



# Google

## Exam Questions Associate-Cloud-Engineer

Google Cloud Certified - Associate Cloud Engineer

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

You recently discovered that your developers are using many service account keys during their development process. While you work on a long term improvement, you need to quickly implement a process to enforce short-lived service account credentials in your company. You have the following requirements:

- All service accounts that require a key should be created in a centralized project called pj-sa.
- Service account keys should only be valid for one day.

You need a Google-recommended solution that minimizes cost. What should you do?

- A. Implement a Cloud Run job to rotate all service account keys periodically in pj-s
- B. Enforce an org policy to deny service account key creation with an exception to pj-sa.
- C. Implement a Kubernetes Cronjob to rotate all service account keys periodical
- D. Disable attachment of service accounts to resources in all projects with an exception to pj-sa.
- E. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hour
- F. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.
- G. Enforce a DENY org policy constraint over the lifetime of service account keys for 24 hour
- H. Disable attachment of service accounts to resources in all projects with an exception to pj-sa.

**Answer: C**

#### Explanation:

According to the Google Cloud documentation, you can use organization policy constraints to control the creation and expiration of service account keys. The constraints are:

➤ constraints/iam.allowServiceAccountKeyCreation: This constraint allows you to specify which projects or folders can create service account keys. You can set the value to true or false, or use a condition to apply the constraint to specific service accounts. By setting this constraint to false for the organization and adding an exception for the pj-sa project, you can prevent developers from creating service account keys in other projects.

➤ constraints/iam.serviceAccountKeyMaxLifetime: This constraint allows you to specify the maximum lifetime of service account keys. You can set the value to a duration in seconds, such as 86400 for one day. By setting this constraint to 86400 for the organization, you can ensure that all service account keys expire after one day.

These constraints are recommended by Google Cloud as best practices to minimize the risk of service account key misuse or compromise. They also help you reduce the cost of managing service account keys, as you do not need to implement a custom solution to rotate or delete them.

References:

- 1: Associate Cloud Engineer Certification Exam Guide | Learn - Google Cloud
- 5: Create and delete service account keys - Google Cloud
- Organization policy constraints for service accounts

### NEW QUESTION 2

Your coworker has helped you set up several configurations for gcloud. You've noticed that you're running commands against the wrong project. Being new to the company, you haven't yet memorized any of the projects. With the fewest steps possible, what's the fastest way to switch to the correct configuration?

- A. Run gcloud configurations list followed by gcloud configurations activate .
- B. Run gcloud config list followed by gcloud config activate.
- C. Run gcloud config configurations list followed by gcloud config configurations activate.
- D. Re-authenticate with the gcloud auth login command and select the correct configurations on login.

**Answer: C**

#### Explanation:

as gcloud config configurations list can help check for the existing configurations and activate can help switch to the configuration.

gcloud config configurations list lists existing named configurations

gcloud config configurations activate activates an existing named configuration

Obtains access credentials for your user account via a web-based authorization flow. When this command completes successfully, it sets the active account in the current configuration to the account specified. If no configuration exists, it creates a configuration named default.

### NEW QUESTION 3

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

- A. Use Shared VPC to connect all projects, and link Stackdriver to one of the projects.
- B. For each project, create a Stackdriver account
- C. In each project, create a service account for that project and grant it the role of Stackdriver Account Editor in all other projects.
- D. Configure a single Stackdriver account, and link all projects to the same account.
- E. Configure a single Stackdriver account for one of the project
- F. In Stackdriver, create a Group and add the other project names as criteria for that Group.

**Answer: C**

#### Explanation:

When you initially click on Monitoring(Stackdriver Monitoring) it creates a workspace(a stackdriver account) linked to the ACTIVE(CURRENT) Project from which it was clicked.

Now if you change the project and again click onto Monitoring it would create an another workspace(a stackdriver account) linked to the changed ACTIVE(CURRENT) Project, we don't want this as this would not consolidate our result into a single dashboard(workspace/stackdriver account).

If you have accidentally created two diff workspaces merge them under Monitoring > Settings > Merge Workspaces > MERGE.

If we have only one workspace and two projects we can simply add other GCP Project under Monitoring > Settings > GCP Projects > Add GCP Projects.

<https://cloud.google.com/monitoring/settings/multiple-projects>

Nothing about groups <https://cloud.google.com/monitoring/settings?hl=en>

#### NEW QUESTION 4

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

- A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances.
- B. Create a private zone on Cloud DNS, and configure the applications with the DNS name.
- C. Configure the IP of the database as custom metadata for each instance, and query the metadata server.
- D. Query the Compute Engine internal DNS from the applications to retrieve the IP of the database.

**Answer: B**

#### Explanation:

Forwarding zones Cloud DNS forwarding zones let you configure target name servers for specific private zones. Using a forwarding zone is one way to implement outbound DNS forwarding from your VPC network. A Cloud DNS forwarding zone is a special type of Cloud DNS private zone. Instead of creating records within the zone, you specify a set of forwarding targets. Each forwarding target is an IP address of a DNS server, located in your VPC network, or in an on-premises network connected to your VPC network by Cloud VPN or Cloud Interconnect.

<https://cloud.google.com/nat/docs/overview>

DNS configuration Your on-premises network must have DNS zones and records configured so that Google domain names resolve to the set of IP addresses for either private.googleapis.com or restricted.googleapis.com. You can create Cloud DNS managed private zones and use a Cloud DNS inbound server policy, or you can configure on-premises name servers. For example, you can use BIND or Microsoft Active Directory DNS.

<https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid#config-domain>

#### NEW QUESTION 5

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

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

**Answer: D**

#### Explanation:

➤ The Datastore emulator provides local emulation of the production Datastore environment. You can use the emulator to develop and test your application locallyRef: <https://cloud.google.com/datastore/docs/tools/datastore-emulator>

#### NEW QUESTION 6

You have an on-premises data analytics set of binaries that processes data files in memory for about 45 minutes every midnight. The sizes of those data files range from 1 gigabyte to 16 gigabytes. You want to migrate this application to Google Cloud with minimal effort and cost. What should you do?

- A. Upload the code to Cloud Function
- B. Use Cloud Scheduler to start the application.
- C. Create a container for the set of binarie
- D. Use Cloud Scheduler to start a Cloud Run job for the container.
- E. Create a container for the set of binaries Deploy the container to Google Kubernetes Engine (GKE) and use the Kubernetes scheduler to start the application.
- F. Lift and shift to a VM on Compute Engin
- G. Use an instance schedule to start and stop the instance.

**Answer: B**

#### NEW QUESTION 7

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

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

**Answer: B**

#### Explanation:

"large quantity" : Cloud Storage or BigQuery "files" a file is nothing but an Object

#### NEW QUESTION 8

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

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

**Answer:** C

**Explanation:**

<https://gtseres.medium.com/using-service-accounts-across-projects-in-gcp-cf9473fef8f0>

You create the service account in proj-sa and take note of the service account email, then you go to proj-vm in IAM > ADD and add the service account's email as new member and give it the Compute Storage Admin role.

<https://cloud.google.com/compute/docs/access/iam#compute.storageAdmin>

**NEW QUESTION 9**

Your company runs its Linux workloads on Compute Engine instances. Your company will be working with a new operations partner that does not use Google Accounts. You need to grant access to the instances to your operations partner so they can maintain the installed tooling. What should you do?

- A. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.
- B. Tag all the instances with the same network tag
- C. Create a firewall rule in the VPC to grant TCP access on port 22 for traffic from the operations partner to instances with the network tag.
- D. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.
- E. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

**Answer:** D

**Explanation:**

IAP controls access to your App Engine apps and Compute Engine VMs running on Google Cloud. It leverages user identity and the context of a request to determine if a user should be allowed access. IAP is a building block toward BeyondCorp, an enterprise security model that enables employees to work from untrusted networks without using a VPN.

By default, IAP uses Google identities and IAM. By leveraging Identity Platform instead, you can authenticate users with a wide range of external identity providers, such as:

Email/password

OAuth (Google, Facebook, Twitter, GitHub, Microsoft, etc.) SAML

OIDC

Phone number Custom Anonymous

This is useful if your application is already using an external authentication system, and migrating your users to Google accounts is impractical.

<https://cloud.google.com/iap/docs/using-tcp-forwarding#grant-permission>

**NEW QUESTION 10**

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

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

**Answer:** B

**Explanation:**

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.

**NEW QUESTION 10**

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

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

**Answer:** A

**Explanation:**

Quickstart: using the Google Cloud Console

This page shows you how to perform basic tasks in Pub/Sub using the Google Cloud Console. Note: If you are new to Pub/Sub, we recommend that you start with the interactive tutorial. Before you begin

Set up a Cloud Console project. Set up a project

Click to:

Create or select a project.

Enable the Pub/Sub API for that project.

You can view and manage these resources at any time in the Cloud Console. Install and initialize the Cloud SDK.

Note: You can run the gcloud tool in the Cloud Console without installing the Cloud SDK. To run the gcloud tool in the Cloud Console, use Cloud Shell .

<https://cloud.google.com/pubsub/docs/quickstart-console>

**NEW QUESTION 15**

You want to add a new auditor to a Google Cloud Platform project. The auditor should be allowed to read, but not modify, all project items.

How should you configure the auditor's permissions?

- A. Create a custom role with view-only project permission
- B. Add the user's account to the custom role.

- C. Create a custom role with view-only service permission
- D. Add the user's account to the custom role.
- E. Select the built-in IAM project Viewer rol
- F. Add the user's account to this role.
- G. Select the built-in IAM service Viewer rol
- H. Add the user's account to this role.

**Answer:** C

#### NEW QUESTION 19

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

- A. Verify that you are the project billing administrato
- B. Select the associated billing account and create a budget and alert for the appropriate project.
- C. Verify that you are the project billing administrato
- D. Select the associated billing account and create a budget and a custom alert.
- E. Verify that you are the project administrato
- F. Select the associated billing account and create a budget for the appropriate project.
- G. Verify that you are project administrato
- H. Select the associated billing account and create a budget and a custom alert.

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 21

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

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

**Answer:** C

#### Explanation:

"Billing Account Viewer access would usually be granted to finance teams, it provides access to spend information, but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account." <https://cloud.google.com/billing/docs/how-to/billing-access>

#### NEW QUESTION 23

You have been asked to set up the billing configuration for a new Google Cloud customer. Your customer wants to group resources that share common IAM policies. What should you do?

- A. Use labels to group resources that share common IAM policies
- B. Use folders to group resources that share common IAM policies
- C. Set up a proper billing account structure to group IAM policies
- D. Set up a proper project naming structure to group IAM policies

**Answer:** B

#### Explanation:

Folders are nodes in the Cloud Platform Resource Hierarchy. A folder can contain projects, other folders, or a combination of both. Organizations can use folders to group projects under the organization node in a hierarchy. For example, your organization might contain multiple departments, each with its own set of Google Cloud resources. Folders allow you to group these resources on a per-department basis. Folders are used to group resources that share common IAM policies. While a folder can contain multiple folders or resources, a given folder or resource can have exactly one parent.

<https://cloud.google.com/resource-manager/docs/creating-managing-folders>

#### NEW QUESTION 25

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

- A. Use the command `gcloud auth login` and point it to the private key
- B. Use the command `gcloud auth activate-service-account` and point it to the private key
- C. Place the private key file in the installation directory of the Cloud SDK and rename it to "credentials ison"
- D. Place the private key file in your home directory and rename it to "GOOGLE\_APPUCATION\_CREDENTIALS".

**Answer:** B

#### Explanation:

Authorizing with a service account

`gcloud auth activate-service-account` authorizes access using a service account. As with `gcloud init` and `gcloud auth login`, this command saves the service account credentials to the local system on successful completion and sets the specified account as the active account in your Cloud SDK configuration.

[https://cloud.google.com/sdk/docs/authorizing#authorizing\\_with\\_a\\_service\\_account](https://cloud.google.com/sdk/docs/authorizing#authorizing_with_a_service_account)

#### NEW QUESTION 26

Your company's security vulnerability management policy wants 3 member of the security team to have visibility into vulnerabilities and other OS metadata for a specific Compute Engine instance. This Compute Engine instance hosts a critical application in your Google Cloud project. You need to implement your company's security vulnerability management policy. What should you do?

- A. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Create a custom metric in the Cloud Monitoring dashboard. • Provide the security team member with access to this dashboard.
- B. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Provide the security team member roles/configure.inventoryViewer permission.
- C. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/configure.vulnerabilityViewer permission.
- D. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Create a log sink to a BigQuery dataset. • Provide the security team member with access to this dataset.

**Answer:** C

#### NEW QUESTION 30

You are building a data lake on Google Cloud for your Internet of Things (IoT) application. The IoT application has millions of sensors that are constantly streaming structured and unstructured data to your backend in the cloud. You want to build a highly available and resilient architecture based on Google-recommended practices. What should you do?

- A. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage
- B. Stream data to Pub/Sub and use Storage Transfer Service to send data to BigQuery.
- C. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage
- D. Stream data to Dataflow, and use Storage Transfer Service to send data to BigQuery.
- E. Stream data to Dataflow, and use Dataprep by Trifacta to send data to Bigtable.

**Answer:** B

#### NEW QUESTION 35

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

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

**Answer:** C

#### Explanation:

A tag is simply a character string added to a tags field in a resource, such as Compute Engine virtual machine (VM) instances or instance templates. A tag is not a separate resource, so you cannot create it separately. All resources with that string are considered to have that tag. Tags enable you to make firewall rules and routes applicable to specific VM instances.

#### NEW QUESTION 39

You are managing a Data Warehouse on BigQuery. An external auditor will review your company's processes, and multiple external consultants will need view access to the data. You need to provide them with view access while following Google-recommended practices. What should you do?

- A. Grant each individual external consultant the role of BigQuery Editor
- B. Grant each individual external consultant the role of BigQuery Viewer
- C. Create a Google Group that contains the consultants and grant the group the role of BigQuery Editor
- D. Create a Google Group that contains the consultants, and grant the group the role of BigQuery Viewer

**Answer:** D

#### NEW QUESTION 42

Your company is using Google Workspace to manage employee accounts. Anticipated growth will increase the number of personnel from 100 employees to 1,000 employees within 2 years. Most employees will need access to your company's Google Cloud account. The systems and processes will need to support 10x growth without performance degradation, unnecessary complexity, or security issues. What should you do?

- A. Migrate the users to Active Directory
- B. Connect the Human Resources system to Active Directory
- C. Turn on Google Cloud Directory Sync (GCDS) for Cloud Identity
- D. Turn on Identity Federation from Cloud Identity to Active Directory.
- E. Organize the users in Cloud Identity into groups
- F. Enforce multi-factor authentication in Cloud Identity.
- G. Turn on identity federation between Cloud Identity and Google Workspace
- H. Enforce multi-factor authentication for domain-wide delegation.
- I. Use a third-party identity provider service through federation
- J. Synchronize the users from Google Workspace to the third-party provider in real time.

**Answer:** B

#### NEW QUESTION 47

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

- A. Upload the image to Cloud Storage and create a Kubernetes Service referencing the image.
- B. Upload the image to Cloud Storage and create a Kubernetes Deployment referencing the image.
- C. Upload the image to Container Registry and create a Kubernetes Service referencing the image.
- D. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

**Answer:** D

**Explanation:**

A deployment is responsible for keeping a set of pods running. A service is responsible for enabling network access to a set of pods.

**NEW QUESTION 49**

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

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

**Answer:** B

**Explanation:**

➤ Run `gcloud builds submit tag gcr.io/img-278322/acme_track_n_trace:v1`. is the right answer.  
 This command correctly tags the image as acme\_track\_n\_trace:v1 and uploads the image to the img-278322 project.  
 Ref: <https://cloud.google.com/sdk/gcloud/reference/builds/submit>

**NEW QUESTION 53**

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

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

**Answer:** D

**Explanation:**

cell phones are sending UDP packets and the only that can receive that type of traffic is a External Network TCP/UDP <https://cloud.google.com/load-balancing/docs/network>  
<https://cloud.google.com/load-balancing/docs/choosing-load-balancer#lb-decision-tree>

**NEW QUESTION 57**

Your development team needs a new Jenkins server for their project. You need to deploy the server using the fewest steps possible. What should you do?

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

**Answer:** D

**NEW QUESTION 61**

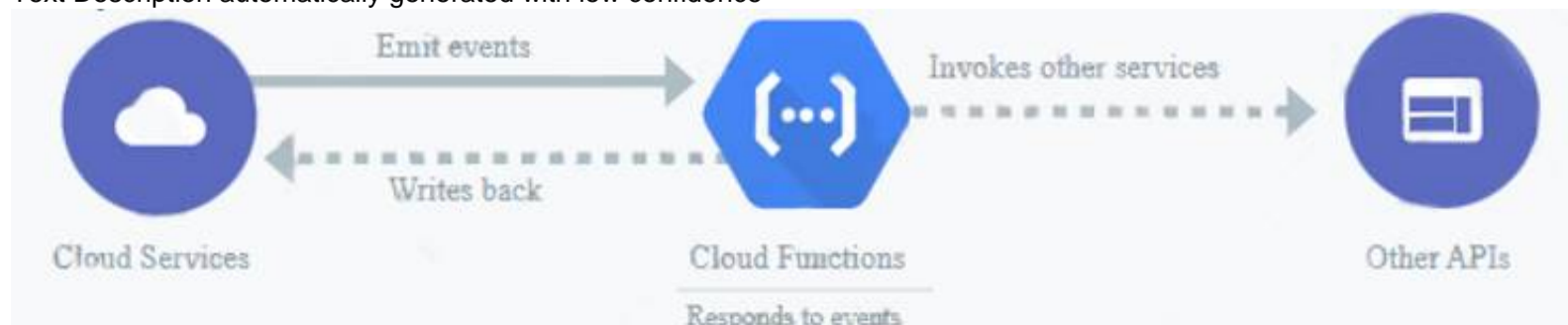
A company wants to build an application that stores images in a Cloud Storage bucket and wants to generate thumbnails as well as resize the images. They want to use a google managed service that can scale up and scale down to zero automatically with minimal effort. You have been asked to recommend a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

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

**Answer:** C

**Explanation:**

Text Description automatically generated with low confidence



Cloud Functions is Google Cloud's event-driven serverless compute platform. It automatically scales based on the load and requires no additional configuration.

You pay only for the resources used.

Ref: <https://cloud.google.com/functions>

While all other options i.e. Google Compute Engine, Google Kubernetes Engine, Google App Engine support autoscaling, it needs to be configured explicitly based on the load and is not as trivial as the scale up or scale down offered by Google's cloud functions.

#### NEW QUESTION 66

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

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

**Answer:** D

#### Explanation:

A simple approach would be to use the command flags available when listing all the IAM policy for a given project. For instance, the following command: `gcloud projects get-iam-policy $PROJECT_ID`

`--flatten="bindings[].members" --format="table(bindings.members)" --filter="bindings.role:roles/owner"`

outputs all the users and service accounts associated with the role 'roles/owner' in the project in question. <https://groups.google.com/g/google-cloud-dev/c/Z6sZs7TvygQ?pli=1>

#### NEW QUESTION 70

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

- A. Project Editor
- B. Storage Admin
- C. Storage Object Admin
- D. Storage Object Creator

**Answer:** B

#### Explanation:

Storage Admin (roles/storage.admin) Grants full control of buckets and objects.

When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket.

`firebase.projects.get resourceanalyzer.projects.get`

`resourceanalyzer.projects.list storage.buckets.* storage.objects.*`

<https://cloud.google.com/storage/docs/access-control/iam-roles>

This role grants full control of buckets and objects. When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket.

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

#### NEW QUESTION 75

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

- A. Manual Scaling with 3 instances.
- B. Basic Scaling with `min_instances` set to 3.
- C. Basic Scaling with `max_instances` set to 3.
- D. Automatic Scaling with `min_idle_instances` set to 3.

**Answer:** D

#### NEW QUESTION 79

You are using Data Studio to visualize a table from your data warehouse that is built on top of BigQuery. Data is appended to the data warehouse during the day. At night, the daily summary is recalculated by overwriting the table. You just noticed that the charts in Data Studio are broken, and you want to analyze the problem. What should you do?

- A. Use the BigQuery interface to review the nightly Job and look for any errors
- B. Review the Error Reporting page in the Cloud Console to find any errors.
- C. In Cloud Logging create a filter for your Data Studio report
- D. Use the open source CLI tool
- E. Snapshot Debugger, to find out why the data was not refreshed correctly.

**Answer:** D

#### Explanation:

Cloud Debugger helps inspect the state of an application, at any code location, without stopping or slowing down the running app //

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

#### NEW QUESTION 83

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

- A. Create the instance without a public IP address.
- B. Create the instance with Private Google Access enabled.

- C. Create a deny-all egress firewall rule on the VPC network.
- D. Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

**Answer:** A

**Explanation:**

VMs cannot communicate over the internet without a public IP address. Private Google Access permits access to Google APIs and services in Google's production infrastructure.

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

**NEW QUESTION 84**

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

- A. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.
- B. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE Cluster Operations resource.
- C. 1. Go to the GKE console, and delete existing clusters.2. Recreate a new cluster.3. Clear the option to enable legacy Stackdriver Logging.
- D. 1. Go to the GKE console, and delete existing clusters.2. Recreate a new cluster.3. Clear the option to enable legacy Stackdriver Monitoring.

**Answer:** A

**Explanation:**

<https://cloud.google.com/logging/docs/api/v2/resource-list> GKE Containers have more log than GKE Cluster Operations:

-GKE Containe:

cluster\_name: An immutable name for the cluster the container is running in. namespace\_id: Immutable ID of the cluster namespace the container is running in.

instance\_id: Immutable ID of the GCE instance the container is running in. pod\_id: Immutable ID of the pod the container is running in.

container\_name: Immutable name of the container. zone: The GCE zone in which the instance is running. VS -GKE Cluster Operations

project\_id: The identifier of the GCP project associated with this resource, such as "my-project". cluster\_name: The name of the GKE Cluster.

location: The location in which the GKE Cluster is running.

**NEW QUESTION 86**

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

- A. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.
- B. Create a Kubernetes Service of type ClusterIP for your applicatio
- C. Configure the public DNS name of your application using the IP of this Service.
- D. Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluste
- E. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing.
- F. Create a HAProxy pod in the cluster to load-balance the traffic to all the pods of the application.Forward the public traffic to HAProxy with an iptable rul
- G. Configure the DNS name of your application using the public IP of the node HAProxy is running on.

**Answer:** A

**NEW QUESTION 87**

You have been asked to create robust Virtual Private Network (VPN) connectivity between a new Virtual Private Cloud (VPC) and a remote site. Key requirements include dynamic routing, a shared address space of 10.19.0.1/22, and no overprovisioning of tunnels during a failover event. You want to follow Google-recommended practices to set up a high availability Cloud VPN. What should you do?

- A. Use a custom mode VPC network, configure static routes, and use active/passive routing
- B. Use an automatic mode VPC network, configure static routes, and use active/active routing
- C. Use a custom mode VPC network use Cloud Router border gateway protocol (86P) routes, and use active/passive routing
- D. Use an automatic mode VPC network, use Cloud Router border gateway protocol (BGP) routes and configure policy-based routing

**Answer:** C

**Explanation:**

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/best-practices>

**NEW QUESTION 92**

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

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

**Answer:** C

**Explanation:**

Types of audit logs Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization: Admin Activity audit logs Data Access audit logs System Event audit logs Policy Denied audit logs \*\*\*Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. <https://cloud.google.com/logging/docs/audit#types>

<https://cloud.google.com/logging/docs/audit#data-access> Cloud Storage: When Cloud Storage usage logs are enabled, Cloud Storage writes usage data to the Cloud Storage bucket, which generates Data Access audit logs for the bucket. The generated Data Access audit log has its caller identity redacted.

#### NEW QUESTION 94

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

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

**Answer: B**

#### NEW QUESTION 97

Your team is running an on-premises ecommerce application. The application contains a complex set of microservices written in Python, and each microservice is running on Docker containers. Configurations are injected by using environment variables. You need to deploy your current application to a serverless Google Cloud solution. What should you do?

- A. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.
- B. Use your existing continuous integration and delivery (CI/CD) pipeline.
- C. Use the generated Docker images and deploy them to Cloud Functions.
- D. Use the same configuration as on-premises.
- E. Use the existing codebase and deploy each service as a separate Cloud Function. Update the configurations and the required endpoints.
- F. Use your existing codebase and deploy each service as a separate Cloud Run. Use the same configurations as on-premises.

**Answer: A**

#### NEW QUESTION 102

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

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

**Answer: B**

#### Explanation:

<https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset> [https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage\\_patterns](https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset#usage_patterns)  
DaemonSets attempt to adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed.

In GKE, DaemonSets manage groups of replicated Pods and adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed. So, this is a perfect fit for our monitoring pod.

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

DaemonSets are useful for deploying ongoing background tasks that you need to run on all or certain nodes, and which do not require user intervention. Examples of such tasks include storage daemons like ceph, log collection daemons like fluentd, and node monitoring daemons like collectd. For example, you could have DaemonSets for each type of daemon run on all of your nodes. Alternatively, you could run multiple DaemonSets for a single type of daemon, but have them use different configurations for different hardware types and resource needs.

#### NEW QUESTION 104

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

- A. Use service account credentials in your on-premises application.
- B. Use gcloud to create a key file for the service account that has appropriate permissions.
- C. Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.
- D. Go to the IAM & admin console, grant a user account permissions similar to the service account permissions, and use this user account for authentication from your data center.

**Answer: B**

#### NEW QUESTION 108

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

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

**Answer: D**

#### Explanation:

A custom image belongs only to your project. To create an instance with a custom image, you must first have a custom image.

#### NEW QUESTION 110

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

- A. Multi-Regional Storage
- B. Regional Storage
- C. Nearline Storage
- D. Coldline Storage

**Answer: D**

#### NEW QUESTION 111

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

- A. Enable the Node Auto-Repair feature for your GKE cluster.
- B. Enable the Node Auto-Upgrades feature for your GKE cluster.
- C. Select the latest available cluster version for your GKE cluster.
- D. Select "Container-Optimized OS (cos)" as a node image for your GKE cluster.

**Answer: B**

#### Explanation:

Creating or upgrading a cluster by specifying the version as latest does not provide automatic upgrades. Enable node auto-upgrades to ensure that the nodes in your cluster are up-to-date with the latest stable version.

<https://cloud.google.com/kubernetes-engine/versioning-and-upgrades>

Node auto-upgrades help you keep the nodes in your cluster up to date with the cluster master version when your master is updated on your behalf. When you create a new cluster or node pool with Google Cloud Console or the gcloud command, node auto-upgrade is enabled by default.

Ref: <https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-upgrades>

#### NEW QUESTION 113

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

- A. After the VM has been created, use your Google Account credentials to log in into the VM.
- B. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.
- C. When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value.
- D. After the VM has been created, download the JSON private key for the default Compute Engine service account
- E. Use the credentials in the JSON file to log in to the VM.

**Answer: B**

#### Explanation:

You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. This option uses the right syntax to reset the windows password.

gcloud compute reset-windows-password windows-instance

Ref: <https://cloud.google.com/compute/docs/instances/windows/creating-passwords-for-windows-instances#gc>

#### NEW QUESTION 115

Your application development team has created Docker images for an application that will be deployed on Google Cloud. Your team does not want to manage the infrastructure associated with this application. You need to ensure that the application can scale automatically as it gains popularity. What should you do?

- A. Create an Instance template with the container image, and deploy a Managed Instance Group with Autoscaling.
- B. Upload Docker images to Artifact Registry, and deploy the application on Google Kubernetes Engine using Standard mode.
- C. Upload Docker images to the Cloud Storage, and deploy the application on Google Kubernetes Engine using Standard mode.
- D. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

**Answer: D**

#### NEW QUESTION 117

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

- A. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.
- B. Add the auditors group to two new custom IAM roles.
- C. Add the auditor user accounts to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.
- D. Add the auditor user accounts to two new custom IAM roles.

**Answer: A**

#### Explanation:

[https://cloud.google.com/iam/docs/job-functions/auditing#scenario\\_external\\_auditors](https://cloud.google.com/iam/docs/job-functions/auditing#scenario_external_auditors)

Because if you directly add users to the IAM roles, then if any users left the organization then you have to remove the users from multiple places and need to revoke his/her access from multiple places. But, if you put a user into a group then its very easy to manage these type of situations. Now, if any user left then you just need to remove the user from the group and all the access got revoked

The organization creates a Google group for these external auditors and adds the current auditor to the group. This group is monitored and is typically granted access to the dashboard application. During normal access, the auditors' Google group is only granted access to view the historic logs stored in BigQuery. If any anomalies are discovered, the group is granted permission to view the actual Cloud Logging Admin Activity logs via the dashboard's elevated access mode. At the

end of each audit period, the group's access is then revoked. Data is redacted using Cloud DLP before being made accessible for viewing via the dashboard application. The table below explains IAM logging roles that an Organization Administrator can grant to the service account used by the dashboard, as well as the resource level at which the role is granted.

#### NEW QUESTION 121

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

- A. Use permissions in your role that use the 'supported' support level for role permission
- B. Set the rolestage to ALPHA while testing the role permissions.
- C. Use permissions in your role that use the 'supported' support level for role permission
- D. Set the role stage to BETA while testing the role permissions.
- E. Use permissions in your role that use the 'testing' support level for role permission
- F. Set the role stage to ALPHA while testing the role permissions.
- G. Use permissions in your role that use the 'testing' support level for role permission
- H. Set the role stage to BETA while testing the role permissions.

**Answer:** A

#### Explanation:

When setting support levels for permissions in custom roles, you can set to one of SUPPORTED, TESTING or NOT\_SUPPORTED.

Ref: <https://cloud.google.com/iam/docs/custom-roles-permissions-support>

#### NEW QUESTION 124

You have an application that runs on Compute Engine VM instances in a custom Virtual Private Cloud (VPC). Your company's security policies only allow the use to internal IP addresses on VM instances and do not let VM instances connect to the internet. You need to ensure that the application can access a file hosted in a Cloud Storage bucket within your project. What should you do?

- A. Enable Private Service Access on the Cloud Storage Bucket.
- B. Add storage.googleapis.com to the list of restricted services in a VPC Service Controls perimeter and add your project to the list to protected projects.
- C. Enable Private Google Access on the subnet within the custom VPC.
- D. Deploy a Cloud NAT instance and route the traffic to the dedicated IP address of the Cloud Storage bucket.

**Answer:** A

#### NEW QUESTION 129

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

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

**Answer:** C

#### Explanation:

<https://cloud.google.com/run/docs/tutorials/pubsub#integrating-pubsub>

\* 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.

#### NEW QUESTION 130

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

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

**Answer:** D

#### Explanation:

Our requirement is to follow Google recommended practices to achieve the end result. Configuring Private Google Access for On-Premises Hosts is best achieved by VPN/Interconnect + Advertise Routes + Use restricted Google IP Range.

➤ Using Cloud VPN or Interconnect, create a tunnel to a VPC in GCP

➤ Using Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel.

➤ In your on-premises network, configure your DNS server to resolve \*.googleapis.com as a CNAME to restricted.googleapis.com is the right answer right, and it is what Google recommends.

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

> You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection, firewall rules on your on-premises firewall to allow the outgoing traffic, and DNS so that traffic to Google APIs resolves to the IP range you've added to your routes.

> You can use Cloud Router Custom Route Advertisement to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network. The Restricted Google APIs IP range is 199.36.153.4/30. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection. Without having a public IP address or access to the internet, the only way you could connect to cloud storage is if you have an internal route to it.

> So Negotiate with the security team to be able to give public IP addresses to the servers is not right.

Following Google recommended practices is synonymous with using Google's services (Not quite, but it is at least for the exam !!).

> So In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance is not right.

> Migrating the VM to Compute Engine is a bit drastic when Google says it is perfectly fine to have Hybrid Connectivity architectures

<https://cloud.google.com/hybrid-connectivity>.

So,

> Use Migrate for Compute Engine (formerly known as Velostrata) to migrate these servers to Compute Engine is not right.

### NEW QUESTION 132

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

```
CREATE TABLE Persons (
    person_id INT64 NOT NULL,    // sequential number based on number of registration
    account_creation_date DATE, // system date
    birthdate DATE,             // customer birthdate
    firstname STRING (255),      // first name
    lastname STRING (255),       // last name
    profile_picture BYTES (255)  // profile picture
) PRIMARY KEY (person_id)
```

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

- A. Remove the profile\_picture field from the table.
- B. Add a secondary index on the person\_id column.
- C. Change the primary key to not have monotonically increasing values.
- D. Create a secondary index using the following Data Definition Language (DDL):

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

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

**Answer: C**

#### Explanation:

As mentioned in Schema and data model, 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 key space. 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. <https://cloud.google.com/spanner/docs/schema-design#primary-key-prevent-hotspots>

### NEW QUESTION 135

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

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

**Answer: D**

**Explanation:**

Keyword need to look for

- "High Throughput",
- "Consistent",
- "Property based data insert/fetch like engine status, distance traveled, fuel level, and more." which can be designed in column,
- "Large Scale Customer Base + Each Customer has multiple sensor which send event in seconds" This will go for per byte situation,
- Export data based on the time of the event.
- Atomic
- o BigTable will fit all requirement. o DataStore is not fully Atomic
- o CloudStorage is not a option where we can export data based on time of event. We need another solution to do that
- o Firestore can be used with MobileSDK.

**NEW QUESTION 139**

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

- A. Use kubectl app deploy <dockerfilename>.
- B. Use gcloud app deploy <dockerfilename>.
- C. Create a docker image from the Dockerfile and upload it to Container Registry
- D. Create a Deployment YAML file to point to that image
- E. Use kubectl to create the deployment with that file.
- F. Create a docker image from the Dockerfile and upload it to Cloud Storage
- G. Create a Deployment YAML file to point to that image
- H. Use kubectl to create the deployment with that file.

**Answer:** C

**NEW QUESTION 142**

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

- A. Verify that both projects are in a GCP Organization
- B. Create a new VPC and add all instances.
- C. Verify that both projects are in a GCP Organization
- D. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.
- E. Verify that you are the Project Administrator of both projects
- F. Create two new VPCs and add all instances.
- G. Verify that you are the Project Administrator of both projects
- H. Create a new VPC and add all instances.

**Answer:** B

**Explanation:**

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. The VPC networks in the host project are called Shared VPC networks. Eligible resources from service projects can use subnets in the Shared VPC network

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

"For example, an existing instance in a service project cannot be reconfigured to use a Shared VPC network, but a new instance can be created to use available subnets in a Shared VPC network."

**NEW QUESTION 145**

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

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

**Answer:** B

**Explanation:**

[https://cloud.google.com/kuberun/docs/architecture-overview#components\\_in\\_the\\_default\\_installation](https://cloud.google.com/kuberun/docs/architecture-overview#components_in_the_default_installation)

**NEW QUESTION 147**

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

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

**Answer:** C

**Explanation:**

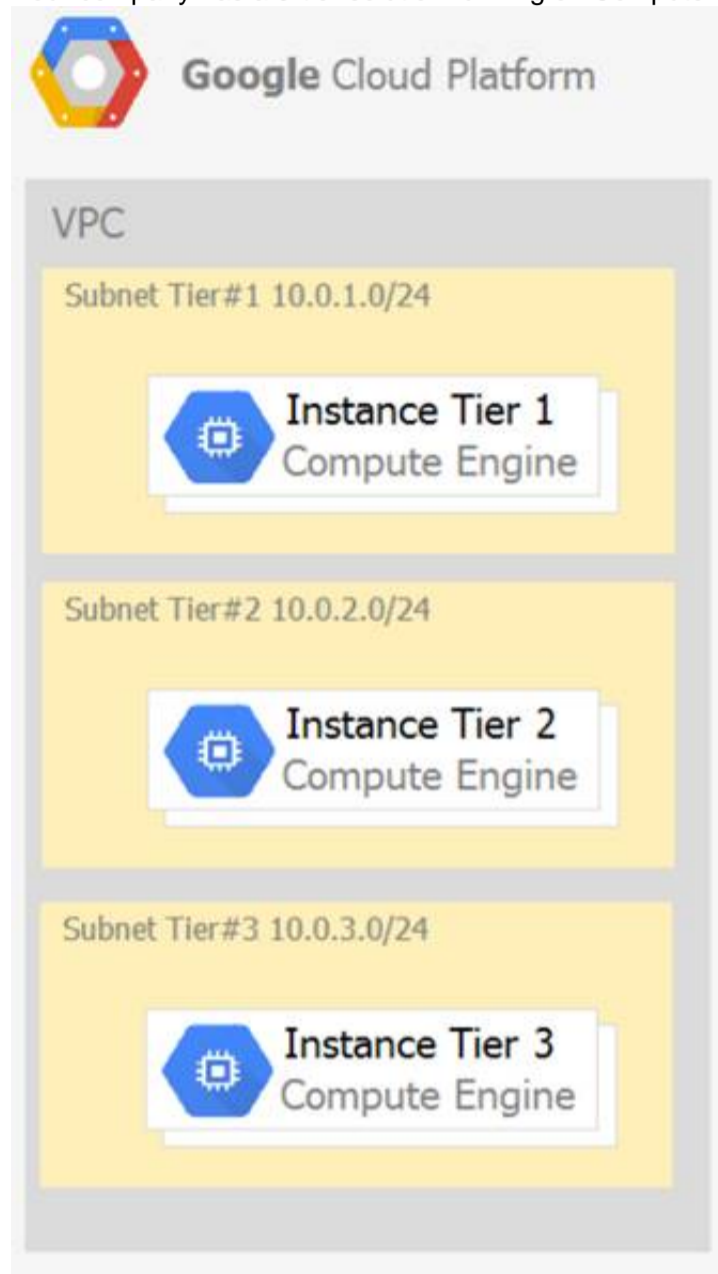
From this source:

[https://cloud.google.com/billing/docs/how-to/custom-roles#permission\\_association\\_and\\_inheritance](https://cloud.google.com/billing/docs/how-to/custom-roles#permission_association_and_inheritance)

"For example, associating a project with a billing account requires the `billing.resourceAssociations.create` permission on the billing account and also the `resourceManager.projects.createBillingAssignment` permission on the project. This is because project permissions are required for actions where project owners control access, while billing account permissions are required for actions where billing account administrators control access. When both should be involved, both permissions are necessary."

#### NEW QUESTION 150

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



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

- 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
  - Source filter: IP ranges (with the range set to 10.0.2.0/24)
  - Protocols: allow all
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 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 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

**Answer: B**

#### Explanation:

\* 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

#### NEW QUESTION 155

You manage three Google Cloud projects with the Cloud Monitoring API enabled. You want to follow Google-recommended practices to visualize CPU and network metrics for all three projects together. What should you do?

- \* 1. Create a Cloud Monitoring Dashboard\* 2. Collect metrics and publish them into the Pub/Sub topics 3. Add CPU and network Charts (or each of (he three projects
- \* 1. Create a Cloud Monitoring Dashboard.\* 2. Select the CPU and Network metrics from the three projects.\* 3. Add CPU and network Charts lot each of the three protects.
- \* 1 Create a Service Account and apply roles/viewer on the three projects\* 2. Collect metrics and publish them lo the Cloud Monitoring API\* 3. Add CPU and network Charts for each of the three projects.
- \* 1. Create a fourth Google Cloud project\* 2 Create a Cloud Workspace from the fourth project and add the other three projects

**Answer:** B

#### NEW QUESTION 157

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

- A. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Set the service's externalTrafficPolicy to Cluster.3. Configure the Compute Engine instance to use the address of the load balancer that has been created.
- B. 1. In GKE, create a Service of type NodePort that uses the application's Pods as backend.2. Create a Compute Engine instance called proxy with 2 network interfaces, one in each VPC.3. Use iptables on this instance to forward traffic from gce-network to the GKE nodes.4. Configure the Compute Engine instance to use the address of proxy in gce-network as endpoint.
- C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal3. Peer the two VPCs together.4. Configure the Compute Engine instance to use the address of the load balancer that has been created.
- D. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend.2. Add a Cloud Armor Security Policy to the load balancer that whitelists the internal IPs of the MIG's instances.3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

**Answer:** A

#### Explanation:

performs a peering between the two VPC's (the statement makes sure that this option is feasible since it clearly specifies that there is no overlapping between the ip ranges of both vpc's), deploy the LoadBalancer as internal with the annotation, and configure the endpoint so that the compute engine instance can access the application internally, that is, without the need to have a public ip at any time and therefore, without the need to go outside the google network. The traffic, therefore, never crosses the public internet.

<https://medium.com/pablo-perez/k8s-externaltrafficpolicy-local-or-cluster-40b259a19404> <https://cloud.google.com/kubernetes-engine/docs/how-to/internal-load-balancing>

clients in a VPC network connected to the LoadBalancer network using VPC Network Peering can also access the Service

<https://cloud.google.com/kubernetes-engine/docs/how-to/service-parameters>

#### NEW QUESTION 162

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

- A. Coldline Storage
- B. Nearline Storage
- C. Regional Storage
- D. Multi-Regional Storage

**Answer:** A

#### Explanation:

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>



# Google Cloud Storage Classes in the Organization

This slide represents the different types of storage classes such as multi-regional, regional, storage nearline, and storage cold line of the Google Cloud.

Storage Class	Characteristics	Use Cases	Price (Per Gb Per Month)*
Multi-Regional Storage	<ul style="list-style-type: none"> <li>99.95% availability</li> <li>Geo-redundant</li> </ul>	Keeps information that is frequently accessed around the globe, such as videos, gaming, and mobile applications	\$0.026 per GB/Month
Regional Storage	<ul style="list-style-type: none"> <li>99.9% availability</li> <li>Low cost per GB stored</li> <li>Data storage in a small region</li> </ul>	Keeps information that is frequently accessed around the globe, such as videos, gaming, and mobile applications	\$0.02 per GB/Month
Storage Nearline	<ul style="list-style-type: none"> <li>99.0% availability</li> <li>Very low cost per GB</li> <li>Data fetching costs</li> <li>Higher per-task costs</li> <li>30-day minimum storage duration</li> </ul>	Keeps data that is not accessed is often ideal for data backups	\$0.01 per GB/Month
Storage Cold line	<ul style="list-style-type: none"> <li>99.0% availability</li> <li>Lowest cost per GB</li> <li>Data fetching costs</li> <li>Higher per-task costs</li> <li>90-day minimum storage duration</li> </ul>	Keeps information that is infrequently ideal for disaster recovery or archived data	\$0.007 per GB/Month

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

## NEW QUESTION 167

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

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

**Answer: B**

### Explanation:

The key to understand the requirement is : "The objects are written once and accessed frequently for 30 days" Standard Storage  
 Standard Storage is best for data that is frequently accessed ("hot" data) and/or stored for only brief periods of time.

Archive Storage

Archive Storage is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Unlike the "coldest" storage services offered by other Cloud providers, your data is available within milliseconds, not hours or days. Archive Storage is the best choice for data that you plan to access less than once a year.

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

## NEW QUESTION 171

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

- `kubectl get deployments --output=pods`
- `gcloud get pods --selector="app=prod"`
- `kubectl get pods -l "app=prod"`
- `gcloud list gke-deployments -filter={pod }`

**Answer: C**

### Explanation:

This command correctly lists pods that have the label `app=prod`. When creating the deployment, we used the label `app=prod` so listing pods that have this label retrieve the pods belonging to nginx deployments. You can list pods by using Kubernetes CLI `kubectl get pods`.

Ref: <https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/>

Ref: <https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/#list-containe>

## NEW QUESTION 176

You created a Kubernetes deployment by running `kubectl run nginx image=nginx replicas=1`. After a few days, you decided you no longer want this deployment.

You identified the pod and deleted it by running `kubectl delete pod`. You noticed the pod got recreated.

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

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

- A. `kubectl delete deployment nginx`
- B. `kubectl delete --deployment=nginx`
- C. `kubectl delete pod nginx-84748895c4-k6bzl --no-restart 2`
- D. `kubectl delete inginx`

**Answer:** A

**Explanation:**

This command correctly deletes the deployment. Pods are managed by kubernetes workloads (deployments). When a pod is deleted, the deployment detects the pod is unavailable and brings up another pod to maintain the replica count. The only way to delete the workload is by deleting the deployment itself using the `kubectl delete deployment` command.

```
> $ kubectl delete deployment nginx
deployment.apps/nginx deleted
```

Ref: <https://kubernetes.io/docs/reference/kubectl/cheatsheet/#deleting-resources>

**NEW QUESTION 178**

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

- A. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.
- B. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.
- C. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.
- D. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

**Answer:** B

**Explanation:**

The resource that you need to get access is in the other project. `roles/bigquery.dataViewer` BigQuery Data Viewer

When applied to a table or view, this role provides permissions to: Read data and metadata from the table or view.

This role cannot be applied to individual models or routines. When applied to a dataset, this role provides permissions to:

Read the dataset's metadata and list tables in the dataset. Read data and metadata from the dataset's tables.

When applied at the project or organization level, this role can also enumerate all datasets in the project. Additional roles, however, are necessary to allow the running of jobs.

**NEW QUESTION 183**

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

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

**Answer:** C

**Explanation:**

Understanding IAM custom roles

Key Point: Custom roles enable you to enforce the principle of least privilege, ensuring that the user and service accounts in your organization have only the permissions essential to performing their intended functions.

Basic concepts

Custom roles are user-defined, and allow you to bundle one or more supported permissions to meet your specific needs. Custom roles are not maintained by Google; when new permissions, features, or services are added to Google Cloud, your custom roles will not be updated automatically.

When you create a custom role, you must choose an organization or project to create it in. You can then grant the custom role on the organization or project, as well as any resources within that organization or project.

[https://cloud.google.com/iam/docs/understanding-custom-roles#basic\\_concepts](https://cloud.google.com/iam/docs/understanding-custom-roles#basic_concepts)

**NEW QUESTION 184**

You have two subnets (subnet-a and subnet-b) in the default VPC. Your database servers are running in subnet-a. Your application servers and web servers are running in subnet-b. You want to configure a firewall rule that only allows database traffic from the application servers to the database servers. What should you do?

- A. \* Create service accounts sa-app and sa-db. • Associate service account: sa-app with the application servers and the service account sa-db with the database servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.
- B. • Create network tags app-server and db-server. • Add the app-server tag to the application servers and the db-server tag to the database servers. • Create an egress firewall rule to allow network traffic from source network tag app-server to target network tag db-server.
- C. \* Create a service account sa-app and a network tag db-server. \* Associate the service account sa-app with the application servers and the network tag db-server with the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-a IP addresses.
- D. • Create a network tag app-server and service account sa-db. • Add the tag to the application servers and associate the service account with the database servers. • Create an egress firewall rule to allow network traffic from source network tag app-server to target service account sa-db.

**Answer:** C

#### NEW QUESTION 188

You just installed the Google Cloud CLI on your new corporate laptop. You need to list the existing instances of your company on Google Cloud. What must you do before you run the `gcloud compute instances list` command?

Choose 2 answers

- A. Run `gcloud auth login`, enter your login credentials in the dialog window, and paste the received login token to `gcloud CLI`.
- B. Create a Google Cloud service account, and download the service account key
- C. Place the key file in a folder on your machine where `gcloud CLI` can find it.
- D. Download your Cloud Identity user account key
- E. Place the key file in a folder on your machine where `gcloud CLI` can find it.
- F. Run `gcloud config set compute/zone $my_zone` to set the default zone for `gcloud CLI`.
- G. Run `gcloud config set project $my_project` to set the default project for `gcloud CLI`.

**Answer:** AE

#### Explanation:

Before you run the `gcloud compute instances list` command, you need to do two things: authenticate with your user account and set the default project for `gcloud CLI`.

To authenticate with your user account, you need to run `gcloud auth login`, enter your login credentials in the dialog window, and paste the received login token to `gcloud CLI`. This will authorize the `gcloud CLI` to access Google Cloud resources on your behalf<sup>1</sup>.

To set the default project for `gcloud CLI`, you need to run `gcloud config set project $my_project`, where

`$my_project` is the ID of the project that contains the instances you want to list. This will save you from having to specify the project flag for every `gcloud` command<sup>2</sup>.

Option B is not recommended, because using a service account key increases the risk of credential leakage and misuse. It is also not necessary, because you can use your user account to authenticate to the `gcloud CLI`<sup>3</sup>. Option C is not correct, because there is no such thing as a Cloud Identity user account key. Cloud Identity is a service that provides identity and access management for Google Cloud users and groups<sup>4</sup>. Option D is not required, because the `gcloud compute instances list` command does not depend on the default zone. You can

list instances from all zones or filter by a specific zone using the `--filter` flag.

References:

- 1: <https://cloud.google.com/sdk/docs/authorizing>
- 2: <https://cloud.google.com/sdk/gcloud/reference/config/set>
- 3: <https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys>
- 4: <https://cloud.google.com/identity/docs/overview>
- : <https://cloud.google.com/sdk/gcloud/reference/compute/instances/list>

#### NEW QUESTION 191

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

- A. Run `gcloud iam roles describe roles/spanner.databaseUser`
- B. Add the users to the role.
- C. Run `gcloud iam roles describe roles/spanner.databaseUser`
- D. Add the users to a new group
- E. Add the group to the role.
- F. Run `gcloud iam roles describe roles/spanner.viewer --project my-projec`
- G. Add the users to the role.
- H. Run `gcloud iam roles describe roles/spanner.viewer --project my-projec`
- I. Add the users to a new group. Add the group to the role.

**Answer:** B

#### Explanation:

<https://cloud.google.com/spanner/docs/iam#spanner.databaseUser>

Using the `gcloud` tool, execute the `gcloud iam roles describe roles/spanner.databaseUser` command on Cloud Shell. Attach the users to a newly created Google group and add the group to the role.

#### NEW QUESTION 195

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

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

**Answer:** B

#### Explanation:

<https://cloud.google.com/logging/docs/audit>

### NEW QUESTION 198

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

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

**Answer: B**

#### Explanation:

➤ Navigate to Stackdriver Logging and select resource.labels.project\_id=\*. is not right.  
Log entries are held in Stackdriver Logging for a limited time known as the retention period which is 30 days (default configuration). After that, the entries are deleted. To keep log entries longer, you need to export them outside of Stackdriver Logging by configuring log sinks.  
Ref: <https://cloud.google.com/blog/products/gcp/best-practices-for-working-with-google-cloud-audit-logging> ➤ Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days. is not right.  
While this works, it makes no sense to use Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery when Google provides a feature (export sinks) that does exactly the same thing and works out of the box. Ref: [https://cloud.google.com/logging/docs/export/configure\\_export\\_v2](https://cloud.google.com/logging/docs/export/configure_export_v2)  
➤ Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days. is not right.  
You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud Storage, BigQuery, and Pub/Sub. Ref: [https://cloud.google.com/logging/docs/export/configure\\_export\\_v2](https://cloud.google.com/logging/docs/export/configure_export_v2)  
Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to exporting from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud organization. Ref: [https://cloud.google.com/logging/docs/export/aggregated\\_sinks](https://cloud.google.com/logging/docs/export/aggregated_sinks)  
Either way, we now have the data in Cloud Storage, but querying logs information from Cloud Storage is harder than Querying information from BigQuery dataset. For this reason, we should prefer Big Query over Cloud Storage.  
➤ Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days. is the right answer.  
You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud Storage, BigQuery, and Pub/Sub. Ref: [https://cloud.google.com/logging/docs/export/configure\\_export\\_v2](https://cloud.google.com/logging/docs/export/configure_export_v2)  
Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to exporting from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud organization. Ref: [https://cloud.google.com/logging/docs/export/aggregated\\_sinks](https://cloud.google.com/logging/docs/export/aggregated_sinks)  
Either way, we now have the data in a BigQuery Dataset. Querying information from a Big Query dataset is easier and quicker than analyzing contents in Cloud Storage bucket. As our requirement is to Quickly analyze the log contents, we should prefer Big Query over Cloud Storage.  
Also, You can control storage costs and optimize storage usage by setting the default table expiration for newly created tables in a dataset. If you set the property when the dataset is created, any table created in the dataset is deleted after the expiration period. If you set the property after the dataset is created, only new tables are deleted after the expiration period. For example, if you set the default table expiration to 7 days, older data is automatically deleted after 1 week. Ref: <https://cloud.google.com/bigquery/docs/best-practices-storage>

### NEW QUESTION 203

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

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

**Answer: A**

#### Explanation:

➤ Google HTTP(S) Load Balancing has native support for the WebSocket protocol when you use HTTP or HTTPS, not HTTP/2, as the protocol to the backend.  
Ref: [https://cloud.google.com/load-balancing/docs/https#websocket\\_proxy\\_support](https://cloud.google.com/load-balancing/docs/https#websocket_proxy_support)  
➤ We dont need to convert WebSocket code to use HTTP streaming or Redesign the application, as  
WebSocket support is offered by Google HTTP(S) Load Balancing. Reviewing the encryption requirements is a good idea but it has nothing to do with WebSockets.

### NEW QUESTION 207

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

- A. Enable the Identity Aware Proxy API on the project.
- B. Scan the bucket using the Data Loss Prevention API.
- C. Allow only a single Service Account access to read the data.
- D. Enable Data Access audit logs for the Cloud Storage API.

**Answer: D**

**Explanation:**

Logged information Within Cloud Audit Logs, there are two types of logs: Admin Activity logs: Entries for operations that modify the configuration or metadata of a project, bucket, or object. Data Access logs: Entries for operations that modify objects or read a project, bucket, or object. There are several sub-types of data access logs: ADMIN\_READ: Entries for operations that read the configuration or metadata of a project, bucket, or object. DATA\_READ: Entries for operations that read an object. DATA\_WRITE: Entries for operations that create or modify an object. <https://cloud.google.com/storage/docs/audit-logs#types>

**NEW QUESTION 210**

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

- A. Using the GCP Console, filter the Activity log to view the information.
- B. Using the GCP Console, filter the Stackdriver log to view the information.
- C. View the bucket in the Storage section of the GCP Console.
- D. Create a trace in Stackdriver to view the information.

**Answer:** A

**Explanation:**

<https://cloud.google.com/storage/docs/audit-logs> [https://cloud.google.com/compute/docs/logging/audit-logging#audited\\_operations](https://cloud.google.com/compute/docs/logging/audit-logging#audited_operations)

**NEW QUESTION 211**

The DevOps group in your organization needs full control of Compute Engine resources in your development project. However, they should not have permission to create or update any other resources in the project. You want to follow Google's recommendations for setting permissions for the DevOps group. What should you do?

- A. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.
- B. Create an IAM policy and grant all comput
- C. instanceAdmIn." permissions to the policy Attach the policy to the DevOps group.
- D. Create a custom role at the folder level and grant all comput
- E. instanceAdmI
- F. \* permissions to the role Grant the custom role to the DevOps group.
- G. Grant the basic role roles/editor to the DevOps group.

**Answer:** A

**NEW QUESTION 213**

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

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

**Answer:** D

**Explanation:**

<https://cloud.google.com/monitoring/audit-logging>

**NEW QUESTION 216**

You are building a multi-player gaming application that will store game information in a database. As the popularity of the application increases, you are concerned about delivering consistent performance. You need to ensure an optimal gaming performance for global users, without increasing the management complexity. What should you do?

- A. Use Cloud SQL database with cross-region replication to store game statistics in the EU, US, and APAC regions.
- B. Use Cloud Spanner to store user data mapped to the game statistics.
- C. Use BigQuery to store game statistics with a Redis on Memorystore instance in the front to provide global consistency.
- D. Store game statistics in a Bigtable database partitioned by username.

**Answer:** B

**NEW QUESTION 219**

You are working in a team that has developed a new application that needs to be deployed on Kubernetes. The production application is business critical and should be optimized for reliability. You need to provision a Kubernetes cluster and want to follow Google-recommended practices. What should you do?

- A. Create a GKE Autopilot cluste
- B. Enroll the cluster in the rapid release channel.
- C. Create a GKE Autopilot cluste
- D. Enroll the cluster in the stable release channel.
- E. Create a zonal GKE standard cluste
- F. Enroll the cluster in the stable release channel.
- G. Create a regional GKE standard cluste
- H. Enroll the cluster in the rapid release channel.

**Answer:** B

**Explanation:**

Autopilot is more reliable and stable release gives more time to fix issues in new version of GKE

#### NEW QUESTION 223

You are planning to migrate your on-premises data to Google Cloud. The data includes:

- 200 TB of video files in SAN storage
- Data warehouse data stored on Amazon Redshift
- 20 GB of PNG files stored on an S3 bucket

You need to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud Storage bucket. You want to follow Google-recommended practices and avoid writing any code for the migration. What should you do?

- A. Use gcloud storage for the video file
- B. Dataflow for the data warehouse data, and Storage Transfer Service for the PNG files.
- C. Use Transfer Appliance for the video
- D. BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.
- E. Use Storage Transfer Service for the video files, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.
- F. Use Cloud Data Fusion for the video files, Dataflow for the data warehouse data, and Storage Transfer Service for the PNG files.

**Answer:** C

#### NEW QUESTION 228

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

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

**Answer:** A

#### Explanation:

"Run gcloud configurations list to start the Compute Engine instances". How the heck are you expecting to "start" GCE instances doing "configuration list". Each gcloud configuration has a 1 to 1 relationship with the region (if a region is defined). Since we have two different regions, we would need to create two separate configurations using gcloud config configurations createRef: <https://cloud.google.com/sdk/gcloud/reference/config/configurations/create> Secondly, you can activate each configuration independently by running gcloud config configurations activate [NAME]Ref: <https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate> Finally, while each configuration is active, you can run the gcloud compute instances start [NAME] command to start the instance in the configurations region.<https://cloud.google.com/sdk/gcloud/reference/compute/instances/start>

#### NEW QUESTION 233

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

- A. Disable the flag "Delete boot disk when instance is deleted."
- B. Enable delete protection on the instance.
- C. Disable Automatic restart on the instance.
- D. Enable Preemptibility on the instance.

**Answer:** D

#### Explanation:

Preventing Accidental VM Deletion This document describes how to protect specific VM instances from deletion by setting the deletionProtection property on an Instance resource. To learn more about VM instances, read the Instances documentation. As part of your workload, there might be certain VM instances that are critical to running your application or services, such as an instance running a SQL server, a server used as a license manager, and so on. These VM instances might need to stay running indefinitely so you need a way to protect these VMs from being deleted. By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails. Only a user that has been granted a role with compute.instances.create permission can reset the flag to allow the resource to be deleted. <https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion>

#### NEW QUESTION 237

You need to deploy an application in Google Cloud using serverless technology. You want to test a new version of the application with a small percentage of production traffic. What should you do?

- A. Deploy the application to Cloud
- B. Run
- C. Use gradual rollouts for traffic splitting.
- D. Deploy the application to Google Kubernetes Engine
- E. Use Anthos Service Mesh for traffic splitting.
- F. Deploy the application to Cloud function
- G. Suffix the version number in the function's name.
- H. Deploy the application to App Engine
- I. For each new version, create a new service.

**Answer:** A

#### NEW QUESTION 242

You have a Bigtable instance that consists of three nodes that store personally identifiable information (PII) data. You need to log all read or write operations, including any metadata or configuration reads of this database table, in your company's Security Information and Event Management (SIEM) system. What should you do?

- A. • Navigate to Cloud Monitoring in the Google Cloud console, and create a custom monitoring job for the Bigtable instance to track all changes. • Create an alert by using webhook endpoint
- B. with the SIEM endpoint as a receiver
- C. Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read and Admin Read logs for the Bigtable instance
- D. Data Write and Admin Read logs for the Bigtable instance • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.
- E. • Install the Ops Agent on the Bigtable instance during configuration
- F. K • Create a service account with read permissions for the Bigtable instance. • Create a custom Dataflow job with this service account to export logs to the company's SIEM system.
- G. • Navigate to the Audit Logs page in the Google Cloud console, and enable Admin Write logs for the Bigtable instance. • Create a Cloud Functions instance to export logs from Cloud Logging to your SIEM.

**Answer:** B

#### NEW QUESTION 243

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

- A. Filter the Activity log to view the Configuration category
- B. Filter the Resource type to Service Account.
- C. Filter the Activity log to view the Configuration category
- D. Filter the Resource type to Google Project.
- E. Filter the Activity log to view the Data Access category
- F. Filter the Resource type to Service Account.
- G. Filter the Activity log to view the Data Access category
- H. Filter the Resource type to Google Project.

**Answer:** A

#### Explanation:

<https://developers.google.com/cloud-search/docs/guides/audit-logging-manual>

#### NEW QUESTION 246

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

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

**Answer:** B

#### Explanation:

Showing Deployment Manager templates to your team will allow you to define the changes you want to implement in your cloud infrastructure. You can use Cloud Source Repositories to store Deployment Manager templates and collaborate with your team. Cloud Source Repositories are fully-featured, scalable, and private Git repositories you can use to store, manage and track changes to your code.

<https://cloud.google.com/source-repositories/docs/features>

#### NEW QUESTION 250

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

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

**Answer:** A

#### NEW QUESTION 252

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

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

**Answer:** A

#### Explanation:

Ref: [https://cloud.google.com/compute/docs/machine-types#n1\\_machine\\_type](https://cloud.google.com/compute/docs/machine-types#n1_machine_type)

#### NEW QUESTION 256

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

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

**Answer: B**

#### NEW QUESTION 260

Your company wants to migrate their on-premises workloads to Google Cloud. The current on-premises workloads consist of:

- A Flask web application
- A backend API
- A scheduled long-running background job for ETL and reporting.

You need to keep operational costs low. You want to follow Google-recommended practices to migrate these workloads to serverless solutions on Google Cloud. What should you do?

- A. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Compute Engine.
- B. Migrate the web application to App Engine and the backend API to Cloud Run.
- C. Use Cloud Tasks to run your background job on Cloud Run.
- D. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.
- E. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run.
- F. Use Cloud Tasks to run your background job on Compute Engine.

**Answer: B**

#### NEW QUESTION 263

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

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

**Answer: C**

#### Explanation:

<https://cloud.google.com/bigquery/external-data-sources>

An external data source is a data source that you can query directly from BigQuery, even though the data is not stored in BigQuery storage.

BigQuery supports the following external data sources: Amazon S3

Azure Storage Cloud Bigtable Cloud Spanner Cloud SQL Cloud Storage

Drive

#### NEW QUESTION 264

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

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

**Answer: D**

#### Explanation:

As part of your workload, there might be certain VM instances that are critical to running your application or services, such as an instance running a SQL server, a server used as a license manager, and so on. These VM instances might need to stay running indefinitely so you need a way to protect these VMs from being deleted. By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails. Only a user that has been granted a role with compute.instances.create permission can reset the flag to allow the resource to be deleted. Ref: <https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion>

#### NEW QUESTION 268

Several employees at your company have been creating projects with Cloud Platform and paying for it with their personal credit cards, which the company reimburses. The company wants to centralize all these projects under a single, new billing account. What should you do?

- A. Contact [cloud-billing@google.com](mailto:cloud-billing@google.com) with your bank account details and request a corporate billing account for your company.
- B. Create a ticket with Google Support and wait for their call to share your credit card details over the phone.
- C. In the Google Platform Console, go to the Resource Manager and move all projects to the root Organization.
- D. In the Google Cloud Platform Console, create a new billing account and set up a payment method.

**Answer: D**

**Explanation:**

([https://cloud.google.com/resource-manager/docs/project-migration#change\\_billing\\_account](https://cloud.google.com/resource-manager/docs/project-migration#change_billing_account)) <https://cloud.google.com/billing/docs/concepts>  
<https://cloud.google.com/resource-manager/docs/project-migration>

**NEW QUESTION 269**

Users of your application are complaining of slowness when loading the application. You realize the slowness is because the App Engine deployment serving the application is deployed in us-central whereas all users of this application are closest to europe-west3. You want to change the region of the App Engine application to europe-west3 to minimize latency. What's the best way to change the App Engine region?

- A. Create a new project and create an App Engine instance in europe-west3
- B. Use the gcloud app region set command and supply the name of the new region.
- C. From the console, under the App Engine page, click edit, and change the region drop-down.
- D. Contact Google Cloud Support and request the change.

**Answer:** A

**Explanation:**

App engine is a regional service, which means the infrastructure that runs your app(s) is located in a specific region and is managed by Google to be redundantly available across all the zones within that region. Once an app engine deployment is created in a region, it cant be changed. The only way is to create a new project and create an App Engine instance in europe-west3, send all user traffic to this instance and delete the app engine instance in us-central.  
 Ref: <https://cloud.google.com/appengine/docs/locations>

**NEW QUESTION 273**

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

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

**Answer:** B

**Explanation:**

Cloud Spanner is a relational database and is highly scalable. Cloud Spanner is a highly scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with a non-relational horizontal scale. This combination delivers high-performance transactions and strong consistency across rows, regions, and continents with an industry-leading 99.999% availability SLA, no planned downtime, and enterprise-grade security  
 Ref: <https://cloud.google.com/spanner>  
 Graphical user interface, application, Teams Description automatically generated

	CLOUD SPANNER	TRADITIONAL RELATIONAL	TRADITIONAL NON-RELATIONAL
Schema	✓ Yes	✓ Yes	✗ No
SQL	✓ Yes	✓ Yes	✗ No
Consistency	✓ Strong	✓ Strong	✗ Eventual
Availability	✓ High	✗ Failover	✓ High
Scalability	✓ Horizontal	✗ Vertical	✓ Horizontal
Replication	✓ Automatic	⚙️ Configurable	⚙️ Configurable

**NEW QUESTION 274**

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

- A. Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.
- B. Select Cloud SQL (MySQL). Select the create failover replicas option.
- C. Select Cloud Spanne
- D. Set up your instance with 2 nodes.
- E. Select Cloud Spanne
- F. Set up your instance as multi-regional.

**Answer:** A

**NEW QUESTION 276**

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

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

- C. Run a test using simulated maintenance event
- D. If the test is successful, use N1 Standard VMs when running future jobs.
- E. Run a test using a managed instance group
- F. If the test is successful, use N1 Standard VMs in the managed instance group when running future jobs.
- G. Run a test using N1 standard VMs instead of N2. If the test is successful, use N1 Standard VMs when running future jobs.

**Answer:** A

**Explanation:**

Creating and starting a preemptible VM instance This page explains how to create and use a preemptible virtual machine (VM) instance. A preemptible instance is an instance you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances will always terminate after 24 hours. To learn more about preemptible instances, read the preemptible instances documentation. Preemptible instances are recommended only for fault-tolerant applications that can withstand instance preemptions. Make sure your application can handle preemptions before you decide to create a preemptible instance. To understand the risks and value of preemptible instances, read the preemptible instances documentation. <https://cloud.google.com/compute/docs/instances/create-start-preemptible-instance>

**NEW QUESTION 277**

You want to permanently delete a Pub/Sub topic managed by Config Connector in your Google Cloud project. What should you do?

- A. Use kubectl to delete the topic resource.
- B. Use gcloud CLI to delete the topic.
- C. Use kubectl to create the label deleted-by-cnrm and to change its value to true for the topic resource.
- D. Use gcloud CLI to update the topic label managed-by-cnrm to false.

**Answer:** A

**NEW QUESTION 279**

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

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

**Answer:** D

**Explanation:**

<https://cloud.google.com/appengine/docs/flexible/managing-projects-apps-billing#:~:text=Each%20Cloud%20p> Two App engine can't be running on the same project: you can check this easy diagram for more info:

[https://cloud.google.com/appengine/docs/standard/an-overview-of-app-engine#components\\_of\\_an\\_application](https://cloud.google.com/appengine/docs/standard/an-overview-of-app-engine#components_of_an_application)

And you can't change location after setting it for your app Engine. <https://cloud.google.com/appengine/docs/standard/locations>

App Engine is regional and you cannot change an apps region after you set it. Therefore, the only way to have an app run in another region is by creating a new project and targeting the app engine to run in the required region (asia-northeast1 in our case).

Ref: <https://cloud.google.com/appengine/docs/locations>

**NEW QUESTION 283**

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?

- A. Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of "email."
- B. Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of "email."
- C. Export the billing data to BigQuery
- D. 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 dollar
- E. Schedule the Cloud Function using Cloud Scheduler to run hourly.
- F. 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 dollar
- G. Schedule the Cloud Function using Cloud Scheduler to run hourly.

**Answer:** C

**Explanation:**

<https://blog.doit-intl.com/the-truth-behind-google-cloud-egress-traffic-6e8f57b5c2f8>

**NEW QUESTION 287**

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

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

**Answer:** B

NEW QUESTION 290  
.....

## Relate Links

**100% Pass Your Associate-Cloud-Engineer Exam with ExamBible Prep Materials**

<https://www.exambible.com/Associate-Cloud-Engineer-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>