HELLO GUYS

60
Questions

PASS

Latest 2022 Questions

100%

GCP Professional Cloud Architect Exam Dumps

- *This video Help you to pass GCP-PCA Exam with these Real Questions and Answer*
- *Watch complete video till the end*
- *Like and Subscribe the Channel for Amazing upcoming videos.*

Let's start!

Question 1:

A company is hosting their Echo application on Google Cloud using Google Kubernetes Engine. The application is deployed with deployment echo-deployment exposed with echo-service. They have a new image that needs to be deployed for the application. How can the change be deployed with minimal downtime?

- ◯ **Update image using kubectl set image deployment**
- ◯ **Delete the deployment and create a new deployment with the updated image**
- ◯ **Delete the service and create a new service with the updated image**
- ◯ **Update image in instance template and use rolling deployment of instance group with Kubernetes engine.**

A company is hosting their Echo application on Google Cloud using Google Kubernetes Engine. The application is deployed with deployment echo-deployment exposed with echo-service. They have a new image that needs to be deployed for the application. How can the change be deployed with minimal downtime?

- ◯ **Update image using kubectl set image deployment** (Correct)
- ◯ **Delete the deployment and create a new deployment with the updated image**
- ◯ **Delete the service and create a new service with the updated image**
- ◯ **Update image in instance template and use rolling deployment of instance group with Kubernetes engine.**

Explanation

You can perform a rolling update to update the images, configuration, labels, annotations, and resource limits/requests of the workloads in your clusters. Rolling updates incrementally replace your resource's Pods with new ones, which are then scheduled on nodes with available resources. Rolling updates are designed to update your workloads without downtime.

You can use kubectl set to make changes to an object's image, resources, or selector fields.

to update a Deployment from nginx version 1.7.9 to 1.9.1, run the following command:

```
kubectl set image deployment nginx nginx=nginx:1.9.1
```

The kubectl set image command updates the nginx image of the Deployment's Pods one at a time.

★ Question 2:

Datachamps is an organization resource and it has many projects under it .The company uses BigQuery for data analysis. They want a user named admin-bigquery to be the admin for all BigQuery data across all of the projects under the Datachamps organization . Monitorbigquery is a service account that's responsible for monitoring the size of all the tables across all projects in the Datachamps organization. What predefined roles must be given to admin-bigquery (user) and Monitorbigquery (service account)?

- ◯ `bigquery.user` **to admin-bigquery and** `bigquery.dataViewer` **to Monitorbigquery service**
- ◯ `bigquery.admin` **to admin-bigquery and** `bigquery.dataViewer` **to Monitorbigquery service account.**
- ◯ `bigquery.admin` **to admin-bigquery and** `bigquery.dataOwner` **to Monitorbigquery service account.**
- ◯ `bigquery.connectionAdmin` **to admin-bigquery and** `bigquery.dataEditor` **to Monitoringbigquery service account**

Question 2: **Skipped**

Datachamps is an organization resource and it has many projects under it .The company uses BigQuery for data analysis. They want a user named admin-bigquery to be the admin for all BigQuery data across all of the projects under the Datachamps organization . Monitorbigquery is a service account that's responsible for monitoring the size of all the tables across all projects in the Datachamps organization. What predefined roles must be given to admin-bigquery (user) and Monitorbigquery (service account)?

- ◯ `bigquery.user` **to admin-bigquery and** `bigquery.dataViewer` **to Monitorbigquery service**
- ◯ `bigquery.admin` **to admin-bigquery and** `bigquery.dataViewer` **to Monitorbigquery service account.** (Correct)
- ◯ `bigquery.admin` **to admin-bigquery and** `bigquery.dataOwner` **to Monitorbigquery service account.**
- ◯ `bigquery.connectionAdmin` **to admin-bigquery and** `bigquery.dataEditor` **to Monitoringbigquery service account**

Explanation

On organization Datachamps add admin-bigquery to the predefined role bigquery.admin this provides permissions to manage all resources across the project and manage all data across the project, and can cancel jobs from other users running across the project. Add Monitor bigquery to the predefined role bigquery.dataViewer ,when applied at the project or organization level, this role can also enumerate all datasets in the project and this the appropriate role to fulfil the objective of monitoring tables across all projects .

- A is the Incorrect choice because , bigquery.user role provides permissions to run jobs, including queries, across the project. The user role can enumerate their own jobs, cancel their own jobs, and enumerate datasets across the projects when applied at an organizational level , but we need bigquery.admin role for the admin-bigquery.

- C is Incorrect because , bigquery.dataOwner When applied to a dataset, dataOwner provides permissions to: Read, update, and delete the dataset ,Create, update, get, and delete the dataset's tables. When applied at the project or organization level, this role can also create new datasets. The bigquery_dataViewer is the appropriate permission for monitoring the size of all the tables across all projects in the Datachamps organization.

- D is Incorrect choice because we would need bigquery.admin not bigquery.connectionAdmin. Also When bigquery.dataEditor role is applied to a dataset, dataEditor provides permissions to , read the dataset's metadata and to list tables in the dataset. Create, update, get, and delete the dataset's tables. When applied at the project or organization level, this role can also create new datasets. . The bigquery_dataViewer is the appropriate permission for monitoring the size of all the tables across all projects in the Datachamps organization.

Question 3:

Container Engine is built on which open source system?

- ○ **Swarm**
- ○ **Kubernetes**
- ○ **Docker Orchastrate**
- ○ **Mesos**

Container Engine is built on which open source system?

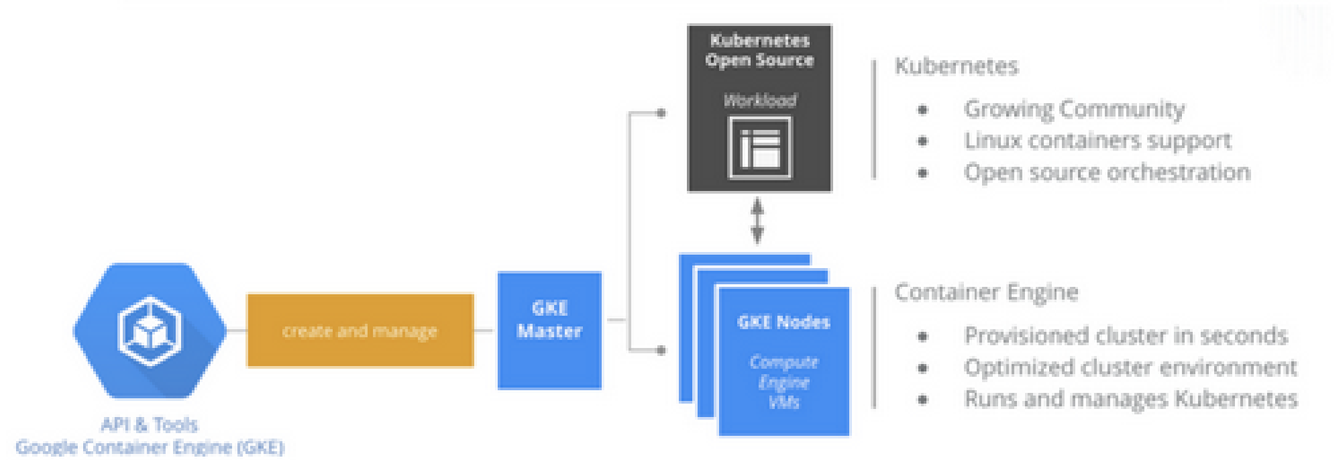
- ○ **Swarm**
- ○ **Kubernetes** (Correct)
- ○ **Docker Orchastrate**
- ○ **Mesos**

Explanation

Google Container Engine is a powerful cluster manager and orchestration system for running your Docker containers. Container Engine schedules your containers into the cluster and manages them automatically based on requirements you define (such as CPU and memory). It's built on the open source

Kubernetes system, giving you the flexibility to take advantage of **on-premises, hybrid, or public cloud** infrastructure.

Reference: https://cloud.google.com/container-engine/



Question 4:

A company is hosting their web hosting platform on Google Cloud using Google Kubernetes Engine. The application now needs to credit payments and needs to be PCI-DSS compliant. How can the company handle the requirement?

- ◯ **As GCP is PCI-DSS complaint, there is no separate handling for individual services**
- ◯ **GKE is not PCI-DSS complaint as services run on shared hosts, the requirement cannot be fulfilled**
- ◯ **GKE and GCP provides you with tools to handle PCI-DSS compliance**
- ◯ **GKE is PCI-DSS complaint and no additional changes are required**

A company is hosting their web hosting platform on Google Cloud using Google Kubernetes Engine. The application now needs to credit payments and needs to be PCI-DSS compliant. How can the company handle the requirement?

- ○ **As GCP is PCI-DSS complaint, there is no separate handling for individual services**
- ○ **GKE is not PCI-DSS complaint as services run on shared hosts, the requirement cannot be fulfilled**
- ○ **GKE and GCP provides you with tools to handle PCI-DSS compliance** (Correct)
- ○ **GKE is PCI-DSS complaint and no additional changes are required**

Explanation
GCP and GKE provides you will tools and approaches to make you hosting and applications PCI-DSS complaint.

PCI-DSS Compliance in GCP

Approach the nodes and pods in a GKE cluster the same way as any merchant-managed server. Implement logging, instrumentation, and patching at both the node and pod level. Don't keep cardholder data at the node level; however, nodes will still be in scope if they contain or might contain any in-scope pods.

To restrict access to your cluster master, use authorized networks to block untrusted IP addresses from outside GCP. These CIDR rules are compatible with private clusters and act as a whitelist.

Implement network policies in the GKE cluster when your in-scope projects contain different types of pods. Network policies work similar to the virtual private cloud (VPC) firewalls that you might already be familiar with. You can allow or deny traffic based on IP rules or labels.

Requirement 2.2.1 stipulates that only one primary function can be implemented per server. This requirement does not prohibit the case of a single GKE cluster hosting more than one pod type. The primary function of GKE nodes is to serve and manage containers. If designed properly, individual pods can also adhere to this primary function rule in a single cluster.

- Options A & D is wrong as the application hosting using GKE to be PCI-DSS complaint is customers responsibility.
- Option B is wrong as GKE hosting can be made PCI-DSS complaint.

Question 5:

A company is migrating its data to Google Cloud using Cloud VPN tunnel. They are trying to setup Virtual Private Network on Cloud Which of the following conditions is true regarding the IPs?

- ○ **Primary IPs between on-premises and Cloud should not overlap, while Secondary IPs can overlap**
- ○ **Primary & Secondary IPs between on-premises and Cloud can overlap**
- ○ **Primary IPs between on-premises and Cloud can overlap, while Secondary IPs should not overlap**
- ○ **Primary & Secondary IPs between on-premises and Cloud should not overlap**

A company is migrating its data to Google Cloud using Cloud VPN tunnel. They are trying to setup Virtual Private Network on Cloud Which of the following conditions is true regarding the IPs?

- ○ **Primary IPs between on-premises and Cloud should not overlap, while Secondary IPs can overlap**
- ○ **Primary & Secondary IPs between on-premises and Cloud can overlap**
- ○ **Primary IPs between on-premises and Cloud can overlap, while Secondary IPs should not overlap**
- ○ **Primary & Secondary IPs between on-premises and Cloud should not overlap** (Correct)

Explanation

The primary and secondary IPs of VPCs should not overlap with **on-premises** data center network.

VM alias IP ranges must be assigned from a range owned by the subnet that the VM is in. All subnets have a primary range, which is the standard range of internal IP addresses that defines the subnet. A subnet may also have one or more secondary IP ranges of internal IP addresses. You can assign alias IP ranges from either the primary or secondary ranges of the subnet.

You must give each secondary range a name that is unique for the subnet. When assigning an alias IP range to a VM, the secondary range name tells GCP from which subnet range to assign the alias IPs.

All ranges, both primary and secondary, must be unique across across all subnets in the VPC network and in any networks attached via VPC Network Peering, VPN, or Interconnect.

★ Question 6:

A Company is planning the migration of their web application to Google App Engine. However, they would still continue to use their on-premises database. How can they setup application?

- ○ **Setup the application using App Engine Standard environment with Cloud VPN to connect to database**
- ○ **Setup the application using App Engine Flexible environment with Cloud VPN to connect to database**
- ○ **Setup the application using App Engine Standard environment with Cloud Router to connect to database**
- ○ **Setup the application using App Engine Flexible environment with Cloud Router to connect to database**

A Company is planning the migration of their web application to Google App Engine. However, they would still continue to use their on-premises database. How can they setup application?

- ○ **Setup the application using App Engine Standard environment with Cloud VPN to connect to database**
- ○ **Setup the application using App Engine Flexible environment with Cloud VPN to connect to database** (Correct)
- ○ **Setup the application using App Engine Standard environment with Cloud Router to connect to database**
- ○ **Setup the application using App Engine Flexible environment with Cloud Router to connect to database**

Explanation
Correct answer is B as Google App Engine provides connectivity to on-premises using Cloud VPN.

App Engine Flexible Network Settings

- **Advanced network configuration:**

You can segment your Compute Engine network into subnetworks. This allows you to enable VPN scenarios, such as accessing databases within your corporate network.

- **To enable subnetworks for your App Engine application:**

1. Create a custom subnet network:
2. Add the network name and subnetwork name to your app.yaml file, as specified above.
3. To establish a simple VPN based on static routing, create a gateway and a tunnel for a custom subnet network. Otherwise, see how to create other types of VPNs.

- Option A is wrong as Google App Engine Standard cannot use Cloud VPN.
- Options C & D are wrong as you need a Cloud VPN to connect to on-premises data center. Cloud Route support dynamic routing.

Question 7:

Container Engine allows orchastration of what type of containers?

- ○ **Blue Whale**
- ○ **LXC**
- ○ **BSD Jails**
- ○ **Docker**

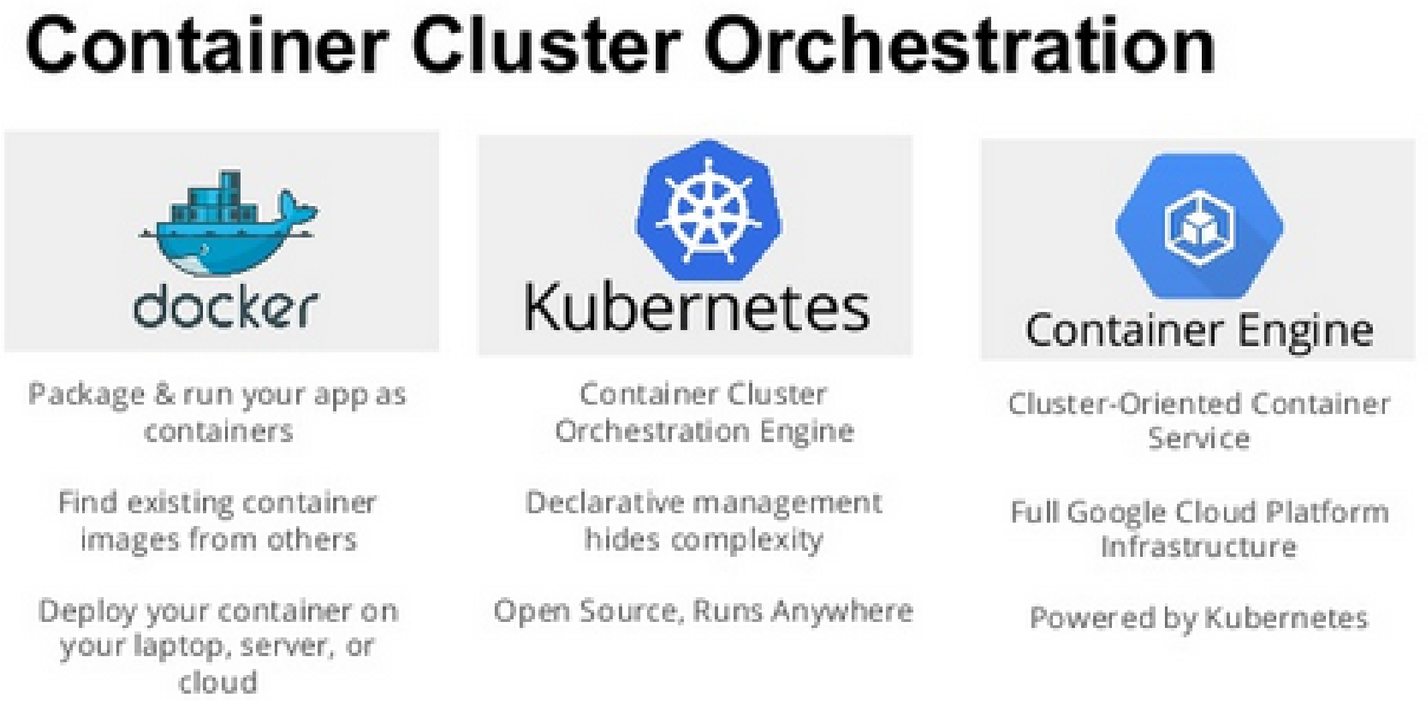
Container Engine allows orchastration of what type of containers?

- ○ **Blue Whale**
- ○ **LXC**
- ○ **BSD Jails**
- ○ **Docker** (Correct)

Explanation

Google Container Engine is a powerful cluster manager and orchestration system for running your Docker containers.

Reference: https://cloud.google.com/container-engine/



★ Question 8:

Company use BigQuery as data warehouse across departments. Each department use Dataset with multiple tables in it. Marketing Analytics (AnalystGroup) team will need to have (ONLY) read access to data from datasets of all departments. How you design your permissions? Make sure AnalystGroup should not have write access to department data ?

- ◯ **Provide AnalystGroup to `bigquery.user` in marketing department project.**
  Provide AnalystGroup to `bigquery.admin` in individual projects.

- ◯ **Provide AnalystGroup to `bigquery.user` in marketing department project.**
  Provide AnalystGroup to `bigquery.dataViewer` in individual projects.

- ◯ **Provide AnalystGroup to `bigquery.admin` in marketing department project.**
  Provide AnalystGroup to `bigquery.dataviewer` in individual projects.

- ◯ **Provide AnalystGroup to `bigquery.admin` in marketing department project.**
  Provide AnalystGroup to `bigquery.admin` in individual projects.

Company use BigQuery as data warehouse across departments. Each department use Dataset with multiple tables in it. Marketing Analytics (AnalystGroup) team will need to have (ONLY) read access to data from datasets of all departments. How you design your permissions? Make sure AnalystGroup should not have write access to department data ?

- ◯ **Provide AnalystGroup to `bigquery.user` in marketing department project.**
  Provide AnalystGroup to `bigquery.admin` in individual projects.

- ◯ **Provide AnalystGroup to `bigquery.user` in marketing department project.**
  Provide AnalystGroup to `bigquery.dataViewer` in individual projects.
  (Correct)

- ◯ **Provide AnalystGroup to `bigquery.admin` in marketing department project.**
  Provide AnalystGroup to `bigquery.dataviewer` in individual projects.

- ◯ **Provide AnalystGroup to `bigquery.admin` in marketing department project.**
  Provide AnalystGroup to `bigquery.admin` in individual projects.

Explanation

Read access to data in a different project

AnalystGroup is a set of data scientists responsible for analytics services within a project named CompanyAnalytics. The data they analyze, however, resides in a separate project named CompanyLogs. OperationsServiceAccount is a service account that's responsible for loading application logs into BigQuery by using bulk load jobs to a variety of datasets in the CompanyLogs project.

AnalystGroup can only read data in the CompanyLogs project and cannot create additional storage or run any query jobs in that project. Instead, the analysts use project CompanyAnalytics to perform their work, and maintain their output within the CompanyAnalytics project.

Read access to data in a different project	
On project CompanyLogs	• Add OperationsServiceAccount to the predefined role `bigquery.admin`. • Add AnalystGroup to the predefined role `bigquery.dataViewer`.
On project CompanyAnalytics	• Add AnalystGroup to the predefined role `bigquery.user`.

Reference: https://cloud.google.com/bigquery/docs/access-control-examples#read_access_to_data_in_a_different_project

Question 9:

Company requires the data stored in BigQuery tables to be deleted after 3 years. The table will be used by reporting system and should not impacted. What will be your solution ?

- ◯ **Use Google Scheduler to delete old data.**
- ◯ **Use Table level expiration configuration.**
- ◯ **Use Time partitioning for table and use partition expiration time configuration either at Dataset or at table**
- ◯ **Use BigQuery Dataset table expiration configuration.**

Company requires the data stored in BigQuery tables to be deleted after 3 years. The table will be used by reporting system and should not impacted. What will be your solution ?

- ◯ **Use Google Scheduler to delete old data.**
- ◯ **Use Table level expiration configuration.** (Correct)
- ◯ **Use Time partitioning for table and use partition expiration time configuration either at Dataset or at table**
- ◯ **Use BigQuery Dataset table expiration configuration.**

Explanation

Best practice: Configure the default table expiration for your datasets, configure the expiration time for your tables, and configure the partition expiration for partitioned tables.

References:

https://cloud.google.com/bigquery/docs/updating-datasets#partition-expiration

https://cloud.google.com/bigquery/docs/best-practices-storage

Question 10:

In your company, there is one application that is running on Compute Engine VM instances having Linux operation system. These VM instances are launched using managed instance group. This application is facing some performance issues on one of the VM instance that host this application and you need to find the cause of this performance issue. You observed that when application is under heavy load, then some application requests are getting dropped and there is a single application process that is consuming all the available CPU on misbehaving instance. Autoscaling of VM instance has reached the upper limit of instances and there is normal load on all other related systems. Database is also working fine.

To solve this production issue, what can you suggest?

- ◯ **Create an autoscaling metric based on percentage of memory used and use this metric to do autoscaling**
- ◯ **Restart the misbehaving instances on a regular scheduled basis.**
- ◯ **Increase the maximum number of instances limit in the autoscaling group.**
- ◯ **Login the misbehaving instance via SSH connection and restart the application process.**

In your company, there is one application that is running on Compute Engine VM instances having Linux operation system. These VM instances are launched using managed instance group. This application is facing some performance issues on one of the VM instance that host this application and you need to find the cause of this performance issue. You observed that when application is under heavy load, then some application requests are getting dropped and there is a single application process that is consuming all the available CPU on misbehaving instance. Autoscaling of VM instance has reached the upper limit of instances and there is normal load on all other related systems. Database is also working fine.

To solve this production issue, what can you suggest?

- ◯ **Create an autoscaling metric based on percentage of memory used and use this metric to do autoscaling**
- ◯ **Restart the misbehaving instances on a regular scheduled basis.**
- ◯ **Increase the maximum number of instances limit in the autoscaling group.** (Correct)
- ◯ **Login the misbehaving instance via SSH connection and restart the application process.**

Explanation

Since existing application instances are using full CPU and autoscaling maximum limit is also reached, so to enable more processing, maximum limit of autoscaling group must be increased.

This way it will create more compute engine instance to handle increasing load on existing application infrastructure.

Question 11:

Your company has an application that performs some complex calculation. This application exposes web API for these calculations. Currently this application runs on a single GKE cluster in us-central1 region only.

Now based on the demand of the application, Your company want to expand its business and need to offer Web API to its customers in Asia region as well. As Google Cloud Architect, What solution would you like to suggest?

- ◯ **Create a second GKE cluster in Asia region.**
- ◯ **Use service of type LoadBalancer to expose web API from both regions.**
- ◯ **Add the public IP address to the Cloud DNS zone.**
- ◯ **Use global HTTP(s) load balancer**
- ◯ **Increase the memory and computation capacity in same GKE cluster.**
- ◯ **Create a second GKE cluster in Asia region.**

Your company has an application that performs some complex calculation. This application exposes web API for these calculations. Currently this application runs on a single GKE cluster in us-central1 region only.

Now based on the demand of the application, Your company want to expand its business and need to offer Web API to its customers in Asia region as well. As Google Cloud Architect, What solution would you like to suggest?

- ◯ **Create a second GKE cluster in Asia region.**
- ◯ **Use service of type LoadBalancer to expose web API from both regions.**
- ◯ **Add the public IP address to the Cloud DNS zone.** (Correct)
- ◯ **Use global HTTP(s) load balancer**
- ◯ **Increase the memory and computation capacity in same GKE cluster.**
- ◯ **Create a second GKE cluster in Asia region.**

Explanation

When you create a Service of type Load Balancer, a Google Cloud controller wakes up and configures a network load balancer in your project. The load balancer has a stable IP address that is accessible from outside of your project.

A Network Load Balancer is not a proxy server. It forwards packets with no change to the source and destination IP addresses.

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

Question 12:

You want to migrate Hadoop jobs without modifying the underlying infrastructure. How can you achieve this with minimum cost and minimum infrastructure management effort?

- ◯ **Create a Dataproc cluster using standard worker instances.**
- ◯ **Create a Dataproc cluster using preemptible worker instances**
- ◯ **Setup a Hadoop cluster manually on Compute Engine VM instances.**
- ◯ **Setup a Hadoop cluster manually using preemptible Compute Engine VM instances**

You want to migrate Hadoop jobs without modifying the underlying infrastructure. How can you achieve this with minimum cost and minimum infrastructure management effort?

- ◯ **Create a Dataproc cluster using standard worker instances.**
- ◯ **Create a Dataproc cluster using preemptible worker instances** (Correct)
- ◯ **Setup a Hadoop cluster manually on Compute Engine VM instances.**
- ◯ **Setup a Hadoop cluster manually using preemptible Compute Engine VM instances**

Explanation

Existing Hadoop jobs can be easily migrated to **Dataproc** cluster and **Preemptible Compute Engine VM** instances can be used to reduce the cost.

Question 13:

Your company has microservices based application running on Anthos clusters. This cluster has both Anthos Service Mesh and Anthos Config Management configured. Application user feels latency in application response

How can you find the microservice that is causing the latency in response?

- ◯ **Use Anthos Config Management to create a namespace selector that select the relevant cluster namespace.**
- ◯ **Filter workloads on GCP cloud console for the namespace.**
- ◯ **Analyze the configurations of the filtered workloads.**
- ◯ **Collect and inspect the telemetry for request latency data between microservice by using Service Mesh visualization in GCP Cloud Console.**
- ◯ **Create a Cluster Selector selecting the relevant cluster via Anthos Config Management.**
- ◯ **Filter workloads on GCP cloud console for the above cluster.**

Your company has microservices based application running on Anthos clusters. This cluster has both Anthos Service Mesh and Anthos Config Management configured. Application user feels latency in application response

How can you find the microservice that is causing the latency in response?

- ◯ **Use Anthos Config Management to create a namespace selector that select the relevant cluster namespace.**
- ◯ **Filter workloads on GCP cloud console for the namespace.**
- ◯ **Analyze the configurations of the filtered workloads.**
- ◯ **Collect and inspect the telemetry for request latency data between microservice by using Service Mesh visualization in GCP Cloud Console.** (Correct)
- ◯ **Create a Cluster Selector selecting the relevant cluster via Anthos Config Management.**
- ◯ **Filter workloads on GCP cloud console for the above cluster.**

Explanation

Anthos Service Mesh is a suite of tools that helps you monitor and manage a reliable service mesh **on-premises** or on **Google Cloud**.

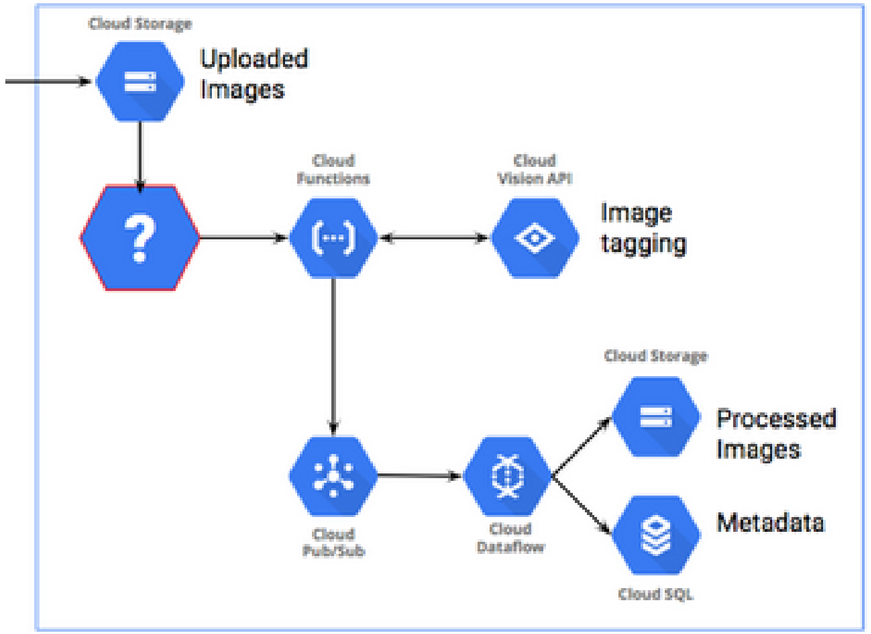
Anthos Service Meshs robust tracing, monitoring, and logging features give you deep insights into how your services are performing, how that performance affects other processes, and any issues that might exist.

Reference: https://cloud.google.com/service-mesh/docs/overview

Question 14:

A company is building an image tagging pipeline.

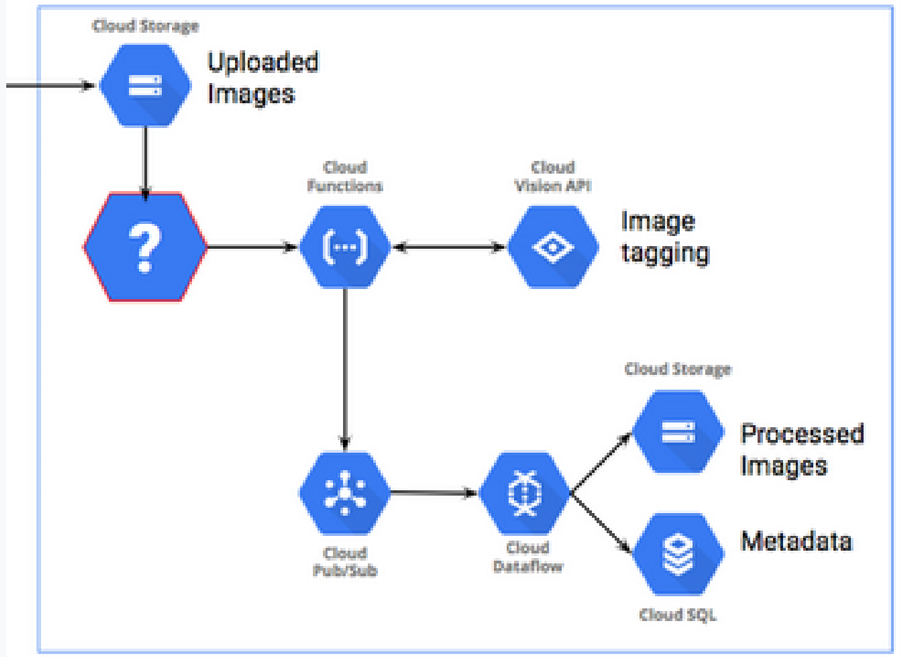
Which service should be used in the icon with the question mark in the diagram ?



- ◯ **Cloud Datastore**
- ◯ **Cloud Dataflow**
- ◯ **Cloud Pub/Sub**
- ◯ **Cloud Bigtable**

A company is building an image tagging pipeline.

Which service should be used in the icon with the question mark in the diagram ?



- ◯ **Cloud Datastore**
- ◯ **Cloud Dataflow**
- ◯ **Cloud Pub/Sub** (Correct)
- ◯ **Cloud Bigtable**

Explanation

Cloud Storage upload events can push Cloud Pub/Sub to trigger a Cloud Function to ingest and process the image.

- **Documentation**: Cloud Storage Pub/Sub Notifications

Cloud Pub/Sub Notifications sends information about changes to objects in your buckets to Cloud Pub/Sub, where the information is added to a Cloud Pub/Sub topic of your choice in the form of messages. For example, you can track objects that are created and deleted in your bucket. Each notification contains information describing both the event that triggered it and the object that changed.

Cloud Pub/Sub Notifications are the recommended way to track changes to objects in your Cloud Storage buckets because they're faster, more flexible, easier to set up, and more cost-effective.

Question 15:

Your company wants to store some secured files in GCS bucket from on-premises data center.

Since its a secured file, so they want to ensure that file stored in GCS bucket is exactly same copy of file stored in on-premises data center.

How can you achieve this with minimal cost and effort?

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Computes CRC32C hashes via custom application in on-premises data center.
  Collect CRC32C hashes of uploaded files via `gsutil ls -L gs://[YOUR_BUCKET_NAME]`.
  Compare the hashes.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Download the uploaded files via gsutil cp command .
  Use Linux diff command to compare the files content.
  Use Linux shasum to compute a digest of the files in on-premises data center.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Download the uploaded files via `gsutil cp` command .
  Use Linux shasum to compute a digest of the downloaded files.
  Compare the hashes.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Calculate CRC32C hashes of all on premise files via gsutil hash -c FILE_NAME.
  Collect CRC32C hashes of uploaded files via `gsutil ls -L gs://[YOUR_BUCKET_NAME].`
  Compare the hashes.

Your company wants to store some secured files in GCS bucket from on-premises data center.

Since its a secured file, so they want to ensure that file stored in GCS bucket is exactly same copy of file stored in on-premises data center.

How can you achieve this with minimal cost and effort?

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Computes CRC32C hashes via custom application in on-premises data center.
  Collect CRC32C hashes of uploaded files via `gsutil ls -L gs://[YOUR_BUCKET_NAME]`.
  Compare the hashes.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Download the uploaded files via gsutil cp command .
  Use Linux diff command to compare the files content.
  Use Linux shasum to compute a digest of the files in on-premises data center.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Download the uploaded files via `gsutil cp` command .
  Use Linux shasum to compute a digest of the downloaded files.
  Compare the hashes.

- ◯ **Upload all the files to GCS bucket via `gsutil -m` command.**
  Calculate CRC32C hashes of all on premise files via gsutil hash -c FILE_NAME.
  Collect CRC32C hashes of uploaded files via `gsutil ls -L gs://[YOUR_BUCKET_NAME].`
  Compare the hashes.

  (Correct)

Explanation

`gsutil -m`

It allows to upload files in parallel using multithreading.

`gsutil hash [-c] [-h] [-m] filename…`

The hash command calculates hashes on a local file that can be used to compare with gsutil ls -L output. If a specific hash option is not provided, this command calculates all gsutil-supported hashes for the file.

Question 16:

You want to deploy application using microservice architecture in GKE but you do not want to expose these microservices end points to external world. All these microservices will be used inside cluster only. All these microservice can have different number of replicas.

Now suggest a way so that all these microservices can communicate with each other in uniform and consistent manner.

- ◯ **Create Deployment for each microservice to deploy in GKE cluster.**
  Use Service to expose the deployment in the cluster.
  One microservices should talk to other microservice in cluster via Service DNS name.

- ◯ **Create Deployment for each microservice to deploy in GKE cluster.**
  Use Ingress to expose the deployment in the cluster.
  One microservice should talk to other microservice in cluster via Ingress IP address.

- ◯ **Create Pod for each microservice to deploy in GKE cluster.**
  Use Service to expose the deployment in the cluster.
  One microservices should talk to other microservice in cluster via Service DNS name.

- ◯ **Create Pod for each microservice to deploy in GKE cluster.**
  Use Ingress to expose the deployment in the cluster.
  One microservice should talk to other microservice in cluster via Ingress IP address.

You want to deploy application using microservice architecture in GKE but you do not want to expose these microservices end points to external world. All these microservices will be used inside cluster only. All these microservice can have different number of replicas.

Now suggest a way so that all these microservices can communicate with each other in uniform and consistent manner.

- ◯ **Create Deployment for each microservice to deploy in GKE cluster. Use Service to expose the deployment in the cluster. One microservices should talk to other microservice in cluster via Service DNS name.** (Correct)

- ◯ **Create Deployment for each microservice to deploy in GKE cluster. Use Ingress to expose the deployment in the cluster. One microservice should talk to other microservice in cluster via Ingress IP address.**

- ◯ **Create Pod for each microservice to deploy in GKE cluster. Use Service to expose the deployment in the cluster. One microservices should talk to other microservice in cluster via Service DNS name.**

- ◯ **Create Pod for each microservice to deploy in GKE cluster. Use Ingress to expose the deployment in the cluster. One microservice should talk to other microservice in cluster via Ingress IP address.**

Explanation

Deployments represent a set of multiple, identical Pods with no unique identities. A Deployment runs multiple replicas of your application and automatically replaces any instances that fail or become unresponsive. In this way, Deployments help ensure that one or more instances of your application are available to serve user requests. Deployments are managed by the Kubernetes Deployment controller.

In GKE, Service is use to group a set of Pod endpoints into a single resource. You can configure various ways to access the grouping. By default, you get a stable cluster IP address that clients inside the cluster can use to contact Pods in the Service. A client sends a request to the stable IP address, and the request is routed to one of the Pods ir the Service.

A Service also provides load balancing. Clients call a single, stable IP address, and their requests are balanced across the Pods that are members of the Service.

Question 17:

Your company needs to design a Data Warehousing solution in GCP. Your team wants to store secured data in BigQuery. Your team requires you to have the encryption keys generated outside Google Cloud Platform.

As a cloud architect what solution would you like to suggest for this?

- ◯ **Generate a new key in Cloud Key Management Service (Cloud KMS).**
  Store all the data in GCS Bucket using the customer-managed key and select the key created in previous step.
  Set up dataflow processing pipeline to read data from GCS bucket, decrypt this data and then store it in a new BigQuery dataset.

- ◯ **Generate a new key in Cloud Key Management Service (Cloud KMS).**
  Create a dataset in BigQuery using the customer-managed key and select the key created in previous step.
  Import a key in Cloud Key Management Service (Cloud KMS).

- ◯ **Store all the data in GCS Bucket using the customer-managed key and select the key created in previous step.**
  Set up a Dataflow processing pipeline to read data from GCS bucket, decrypt this data and then store it in a new BigQuery dataset.

- ◯ **Import a key in Cloud Key Management Service (Cloud KMS).**
  Create a dataset in BigQuery using the customer-managed key and select the key created in previous step.

Your company needs to design a Data Warehousing solution in GCP. Your team wants to store secured data in BigQuery. Your team requires you to have the encryption keys generated outside Google Cloud Platform.

As a cloud architect what solution would you like to suggest for this?

- ◯ **Generate a new key in Cloud Key Management Service (Cloud KMS). Store all the data in GCS Bucket using the customer-managed key and select the key created in previous step. Set up dataflow processing pipeline to read data from GCS bucket, decrypt this data and then store it in a new BigQuery dataset.**

- ◯ **Generate a new key in Cloud Key Management Service (Cloud KMS). Create a dataset in BigQuery using the customer-managed key and select the key created in previous step. Import a key in Cloud Key Management Service (Cloud KMS).**

- ◯ **Store all the data in GCS Bucket using the customer-managed key and select the key created in previous step. Set up a Dataflow processing pipeline to read data from GCS bucket, decrypt this data and then store it in a new BigQuery dataset.**

- ◯ **Import a key in Cloud Key Management Service (Cloud KMS). Create a dataset in BigQuery using the customer-managed key and select the key created in previous step.** (Correct)

Explanation

BigQuery encrypts customer content stored at rest. BigQuery handles and manages this default encryption for you without any additional actions on your part.

If you want to control encryption yourself, you can use customer-managed encryption keys (CMEK) for BigQuery. Instead of Google managing the encryption keys that protect your data, you control and manage encryption keys in Cloud KMS

https://cloud.google.com/bigquery/docs/customer-managed-encryption

Since key needs to be generated outside GCP, so we can import that key in KMS to be used by BigQuery.

Question 18:

Your company has an application deployed in a GKE cluster. You have three clusters for development, staging and production environments.

Your operation team found that the team can do application deployment to the production cluster without first testing the application in lower environments like development and staging environment.

As operation team head, You want team to be autonomous but want to prevent the direct production deployment.

As Google Cloud architect, what solution you can suggest to achieve this quickly with less effort?

- ◯ **First, configure the binary authorization policies for all GKE clusters, development. staging and production clusters.**
- ◯ **Set up a CI/CD pipeline that require the attestations as part of the pipeline processing.**
- ◯ **Create an IAM group of all team leads**
- ◯ **Create a policy to allow team leads in this group to do deployment on production GKE cluster**
- ◯ **Create a GKE lifecycle hook to prevent the container from starting if container image is not approved for usage in the given environment.**
- ◯ **Implement a corporate policy to prevent teams from deploying Docker images to an environment unless the Docker image was tested in an earlier environment.**

Your company has an application deployed in a GKE cluster. You have three clusters for development, staging and production environments.

Your operation team found that the team can do application deployment to the production cluster without first testing the application in lower environments like development and staging environment.

As operation team head, You want team to be autonomous but want to prevent the direct production deployment.

As Google Cloud architect, what solution you can suggest to achieve this quickly with less effort?

- ◯ **First, configure the binary authorization policies for all GKE clusters, development. staging and production clusters.**
- ◯ **Set up a CI/CD pipeline that require the attestations as part of the pipeline processing.** (Correct)
- ◯ **Create an IAM group of all team leads**
- ◯ **Create a policy to allow team leads in this group to do deployment on production GKE cluster**
- ◯ **Create a GKE lifecycle hook to prevent the container from starting if container image is not approved for usage in the given environment.**
- ◯ **Implement a corporate policy to prevent teams from deploying Docker images to an environment unless the Docker image was tested in an earlier environment.**

Explanation

Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run. With Binary Authorization, you can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying. By enforcing validation, you can gain tighter control over your container environment by ensuring that only verified images are integrated into the build-and-release process.

https://cloud.google.com/binary-authorization

Question 19:

Your company has a monolithic application. This application has lots of issues in terms of reliability, and being a monolithic application, it is difficult to do any enhancements in this application. Now this team want to break this monolithic application into multiple microservices but they want to minimize the operation overhead of microservice architecture. So this team is more interested in using fully managed service for this microservice architecture.

How can this team convince their top management to provide approval for this transition from monolithic to microservice architecture.

What are the advantages that this team can highlight?

- ◯ **Microservice architecture will decouple infrastructure from application.**
- ◯ **Development and release cycle of new features will become easy.**
- ◯ **It is easy to set up CI/CD pipeline for each microservice in cloud.**
- ◯ **A/B testing can be done easily for each microservice.**
- ◯ **Microservices are easy to scale.**

Your company has a monolithic application. This application has lots of issues in terms of reliability, and being a monolithic application, it is difficult to do any enhancements in this application. Now this team want to break this monolithic application into multiple microservices but they want to minimize the operation overhead of microservice architecture. So this team is more interested in using fully managed service for this microservice architecture.

How can this team convince their top management to provide approval for this transition from monolithic to microservice architecture.

What are the advantages that this team can highlight?

- ◯ **Microservice architecture will decouple infrastructure from application.**
- ◯ **Development and release cycle of new features will become easy.**
- ◯ **It is easy to set up CI/CD pipeline for each microservice in cloud.**
- ◯ **A/B testing can be done easily for each microservice.**
- ◯ **Microservices are easy to scale.** (Correct)

Explanation
All the reason mentioned in choice A are obvious advantages of using microservice.

https://cloud.google.com/architecture/migrating-a-monolithic-app-to-microservices-gke

★ Question 20:

You need to migrate your application running in on-premises data center to Google Cloud. You are not able to select right machine configuration in terms of CPU and memory in cloud. In on-premises data center this application was optimally configured for efficient usage of resources. This application has been getting used uniformly throughout the week since multiple weeks.
As Google Cloud architect how can you optimize the resource usage of VM instance running in Cloud?

- ◯ **You also need to take care of costing of VM as well.**
  Select the machine type having CPU and memory configuration similar to on-premises instance.
  Use this machine type to create VM instance in Google Cloud.
  Configure the Cloud Monitoring agent and deploy the third party application on these VM instances.
  Do load testing of your application in cloud for usual traffic that you were getting in on-premises data center.
  Follow the recommendations shown in Cloud Console for rightsizing of the VM instances running in cloud..

- ◯ **Create multiple compute engine instances with varying CPU and memory options.**
  Configure the Cloud Monitoring agent and deploy the third party application on these VM instances.
  Do load testing of your application in cloud for peak traffic.
  Use load testing results to tune in the configuration of CPU and memory

- ◯ **Create an image of the third-party application running in on-premises virtual machine.**
  Create an instance template with the smallest available machine type that use image created in previous step.
  Create a managed instance group.
  Use average CPU utilization to autoscale the number of instances in the group.

- ◯ **Optimize the number of instances running based on the average CPU utilization threshold.**
  Use App Engine Flexible environment to deploy the third-party application using a Dockerfile.
  Configure CPU and memory options similar to your application's current on-premises virtual machine in the app.yaml file

You need to migrate your application running in on-premises data center to Google Cloud. You are not able to select right machine configuration in terms of CPU and memory in cloud. In on-premises data center this application was optimally configured for efficient usage of resources. This application has been getting used uniformly throughout the week since multiple weeks.
As Google Cloud architect how can you optimize the resource usage of VM instance running in Cloud?

- ◯ **You also need to take care of costing of VM as well.**
  Select the machine type having CPU and memory configuration similar to on-premises instance.
  Use this machine type to create VM instance in Google Cloud.
  Configure the Cloud Monitoring agent and deploy the third party application on these VM instances.
  Do load testing of your application in cloud for usual traffic that you were getting in on-premises data center.
  Follow the recommendations shown in Cloud Console for rightsizing of the VM instances running in cloud..
  (Correct)

- ◯ **Create multiple compute engine instances with varying CPU and memory options.**
  Configure the Cloud Monitoring agent and deploy the third party application on these VM instances.
  Do load testing of your application in cloud for peak traffic.
  Use load testing results to tune in the configuration of CPU and memory

- ◯ **Create an image of the third-party application running in on-premises virtual machine.**
  Create an instance template with the smallest available machine type that use image created in previous step.
  Create a managed instance group.
  Use average CPU utilization to autoscale the number of instances in the group.

- ◯ **Optimize the number of instances running based on the average CPU utilization threshold.**
  Use App Engine Flexible environment to deploy the third-party application using a Dockerfile.
  Configure CPU and memory options similar to your application's current on-premises virtual machine in the app.yaml file

Explanation
Since this application is already configured in optimal manner in on-premises data center so it make sense to use similar configurations in GCP as well.

- Option A looks like the right option.
- Option B is incorrect because we can not create a VM with varying number of CPU and memory.
- Option C look incorrect because only CPU is considered for optimal configuration of application.
- Option D is not correct because it is a simple lift and shift approach to migrate to cloud. In this case, first application might need to be containerized using Docker. This is an extra development effort so this is not preferred.

Question 21:

You need to run an application on Compute Engine VM instance in Google Cloud Platform that use Ubuntu Linux operating system. This application needs very complex configurations in order to run it properly.

How can you ensure that you can install Ubuntu distribution updates with minimal manual intervention whenever such update is available?

- ◯ **Create a Compute Engine instance using a latest image of Ubuntu Linux operating system.**
  Install and configure the application on this VM.
  Use OS patch management to install available updates.

- ◯ **Create a Compute Engine instance template using a latest image of Ubuntu Linux operating system.**
  Create an instance from this template.
  Install and configure the application as part of the startup script.
  Repeat the process whenever a new Google-managed Ubuntu image becomes available

- ◯ **Create a Compute Engine instance using a latest image of Ubuntu Linux operating system.**
  Install and configure the application on the instance after connecting to this instance via SSH.
  Repeat this process whenever a new Google Cloud managed Ubuntu image becomes available

- ◯ **Create a Docker container image with Ubuntu as the base image.**
  Install and configure the application as part of Docker image creation process.
  Host the container on GKE.
  Restart the container whenever a new update is available.

You need to run an application on Compute Engine VM instance in Google Cloud Platform that use Ubuntu Linux operating system. This application needs very complex configurations in order to run it properly.

How can you ensure that you can install Ubuntu distribution updates with minimal manual intervention whenever such update is available?

- ◯ **Create a Compute Engine instance using a latest image of Ubuntu Linux operating system.**
  Install and configure the application on this VM.
  Use OS patch management to install available updates.

- ◯ **Create a Compute Engine instance template using a latest image of Ubuntu Linux operating system.**
  Create an instance from this template.
  Install and configure the application as part of the startup script.
  Repeat the process whenever a new Google-managed Ubuntu image becomes available
  (Correct)

- ◯ **Create a Compute Engine instance using a latest image of Ubuntu Linux operating system.**
  Install and configure the application on the instance after connecting to this instance via SSH.
  Repeat this process whenever a new Google Cloud managed Ubuntu image becomes available

- ◯ **Create a Docker container image with Ubuntu as the base image.**
  Install and configure the application as part of Docker image creation process.
  Host the container on GKE.
  Restart the container whenever a new update is available.

Explanation

- Option A and Option C, are incorrect because in both options, application configurations has to be done manually again and again with release of new Ubuntu Image. Since application configuration is very extensive, so manual configuration of application repeatedly is not the right choice. It is both time consuming and error prone because there can be some mistake in doing the manual configuration.
- Option D, is incorrect because it requires to create a Docker image that contains both OS and application configuration. It is not a good idea to have OS in docker image. In addition to this, creating a docker image is additional development effort as well.
- Option B is the correct choice because in this option Startup Script is used to install and configure application. Startup Script execution is an automated process which will be executed automatically whenever new instance is created.

With combination of instance template and Startup Script, we can create any number of compute engine instances very quickly with exactly same configurations.

Question 22:

Your company is designing its data lake on Google Cloud and wants to develop different ingestion pipelines to collect unstructured data from different sources. After the data is stored in Google Cloud, it will be processed in several data pipelines to build a recommendation engine for the end users on the website. The structure of the data retrieved from the source system can change at any time. The data must be stored exactly as it was retrieved for reprocessing purpose in case the data structure is incompatible with the current processing pipelines.

How will you design an architecture to support the use case after you retrieve the data?

- ◯ **Send the data through the processing pipeline, and then store the processed data in a Cloud Storage bucket for reprocessing.**
- ◯ **Send the data through the processing pipeline, and then store the processed data in a BigQuery table for reprocessing.**
  Store the data in a BigQuery table.
- ◯ **Design the processing pipelines to retrieve the data from the table.**
  Store the data in a Cloud Storage bucket.
- ◯ **Design the processing pipelines to retrieve the data from the bucket.**

Your company is designing its data lake on Google Cloud and wants to develop different ingestion pipelines to collect unstructured data from different sources. After the data is stored in Google Cloud, it will be processed in several data pipelines to build a recommendation engine for the end users on the website. The structure of the data retrieved from the source system can change at any time. The data must be stored exactly as it was retrieved for reprocessing purpose in case the data structure is incompatible with the current processing pipelines.

How will you design an architecture to support the use case after you retrieve the data?

- ◯ **Send the data through the processing pipeline, and then store the processed data in a Cloud Storage bucket for reprocessing.**
- ◯ **Send the data through the processing pipeline, and then store the processed data in a BigQuery table for reprocessing.**
  Store the data in a BigQuery table.
- ◯ **Design the processing pipelines to retrieve the data from the table.**
  Store the data in a Cloud Storage bucket.
- ◯ **Design the processing pipelines to retrieve the data from the bucket.** (Correct)

Explanation

Option A and Option B are incorrect because in both cases, processed data is stored. As per requirement, our solution must store the input data as it is in raw format for processing purpose because structure of the data retrieved from the source system can change at any time.

Option C is incorrect because we can not store raw data in BigQuery. BigQuery store only structured data.

Option D is correct choice here because in this option we are storing raw data in Cloud Storage bucket and then creating data processing pipeline using this raw data as input

Question 23:

Your company is running a solution in App Engine Standard environment. The project that contains the App Engine application has a VPC network and this VPC network is connected with company's on-premises environment via a Cloud VPN tunnel.

What solution can you suggest so that the App Engine application can access database running inside the on-premises environment?

- ◯ **Configure serverless VPC access.**
- ◯ **Configure private services access**
- ◯ **Configure private Google access.**
- ◯ **Configure private Google access for on-premises hosts only.**

Your company is running a solution in App Engine Standard environment. The project that contains the App Engine application has a VPC network and this VPC network is connected with company's on-premises environment via a Cloud VPN tunnel.

What solution can you suggest so that the App Engine application can access database running inside the on-premises environment?

- ◯ **Configure serverless VPC access.** (Correct)
- ◯ **Configure private services access**
- ◯ **Configure private Google access.**
- ◯ **Configure private Google access for on-premises hosts only.**

Explanation
Serverless VPC Access enables you to connect from a serverless environment on Google Cloud directly to your VPC network. This connection makes it possible for your serverless environment to access resources in your VPC network via internal IP addresses.

With Serverless VPC Access, you create a connector in your Google Cloud project and attach it to a VPC network. You then configure your serverless services (such as Cloud Run services, App Engine apps, or Cloud Functions) to use the connector for internal network traffic.

Serverless VPC Access only allows requests to be initiated by the serverless environment. Requests initiated by a VM must use the external address of your serverless service

https://cloud.google.com/vpc/docs/serverless-vpc-access

Question 24:

Your company is using Compute Engine instances to host its applications. There are 3 different environments: production, staging, and development environments.

The production environment is very critical and used for whole day, while other non production environments are critical during office time only.

What solution can you suggest for optimum usage of these environments which can save cost during non working office hours?

- ◯ **Use regular VM instances for the production environment**
  Use preemptible VMs for non production environments.

- ◯ **Create Cloud Functions to stop the non production environments after office hours and start them just before office hours.**
  Use Cloud Scheduler to invoke these Cloud Functions

- ◯ **Create a shell script that uses the gcloud command to change the machine type of the non production VM instances to a smaller machine type outside of office hours.**

- ◯ **Create a cron job on one of the production environment VM instance that will execute this shell script at regular scheduled time to automate the task**

- ◯ **Deploy the non production VM instances using a Managed Instance Group and enable autoscaling.**

Your company is using Compute Engine instances to host its applications. There are 3 different environments: production, staging, and development environments.

The production environment is very critical and used for whole day, while other non production environments are critical during office time only.

What solution can you suggest for optimum usage of these environments which can save cost during non working office hours?

- ◯ **Use regular VM instances for the production environment Use preemptible VMs for non production environments.**
- ◯ **Create Cloud Functions to stop the non production environments after office hours and start them just before office hours. Use Cloud Scheduler to invoke these Cloud Functions** (Correct)
- ◯ **Create a shell script that uses the gcloud command to change the machine type of the non production VM instances to a smaller machine type outside of office hours.**
- ◯ **Create a cron job on one of the production environment VM instance that will execute this shell script at regular scheduled time to automate the task**
- ◯ **Deploy the non production VM instances using a Managed Instance Group and enable autoscaling.**

Explanation

- Option A is incorrect because preemptible VM can be stopped any time with short notice of 30 seconds. So in this case it is not good choice even for development and staging environment as well.
- Option C is incorrect because even if machine type is changed after office hours, it will still incur some cost and It's not good practice to schedule such script on production environment. Ideally production environment should not have access to any other environment. So this script will not work even if it is scheduled on production environment.
- Option D look like a close call but it is also incorrect because minimum number of instances in case of autoscaling group is one.
- Option B is most accurate choice here because it will stop all the VMs in development and staging environment after office hours and start them just before office hours.

Question 25:

Your company has an enterprise application running on GCE VM instances. This application has requirement of high availability and high performance. The application has been deployed on two instances in two zones in the same region where one instance is active instance and other instance runs in passive mode.

This application writes data to a persistent disk and you need to make this application fault tolerant so that if there is a zonal failure in one zone, then data should be immediately made available to the other instance running in 2nd zone.

As Google Cloud architect how can you maximize performance of this application with minimum downtime and minimum data loss?

- ◯ **1. Attach a regional SSD persistent disk to the first instance.**
  2. In case of a zone outage, force-attach the disk to the other instance.

- ◯ **1. Create a GCS bucket.**
  2. Mount this bucket into the first instance with gcs-fuse.
  3. If zonal failure happens, then mount the same GCS bucket to the second instance with gcs-fuse

- ◯ **1. Create a persistent SSD disk for first instance.**
  2. Create a snapshot of this SSD persistent disk every 30 minutes.
  3. If zonal failure happens, then recreate a persistent SSD disk from last snapshot and attach that disk with the second instance running in 2nd zone

- ◯ **1. Use a local SSD disk with the first instance.**
  2. Attach a persistent disk with 2nd VM instance running in 2nd zone.
  2. Execute rsync command every 30 minutes where the target is a persistent SSD disk attached with 2nd VM instance
  3. If zonal failure happens, then use the second instance.

Your company has an enterprise application running on GCE VM instances. This application has requirement of high availability and high performance. The application has been deployed on two instances in two zones in the same region where one instance is active instance and other instance runs in passive mode.

This application writes data to a persistent disk and you need to make this application fault tolerant so that if there is a zonal failure in one zone, then data should be immediately made available to the other instance running in 2nd zone.

As Google Cloud architect how can you maximize performance of this application with minimum downtime and minimum data loss?

- ◯ **1. Attach a regional SSD persistent disk to the first instance.**
  2. In case of a zone outage, force-attach the disk to the other instance. (Correct)

- ◯ **1. Create a GCS bucket.**
  2. Mount this bucket into the first instance with gcs-fuse.
  3. If zonal failure happens, then mount the same GCS bucket to the second instance with gcs-fuse

- ◯ **1. Create a persistent SSD disk for first instance.**
  2. Create a snapshot of this SSD persistent disk every 30 minutes.
  3. If zonal failure happens, then recreate a persistent SSD disk from last snapshot and attach that disk with the second instance running in 2nd zone

- ◯ **1. Use a local SSD disk with the first instance.**
  2. Attach a persistent disk with 2nd VM instance running in 2nd zone.
  2. Execute rsync command every 30 minutes where the target is a persistent SSD disk attached with 2nd VM instance
  3. If zonal failure happens, then use the second instance.

Explanation

- Option C and Option D are incorrect because in both cases, 30 minutes of data can still be lost because snapshot or rsync happen at an interval of 30 minutes.
- Option B is incorrect because using Cloud Storage Bucket as disk via gcs-fuse is not a good choice as it will be very slow as compare to persistent disk
- Option A is correct choice here because in case of regional persistent disk, data is automatically copied in multiple zones. In case of zone outage; just start a new VM in another zone and force-attach the existing disk; will work perfectly fine.

Question 26:

Your team want to deploy a web application in GKE cluster. You need to ensure that application is highly scalable so that it can handle the high number of concurrent users.

How can you ensure that latency of this application stays below a certain threshold?

- ◯ **Do load testing of application for expected number of concurrent users via load testing tool and inspect the results.**
- ◯ **Enable autoscaling on the GKE cluster and enable horizontal pod autoscaling on your application deployments.**
  Validate the autoscaling of cluster via curl request.
- ◯ **Create multiple GKE cluster in every cloud region in GCP and deploy application in each cluster.**
- ◯ **Use global HTTP(S) load balancer to load balance the traffic among all clusters.**
- ◯ **Use Service Mesh to understand the latency between the different microservices.**

Your team want to deploy a web application in GKE cluster. You need to ensure that application is highly scalable so that it can handle the high number of concurrent users.

How can you ensure that latency of this application stays below a certain threshold?

- ◯ **Do load testing of application for expected number of concurrent users via load testing tool and inspect the results.**
- ◯ **Enable autoscaling on the GKE cluster and enable horizontal pod autoscaling on your application deployments. Validate the autoscaling of cluster via curl request.** (Correct)
- ◯ **Create multiple GKE cluster in every cloud region in GCP and deploy application in each cluster.**
- ◯ **Use global HTTP(S) load balancer to load balance the traffic among all clusters.**
- ◯ **Use Service Mesh to understand the latency between the different microservices.**

Explanation
Option B is correct choice here because once horizonal pod autoscaling is configured then GKE cluster will automatically adjust number of pods required for your application based on the application traffic.

When you first deploy your workload to a Kubernetes cluster, you may not be sure about its resource requirements and how those requirements might change based on usage patterns, external dependencies, or other factors.

Horizontal Pod autoscaling helps to ensure that your workload functions consistently in different situations, and allows you to control costs by only paying for extra capacity when you need it.

It's not always easy to predict the indicators that show whether your workload is under-resourced or under-utilized. The Horizontal Pod Autoscaler can automatically scale the number of Pods in your workload.

There is no need to deploy same application on multiple cluster like Option C. It is unnecessary pain.

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

★ Question 27:

Your company has developed a recommendation engine for its customers which is exposed via a REST API for its customers where user will provide a user ID as input and the REST API will return a list of recommendations as output for the given user ID.

You need to manage the API lifecycle. You also need to ensure stability for your customers in case the API makes backward-incompatible changes.

As a Google Cloud architect what solution you would like to suggest as per Google Cloud recommendations?

- ◯ **Create a distribution list of all customers.**

- ◯ **Use this distribution list to inform customers of an upcoming backward incompatible change at least one month before replacing the old API with the new API.**
  Use a versioning strategy that will add the suffix 'DEPRECATED' to the current API version number in case API changes are backward-incompatible.

- ◯ **Use the current version number for the new API.**
  Use a versioning strategy for the APIs that increases the version number on every backward incompatible change.

- ◯ **Generate API documentation in automated manner.**
  Set up CI/CD pipeline in way, that will update the public API documentation whenever new API is deployed.

Your company has developed a recommendation engine for its customers which is exposed via a REST API for its customers where user will provide a user ID as input and the REST API will return a list of recommendations as output for the given user ID.

You need to manage the API lifecycle. You also need to ensure stability for your customers in case the API makes backward-incompatible changes.

As a Google Cloud architect what solution you would like to suggest as per Google Cloud recommendations?

- ◯ **Create a distribution list of all customers.**

- ◯ **Use this distribution list to inform customers of an upcoming backward incompatible change at least one month before replacing the old API with the new API.**
  Use a versioning strategy that will add the suffix 'DEPRECATED' to the current API version number in case API changes are backward-incompatible.

- ◯ **Use the current version number for the new API.**
  Use a versioning strategy for the APIs that increases the version number on every backward incompatible change. (Correct)

- ◯ **Generate API documentation in automated manner.**
  Set up CI/CD pipeline in way, that will update the public API documentation whenever new API is deployed.

Explanation
Increasing the version number will inform client that new API might introduce breaking changes.

https://cloud.google.com/apis/design/compatibility

https://cloud.google.com/apis/design/versioning

Question 28:

Your company is developing a microservices application on GKE cluster. You need to simulate and validate how application will respond in case one of the microservice crash all of a sudden.

As Google Cloud Architect, what solution you would like to suggest?

- **Destroy one node in GKE cluster to validate required failure scenario**
  Configure Istio in GKE cluster.
- **Use traffic management feature of Istio to divert the traffic away from a crashing microservice.**
- **Add bug in one of the microservice code and redeploy that service in cluster**
  Use Istio's fault injection feature.
- **With this fault injection feature, you can simulate the behavior where one of the microservice is faulty**

Your company is developing a microservices application on GKE cluster. You need to simulate and validate how application will respond in case one of the microservice crash all of a sudden.

As Google Cloud Architect, what solution you would like to suggest?

- ◯ **Destroy one node in GKE cluster to validate required failure scenario Configure Istio in GKE cluster.**
- ◯ **Use traffic management feature of Istio to divert the traffic away from a crashing microservice.**
- ◯ **Add bug in one of the microservice code and redeploy that service in cluster Use Istio's fault injection feature.**
- ◯ **With this fault injection feature, you can simulate the behavior where one of the microservice is faulty** (Correct)

Explanation
Istio is an open service mesh that provides a uniform way to connect, manage, and secure microservices. It supports managing traffic flows between services, enforcing access policies, and aggregating telemetry data, all without requiring changes to the microservice code.

Istio gives you:

Automatic load balancing for HTTP, gRPC, WebSocket, MongoDB, and TCP traffic.

Fine-grained control of traffic behavior with rich routing rules, retries, failovers, and fault injection.

A configurable policy layer and API supporting access controls, rate limits, and quotas.

Automatic metrics, logs, and traces for all traffic within a cluster, including cluster ingress, and egress.

Secure service-to-service communication in a cluster with strong identity based authentication and authorization.

Istio on GKE is a tool that provides automated installation and upgrade of Istio in your GKE cluster. When you upgrade GKE, the add-on is automatically upgraded to the most recent GKE-supported version of Istio. This lets you easily manage the installation and upgrade of Istio as part of the GKE cluster lifecycle.

Question 29:

For a web application, how can you ensure that production deployment of application is linked to source code commits?

- ◯ **This deployment process should be fully auditable.**
  All developers must follow practice of tagging the code commit with commit timestamp.
- ◯ **All developers must follow practice of adding a comment to the commit that tells which commit is used for a particular commit.**
- ◯ **Make sure that container tag match the source code commit hash**
- ◯ **All developers must follow practice of tagging the code commits with :latest**

For a web application, how can you ensure that production deployment of application is linked to source code commits?

- ◯ **This deployment process should be fully auditable.**
  All developers must follow practice of tagging the code commit with commit timestamp.

- ◯ **All developers must follow practice of adding a comment to the commit that tells which commit is used for a particular commit.**

- ◯ **Make sure that container tag match the source code commit hash** (Correct)

- ◯ **All developers must follow practice of tagging the code commits with :latest**

Explanation

- Option A , Option B and Option D are just adding a tag or comment on source code only. This way we can not establish the relationship between deployment (container image) and source code commit after which this deployment was built.

Relationship between deployment (container image) and source code commit can be established by adding a tag to container image with tag value as source code commit.

Question 30:

Your team needs to deploy application on Google Kubernetes Engine (GKE) cluster. This application need access to third-party services on the internet.

As per company policy, no Compute Engine VM instance can have a public IP address in GCP.

How can you create a deployment strategy that meets these guidelines?

- **Configure the GKE cluster as a private cluster.**
  Configure Cloud NAT Gateway for the cluster subnet.

- **Configure the GKE cluster as a private cluster.**
  Configure Private Google Access in the VPC in which cluster nodes are created.

- **Configure the Kubernetes cluster as a route-based cluster.**
  Configure Private Google Access on the VPC in which cluster nodes are created.

- **Install a NAT Proxy on one Compute Engine VM Instance.**
  Configure all workloads on Kubernetes in a way that all request for third-party services on internet pass through this proxy.

Your team needs to deploy application on Google Kubernetes Engine (GKE) cluster. This application need access to third-party services on the internet.

As per company policy, no Compute Engine VM instance can have a public IP address in GCP.

How can you create a deployment strategy that meets these guidelines?

- ◯ **Configure the GKE cluster as a private cluster.**
  Configure Cloud NAT Gateway for the cluster subnet. (Correct)

- ◯ **Configure the GKE cluster as a private cluster.**
  Configure Private Google Access in the VPC in which cluster nodes are created.

- ◯ **Configure the Kubernetes cluster as a route-based cluster.**
  Configure Private Google Access on the VPC in which cluster nodes are created.

- ◯ **Install a NAT Proxy on one Compute Engine VM Instance.**
  Configure all workloads on Kubernetes in a way that all request for third-party services on internet pass through this proxy.

Explanation
Private clusters

By default, all nodes in a GKE cluster have public IP addresses. A good practice is to create private clusters, which gives all worker nodes only private RFC 1918 IP addresses. Private clusters enforce network isolation, reducing the risk exposure surface for your clusters. Using private clusters means that by default only clients inside your network can access services in the cluster. In order to allow external services to reach services in your cluster, you can use an HTTP(S) load balancer or a network load balancer.

Private clusters in GKE gives you the ability to isolate nodes from having inbound and outbound connectivity to the public internet. This isolation is achieved as the nodes have internal IP addresses only.

If you want to provide outbound internet access for certain private nodes, you can use Cloud NAT or manage your own NAT gateway.

Question 31:

Your company wants to store some critical data in a GCS bucket. and your company needs to rotate the encryption key used to encrypt the data in the bucket. This data will be processed in Cloud Dataflow.

As per Google Cloud's recommendation for the security, what solution would you like to suggest for this use case?

- ◯ **Create a key with Cloud Key Management Service (KMS).**
  Use encrypt method of Cloud KMS to encrypt the data.
- ◯ **Create a key with Cloud Key Management Service (KMS).**
  Set the encryption key on the bucket to the Cloud KMS key.
- ◯ **Generate a symmetric key.**
  Encrypt the data using above key.
- ◯ **Upload the encrypted data to the GCS bucket.**
  Use same key to decrypt data at the time of data read.
- ◯ **Generate an AES-256 encryption key.**
  Encrypt the data in the bucket using the customer-supplied encryption key feature.

Your company wants to store some critical data in a GCS bucket. and your company needs to rotate the encryption key used to encrypt the data in the bucket. This data will be processed in Cloud Dataflow.

As per Google Cloud's recommendation for the security, what solution would you like to suggest for this use case?

- ◯ **Create a key with Cloud Key Management Service (KMS).**
  Use encrypt method of Cloud KMS to encrypt the data.

- ◯ **Create a key with Cloud Key Management Service (KMS).**
  Set the encryption key on the bucket to the Cloud KMS key. (Correct)

- ◯ **Generate a symmetric key.**
  Encrypt the data using above key.

- ◯ **Upload the encrypted data to the GCS bucket.**
  Use same key to decrypt data at the time of data read.

- ◯ **Generate an AES-256 encryption key.**
  Encrypt the data in the bucket using the customer-supplied encryption key feature.

Explanation

All the data on Cloud Storage Bucket is encrypted. By default this encryption happens via Google Managed encryption keys. But in place of using Google Managed encryption keys, you can choose to use keys generated by Cloud Key Management Service. Such keys are known as customer- managed encryption keys. You can use customer-managed encryption keys on individual objects, or configure your bucket to use a key by default on all new objects added to a bucket.

If you use a customer-managed encryption key, your encryption keys are stored within Cloud KMS. The project that holds your encryption keys can then be independent from the project that contains your buckets, thus allowing for better separation of duties.

Question 32:

Your company wants to do outsourcing of operation functions. They want their developers to deploy new versions of application in staging environment for verification purpose. After verification in staging environment, they want to allow the outsourced operations team to promote this verified deployment version to production environment.

Which GCP products should you use to minimize the operation overhead of the solution?

- ◯ **App Engine**
- ◯ **GKE On-Prem**
- ◯ **Compute Engine**
- ◯ **Google Kubernetes Engine**

Your company wants to do outsourcing of operation functions. They want their developers to deploy new versions of application in staging environment for verification purpose. After verification in staging environment, they want to allow the outsourced operations team to promote this verified deployment version to production environment.

Which GCP products should you use to minimize the operation overhead of the solution?

- ◯ **App Engine** (Correct)
- ◯ **GKE On-Prem**
- ◯ **Compute Engine**
- ◯ **Google Kubernetes Engine**

Explanation
App Engine has less operation overhead as compare to any other option.

GKE and Compute Engine services are more flexible but has more operation overhead.

Question 33:

Your company is using BigQuery in Google Cloud Project. Company's on-premise environment is connected to Google Cloud via VPN tunnel.
What solution can you suggest to ensure security in this system to avoid data exfiltration and accidental oversharing?

- ◯ **Configure VPC Service Controls and configure Private Google Access**
- ◯ **Configure Private Google Access for on-premises only**
  Perform the following task
  1. Create a service account.
  2. Give the role to run BigQuery Jobs to the service account.
  3. Remove all other IAM access from the project
- ◯ **Use Private Google Access.**

Your company is using BigQuery in Google Cloud Project. Company's on-premise environment is connected to Google Cloud via VPN tunnel.
What solution can you suggest to ensure security in this system to avoid data exfiltration and accidental oversharing?

- ◯ **Configure VPC Service Controls and configure Private Google Access** (Correct)

- ◯ **Configure Private Google Access for on-premises only**
  Perform the following task
  1. Create a service account.
  2. Give the role to run BigQuery Jobs to the service account.
  3. Remove all other IAM access from the project

- ◯ **Use Private Google Access.**

Explanation
VPC Service Control helps in following things

1. Mitigate exfiltration risks by isolating multi-tenant services
2. Ensure sensitive data can only be accessed from authorized networks
3. Restrict resource access to allowed IP addresses, identities, and trusted client devices
4. Control which Google Cloud services are accessible from a VPC network

Private Google Access

Private Google Access offers private connectivity to hosts either in a VPC network or on-premises network that use private IP addresses to access Google APIs and services.

VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access. They can reach the external IP addresses of Google APIs and services. The source IP address of the packet can be the primary internal IP address of the network interface or an address in an alias IP range that is assigned to the interface.

Question 34:

One team in your company has been running one application in Google Cloud. This team has recently started using Cloud Pub/Sub with this application. Due to increase in load on the application servers, this application has started giving many timeout error. This application is not logging any Pub/Sub publishing errors. You want to improve publishing latency.

As Google Cloud Architect what will you suggest in this case?

- ◯ **Create more Pub/Sub message queues**
- ◯ **Use Push model of Pub/Sub for subscription**
- ◯ **Increase the Pub/Sub total timeout retry value**
- ◯ **Stop using Pub/Sub message batching**

One team in your company has been running one application in Google Cloud. This team has recently started using Cloud Pub/Sub with this application. Due to increase in load on the application servers, this application has started giving many timeout error. This application is not logging any Pub/Sub publishing errors. You want to improve publishing latency.

As Google Cloud Architect what will you suggest in this case?

- ◯ **Create more Pub/Sub message queues**
- ◯ **Use Push model of Pub/Sub for subscription**
- ◯ **Increase the Pub/Sub total timeout retry value**
- ◯ **Stop using Pub/Sub message batching** (Correct)

Explanation
Batching messages

The Pub/Sub client libraries batch multiple messages into a single call to the service. Larger batch sizes increase message throughput (rate of messages sent per CPU). The cost of batching is latency for individual messages, which are queued in memory until their corresponding batch is filled and ready to be sent over the network. To minimize latency, batching should be turned off. This is particularly important for applications that publish a single message as part of a request-response sequence.

Question 35:

How can you ensure that use of Google Cloud for health care industry will comply with an upcoming privacy compliance audit?

- [ ] **Implement Prometheus to detect and prevent security breaches on your web-based applications.**
- [ ] **Verify list of Google cloud products to be used in your application against the list of compliant product on the Google Cloud compliance page**
- [ ] **Use Firebase Authentication for your user facing applications.**
- [ ] **You should execute a Business Associate Agreement(BAA) with Google Cloud**
- [ ] **Use Google Kubernetes Engine private cluster for all containerized applications.**

How can you ensure that use of Google Cloud for health care industry will comply with an upcoming privacy compliance audit?

- [ ] **Implement Prometheus to detect and prevent security breaches on your web-based applications.**
- [ ] **Verify list of Google cloud products to be used in your application against the list of compliant product on the Google Cloud compliance page** (Correct)
- [ ] **Use Firebase Authentication for your user facing applications.**
- [ ] **You should execute a Business Associate Agreement(BAA) with Google Cloud** (Correct)
- [ ] **Use Google Kubernetes Engine private cluster for all containerized applications.**

Explanation
Under HIPAA, certain information about a persons health or health care services is classified as Protected Health Information (PHI). Google Workspace and Cloud Identity customers who are subject to HIPAA and wish to use Google Workspace or Cloud Identity with PHI must sign a Business Associate Agreement (BAA) with Google.

Reference:

https://support.google.com/a/answer/3407054?hl=en

Customers that are subject to HIPAA and want to utilize any Google Cloud products in connection with PHI must review and accept Google's Business Associate Agreement (BAA). Google ensures that the Google products covered under the BAA meet the requirements under HIPAA and align with our ISO/IEC 27001, 27017, and 27018 certifications and SOC 2 report.

References:

https://cloud.google.com/security/compliance/hipaa-compliance

https://cloud.google.com/security/compliance

Question 36:

While deploying containerized application on GKE cluster, how can you ensure that only verified containers are deployed using Google Cloud services?

- ○ **Use service account to create and deploy containers from container registry.**
- ○ **Set up a Jenkins job that will cryptographically sign a container as part of a CI/CD pipeline.**
- ○ **Enable Binary Authorization on GKE, and sign containers as part of a CI/CD pipeline.**
- ○ **Use Vulnerability Scanning feature of Container Registry before deploying the workload. Don't deploy the workload if any vulnerability is found during this scanning.**

While deploying containerized application on GKE cluster, how can you ensure that only verified containers are deployed using Google Cloud services?

- ○ **Use service account to create and deploy containers from container registry.**
- ○ **Set up a Jenkins job that will cryptographically sign a container as part of a CI/CD pipeline.**
- ○ **Enable Binary Authorization on GKE, and sign containers as part of a CI/CD pipeline.** (Correct)
- ○ **Use Vulnerability Scanning feature of Container Registry before deploying the workload. Don't deploy the workload if any vulnerability is found during this scanning.**

Explanation

Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run. With Binary Authorization, you can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying. By enforcing validation, you can gain tighter control over your container environment by ensuring only verified images are integrated into the build-and-release process.

https://cloud.google.com/binary-authorization

https://cloud.google.com/architecture/binary-auth-with-cloud-build-and-gke

Question 37:

In your company, public IP addresses was assigned by mistake to backend application servers. This public IP address assignment made these backend servers accessible from the internet.

- ◯ **In your organization how can you ensure that public IP addresses can not be assigned to backend server by any one. External IP addresses should be assigned to frontend servers only.**
- ◯ **Create an Organizational Policy with a constraint that will allow public IP addresses only on the frontend servers only.**
- ◯ **Create VM instances using Deployment Manager and do manual review of deployment configuration yaml file to ensure that public IP is not assigned to VM instances**
- ◯ **Create an identity and Access Management (IAM) policy that will revoke permission to create public IP address in your project**
- ◯ **Create a custom Identity and Access Management (IAM) role that will revoke permission to create public IP address**
- ◯ **Create a policy at project level that associate this role with all users in your project.**

In your company, public IP addresses was assigned by mistake to backend application servers. This public IP address assignment made these backend servers accessible from the internet.

- ◯ **In your organization how can you ensure that public IP addresses can not be assigned to backend server by any one. External IP addresses should be assigned to frontend servers only.**
- ◯ **Create an Organizational Policy with a constraint that will allow public IP addresses only on the frontend servers only.** (Correct)
- ◯ **Create VM instances using Deployment Manager and do manual review of deployment configuration yaml file to ensure that public IP is not assigned to VM instances**
- ◯ **Create an identity and Access Management (IAM) policy that will revoke permission to create public IP address in your project**
- ◯ **Create a custom Identity and Access Management (IAM) role that will revoke permission to create public IP address**
- ◯ **Create a policy at project level that associate this role with all users in your project.**

Explanation
Rules created at Organization Policy level have highest priority. These rules even have more priority than IAM policy defined at other resource level like Project, Folder and Organization.

So if we define deny rule as Organization Policy with a constraint to allow external IP addresses only on the frontend Compute Engine instances then no one can assign public IP address to any other instance even by mistake.

Question 38:

There is a single Dedicated Interconnect connection between your primary on-premises data center and Google Cloud. This connection should adheres to following policies:

1. Any on-premise server with private IP should connect to cloud resources via private IP of cloud resources.
2. Egress traffic from production network management servers to Google Compute Engine virtual machines should never use public internet.
3. Network should meet SLA (Service level Agreement) of any business critical application.

What solution will you suggest to meet these requirements?

- ◯ **Add a new Dedicated Interconnect connection.**
- ◯ **Upgrade the bandwidth on the Dedicated Interconnect connection to 100G**
- ◯ **Add four new Cloud VPN connections.**
- ◯ **Use a new Carrier Peering connection.**

There is a single Dedicated Interconnect connection between your primary on-premises data center and Google Cloud. This connection should adheres to following policies:

1. Any on-premise server with private IP should connect to cloud resources via private IP of cloud resources.
2. Egress traffic from production network management servers to Google Compute Engine virtual machines should never use public internet.
3. Network should meet SLA (Service level Agreement) of any business critical application.

What solution will you suggest to meet these requirements?

- ◯ **Add a new Dedicated Interconnect connection.** (Correct)
- ◯ **Upgrade the bandwidth on the Dedicated Interconnect connection to 100G**
- ◯ **Add four new Cloud VPN connections.**
- ◯ **Use a new Carrier Peering connection.**

Explanation
Dedicated Interconnect provides direct physical connections between your on-premises network and Google's network. Dedicated Interconnect enables you to transfer large amounts of data between networks, which can be more cost-effective than purchasing additional bandwidth over the public internet.

For the highest level availability, it is recommended to set up configuration for 99.99% availability as the base configuration, as shown in the following diagram. Clients in the on-premises network can reach the IP addresses of virtual machine (VM) instances in the us-central1 region through at least one of the redundant paths. If one path is unavailable, the other paths can continue to serve traffic.

As per Google recommendation:

With 100 Gbps Dedicated Interconnect, you can scale your connection capacity to meet your particular requirements. Connect up to 2x 100G transport circuits for private cloud traffic to Google Cloud at any of our POPs.

Question 39:

Your company needs to design Google Cloud network architecture for GKE cluster. This cluster will be used to run business critical internet facing application. As per Google Cloud's best practices, how will you design this network so that you can manage this cluster from your data center and there is very less chances of attack from malicious attacker?

- ◯ **Create a public cluster with master authorized networks enabled and firewall rules.**
- ◯ **Create a public cluster with firewall rules and Virtual Private Cloud (VPC) routes**
- ◯ **Create a private cluster with a private endpoint with master authorized networks configured.**
- ◯ **Create a private cluster with public endpoint with master authorized networks configured.**

Your company needs to design Google Cloud network architecture for GKE cluster. This cluster will be used to run business critical internet facing application. As per Google Cloud's best practices, how will you design this network so that you can manage this cluster from your data center and there is very less chances of attack from malicious attacker?

- ◯ **Create a public cluster with master authorized networks enabled and firewall rules.**
- ◯ **Create a public cluster with firewall rules and Virtual Private Cloud (VPC) routes**
- ◯ **Create a private cluster with a private endpoint with master authorized networks configured.**
- ◯ **Create a private cluster with public endpoint with master authorized networks configured.** (Correct)

Explanation

In a private cluster, nodes only have internal IP addresses, which means that nodes and Pods are isolated from the internet by default.

In private clusters, the control plane (master) has a private and public endpoint. There are three configuration combinations to control access to the cluster endpoints:

1. Public endpoint access disabled: creates a private cluster with no client access to the public endpoint.
2. Public endpoint access enabled, authorized networks enabled: creates a private cluster with limited access to the public endpoint.
3. Public endpoint access enabled, authorized networks disabled: creates a private cluster with unrestricted access to the public endpoint.

Question 40:

Your company wants to scale existing business critical application. They have customers across the globe. For this application, GKE cluster will be used to host the application. Currently, company is not interested in migrating its existing MySQL on-premises database to cloud. So application servers need high speed, consistent and highly available connectivity between their on-premises data center and Google Cloud to access on-premises database.

As per Google's recommended practices for production-level applications, what solution will you suggest for hybrid connectivity between your company's on-premises systems and Google Cloud?

- ◯ **Configure two dedicated interconnect connections in one metro (City) and two connections in another metro.**
  Ensure that Interconnect connections are placed in different metro zones.

- ◯ **Configure two Partner interconnect connections in one metro (City).**
  Ensure that Interconnect connections are placed in different metro zones.

- ◯ **Configure Direct Peering between your data center and Google Cloud.**
  Ensure that you are peering at least two Google locations.

- ◯ **Configure two or more VPN connections from on-premises to Google Cloud.**
  Ensure that VPN devices in on-premises data center are in separate racks.

Your company wants to scale existing business critical application. They have customers across the globe. For this application, GKE cluster will be used to host the application. Currently, company is not interested in migrating its existing MySQL on-premises database to cloud. So application servers need high speed, consistent and highly available connectivity between their on-premises data center and Google Cloud to access on-premises database.

As per Google's recommended practices for production-level applications, what solution will you suggest for hybrid connectivity between your company's on-premises systems and Google Cloud?

- ◯ **Configure two dedicated interconnect connections in one metro (City) and two connections in another metro. Ensure that Interconnect connections are placed in different metro zones.** (Correct)
- ◯ **Configure two Partner interconnect connections in one metro (City). Ensure that Interconnect connections are placed in different metro zones.**
- ◯ **Configure Direct Peering between your data center and Google Cloud. Ensure that you are peering at least two Google locations.**
- ◯ **Configure two or more VPN connections from on-premises to Google Cloud. Ensure that VPN devices in on-premises data center are in separate racks.**

Explanation

For the highest level availability, Google recommend the configuration for 99.99% availability as the base configuration, as shown in the following diagram. Clients in the on-premises network can reach the IP addresses of virtual machine (VM) instances in the us-centra-1 region through at least one of the redundant paths. If one path is unavailable, the other paths can continue to serve traffic.

Question 41:

You want to build an application and you are interested in using serverless Cloud Functions for backend services.

In your application, you have requirements that cloud Function functionA should be able to invoke another Cloud Function functionB.

As per Google Cloud recommendation, what solution will you suggest to ensure that functionB accept request from functionA only.

- ◯ **Make functionB 'Require authentication'**
  Make functionB only accept internal traffic.
  Create both Cloud Functions in the same VPC.
  Create an ingress firewall for functionB to only allow traffic from functionA .

- ◯ **Make functionB 'Require authentication'.**
  Create a unique service account and associate it to functionA.
  Grant the service account invoker role for functionB .
  Create an id token in functionA and pass the token with request when invoking functionB.

- ◯ **Create a token and pass it in as an environment variable to functionA.**
  While invoking functionB, include the token in the request.
  Pass the same token to functionB
  Reject the invocation if the tokens are different.

- ◯ **Create two functions in the same project and VPC.**
  Make functionB only accept internal traffic.
  Create an ingress firewall for functionB to only allow traffic from functionA.
  Ensure that both functions use the same service account.

You want to build an application and you are interested in using serverless Cloud Functions for backend services.

In your application, you have requirements that cloud Function functionA should be able to invoke another Cloud Function functionB.

As per Google Cloud recommendation, what solution will you suggest to ensure that functionB accept request from functionA only.

- ◯ **Make functionB 'Require authentication'**
  Make functionB only accept internal traffic.
  Create both Cloud Functions in the same VPC.
  Create an ingress firewall for functionB to only allow traffic from functionA .

- ◯ **Make functionB 'Require authentication'.**
  Create a unique service account and associate it to functionA.
  Grant the service account invoker role for functionB . (Correct)
  Create an id token in functionA and pass the token with request when invoking functionB.

- ◯ **Create a token and pass it in as an environment variable to functionA.**
  While invoking functionB, include the token in the request.
  Pass the same token to functionB
  Reject the invocation if the tokens are different.

- ◯ **Create two functions in the same project and VPC.**
  Make functionB only accept internal traffic.
  Create an ingress firewall for functionB to only allow traffic from functionA.
  Ensure that both functions use the same service account.

Explanation
There are two approaches to controlling access for Cloud Functions:

Identity-based

1. Evaluating credentials that the entity presents to ensure that it is who it says it is (Authentication).

2. Allowing that entity to access your resources based on what permissions that identity has been granted (Authorization).

Network-based

You can also limit access by specifying network settings for individual functions. This allows for fine-tuned control over the network ingress and egress to and from your functions.

Question 42:

Your company has a legacy web application running in on-premises data center. You want to use Google Cloud to monitor this application.

In case of application failure or during maintenance, you want to redirect users to a "Application is not available" page as soon as possible. Your Operation team should be able to receive a notification for the issue.

What solution will you suggest for this requirement? You also have goal to minimize the cost.

- ◯ **Use Cloud Error Reporting to check the application URL.**
  In case of failure, switch the URL to the "Application is not available" page
  Notify the Operation team about this incident.
  Create a Cloud Monitoring uptime check to validate the application URL.

- ◯ **In case of health check failure, send a message to Pub/Sub queue.**
  Create a Cloud Function that subscribe to this event.
  This Cloud Function will switch the URL to the "Application is not available" page, and notify the Operation team.

- ◯ **Create a cron job on a GCE VM instance that runs every 30 seconds.**
  The cron job invokes a shell script to check the application URL.
  In case of failure, switch the URL to the "Application is not available" page, and notify the Operation team.

- ◯ **Create a schedule job in Cloud Run to invoke a container every 30 seconds.**
  The container will check the application URL.
  In case of failure, switch the URL to the "Application is not available" page, and notify the Operation team.

Your company has a legacy web application running in on-premises data center. You want to use Google Cloud to monitor this application.

In case of application failure or during maintenance, you want to redirect users to a "Application is not available" page as soon as possible. Your Operation team should be able to receive a notification for the issue.

What solution will you suggest for this requirement? You also have goal to minimize the cost.

- ◯ **Use Cloud Error Reporting to check the application URL.**
  In case of failure, switch the URL to the “Application is not available“ page
  Notify the Operation team about this incident.
  Create a Cloud Monitoring uptime check to validate the application URL.

- ◯ **In case of health check failure, send a message to Pub/Sub queue.**
  Create a Cloud Function that subscribe to this event.
  This Cloud Function will switch the URL to the “Application is not available“ page, and notify the Operation team. (Correct)

- ◯ **Create a cron job on a GCE VM instance that runs every 30 seconds.**
  The cron job invokes a shell script to check the application URL.
  In case of failure, switch the URL to the “Application is not available“ page, and notify the Operation team.

- ◯ **Create a schedule job in Cloud Run to invoke a container every 30 seconds.**
  The container will check the application URL.
  In case of failure, switch the URL to the “Application is not available“ page, and notify the Operation team.

Explanation

An uptime check is a request sent to a resource to see if it responds. You can use uptime checks to determine the availability of a VM instance, an App Engine service, a URL, or an AWS load balancer.

You can monitor the availability of a resource by creating an alerting policy that creates an incident if the uptime check fails. The alerting policy can be configured to notify you by email or through a different channel, and that notification can include details about the resource that failed to respond. You also have the option to observe the results of uptime checks in the Monitoring uptime-check dashboards.

Question 43:

Your company has about 1 petabyte (PB) of critical data in on-premises data center. You want to export this data to Google Cloud Storage Bucket . There is a 1-Gbps interconnect link between on-premises data center and Google Cloud. Other team wants to use data stored in Google Cloud Storage bucket after one month.

What solution will you suggest for such data export?

- ◯ **Use Transfer Appliances from Google Cloud to export the data to Google's Cloud storage bucket.**
- ◯ **Export files to an encrypted USB device**
- ◯ **Send the device to Google**
- ◯ **Request Google cloud for import of the data to Cloud Storage bucket from this USB device.**
- ◯ **Ensure that there are no other users consuming the 1Gbps link**

Your company has about 1 petabyte (PB) of critical data in on-premises data center. You want to export this data to Google Cloud Storage Bucket . There is a 1-Gbps interconnect link between on-premises data center and Google Cloud. Other team wants to use data stored in Google Cloud Storage bucket after one month.

What solution will you suggest for such data export?

- ◯ **Use Transfer Appliances from Google Cloud to export the data to Google's Cloud storage bucket.** (Correct)
- ◯ **Export files to an encrypted USB device**
- ◯ **Send the device to Google**
- ◯ **Request Google cloud for import of the data to Cloud Storage bucket from this USB device.**
- ◯ **Ensure that there are no other users consuming the 1Gbps link**
- ◯ **Use multi-thread transfer using gcloud -m command line utility to transfer data to Cloud Storage.**

Explanation

With 1Gbps, it can take 124 or more number of days to transfer 1 PB of data, so gsutil and Storage Transfer service is not right choice here in this case because both are dependent on network bandwidth.

Question 44:

You want to migrate on-premises Linux-based virtual machines to Google Cloud. Your infrastructure team sent you several recent Linux vulnerabilities published by Common Vulnerabilities and Exposure (CVE).

How can you assess these Vulnerabilities that can affect your VM migration?

- [ ] **Open a support case regarding the CVE**
- [ ] **Chat with the Google Cloud support team.**
- [ ] **Post a query related to CVE in a Google Cloud discussion forum to get more information about this.**
- [ ] **Check the Google Cloud Status Dashboard to understand about CVEs that can affect VM migration.**
- [ ] **Check Google Cloud Platform Security Bulletins to understand about CVEs that can affect VM migration.**

You want to migrate on-premises Linux-based virtual machines to Google Cloud. Your infrastructure team sent you several recent Linux vulnerabilities published by Common Vulnerabilities and Exposure (CVE).

How can you assess these Vulnerabilities that can affect your VM migration?

- [ ] **Open a support case regarding the CVE**
- [ ] **Chat with the Google Cloud support team.** (Correct)
- [ ] **Post a query related to CVE in a Google Cloud discussion forum to get more information about this.**
- [ ] **Check the Google Cloud Status Dashboard to understand about CVEs that can affect VM migration.**
- [ ] **Check Google Cloud Platform Security Bulletins to understand about CVEs that can affect VM migration.** (Correct)
- [ ] **Post your CVE related query on other internet forums like Stack Overflow to understand it in better way.**

Explanation

Google Cloud publish **CVE** report from time to time on its security Bulletin.

Question 45:

Your company wants to build microservice based application. Your team want to deploy this application using Docker containers. How would you like to set up pipeline that can store the build artifacts and can do CI/CD for your application?

- Create a Cloud Build trigger for new source code changes.
  The trigger invokes build jobs and build container images for the microservices.
  Tag the images with a version number, and push them to Cloud Storage.

- Create a Cloud Build trigger for new source code changes.
  Invoke Cloud Build that will first build the container image, and then tag the image with the label 'latest'.
  Push that image to Container Registry.

- Create a Cloud Build trigger for new source code changes.
  Invoke Cloud Build that will first build the container image, and then tag the image with the code commit hash.
  Push that images to the Container Registry.

- Create a Scheduler job to check the code repository every minute.
  For any new change, invoke Cloud Build to build container images for the microservices.
  Tag the images with current timestamp.
  Push container image to Container Registry.

Your company wants to build microservice based application. Your team want to deploy this application using Docker containers. How would you like to set up pipeline that can store the build artifacts and can do CI/CD for your application?

- ○ Create a Cloud Build trigger for new source code changes.
  The trigger invokes build jobs and build container images for the microservices.
  Tag the images with a version number, and push them to Cloud Storage.

- ○ Create a Cloud Build trigger for new source code changes.
  Invoke Cloud Build that will first build the container image, and then tag the image with the label 'latest;.
  Push that image to Container Registry.

- ○ Create a Cloud Build trigger for new source code changes.
  Invoke Cloud Build that will first build the container image, and then tag the image with the code commit hash.
  Push that images to the Container Registry. (Correct)

- ○ Create a Scheduler job to check the code repository every minute.
  For any new change, invoke Cloud Build to build container images for the microservices.
  Tag the images with current timestamp.
  Push container image to Container Registry.

Explanation

Option B and Option C are very close but I will prefer Option C more.

With this I can directly map any deployment with source code commit used to build this deployment.

CI/CD pipeline for GKE

Question 46:

Your company wants to convert a monolithic application into RESTful microservices. Your team want to run those microservices on Cloud Run by using Docker containers. Your application has customer across the globe.

How can you ensure that these services are highly available? Also, customers expect low latency from your solution?

- ◯ **Deploy Cloud Run services in multiple regions.**
  Create serverless network endpoint groups pointing to the services.
  Use serverless NEG's as a backend service for the global HTTP(S) Load Balancer.

- ◯ **Deploy Cloud Run services to multiple availability zones.**
  Create Cloud Endpoints that point for these services.
  Create a global HTTP(S) Load Balancer.

- ◯ **Attach the Cloud Endpoints as backend service for above load balancer.**
  Deploy Cloud Run services in multiple regions.
  Configure Cloud DNS to route traffic based on latency.

- ◯ **Deploy Cloud Run services in multiple availability zones.**
  Create a TCP/IP global load balancer.
  Add the Cloud Run Endpoints as backend services for above load balancer.

Your company wants to convert a monolithic application into RESTful microservices. Your team want to run those microservices on Cloud Run by using Docker containers. Your application has customer across the globe.

How can you ensure that these services are highly available? Also, customers expect low latency from your solution?

- ◯ **Deploy Cloud Run services in multiple regions.**
  Create serverless network endpoint groups pointing to the services. (Correct)
  Use serverless NEG's as a backend service for the global HTTP(S) Load Balancer.

- ◯ **Deploy Cloud Run services to multiple availability zones.**
  Create Cloud Endpoints that point for these services.
  Create a global HTTP(S) Load Balancer.

- ◯ **Attach the Cloud Endpoints as backend service for above load balancer.**
  Deploy Cloud Run services in multiple regions.
  Configure Cloud DNS to route traffic based on latency.

- ◯ **Deploy Cloud Run services in multiple availability zones.**
  Create a TCP/IP global load balancer.
  Add the Cloud Run Endpoints as backend services for above load balancer.

Explanation
This is how a serverless NEG fits into the HTTP(S) Load Balancing model.

A network endpoint group (NEG) specifies a group of backend endpoints for a load balancer. A serverless NEG is a backend that points to a Cloud Run, App Engine, or Cloud Functions service.

A serverless NEG can represent one of the following:

1. A Cloud Run service or a group of services sharing the same URL pattern.
2. A Cloud Functions function or a group of functions sharing the same URL pattern.
3. An App Engine app (Standard or Flex), a specific service within an app, a specific version of an app, or a group of services sharing the same URL pattern.

When HTTP(S) Load Balancing is enabled for serverless apps, you can:

1. Configure your serverless app to serve from a dedicated IPv4 and/or IPv6 IP address that is not shared with other services.
2. Map a single URL to multiple functionally-identical serverless applications running in different regions, allowing requests to be routed to the region closest to the user. This is supported only for Cloud Run and Cloud Functions.
3. Reuse the same SSL certificates and private keys that you use for Compute Engine, Google Kubernetes Engine and Cloud Storage. This eliminates the need to manage separate certificates for serverless apps.

Endpoint types:

Serverless NEGs do not have any network endpoints such as ports or IP addresses. They can only point to an existing Cloud Run, App Engine, or Cloud Functions service residing in the same region as the NEG.

When you create a serverless NEG, you specify the fully-qualified domain name (FQDN) of the Cloud Run, App Engine, or Cloud Functions service. The endpoint is of type SERVERLESS. Other endpoint types are not supported in a serverless NEG.

A serverless NEG cannot have more than one endpoint. Because only one endpoint is allowed in each serverless NEG, the load balancer serves as the frontend only, and proxies traffic to the specified serverless endpoint. However, if the backend service contains multiple serverless NEGs, the load balancer balances traffic between these NEGs, thus minimizing request latency.

Question 47:

Your company is hosting all its applications in single VPC and VPC has required firewall rules in place. Your company wants to use Firewall insights feature in the Google Network Intelligence Center to analyze the efficiency of the applied firewall ruleset. But network team did not find any row in Firewall Insight on Cloud Console.

How can this problem be fixed?

- ◯ **Use Google Cloud SDK to check Firewall logs.**
- ◯ **Assigned the correct IAM role to users to check Firewall logs.**
- ◯ **Enable Virtual Private Cloud (VPC) flow logging.**
- ◯ **Enable Firewall Rules Logging for the firewall rules that you want to monitor.**

Your company is hosting all its applications in single VPC and VPC has required firewall rules in place. Your company wants to use Firewall insights feature in the Google Network Intelligence Center to analyze the efficiency of the applied firewall ruleset. But network team did not find any row in Firewall Insight on Cloud Console.

How can this problem be fixed?

- ◯ **Use Google Cloud SDK to check Firewall logs.**
- ◯ **Assigned the correct IAM role to users to check Firewall logs.**
- ◯ **Enable Virtual Private Cloud (VPC) flow logging.**
- ◯ **Enable Firewall Rules Logging for the firewall rules that you want to monitor.** (Correct)

Explanation

Firewall Insights enables you to better understand and safely optimize your firewall configurations. Firewall Insights provides reports that contain information about firewall usage and the impact of various firewall rules on your Virtual Private Cloud (VPC) network.

Firewall rule usage metrics are accurate only for the period of time during which Firewall Rules Logging is enabled.

Question 48:

Your team is developing an application that process and stores very sensitive documents. Team is considering Cloud Storage in Google Cloud to store these documents. Any change to these sensitive documents must be uploaded as a separate copy of the document.

For compliance requirements, how can to ensure that these documents cannot be deleted or overwritten for the next 7 years.

- ◯ **Generate customer-managed key in Cloud KMS.**
  Use above key for the encryption of the bucket data.
  Rotate the key after 7 years.
  Create the bucket with fine-grained access control.
  Create a service account.

- ◯ **Assign role of Object Writer to above service account.**
  Use above created service account to upload new files.
  Create a retention policy on the bucket for the duration of 7 years.
  Create a lock on the retention policy.

- ◯ **Create the bucket with uniform bucket-level access control.**
  Create a service account.
  Assign role of Object Writer to above service account.
  Use above created service account to upload new files.

Your team is developing an application that process and stores very sensitive documents. Team is considering Cloud Storage in Google Cloud to store these documents. Any change to these sensitive documents must be uploaded as a separate copy of the document.

For compliance requirements, how can to ensure that these documents cannot be deleted or overwritten for the next 7 years.

- ◯ **Generate customer-managed key in Cloud KMS.**
  Use above key for the encryption of the bucket data.
  Rotate the key after 7 years.
  Create the bucket with fine-grained access control.
  Create a service account.

- ◯ **Assign role of Object Writer to above service account.**
  Use above created service account to upload new files.
  Create a retention policy on the bucket for the duration of 7 years.
  Create a lock on the retention policy.
  (Correct)

- ◯ **Create the bucket with uniform bucket-level access control.**
  Create a service account.
  Assign role of Object Writer to above service account.
  Use above created service account to upload new files.

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

This feature can provide immutable storage on Cloud Storage. In conjunction with Detailed audit logging mode, which logs Cloud Storage request and response details, Bucket Lock can help with regulatory and compliance requirements, such as those associated with FINRA, SEC, and CFTC. Bucket Lock may also help you address certain health care industry retention regulations.

You can add a retention policy to a bucket to specify a retention period:

1. If a bucket does not have a retention policy, you can delete or replace objects in the bucket at any time

2. If a bucket has a retention policy, objects in the bucket can only be deleted or replaced once their age is greater than the retention period.

3. A retention policy retroactively applies to existing objects in the bucket as well as new objects added to the bucket.

You can lock a retention policy to permanently set it on the bucket:

1. Once you lock a retention policy, you cannot remove it or reduce the retention period it has.

2. You cannot delete a bucket with a locked retention policy unless every object in the bucket has met the retention period.

3. You can increase the retention period of a locked retention policy.

4. Locking a retention policy can help your data comply with record retention regulations.

Question 49:

There is an existing Application which is running on Compute Engine instances which are managed via a Managed Instance Group.

Now you need to upgrade this application with some non critical update. You have created a new instance template for this non critical update.

How can you deploy this non critical update with no impact on existing VM instances? You need to ensure that only new VM instances has updated application running inside them.

- **Start a new rolling restart operation.**
- **Start a new rolling replace operation.**
- **Start a new rolling update with Proactive update mode.**
- **Start a new rolling update with Opportunistic update mode.**

There is an existing Application which is running on Compute Engine instances which are managed via a Managed Instance Group.

Now you need to upgrade this application with some non critical update. You have created a new instance template for this non critical update.

How can you deploy this non critical update with no impact on existing VM instances? You need to ensure that only new VM instances has updated application running inside them.

- ◯ **Start a new rolling restart operation.**
- ◯ **Start a new rolling replace operation.**
- ◯ **Start a new rolling update with Proactive update mode.**
- ◯ **Start a new rolling update with Opportunistic update mode.** (Correct)

Explanation
To automatically roll out new configuration to all or to a subset of the instances in a MIG, set the MIG's update type to PROACTIVE. If an automated update is potentially too disruptive, or you want more control over the update, set the MIG's update type to OPPORTUNISTIC then selectively update specific instances.

Opportunistic updates:

When the update type is set to OPPORTUNISTIC, the MIG applies updates only when you selectively apply the update to specific instances or when new instances are created by the MIG. A MIG creates new instances when it is resized to add instances, either automatically or manually. Compute Engine does not actively initiate requests to apply opportunistic updates.

In certain scenarios, an opportunistic update is useful because you don't want to cause instability to the system if it can be avoided. For example, if you have a non-critical update that can be applied as necessary without any urgency and you have a MIG that is actively being autoscaled, perform an opportunistic update so that Compute Engine does not actively tear down your existing instances to apply the update. When resizing down, the autoscaler preferentially terminates instances with the old template as well as instances that are not yet in a RUNNING state.

Question 50:

One team in your company is developing a Web Application using Go 1.12. The expected load on this application is not predictable.

How would you like to deploy this application in GCP with minimum operation overhead? You also need to ensure availability of application during peak traffic as well.

- ◯ **Develop the application on App Engine standard environment.**
- ◯ **Use a Managed Instance Group to deploy application.**
  Create Docker container for this application
- ◯ **Develop the application on App Engine flexible environment using above container.**
  Create Docker container for this application.
- ◯ **Deploy application on GKE cluster.**

One team in your company is developing a Web Application using Go 1.12. The expected load on this application is not predictable.

How would you like to deploy this application in GCP with minimum operation overhead? You also need to ensure availability of application during peak traffic as well.

- ◯ **Develop the application on App Engine standard environment.** (Correct)
- ◯ **Use a Managed Instance Group to deploy application.**
  Create Docker container for this application
- ◯ **Develop the application on App Engine flexible environment using above container.**
  Create Docker container for this application.
- ◯ **Deploy application on GKE cluster.**

Explanation

Go1.12 is supported in App Engine Standard Environment, Option A is best choice to deploy application with minimum operational overhead for given use case.

Question 51:

One team in you company has deployed a business critical application on Athos cluster. This application must be highly available and should serve request with low latency.

What solution will you suggest to receive alerts if request latency of this critical application goes beyond a certain threshold value for specified period of time?

- ◯ **Enable the Cloud Trace API on your project.**
  Use Cloud Monitoring Alerts to send an alert based on the Cloud Trace metrics.
  Configure Anthos Config Management on your cluster.

- ◯ **Create a** `yaml` **file that defines the SLO.**
  Create an alerting policy in your cluster.
  Install Anthos Service Mesh on your cluster.

- ◯ **Define a Service Level Objective(SLO) on cloud console.**
  Create an alerting policy based on this SLO.

- ◯ **Use Cloud Profiler to track request latency.**
  Create a custom metric in Cloud Monitoring based on the request latency calculated in above step.
  Create an Alerting policy in case this metric exceeds the threshold value.

One team in you company has deployed a business critical application on Athos cluster. This application must be highly available and should serve request with low latency.

What solution will you suggest to receive alerts if request latency of this critical application goes beyond a certain threshold value for specified period of time?

- ◯ **Enable the Cloud Trace API on your project.**
  Use Cloud Monitoring Alerts to send an alert based on the Cloud Trace metrics.
  Configure Anthos Config Management on your cluster.

- ◯ **Create a `yaml` file that defines the SLO.**
  Create an alerting policy in your cluster.
  Install Anthos Service Mesh on your cluster.

- ◯ **Define a Service Level Objective(SLO) on cloud console.**
  Create an alerting policy based on this SLO. (Correct)

- ◯ **Use Cloud Profiler to track request latency.**
  Create a custom metric in Cloud Monitoring based on the request latency calculated in above step.
  Create an Alerting policy in case this metric exceeds the threshold value.

Explanation

What is a service mesh?

A service mesh is an architecture that enables managed, observable, and secure communication across your services, letting you create robust enterprise applications made up of many microservices on your chosen infrastructure. Service meshes factor out all the common concerns of running a service such as monitoring, networking, and security, with consistent, powerful tools, making it easier for service developers and operators to focus on creating and managing great applications for their users.

The Anthos Service Mesh pages in the Google Cloud Console provides you to define Service level objectives (SLOs) that give you insight into the health of your services. You can easily define an SLO and alert on your own standards of service health.

Question 52:

You are GCP practice head in your company. In your company, there are multiple departments and these departments need access to their own projects. Members within each department will have the same project responsibilities.

You want to set up your cloud environment in a way that require minimum maintenance.

You also need to ensure that IAM permissions are easy to set up as each department's project start and end.

What solution will you suggest for this requirement?

- **Create a folder for each department.**
  Assign the respective members of the department the required IAM permissions at the folder level.
  Arrange all projects for each department under the respective folders.

- **Create a Google Group for each department.**
  Associate all department members with respective groups.
  Assign each group the required IAM permissions for their respective projects.

- **Assign all department members the required IAM permissions for their respective projects.**
  Create a Google Group for each department.
  Associate all department members to their respective groups.

- **Create a folder for each department.**
  Assign the respective group the required IAM permissions at the folder level.
  Create the projects under the respective folders.

You are GCP practice head in your company. In your company, there are multiple departments and these departments need access to their own projects. Members within each department will have the same project responsibilities.

You want to set up your cloud environment in a way that require minimum maintenance.

You also need to ensure that IAM permissions are easy to set up as each department's project start and end.

What solution will you suggest for this requirement?

- ◯ **Create a folder for each department.**
  Assign the respective members of the department the required IAM permissions at the folder level.
  Arrange all projects for each department under the respective folders.

- ◯ **Create a Google Group for each department.**
  Associate all department members with respective groups.
  Assign each group the required IAM permissions for their respective projects.

- ◯ **Assign all department members the required IAM permissions for their respective projects.**
  Create a Google Group for each department.
  Associate all department members to their respective groups.

- ◯ **Create a folder for each department.**
  Assign the respective group the required IAM permissions at the folder level. (Correct)
  Create the projects under the respective folders.

Explanation

- Option A and Option C are incorrect because permissions are assigned to each member is individual member. Group is more recommended way to assign permission to members rather that giving permission to individual member.
- Option B is incorrect because permission are granted at project level. Since all members in one department need same project responsibilities for all the projects so it make more sense to assign permission at folder level rather.
- So Option D is most appropriate choice for this.

Question 53:

One team in you company wants to develop a web application. This application has only few API which needs to be exposed to internet. User traffic will also be less for this application most of the time. Only on some rare occasions traffic cloud spike.

What solution will you suggest to deploy this application in cloud in cost effective way (You also need to ensure high availability of this application) ?

- **Store static content such as HTML and images in a GCS bucket.**
  Use Cloud Functions to host the APIs and save the user data in Firestore.

- **Use Cloud CDN to store static content such as HTML and images.**
  Host the APIs on App Engine.

- **Store the user data in Cloud SQL.**
  Store static content such as HTML and images in a GCS bucket.

- **Host the APIs on a zonal GKE cluster with worker nodes in multiple zones.**
  Save the user data in Cloud Spanner.

- **Use Cloud CDN to store static content such as HTML and images.**
  Use cloud Run to host the APIs.
  Save the user data in Cloud SQL.

One team in you company wants to develop a web application. This application has only few API which needs to be exposed to internet. User traffic will also be less for this application most of the time. Only on some rare occasions traffic cloud spike.

What solution will you suggest to deploy this application in cloud in cost effective way (You also need to ensure high availability of this application) ?

- ◯ **Store static content such as HTML and images in a GCS bucket. Use Cloud Functions to host the APIs and save the user data in Firestore.** (Correct)
- ◯ **Use Cloud CDN to store static content such as HTML and images. Host the APIs on App Engine.**
- ◯ **Store the user data in Cloud SQL. Store static content such as HTML and images in a GCS bucket.**
- ◯ **Host the APIs on a zonal GKE cluster with worker nodes in multiple zones. Save the user data in Cloud Spanner.**
- ◯ **Use Cloud CDN to store static content such as HTML and images. Use cloud Run to host the APIs. Save the user data in Cloud SQL.**

Explanation
Since traffic is very low, so serverless option is better choice in such case because in case of serverless deployment, there will be no charge if there is no traffic.

- So With this point, Both Option A and Option D looks like correct choice.
- Option B can also be correct choice if App Engine standard environment is used.
- Option A is best choice among all possible cases because only few number of API needs to be hosted.

  So Cloud Function will cost lesser in this case as compare to other choices.

Also Firestore is better option to store user data as compare to Cloud SQL.

Question 54:

Your company has developed an application for hospitals. This application need to store large amount of sensitive patient data in BigQuery.

As per some compliance requirements, you must delete this sensitive information upon request of the subject.

What solution will you suggest for this requirement?

- **Create a BigQuery view over the table that contains all data.**
  Exclude the rows that affect the subject's data from this view when deletion request is made.

- **Use this view instead of the source table for all analysis tasks.**
  Use a unique identifier for each individual.

- **When deletion request is received, overwrite the column with the unique identifier with a its hashed value.**
  When ingesting new data in BigQuery, run the data through the Data Loss Prevention (DLP) API to identify any personal information.

- **As part of the DLP scan, save the result to Data Catalog.**
  When deletion request is received, query Data Catalog to find the column with personal information.

- **Use a unique identifier for each individual.**
  When deletion request is received, delete all rows from BigQuery with this identifier.

Your company has developed an application for hospitals. This application need to store large amount of sensitive patient data in BigQuery.

As per some compliance requirements, you must delete this sensitive information upon request of the subject.

What solution will you suggest for this requirement?

- ◯ **Create a BigQuery view over the table that contains all data.**
  Exclude the rows that affect the subject's data from this view when deletion request is made.

- ◯ **Use this view instead of the source table for all analysis tasks.**
  Use a unique identifier for each individual.

- ◯ **When deletion request is received, overwrite the column with the unique identifier with a its hashed value.**
  When ingesting new data in BigQuery, run the data through the Data Loss Prevention (DLP) API to identify any personal information.

- ◯ **As part of the DLP scan, save the result to Data Catalog.**
  When deletion request is received, query Data Catalog to find the column with personal information. (Correct)

- ◯ **Use a unique identifier for each individual.**
  When deletion request is received, delete all rows from BigQuery with this identifier.

Explanation
Cloud Data Loss Prevention (DLP) helps you find, understand, and manage the sensitive data that exists within your infrastructure.

DLP is a managed Google Cloud service designed to help you discover, classify, and protect your most sensitive data.

Once you've scanned your content for sensitive data using Cloud DLP, you have several options for what to do with that data intelligence like:

1. Store Cloud DLP scan results directly in BigQuery.
2. Generate reports on where sensitive data resides in your infrastructure.
3. Run rich SQL analytics to understand where sensitive data is stored and what kind it is.
4. Automate alerts, or actions to trigger based on a single set or a combination of findings.

Reference: https://cloud.google.com/bigquery/docs/scan-with-dlp

Question 55:

Your team wants to deploy you application servers in GCP. But database will resides in on premise data center. So your team needs to setup a hybrid networking. What suggestion will you give to your team to set up VPC in GCP?

- ◯ **Setup VPC in a way that both Primary and Secondary IP ranges of the VPC do not overlap with the on-premises VLAN.**
- ◯ **Setup the VPC with same IP range as on-premises VLAN.**
- ◯ **Set up the Secondary IP range of the VPC in GCP to use the same Secondary IP range as on-premises VLAN**
- ◯ **Make sure than Primary IP range of VPC do not overlap with On-Premises Primary IP range.**
- ◯ **Set up the Primary IP range of the VPC in GCP to use the same IP range as on-premises VLAN**
- ◯ **Make sure than Secondary IP range of VPC do not overlap with On-Premises Secondary IP range.**

Your team wants to deploy you application servers in GCP. But database will resides in on premise data center. So your team needs to setup a hybrid networking. What suggestion will you give to your team to set up VPC in GCP?

- ◯ **Setup VPC in a way that both Primary and Secondary IP ranges of the VPC do not overlap with the on-premises VLAN.** (Correct)
- ◯ **Setup the VPC with same IP range as on-premises VLAN.**
- ◯ **Set up the Secondary IP range of the VPC in GCP to use the same Secondary IP range as on-premises VLAN**
- ◯ **Make sure than Primary IP range of VPC do not overlap with On-Premises Primary IP range.**
- ◯ **Set up the Primary IP range of the VPC in GCP to use the same IP range as on-premises VLAN**
- ◯ **Make sure than Secondary IP range of VPC do not overlap with On-Premises Secondary IP range.**

Explanation

In 2 connected networks, IP address range should not overlap. Otherwise it is not possible to find the device for the given IP address.

Question 56:

Your team has created an autoscaling instance group to serve web traffic for an application. This instance group is used as backend service for HTTP(S) Load Balancer.

But you noticed that this deployment configuration is not working as expected. All virtual machine (VM) instances in instance group are being terminated and re-launched every minute. Public IP address is not assigned to any instance. You are getting correct response from each instance using the curl command.

How can you fix above problem?

- ◯ **Make sure that a firewall rule exists to allow source traffic on HTTP(S) to reach the load balancer.**
- ◯ **Assign a public IP to each instance.**
  Add a firewall rule in VPC to allow HTTP(s) traffic from load balancer to instance public IP.
- ◯ **Ensure that a firewall rule exists to allow Load Balancer health checks to reach the instances in the instance group.**
- ◯ **Create a network tag for the load balancer.**
- ◯ **Create another network tag for VM instances.**
- ◯ **Configure a firewall rule to allow HTTP(S) traffic with above created load balancer network tag as the source and the instance network tag as the destination.**

Your team has created an autoscaling instance group to serve web traffic for an application. This instance group is used as backend service for HTTP(S) Load Balancer.

But you noticed that this deployment configuration is not working as expected. All virtual machine (VM) instances in instance group are being terminated and re-launched every minute. Public IP address is not assigned to any instance. You are getting correct response from each instance using the curl command.

How can you fix above problem?

- ◯ **Make sure that a firewall rule exists to allow source traffic on HTTP(S) to reach the load balancer.**
- ◯ **Assign a public IP to each instance.**
  Add a firewall rule in VPC to allow HTTP(s) traffic from load balancer to instance public IP.
- ◯ **Ensure that a firewall rule exists to allow Load Balancer health checks to reach the instances in the instance group.** (Correct)
- ◯ **Create a network tag for the load balancer.**
- ◯ **Create another network tag for VM instances.**
- ◯ **Configure a firewall rule to allow HTTP(S) traffic with above created load balancer network tag as the source and the instance network tag as the destination.**

Explanation

- Option C is correct here. Since instances are getting terminated and relaunched, it means load balancer is considering instance to be unhealthy. It could be because load balancer is not able to reach to compute engine instance.

  So to fix this, we must ensure that a firewall rule exists to allow load balancer health checks to reach the instances in the instance group.

Question 57:

Your company want to scale its Apache spark and Hadoop jobs, which are currently hosted in on-premises data center. Because of limited capacity in on-premises data center, your team is exploring various Cloud options.

What Google Cloud Platform offering can you suggest to your team in such case?

- ◯ **Use GKE cluster and set up your Hadoop cluster there.**
- ◯ **Set up your own Hadoop cluster using Google Managed Instances.**
- ◯ **Manage these instances via Managed Instance Group.**
- ◯ **Set up your own Hadoop cluster using Google Managed Instances.**
- ◯ **Manage these instances via Unmanaged Instance Group.**
- ◯ **Use Cloud Dataproc to configure Hadoop cluster in Google Cloud.**

Question 57: Skipped

Your company want to scale its Apache spark and Hadoop jobs, which are currently hosted in on-premises data center. Because of limited capacity in on-premises data center, your team is exploring various Cloud options.

What Google Cloud Platform offering can you suggest to your team in such case?

- ◯ **Use GKE cluster and set up your Hadoop cluster there.**
- ◯ **Set up your own Hadoop cluster using Google Managed Instances.**
- ◯ **Manage these instances via Managed Instance Group.**
- ◯ **Set up your own Hadoop cluster using Google Managed Instances.**
- ◯ **Manage these instances via Unmanaged Instance Group.**
- ◯ **Use Cloud Dataproc to configure Hadoop cluster in Google Cloud.** (Correct)

Explanation

Dataproc is a **fully managed** and **highly scalable** service for running Apache Spark, Apache Flink, Presto, and 30+ open source tools and frameworks.

You can use Dataproc for data lake modernization, ETL, and secure data science, at planet scale, fully integrated with Google Cloud, at a fraction of the cost.

This solution must be cost effective and should not require much overhead or re writing of an existing code.

Question 58:

Your team wants to migrate existing microservices based application to Google Cloud using Compute Engine Instances. Team is not aware about how to aggregate logs from all the microservices in Google Cloud. Currently team was using some custom solution for log aggregation in on-premises data center but this custom utility can not be used in Google Cloud.

What solution will you suggest to your team in this case?

- ◯ **Install Istio service mesh on Compute Engine Instances.**
- ◯ **Write new custom solution for log aggregation that can run in GCP.**
- ◯ **Install Cloud Logging agent on each Compute Engine Instance via Startup Script.**
- ◯ **Use Cloud Logging service to manage logs collected by these logging agents.**
- ◯ **Install Cloud logging agent on each Compute Engine Instance via SSH logging in to VM.**
- ◯ **Use Cloud logging service to manage logs collected by these logging agents.**

Your team wants to migrate existing microservices based application to Google Cloud using Compute Engine Instances. Team is not aware about how to aggregate logs from all the microservices in Google Cloud. Currently team was using some custom solution for log aggregation in on-premises data center but this custom utility can not be used in Google Cloud.

What solution will you suggest to your team in this case?

- ◯ **Install Istio service mesh on Compute Engine Instances.**
- ◯ **Write new custom solution for log aggregation that can run in GCP.**
- ◯ **Install Cloud Logging agent on each Compute Engine Instance via Startup Script.**
- ◯ **Use Cloud Logging service to manage logs collected by these logging agents.** (Correct)
- ◯ **Install Cloud logging agent on each Compute Engine Instance via SSH logging in to VM.**
- ◯ **Use Cloud logging service to manage logs collected by these logging agents.**

Explanation

Cloud Logging allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services.

Logging agents can be easily installed on each VM automatically via Startup Script.

Question 59:

Your company is running primary MySQL instance in on-premises data center. Team has also configured Cloud SQL instance as failover instance for on-premises database instance. Sometimes operation team noticed that replication time between on-premises database and Cloud SQL database is more that defined SLA. It is mainly due to network issue between on-premises data center and Google Cloud.
What solution will you suggest to solve this issue?

- ◯ **Use Cloud Function to synchronize both databases**
- ◯ **Setup Dataflow job to replicate the data from on-premises database to Cloud SQL instance**
- ◯ **Set up a Dedicated Interconnect between on-premises data center and Google Cloud.**
- ◯ **Also configure multiple VPN connections between on-premises data center and Google Cloud.**
- ◯ **VPN connections should be used in case Dedicated Interconnect is not working.**
- ◯ **Increase the bandwidth of existing connection between on-premises data center and Google Cloud.**

Your company is running primary MySQL instance in on-premises data center. Team has also configured Cloud SQL instance as failover instance for on-premises database instance. Sometimes operation team noticed that replication time between on-premises database and Cloud SQL database is more that defined SLA. It is mainly due to network issue between on-premises data center and Google Cloud.
What solution will you suggest to solve this issue?

- ◯ **Use Cloud Function to synchronize both databases**
- ◯ **Setup Dataflow job to replicate the data from on-premises database to Cloud SQL instance**
- ◯ **Set up a Dedicated Interconnect between on-premises data center and Google Cloud.**
- ◯ **Also configure multiple VPN connections between on-premises data center and Google Cloud.**
- ◯ **VPN connections should be used in case Dedicated Interconnect is not working.** (Correct)
- ◯ **Increase the bandwidth of existing connection between on-premises data center and Google Cloud.**

Explanation

Since issue is primarily because of occasional network problem, so it's better to have backup up VPN network configured between on-premises data center and Google Cloud.

This VPN network will be used if Dedicated Interconnect is not working for any reason.

Question 60:

Your company wants to migrate its existing microservices based application to Google Cloud. For this they need to setup CI/CD pipeline in Google Cloud Platform. Your security team follows very high standard security practices and do no want to compromise this on Cloud as well.
By considering right security practices, what solution will you suggest to your team to set up CI/CD pipeline in Google Cloud Platform? (select 2)

- [ ] **Use Jenkins to manage CI/CD in Google Cloud.**
- [ ] **Use signed binaries from private repositories for CI/CD pipeline.**
- [ ] **Ask team to do manual security check of source code before doing any commit.**
- [ ] **Configure static source code security scan with in CI/CD pipeline. Stop the pipeline execution if security scan check fails.**
- [ ] **Configure security vulnerability scan and deploy changes only if there is no issue in this scan.**

Your company wants to migrate its existing microservices based application to Google Cloud. For this they need to setup CI/CD pipeline in Google Cloud Platform. Your security team follows very high standard security practices and do no want to compromise this on Cloud as well.
By considering right security practices, what solution will you suggest to your team to set up CI/CD pipeline in Google Cloud Platform? (select 2)

- [ ] **Use Jenkins to manage CI/CD in Google Cloud.**
- [ ] **Use signed binaries from private repositories for CI/CD pipeline.**
- [ ] **Ask team to do manual security check of source code before doing any commit.**
- [ ] **Configure static source code security scan with in CI/CD pipeline. Stop the pipeline execution if security scan check fails.** (Correct)
- [ ] **Configure security vulnerability scan and deploy changes only if there is no issue in this scan.** (Correct)

Explanation

Source code security scan and security vulnerability scan can help in finding any security loophole in application. So it must be configured with CI/CD pipeline.

PART 2 Coming Soon