.
While it is possible to configure a custom retention period of 10 years in Stackdriver logging, storing logs in Stackdriver is expensive compared to Cloud Storage. Stackdriver charges $0.01 per GB per month, whereas something like Cloud Storage Coldline Storage costs $0.007 per GB per month (30% cheaper) and Cloud Storage Archive Storage costs 0.004 per GB per month (60% cheaper than Stackdriver)
Ref: https://cloud.google.com/logging/docs/storage#pricing
Ref: https://cloud.google.com/storage/pricing

Export audit logs to BigQuery via an export sink. is not right.
Storing logs in BigQuery is expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

Export audit logs to Cloud Filestore via a Pub/Sub export sink. is not right.
Storing logs in Cloud Filestore is expensive. In Cloud Filestore, Standard Tier pricing costs $0.2 per GB per month and Premium Tier pricing costs $0.3 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

Export audit logs to Cloud Storage via an export sink. is the right answer.
Among all the storage solutions offered by Google Cloud Platform, Cloud storage offers the best pricing for long term storage of logs. Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.
Ref: https://cloud.google.com/storage/pricing

Generate a signed URL to the Stackdriver export destination for auditors to access. is the right answer.
In Google Cloud Storage, you can generate a signed URL to provide limited permission and time to make a request. Anyone who possesses it can use the signed URL to perform specified actions, such as reading an object, within a specified period of time.
In our scenario, we do not need to create accounts for our auditors to provide access to logs in Cloud Storage. Instead, we can generate them signed URLs which are time-bound and lets them access/download log files.
Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

.

55. Question

.

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 registrations
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?

.

- Remove the profile_picture field from the table.
- Add a secondary index on the person_id column.
- **Change the primary key to not have monotonically increasing values.**
- 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)

Unattempted

Change the primary key to not have monotonically increasing values. is the right answer.
You should be careful when choosing a primary key to not accidentally create hotspots in your database. One

cause of hotspots is having a column whose value monotonically increases as the first key part because this results in all inserts occurring at the end of your keyspace. This pattern is undesirable because Cloud Spanner divides data among servers by key ranges, which means all your inserts will be directed at a single server that will end up doing all the work.
Ref: https://cloud.google.com/spanner/docs/schema-design#primary-key-prevent-hotspots

All other options make no sense. The problem is with the monotonically increasing values in the primary key and removing profile_picture or adding a secondary index isn't going to alleviate the problem.

56. Question

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?

- Create a new Compute Engine instance and install Jenkins through the command-line interface.
- Download and deploy the Jenkins Java WAR to App Engine Standard.
- **Use GCP Marketplace to launch the Jenkins solution.**
- Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image.

Unattempted

Create a new Compute Engine instance and install Jenkins through the command line interface. is not right.
While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image. is not right.
While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

Download and deploy the Jenkins Java WAR to App Engine Standard. is not right.
While this is possible, we need to ensure App Engine is enabled, we then need to download the Java project/WAR, and run gcloud app deploy to set up a Jenkins server. This involves more steps than spinning up an instance from GCP Marketplace.
Ref: https://cloud.google.com/appengine/docs/standard/java/tools/uploadinganapp
Ref: https://cloud.google.com/solutions/using-jenkins-for-distributed-builds-on-compute-engine

Use GCP Marketplace to launch the Jenkins solution. is the right answer.
The simplest way to launch a Jenkins server is from GCP Market place. GCP market place has a number of builds available for Jenkins: https://console.cloud.google.com/marketplace/browse?q=jenkins. All you need to do is spin up an instance from a suitable market place build and you have a Jenkins server in a few minutes with just a few clicks.

57. Question

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?

- Add the group for the finance team to roles/billing.user role.
- Add the group for the finance team to roles/billing.admin role.
- **Add the group for the finance team to roles/billing.viewer role.**
- Add the group for the finance team to roles/billing.projectManager role.

Unattempted

Add the group for the finance team to roles/billing.user role. is not right.
This role has very restricted permissions, so you can grant it broadly, typically in combination with Project Creator. These two roles allow a user to create new projects linked to the billing account on which the role is granted.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.admin role. is not right.
This role is an owner role for a billing account. Use it to manage payment instruments, configure billing exports, view cost information, link and unlink projects, and manage other user roles on the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.projectManager role. is not right.
This role allows a user to attach the project to the billing account, but does not grant any rights over resources. Project Owners can use this role to allow someone else to manage the billing for the project without granting them resource access.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.viewer role. is the right answer.
Billing Account Viewer access would usually be granted to finance teams, it provides access to spending information but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

58. Question

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?

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

Unattempted

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. is the right answer.

As described in this article, “My managed instance group keeps failing to create a VM. What’s going on?”
https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances#troubleshooting

The likely causes are
1. A persistent disk already exists with the same name as VM Instance
2. disks.autoDelete option is set to false
3. instance template might be invalid

Therefore, we need to ensure that instance template is valid, disks.autoDelete is turned on, and that there are no existing persistent disks with the same name as VM instance.

59. Question

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?

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

Unattempted

Ask the auditor for their Google account, and give them the Viewer role on the project. is not right.
Since the auditor’s account is not part of your company’s Cloud Identity domain, the auditor can not access resources from your GCP projects. Domain restriction constraint can be used in organization policies to limit resource sharing based on domain. This constraint allows you to restrict the set of identities that are allowed to be used in Cloud Identity and Access Management policies. In this scenario, since we are restricting based on the Cloud Identity domain, only the users in the Cloud Identity domain can access GCP services.
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

Ask the auditor for their Google account, and give them the Security Reviewer role on the project. is not right.
Since the auditor’s account is not part of your company’s Cloud Identity domain, the auditor can not access resources from your GCP projects. Domain restriction constraint can be used in organization policies to limit resource sharing based on domain. This constraint allows you to restrict the set of identities that are allowed to be used in Cloud Identity and Access Management policies. In this scenario, since we are restricting based on the Cloud Identity domain, only the users in the Cloud Identity domain can access GCP services.
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project. is not right.
Creating a temporary account for the auditor in your cloud identity is the right approach as this makes the auditor part of the Cloud identity domain and the organization policy in place lets the auditor access resources. However, the role granted here is not suitable, it provides permissions to list all resources and Cloud IAM policies. Note that list permissions only allow you to list but not view resources. You need to get permission to view the resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#iam-roles

Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project. is the right answer.
The primitive viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data. This fits our requirements.
In addition, adding the auditor to Cloud Identity ensures that Organization Policy for Domain Restricted Sharing doesn't block them from accessing resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_role_definitions

60. Question

Your networks team has set up Google compute network as shown below. In addition, firewall rules in the VPC network have been configured to allow egress to 0.0.0.0/0
Larger image
Which instances have access to Google APIs and Services such as Google Cloud Storage?

- VM A1, VM A2, VM B1
- VM A1, VM A2, VM B1, VM B2
- VM A1, VM A2
- **VM A1, VM A2, VM B2**

Unattempted

VM A1 can access Google APIs and services, including Cloud Storage because its network interface is located in subnet-a, which has Private Google Access enabled. Private Google Access applies to the instance because it only has an internal IP address.

VM B1 cannot access Google APIs and services because it only has an internal IP address and Private Google Access is disabled for subnet-b.

VM A2 and VM B2 can both access Google APIs and services, including Cloud Storage, because they each have external IP addresses. Private Google Access has no effect on whether or not these instances can access Google APIs and services because both have external IP addresses.

So the correct answer is VM A1, VM A2, VM B2

Ref: https://cloud.google.com/vpc/docs/private-access-options#example

61. Question

Your operations team has configured a lifecycle management rule on a bucket. The bucket is multi-regional and has versioning enabled. Which of the following statement accurately reflects the following lifecycle config?
{
"rule":[
{
"action":{
"type":"Delete"
},
"condition":{
"age":60,

```
"isLive":false
}
},
{
"action":{
"type":"SetStorageClass",
"storageClass":"COLDLINE"
},
"condition":{
"age":366,
"matchesStorageClass":"MULTI_REGIONAL"
}
}
]
}
```

.

- Move objects to Coldline Storage after 366 days if the storage class in Multi-regional First rule has no effect on the bucket.
- Archive objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class in Multi-regional.
- Delete objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class in Multi-regional.
- **Delete archived objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class is Multi-regional.**

Unattempted

Archive objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class in Multi-regional. is not right.
The action has "type":"Delete" which means we want to Delete, not archive.
Ref: https://cloud.google.com/storage/docs/managing-lifecycles

Delete objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class in Multi-regional. is not right.
We want to delete objects as indicated by the action, however, we don't want to delete all objects older than 60 days. We only want to delete archived objects as indicated by "isLive":false condition
Ref: https://cloud.google.com/storage/docs/managing-lifecycles

Move objects to Coldline Storage after 366 days if the storage class in Multi-regional. First rule has no effect on the bucket. is not right.
The first rule certainly has an effect. It deletes archived objects older than 60 days.

Delete archived objects older than 60 days and move objects to Coldline Storage after 366 days if the storage class is Multi-regional. is the right answer.
The first part of the rule: The action has "type":"Delete" which means we want to Delete. "isLive":false condition means we are looking for objects that are not Live i.e. objects that are archived. Together, it means we want to delete archived objects older than 60 days. Note that if an object is deleted, it cannot be undeleted. Take care in setting up your lifecycle rules so that you do not cause more data to be deleted than you intend.
Ref: https://cloud.google.com/storage/docs/managing-lifecycles
The second part of the rule: The action indicates we want to set storage class to Coldline. The condition is true if the existing storage class is multi-regional and the age of the object is 366 days or over. Together it means we want to set the storage class to Coldline if existing storage class is multi-regional and age of the object is 366 days or over

.

62. Question

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?

- Add the user to roles/iam.roleAdmin role.
- Add the user to roles/iam.securityAdmin role.
- Add the user to roles/iam.serviceAccountUser role.
- **Add the user to roles/iam.serviceAccountAdmin role.**

Unattempted

Add the user to roles/iam.roleAdmin role. is not right.
roles/iam.roleAdmin is an administrator role that provides access to all custom roles in the project. This doesn't include permissions needed to manage service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#roles-roles

Add the user to roles/iam.securityAdmin role. is not right.
roles/iam.securityAdmin role is a Security admin role, with permissions to get and set any IAM policy. This role is too broad i.e. includes too many permissions and goes against the principle of least privilege. Moreover, although this role provides iam.serviceAccounts.get/list, it doesn't provide iam.serviceAccounts.create, iam.serviceAccounts.delete and iam.serviceAccounts.update permissions that are needed for managing service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#iam-roles

Add the user to roles/iam.serviceAccountUser role. is not right.
roles/iam.serviceAccountUser is a service Account User role which is used for running operations as the service account. This role does not provide the permissions iam.serviceAccounts.create, iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list which are required for managing service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

Add the user to roles/iam.serviceAccountAdmin role. is the right answer.
roles/iam.serviceAccountAdmin is a Service Account Admin role that lets you Create and manage service accounts. This grants all the required permissions for managing service accounts (iam.serviceAccounts.create iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list etc) and therefore fits our requirements.
Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

63. Question

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?

- Add your SREs to roles/iam.roleAdmin role.
- Add your SREs to roles/accessapproval.approver role.
- Add your SREs to a group and then add this group to roles/iam.roleAdmin role.
- **Add your SREs to a group and then add this group to roles/accessapproval.approver role.**

Unattempted

Add your SREs to roles/iam.roleAdmin role. is not right.
roles/iam.roleAdmin provides access to all custom roles in the project. This doesn't fit our requirement of SREs being able to approve requests.

Add your SREs to a group and then add this group to roles/iam.roleAdmin role. is not right.
roles/iam.roleAdmin provides access to all custom roles in the project. This doesn't fit our requirement of SREs being able to approve requests.

Add your SREs to roles/accessapproval.approver role. is not right.
roles/accessapproval.approver is an Access Approval Approver role and provides the ability to view or act on access approval requests and view configuration. Although this is the role we require, you want to follow Google recommended practices which means we should instead add the group to the role and add users to the group instead of granting the role individually to users.
Ref: https://cloud.google.com/iam/docs/understanding-roles#access-approval-roles
Ref: https://cloud.google.com/iam/docs/overview

Add your SREs to a group and then add this group to roles/accessapproval.approver role. is the right answer.
roles/accessapproval.approver is an Access Approval Approver role and provides the ability to view or act on access approval requests and view configuration. And you follow Google recommended practices by adding users to the group and group to the role. Groups are a convenient way to apply an access policy to a collection of users. You can grant and change access controls for a whole group at once instead of granting or changing access controls one at a time for individual users or service accounts. You can also easily add members to and remove members from a Google group instead of updating a Cloud IAM policy to add or remove users.
Ref: https://cloud.google.com/iam/docs/understanding-roles#access-approval-roles
Ref: https://cloud.google.com/iam/docs/overview

.

64. Question

.

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?

.

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

Unattempted

Use the cloud Identity APIs and write a script to synchronize users to Cloud Identity. is not right.
You could do this, but this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console. is not right.
You could do this, but like above this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

Ask each employee to create a Google account using self signup. Require that each employee use their company email address and password. is not right.
If you let employees create accounts, your organization no longer has full control over the Google accounts used. This approach has several other issues with respect to creating/managing user accounts and should be avoided.

65. Question

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?

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

Unattempted

Create an export to the sink that saves logs from Cloud Audit to BigQuery. is not right.
You can export logs into BigQuery by creating one or more sinks that include a logs query and an export destination (big query). However, this option is very expensive compared to the cost of Cloud Storage.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

Write a custom script that uses logging API to copy the logs from Stackdriver logs to BigQuery. is not right.
Stackdriver already offers sink exports that let you copy logs from Stackdriver logs to BigQuery. While BigQuery is already quite expensive compared to Cloud Storage, coming up with a custom script and maintaining it to copy the logs from Stackdriver logs to BigQuery is going to add to the cost. This option is very inefficient and expensive.

Export these logs to Cloud Pub/Sub and write a Cloud Dataflow pipeline to store logs to Cloud SQL. is not right.
Cloud SQL is primarily used for storing relational data. Storing huge quantities of logs in Cloud SQL is very expensive compared to Cloud Storage. And add to it the fact that you also need to pay for Cloud Pub/Sub and Cloud Dataflow pipeline, and this option gets very expensive very soon.

Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket. is the right answer.
Coldline Storage is the perfect service to store audit logs from all the projects and is very cost-efficient as well. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline Storage is ideal for data you plan to read or modify at most once a quarter.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

66. Question

Your organization is planning the infrastructure for a new large-scale application that will need to store anything between 200 TB to a petabyte of data in NoSQL format for Low-latency read/write and High-throughput analytics. Which storage option should you use?

.

- Cloud SQL.
- **Cloud Bigtable.**
- Cloud Datastore.
- Cloud Spanner.

Unattempted

Cloud Spanner. is not right.
Cloud Spanner is not a NoSQL database. Cloud SQL is a fully-managed relational database service.
Ref: https://cloud.google.com/sql/docs

Cloud SQL. is not right.
Cloud SQL is not a NoSQL database. Cloud Spanner is a highly scalable, enterprise-grade, globally-distributed, and strongly consistent relational database service
Ref: https://cloud.google.com/spanner

Cloud Datastore. is not right.
While Cloud Datastore is a highly scalable NoSQL database, it can't handle petabyte-scale data.
https://cloud.google.com/datastore

Cloud Bigtable. is the right answer.
Cloud Bigtable is a petabyte-scale, fully managed NoSQL database service for large analytical and operational workloads.
Ref: https://cloud.google.com/bigtable/

.

67. Question

.

Your organization is planning to deploy a Python web application to Google Cloud. The web application uses a custom Linux distribution and you want to minimize rework. The web application underpins an important website that is accessible to the customers globally. You have been asked to design a solution that scales to meet demand. What would you recommend to fulfill this requirement? (Select Two)

.

- **HTTP(S) Load Balancer**
- App Engine Standard environment
- Cloud Functions
- **Managed Instance Group on Compute Engine**
- Network Load Balance

Unattempted

Requirements are – use custom Linux distro, global access, auto scale.

Cloud Functions. is not right.
Cloud Functions is a serverless compute platform. You can not use a custom Linux distribution with Cloud Functions. Ref: https://cloud.google.com/functions

App Engine Standard environment. is not right.
The App Engine Standard Environment is based on container instances running on Google's infrastructure. Containers are preconfigured with one of several available runtimes such as Python, Java, NodeJS, PHP, Ruby,

GO etc. It is not possible to specify a custom Linux distribution with App Engine Standard.
Ref: https://cloud.google.com/appengine/docs/standard

Network Load Balance. is not right.
The external (TCP/UDP) Network Load Balancing is a regional load balancer. Since we need to cater to a global user base, this load balancer is not suitable.
Ref: https://cloud.google.com/load-balancing/docs/network

HTTP(S) Load Balancer. is the right answer.
HTTP(S) Load Balancing is a global service (when the Premium Network Service Tier is used). We can create backend services in more than one region and have them all serviced by the same global load balancer
Ref: https://cloud.google.com/load-balancing/docs/https

Managed Instance Group on Compute Engine. is the right answer.
Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An autohealing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.
Ref: https://cloud.google.com/compute/docs/instance-groups

.

68. Question

.

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?

.

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

Unattempted

Add users to roles/bigquery.dataEditor role only, instead of roles/bigquery.dataOwner. is not right.
roles/bigquery.dataEditor is a BigQuery Data Editor role which when applied to a dataset provides permissions to read the dataset's metadata and to list tables in the dataset; Create, update, get, and delete the dataset's tables. When applied at the project or organization level, this role can also create new datasets. We want to grant users access to query but not modify/delete.

Create a custom role by removing delete permissions, and add users to that role only. is not right.
This might work but this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role. is not right.
This might work but like above this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

Add users to roles/bigquery.user role only, instead of roles/bigquery.dataOwner. is the right answer.
roles/bigquery.user is a BigQuery User role which when applied to a project provides the ability to run jobs, including queries, within the project. A member with this role can enumerate their own jobs, cancel their own jobs,

and enumerate datasets within a project.
Ref: https://cloud.google.com/iam/docs/understanding-roles#bigquery-roles

69. Question

Your organization processes a very high volume of timestamped IoT data. The total volume can be several petabytes. The data needs to be written and changed at a high speed. You want to use the most performant storage option for your data. Which product should you use?

- BigQuery
- **Cloud Bigtable**
- Cloud Storage
- Cloud Datastore

Unattempted

Our requirement is to write/update a very high volume of data at a high speed. Performance is our primary concern, not cost.

Cloud Bigtable is the right answer.
Cloud Bigtable is Google's flagship product for ingest and analyze large volumes of time series data from sensors in real-time, matching the high speeds of IoT data to track normal and abnormal behavior.
Ref: https://cloud.google.com/bigtable/

While all other options are capable of storing high volumes of the order of petabytes, they are not as efficient as Bigtable at processing IoT time-series data.

70. Question

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?

- Enable Cloud Identity in the GCP Console for your domain.
- **Grant them the required IAM roles using their G Suite email address.**
- Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.
- 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.