[Home](https://cognizant.udemy.com/)

[Google Certified Associate Cloud Engineer Practice Tests…](https://cognizant.udemy.com/course/gcp-ace-practice-tests-latest/)

[Add to learning path](https://cognizant.udemy.com/course/gcp-ace-practice-tests-latest/learn/)

[Favorite this course](javascript:void(0))

[Archive this course](javascript:void(0))

[Unenroll from course](javascript:void(0))

Premium Practice Test 4 (Updated: October 2020) - Results

Return to review

Created with Highcharts 6.1.0

Attempt 1

All questions

[All questions](javascript:void(0))

[Correct](javascript:void(0))

[Incorrect](javascript:void(0))

[Skipped](javascript:void(0))

[Marked for review](javascript:void(0))

Top of Form

Question 1: Incorrect

You developed a new mobile game that uses Cloud Spanner for storing user state, player profile and leaderboard. Your performance testing team identified slow reads in all their tests. You suspect it might be down to how the table configuration. You created the table by executing this DDL:

CREATE TABLE users {

user\_id INT64 NOT NULL, // This is populated from a sequence

user\_name STRING (255), // Game username

…

…

email\_address STRING (255) // Email Address

} PRIMARY KEY (user\_id)

What should you do to fix this read latency issue?

​

Change the primary key to not have monotonically increasing values.

(Correct)

​

Remove the email\_address field from the table.

​

Add a secondary index on the user\_id column.

​

Create a secondary index using the following Data Definition Language (DDL):

CREATE INDEX users\_id\_ix

ON users (

user\_id,

user\_name

) STORING (

email\_address

)

(Incorrect)

Explanation

Change the primary key to not have monotonically increasing values. is the right answer.

You should be careful when choosing a primary key to not accidentally create hotspots in your database. One cause of hotspots is having a column whose value monotonically increases as the first key part because this results in all inserts occurring at the end of your keyspace. This pattern is undesirable because Cloud Spanner divides data among servers by key ranges, which means all your inserts will be directed at a single server that will end up doing all the work.

Ref: https://cloud.google.com/spanner/docs/schema-design#primary-key-prevent-hotspots

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

Bottom of Form

Top of Form

Question 2: Correct

Your company runs a popular online retail platform that lets individual retailers sell their products to millions of customers around the world. Your company places a high value in delivering web requests with low latency, and customers have found this to be a key selling feature of the online platform. However, a recent surge in customers buying gifts for Thanksgiving has seen product pages load slower than usual. Your manager has suggested sticking in a reverse proxy layer to cache images. Your performance testing lead has estimated requiring 30 GB in-memory cache for caching images of the most popular products in Thanksgiving sale. The reverse proxy also requires approximately 2 GB memory for various other processes and no CPU at all. How should you design this system?

​

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

​

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

​

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

(Correct)

​

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

Explanation

Requirements

1. latency sensitive

2. 30 GB in-memory cache

3. 2 GB for rest of processes

4. Cost-effective

Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB. is not right.

Fetching data from disk is slower compared to fetching from in-memory. Our requirements state we need 30GB in-memory cache for a latency-sensitive website and a compute engine with disk can't provide in-memory cache.

Run it on Compute Engine and choose a custom instance type with 6 vCPUs and 32 GB of memory. is not right.

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

Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes. is not right.

Without going into details of the feasibility of this option, let’s assume for now that this option is possible. But this option is quite expensive. At the time of writing, just the compute cost for a n1-standard-32 instance is $1.5200 per hour in the Iowa region.

Ref: https://cloud.google.com/compute/all-pricing

In comparison, the cost of GCP Cloud Memorystore which is $0.023 per GB-hr which is $0.736 for 32GB per hour. Ref: https://cloud.google.com/memorystore

Create a Cloud Memorystore for Redis instance with 32-GB capacity. is the right answer.

This is the only option that fits the requirements. Cloud Memorystore is a fully managed in-memory data store service for Redis built on scalable, secure, and highly available infrastructure managed by Google. Use Memorystore to build application caches that provide sub-millisecond data access.

Ref: https://cloud.google.com/memorystore

Memorystore for Redis instance pricing is charged per GB-hour and you can scale as needed. You can also specify eviction (maxmemory) policies to restrict the rest of processes to 2GB or the reverse proxy to 30GB or both; you can select a suitable maxmemory policy to handle scenarios when memory is full.

Ref: https://cloud.google.com/memorystore/docs/reference/redis-configs#maxmemory\_policies

Bottom of Form

Top of Form

Question 3: Correct

A Data Support Engineer at your company accidentally disclosed customer PII data in a support case in Google Cloud Console. Your compliance team wants to prevent this from occurring again and has asked you to set them up as approvers for support cases raised by support teams. What IAM access does the compliance team need?

​

Add your Compliance team to a group and then add this group to roles/iam.roleAdmin role.

​

Add your Compliance team to roles/accessapproval.approver role.

​

Add your Compliance team to roles/iam.roleAdmin role.

​

Add your Compliance team to a group and then add this group to roles/accessapproval.approver role.

(Correct)

Explanation

Add your Compliance team to roles/iam.roleAdmin role. is not right.

roles/iam.roleAdmin provides access to all custom roles in the project. This doesn't fit our requirement of Compliance team being able to approve requests.

Add your Compliance team to a group and then add this group to roles/iam.roleAdmin role. is not right.

roles/iam.roleAdmin provides access to all custom roles in the project. This doesn't fit our requirement of Compliance team being able to approve requests.

Add your Compliance team to roles/accessapproval.approver role. is not right.

roles/accessapproval.approver is an Access Approval Approver role and provides the ability to view or act on access approval requests and view configuration. Although this is the role we require, you want to follow Google recommended practices which means we should instead add the group to the role and add users to the group instead of granting the role individually to users.

Ref: https://cloud.google.com/iam/docs/understanding-roles#access-approval-roles

Ref: https://cloud.google.com/iam/docs/overview

Add your Compliance team to a group and then add this group to roles/accessapproval.approver role. is the right answer.

roles/accessapproval.approver is an Access Approval Approver role and provides the ability to view or act on access approval requests and view configuration. And you follow Google recommended practices by adding users to the group and group to the role. Groups are a convenient way to apply an access policy to a collection of users. You can grant and change access controls for a whole group at once instead of granting or changing access controls one at a time for individual users or service accounts. You can also easily add members to and remove members from a Google group instead of updating a Cloud IAM policy to add or remove users.

Ref: https://cloud.google.com/iam/docs/understanding-roles#access-approval-roles

Ref: https://cloud.google.com/iam/docs/overview

Bottom of Form

Top of Form

Question 4: Correct

You have developed an enhancement for a photo compression application running on the App Engine Standard service in Google Cloud Platform, and you want to canary test this enhancement on a small percentage of live users before switching off the old version. How can you do this?

​

Deploy a new version as a separate app in App Engine. Then configure App Engine using GCP Console to split traffic between the two apps.

​

Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

(Correct)

​

Deploy a new version of your application in Google Kubernetes Engine instead of App Engine and then use GCP Console to split traffic.

​

Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic.

Explanation

Deploy a new version of your application in Google Kubernetes Engine instead of App Engine and then use GCP Console to split traffic. is not right.

When you can achieve this natively in GCP app engine using versions, there is no need to do it outside App Engine.

Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic. is not right.

When you can achieve this natively in GCP app engine using versions, there is no need to do it outside App Engine.

Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

Deploy a new version as a separate app in App Engine. Then configure App Engine using GCP Console to split traffic between the two apps. is not right.

You can achieve this natively in GCP app engine using versions but App Engine doesn't let you split traffic between apps. If you need to do it between apps, you are probably looking at doing this at the load balancer layer or at the DNS layer - either increasing the cost/complexity or introduce other problems such as caching issues.

Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly. is the right answer.

GCP App Engine natively offers traffic splitting functionality between versions. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.

Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

Bottom of Form

Top of Form

Question 5: Incorrect

You created a deployment manager template to automate the provisioning of a production Google Kubernetes Engine (GKE) cluster. The GKE cluster requires a monitoring pod running on each node (DaemonSet), and your manager has asked you to identify if it is possible to automate the provisioning of the monitoring pod along with the cluster. How should you do this?

​

Use the Deployment Manager Runtime Configurator to create a new Config resource that contains the DaemonSet definition.

(Incorrect)

​

With Deployment Manager, create a Compute Engine instance with a startup script that uses kubectl to create the DaemonSet.

​

In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value.

​

Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

(Correct)

Explanation

In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value. is not right.

Metadata entries are key-value pairs and do not influence this behavior.

Ref: https://cloud.google.com/compute/docs/storing-retrieving-metadata

With Deployment Manager, create a Compute Engine instance with a startup script that uses kubectl to create the DaemonSet. is not right.

It is possible to spin up a compute engine instance with a startup script that executes kubectl to create a DaemonSet deployment.

kubectl apply -f https://k8s.io/examples/controllers/daemonset.yaml

Ref: https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/

But this involves using the compute engine service which is an additional service. Our requirement is to achieve using the fewest possible services and as you'll notice later, the correct answer uses fewer services.

Use the Deployment Manager Runtime Configurator to create a new Config resource that contains the DaemonSet definition. is not right.

You can configure the GKE nodes (provisioned by Deployment manager) to report their status to the Runtime Configurator, and when they are UP, you can run a task to create a DaemonSet. While this is possible, it involves one additional service - to run a task e.g. using Cloud Functions, etc. Our requirement is to achieve using the fewest possible services and as you'll notice later, the correct answer uses fewer services.

Here is some more info about Runtime Configurator. The Runtime Configurator feature lets you define and store data as a hierarchy of key-value pairs in Google Cloud Platform. You can use these key-value pairs as a way to:

1. Dynamically configure services

2. Communicate service states

3. Send notification of changes to data

4. Share information between multiple tiers of services

For example, imagine a scenario where you have a cluster of nodes that run a startup procedure. During startup, you can configure your nodes to report their status to the Runtime Configurator, and then have another application query the Runtime Configurator and run specific tasks based on the status of the nodes.

The Runtime Configurator also offers a Watcher service and a Waiter service. The Watcher service watches a specific key pair and returns when the value of the key pair changes, while the Waiter service waits for a specific end condition and returns a response once that end condition has been met.

Ref: https://cloud.google.com/deployment-manager/runtime-configurator

Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet. is the right answer.

A type provider exposes all resources of a third-party API to Deployment Manager as base types that you can use in your configurations. If you have a cluster running on Google Kubernetes Engine, you could add the cluster as a type provider and access the Kubernetes API using Deployment Manager. Using these inherited API, you can create a DaemonSet.

This option uses just the Deployment Manager to create a DaemonSet and is, therefore, the right answer.

Ref: https://cloud.google.com/deployment-manager/docs/configuration/type-providers/creating-type-provider

Bottom of Form

Top of Form

Question 6: Incorrect

You developed a new order tracking application and created a test environment in your GCP project. The order tracking system uses Google Compute engine to serve requests and relies on Cloud SQL to persist order data. Unit testing and user acceptance testing has succeeded, and you want to deploy the production environment. You want to do this in the same GCP project while ensuring there are no routes between the test environment and the production environment. How should you do this?

​

Ask the security team to grant you the Project Editor role in an existing production project used by another division of your company. Once they grant you that role, replicate the setup you have in the development environment in that project.

​

Create a new project, modify your existing VPC to be a Shared VPC, share that VPC with your new project, and replicate the setup you have in the development environment in that new project, in the Shared VPC.

​

Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

(Correct)

​

Create a new production subnet in the existing VPC and a new production Cloud SQL instance in your existing project, and deploy your application using those resources.

(Incorrect)

Explanation

Create a new project, modify your existing VPC to be a Shared VPC, share that VPC with your new project, and replicate the setup you have in the development environment in that new project, in the Shared VPC. is not right.

A Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. This goes totally against the recommendations of the security team.

Ref: https://cloud.google.com/vpc/docs/shared-vpc

Create a new production subnet in the existing VPC and a new production Cloud SQL instance in your existing project, and deploy your application using those resources. is not right.

You can't achieve complete isolation between development and production environments. When configuration access in Cloud SQL, while you can grant any application access to a Cloud SQL instance by authorizing the public IP addresses that the application uses to connect, you can not specify a private network (for example, 10.x.x.x) as an authorized network. The compute engine instances use their private IP addresses to reach out to Cloud SQL and because of the above limitation, we can't prevent the development compute engine reach out to production MySQL and vice versa. Since the security team has forbidden the existence of network routes between these 2 environments, having the production and development environments in a single project is not an option.

https://cloud.google.com/sql/docs/mysql/connect-external-app#appaccessIP

Ask the security team to grant you the Project Editor role in an existing production project used by another division of your company. Once they grant you that role, replicate the setup you have in the development environment in that project. is not right.

While this would technically isolate the development environment from the production environment, your production application is running in a project that is also hosting production applications of another division of your company. This goes against Google's recommended practices. You can use folders to isolate requirements for different departments and teams in the parent organization. And you have separate projects under the folders so as per Google recommendations we should be deploying the production application to a separate project that is just for one company division/department.

Ref: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#define-hierarchy

Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment. is the right answer.

This aligns with Google's recommended practices. By creating a new project, we achieve complete isolation between development and production environments; as well as isolate this production application from production applications of other departments.

Ref: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#define-hierarchy

Bottom of Form

Top of Form

Question 7: Incorrect

The compliance team has requested you to provide an external auditor with a report of when Cloud Identity users in your company were updated to include IAM roles for a Cloud Spanner instance. What should you do?

​

Go to the Stackdriver Monitoring console and review information for Cloud Spanner.

​

Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

(Correct)

​

Open the Cloud Spanner console to review configurations.

​

Open the IAM & admin console to review IAM policies for Cloud Spanner roles.

(Incorrect)

Explanation

Go to the Stackdriver Monitoring console and review information for Cloud Spanner. is not right.

Monitoring collects metrics, events, and metadata from Google Cloud and lets you generate insights via dashboards, charts, and alerts. It can't provide information on when a role has been granted to a user.

Ref: https://cloud.google.com/monitoring/docs

Open the IAM & admin console to review IAM policies for Cloud Spanner roles. is not right.

You can't find the role bindings and the timestamps in the policies.

https://cloud.google.com/iam/docs/overview

Open the Cloud Spanner console to review configurations. is not right.

You manage cloud spanner instances in the console but you can't check when a role has been granted to a user.

Ref: https://cloud.google.com/spanner/docs/quickstart-console

Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles. is the right answer.

Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions. Admin Activity audit logs are always written; you can't configure or disable them. There is no charge for your Admin Activity audit logs.

Ref: https://cloud.google.com/logging/docs/audit#admin-activity

See below a screenshot from GCP console showing this in action.

Among other things, the payload contains

{

action: "ADD"

role: "roles/spanner.admin"

member: "user:testuser@gmail.com"

}

Bottom of Form

Top of Form

Question 8: Correct

Your company wants to move all its on-premises applications to Google Cloud. Most applications depend on Kubernetes orchestration, and you have chosen to deploy these applications in Google Kubernetes Engine (GKE). The security team have requested you to store all container images in a Google Container Registry (GCR) in a separate project which has an automated vulnerability management scanning set up by a security partner organization. You want to ensure the GKE cluster running in your project can download the container images from the GCR repo in the other project. How should you do this?

​

When you create the GKE cluster, choose the Allow full access to all Cloud APIs option under 'Access scopes'.

​

In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

(Correct)

​

Create a service account, and give it access to Cloud Storage. Create a P12 key for this service account and use it as an imagePullSecrets in Kubernetes.

​

Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account.

Explanation

Here's some info about where Container Registry stores images and how access is controlled.

Container Registry uses Cloud Storage buckets as the underlying storage for container images. You control access to your images by granting appropriate Cloud Storage permissions to a user, group, service account, or another identity. Cloud Storage permissions granted at the project level apply to all storage buckets in the project, not just the buckets used by Container Registry. To configure permissions specific to Container Registry, grant permissions on the storage bucket used by the registry. Container Registry ignores permissions set on individual objects within the storage bucket.

Ref: https://cloud.google.com/container-registry/docs/access-control

Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account. is not right.

As mentioned above, Container Registry ignores permissions set on individual objects within the storage bucket so this isn't going to work.

Ref: https://cloud.google.com/container-registry/docs/access-control

When you create the GKE cluster, choose the Allow full access to all Cloud APIs option under 'Access scopes'. is not right.

Selecting Allow full access to all Cloud APIs does not provide access to GCR images in a different project. If the Google Kubernetes Engine cluster and the Container Registry storage bucket are in the same Google Cloud project, the Compute Engine default service account is configured with the appropriate permissions to push or pull images. But if the cluster is in a different project or if the VMs in the cluster use a different service account, you must grant the service account the appropriate permissions to access the storage bucket used by Container Registry.

Ref: https://cloud.google.com/container-registry/docs/using-with-google-cloud-platform

In this case, since there is no mention of a service account, we have to assume we are using a default service account that hasn't been provided permissions to access the storage bucket used by Container Registry in another project so the image pull isn't going to work. You would end up with an error like:

Failed to pull image "gcr.io/kubernetes2-278322/simple-python-image": rpc error: code = Unknown desc = Error response from daemon: pull access denied for gcr.io/kubernetes2-278322/simple-python-image, repository does not exist or may require 'docker login'

Create a service account, and give it access to Cloud Storage. Create a P12 key for this service account and use it as an imagePullSecrets in Kubernetes. is not right.

It is technically possible to do it this way but using the JSON key and not P12 key as mentioned in this option. If you would like to understand how to do this, please look at these blogs.

Ref: https://medium.com/hackernoon/today-i-learned-pull-docker-image-from-gcr-google-container-registry-in-any-non-gcp-kubernetes-5f8298f28969

Ref: https://medium.com/@michaelmorrissey/using-cross-project-gcr-images-in-gke-1ddc36de3d42

Moreover, this approach is suitable for accessing GCR images in a non-Google Cloud Kubernetes environment. While it can be used in GKE too, it is not as secure as using Role Bindings since it involves downloading service account keys and setting them up as secret in Kubernetes.

In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes. is the right answer.

Granting the storage object viewer IAM role in the project where images are stored to the service account used by the Kubernetes cluster ensures that the nodes in the cluster can Read Images from the storage bucket. It would be ideal to further restrict the role binding to provide access just to the Cloud Storage bucket that is used as the underlying storage for container images. This follows the principle of least privilege.

For more information about Storage Object Viewer IAM Role for GCR refer: https://cloud.google.com/container-registry/docs/access-control#permissions\_and\_roles

Bottom of Form

Top of Form

Question 9: Correct

Your machine learning team runs training models on compute engines with NVIDIA® Tesla® T4: nvidia-tesla-t4 GPUs but the processing is slower than the requirement. The performance tuning team has suggested upgrading to NVIDIA® Tesla® K80: nvidia-tesla-k80 GPU accelerator which delivers exceptional performance and increased throughput that allows researchers to advance their scientific discoveries quicker. You manage the GKE clusters and want to facilitate this request. What should you do?

​

Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-k80 nodeSelector to their pod specification.

(Correct)

​

Recreate all the nodes of the GKE cluster to enable GPUs on all of them.

​

Create your own Kubernetes cluster on top of Compute Engine with nodes that have GPUs. Dedicate this cluster to your ML team.

​

Ask your ML team to add the "accelerator: gpu" annotation to their pod specification.

Explanation

Ask your ML team to add the "accelerator: gpu" annotation to their pod specification. is not right.

There are two issues with this approach. One - the syntax is invalid. Two - You cannot add GPUs to existing node pools.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus

Recreate all the nodes of the GKE cluster to enable GPUs on all of them. is not right.

There are two issues with this approach. One - recreating all nodes to enable GPUs makes the cluster very expensive. Only the ML team needs access to GPUs to train their models. Recreating all nodes to enable GPUs helps your ML team use them but they are left unused for all other workloads yet cost you money. Two - Even though your nodes have GPUs enabled, you still have to modify pod specifications to request GPU. This step isn't performed in this option.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus

Create your own Kubernetes cluster on top of Compute Engine with nodes that have GPUs. Dedicate this cluster to your ML team. is not right.

While this works, it increases the cost as you now pay the Kubernetes cluster management fee for two clusters instead of one. GKE clusters accrue a management fee that is per cluster per hour, irrespective of cluster size or topology.

Ref: https://cloud.google.com/kubernetes-engine/pricing

Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-k80 nodeSelector to their pod specification. is the right answer.

This is the most optimal solution. Rather than recreating all nodes, you create a new node pool with GPU enabled. You then modify the pod specification to target particular GPU types by adding node selector to your workload's Pod specification. YOu still have a single cluster so you pay Kubernetes cluster management fee for just one cluster thus minimizing the cost.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus

Ref: https://cloud.google.com/kubernetes-engine/pricing

Example:

apiVersion: v1

kind: Pod

metadata:

name: my-gpu-pod

spec:

containers:

- name: my-gpu-container

image: nvidia/cuda:10.0-runtime-ubuntu18.04

command: ["/bin/bash"]

resources:

limits:

nvidia.com/gpu: 2

nodeSelector:

cloud.google.com/gke-accelerator: nvidia-tesla-k80 # or nvidia-tesla-p100 or nvidia-tesla-p4 or nvidia-tesla-v100 or nvidia-tesla-t4

Bottom of Form

Top of Form

Question 10: Incorrect

Your company has three GCP projects – development, test and production – that are all linked to the same billing account. Your finance department has asked you to set up an alert to notify the testing team with the Google Compute Engine charges in the test project exceed a threshold. How should you do this?

​

Verify that you have Billing Account Administrator role. Select the associated billing account and create a budget and a custom alert.

​

Verify that you have Project Billing Manager role. Select the associated billing account and create a budget for the appropriate project.

​

Verify that you have Project Billing Manager role. Select the associated billing account and create a budget and a custom alert.

(Incorrect)

​

Verify that you have Billing Account Administrator role. Select the associated billing account and create a budget and alert for the appropriate project.

(Correct)

Explanation

Verify that you have Project Billing Manager role. Select the associated billing account and create a budget for the appropriate project. is not right.

Project Billing Manager role allows a user to attach the project to the billing account, but does not grant any rights over resources. This role does not provide user permissions to view spending, create budgets and alerts.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam

Verify that you have Project Billing Manager role. Select the associated billing account and create a budget and a custom alert. is not right.

Project Billing Manager role allows a user to attach the project to the billing account, but does not grant any rights over resources. This role does not provide user permissions to view spending, create budgets and alerts.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam

Verify that you have Billing Account Administrator role. Select the associated billing account and create a budget and a custom alert. is not right.

Billing Account Administrator role enables a user to view spend and set budget alerts. But the budget here isn't scoped to the single project that we are interested in. Since the single billing account is linked to all three projects, this results in budget alerts being triggered for Compute Engine usage on all three projects - which is against our requirements.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam

Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

Verify that you have Billing Account Administrator role. Select the associated billing account and create a budget and alert for the appropriate project. is the right answer.

Billing Account Administrator role enables a user to view spend and set budget alerts. In addition, the budget here is scoped to a single project. Therefore, when the compute engine spend exceeds the budget threshold in the project, we send an alert, and this only works for the scoped project, and not all projects linked to the billing account.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam

Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

Bottom of Form

Top of Form

Question 11: Incorrect

You want to identify a cost-efficient storage class for archival of audit logs in Google Cloud Storage. Some of these audit logs may need to be retrieved during the quarterly audit. What Storage Class should you use to minimize costs?

​

Multi-Regional Storage

​

Coldline Storage

(Correct)

​

Regional Storage

​

Nearline Storage

(Incorrect)

Explanation

Nearline Storage. is not right.

Nearline Storage is a low-cost, highly durable storage service for storing infrequently accessed data. Nearline Storage is ideal for data you plan to read or modify on average once per month or less. Nearline storage is more expensive than Coldline Storage which is more suitable for our requirements.

https://cloud.google.com/storage/docs/storage-classes#nearline

Regional Storage. is not right.

While this would certainly let you access your files once a quarter, it would be too expensive compared to Coldline storage which is more suitable for our requirement.

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

Multi-Regional Storage. is not right.

While this would certainly let you access your files once a quarter, it would be too expensive compared to Coldline storage which is more suitable for our requirement.

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

Coldline Storage. is the right answer.

Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Since we have a requirement to access data once a quarter and want to go with the most cost-efficient option, we should select Coldline Storage.

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

Bottom of Form

Top of Form

Question 12: Correct

Your company's backup strategy involves creating snapshots for all VMs at midnight every day. You want to write a script to retrieve a list of compute engine instances in all development and production projects and feed it to the backup script for snapshotting. What should you do?

​

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

​

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

​

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

​

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

(Correct)

Explanation

Go to Cloud Shell and export this information to Cloud Storage on a daily basis. is not right.

You want an automated process but this is a manual activity that needs to be executed daily.

Go to GCP Console and export this information to Cloud SQL on a daily basis. is not right.

You want an automated process but this is a manual activity that needs to be executed daily.

Create two configurations using gsutil config. Write a script that sets configurations as active, individually. For each configuration, use gsutil compute instances list to get a list of compute resources. is not right.

The gsutil config command applies to users who have installed gsutil as a standalone tool and is used for obtaining access credentials for Cloud Storage and writes a boto/gsutil configuration file containing the obtained credentials along with a number of other configuration-controllable values.

Ref: https://cloud.google.com/storage/docs/gsutil/commands/config

It is not used for creating Gcloud configurations. You use gcloud config to do that.

https://cloud.google.com/sdk/gcloud/reference/config/configurations/create

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

You can create two configurations - one for the development project and another for the production project. And you do that by running "gcloud config configurations create" command.

https://cloud.google.com/sdk/gcloud/reference/config/configurations/create

In your custom script, you can load these configurations one at a time and execute gcloud compute instances list to list Google Compute Engine instances in the project that is active in the gcloud configuration.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

Once you have this information, you can export it in a suitable format to a suitable target e.g. export as CSV or export to Cloud Storage/BigQuery/SQL, etc.

Bottom of Form

Top of Form

Question 13: Incorrect

There has been an increased phishing email activity recently, and you deployed a new application to a GKE cluster to help scan and detect viruses in uploaded files. Each time the Finance or HR department receive an email with an attachment, they use this application to scan the email attachment for viruses. The application pods open the email attachment in a sandboxed environment before initiating a virus scan. Some infected email attachments may run arbitrary code with elevated privileges in the container. You want to ensure that the pods that run these scans do not the impact pods of other applications running in the same GKE cluster. How can you achieve this isolation between pods?

​

Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

(Correct)

​

Use Binary Authorization and whitelist only the container images used by your customers' Pods.

​

Use the cos\_containerd image for your GKE nodes. Add a nodeSelector with the value cloud.google.com/gke-os-distribution: cos\_containerd to the specification of your customers' Pods.

(Incorrect)

​

Use the Container Analysis API to detect vulnerabilities in the containers used by your customers' Pods.

Explanation

Use Binary Authorization and whitelist only the container images used by your customers' Pods. is not right.

Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE). 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.

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

Use the Container Analysis API to detect vulnerabilities in the containers used by your customers' Pods. is not right.

Container Analysis is a service that provides vulnerability scanning and metadata storage for software artifacts. The scanning service performs vulnerability scans on images in Container Registry, then stores the resulting metadata and makes it available for consumption through an API. Metadata storage allows storing information from different sources, including vulnerability scanning, other Cloud services, and third-party providers.

Ref: https://cloud.google.com/container-registry/docs/container-analysis

Use the cos\_containerd image for your GKE nodes. Add a nodeSelector with the value cloud.google.com/gke-os-distribution: cos\_containerd to the specification of your customers' Pods. is not right.

The cos\_containerd and ubuntu\_containerdimages let you use containerd as the container runtime in your GKE cluster. This doesn't directly provide the isolation we require.

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

Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods. is the right answer.

GKE Sandbox provides an extra layer of security to prevent untrusted code from affecting the host kernel on your cluster nodes when containers in the Pod execute unknown or untrusted code. Multi-tenant clusters and clusters whose containers run untrusted workloads are more exposed to security vulnerabilities than other clusters. Examples include SaaS providers, web-hosting providers, or other organizations that allow their users to upload and run code. When you enable GKE Sandbox on a node pool, a sandbox is created for each Pod running on a node in that node pool. In addition, nodes running sandboxed Pods are prevented from accessing other Google Cloud services or cluster metadata. Each sandbox uses its own userspace kernel. With this in mind, you can make decisions about how to group your containers into Pods, based on the level of isolation you require and the characteristics of your applications.

Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/sandbox-pods

Bottom of Form

Top of Form

Question 14: Incorrect

Your company has two GCP organizations – one for development (and test resources), and another for production resources. Each GCP organization has a billing account and several GCP projects. The new CFO doesn’t like this billing structure and has asked your team to consolidate costs from all GCP projects in both the organizations into a single bill. What should you do?

​

Migrate the production projects into development GCP organization. Link the migrated projects to development billing account.

​

Create a new GCP organization and a new billing account. Migrate the production projects and development projects into the new GCP organization and link the projects to the new billing account.

(Incorrect)

​

Link the production projects to development billing account.

(Correct)

​

Configure the production billing account and development billing account to export the billing data into the same BigQuery dataset.

Explanation

Configure the production billing account and development billing account to export the billing data into the same BigQuery dataset. is not right.

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

Migrate the production projects into development GCP organization. Link the migrated projects to development billing account. is not right.

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

Create a new GCP organization and a new billing account. Migrate the production projects and development projects into the new GCP organization and link the projects to the new billing account. is not right.

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

Link the production projects to your company's billing account. is the right answer.

This option is the quickest that lets us achieve our end requirement of having all GCP billing in a single invoice. Linking the production projects to development billing account can be very quick and can be scripted using gcloud.

Ref: https://cloud.google.com/logging/docs/reference/tools/gcloud-logging

Bottom of Form

Top of Form

Question 15: Correct

Your finance team owns two GCP projects in separate networks (VPC) – one project for payroll applications and another project for accounts. You need the compute engine instances in the payroll project to communicate with compute engine instances in accounts project and vice versa. How should you do it?

​

Verify that both projects are in a GCP Organization. Create a new VPC and add all instances.

​

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

​

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

​

Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.

(Correct)

Explanation

Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC. is the right answer.

All other options make no sense. Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it.

Ref: https://cloud.google.com/vpc/docs/shared-vpc

All other options make no sense.

Bottom of Form

Top of Form

Question 16: Incorrect

Your company stores terabytes of image thumbnails in Google Cloud Storage bucket with versioning enabled. An engineer deleted a current (live) version of an image and a non-current (not live) version of another image. What is the outcome of this operation?

​

1. The live version becomes a noncurrent version and a lifecycle rule is applied to delete after 30 days.

2. A lifecycle rule is applied on the noncurrent version to delete after 30 days.

​

1. The live version becomes a noncurrent version.

2. The noncurrent version is deleted permanently.

(Correct)

​

1. The live version is deleted permanently.

2. The noncurrent version is deleted permanently.

(Incorrect)

​

1. The live version becomes a noncurrent version and a lifecycle rule is applied to transition to Nearline Storage after 30 days.

2. A lifecycle rule is applied on the noncurrent version to transition to Nearline Storage after 30 days.

Explanation

1. The live version becomes a noncurrent version.

2. The noncurrent version is deleted permanently. is the right answer.

In buckets with object versioning enabled, deleting the live version of an object creates a noncurrent version while deleting a noncurrent version deletes that version permanently.

Ref: https://cloud.google.com/storage/docs/lifecycle#actions

Bottom of Form

Top of Form

Question 17: Correct

Your company is migrating its on-premises data centre to Google Cloud Platform in several phases. The current phase requires the migration of the LDAP server onto a Compute Engine instance. However, several legacy applications in your on-premises data centre and few third-party applications still depend on the LDAP server for user authentication. How can you ensure the LDAP server is publicly reachable via TLS on UDP port 636?

​

Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server.

​

Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag.

​

Add the network tag allow-udp-636 to the VM instance running the LDAP server.

​

Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

(Correct)

Explanation

Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server. is not right.

Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations. These destinations can be inside your Google Cloud Virtual Private Cloud (VPC) network (for example, in another VM) or outside it. Routes aren't a suitable solution for our requirement as we need to enable EXTERNAL clients to reach our VM on port 636 using UDP.

Ref: https://cloud.google.com/vpc/docs/routes

Add the network tag allow-udp-636 to the VM instance running the LDAP server. is not right.

Tags enable you to make firewall rules and routes applicable to specific VM instances but allow-udp-636 is not a network tag that GCP provides. The default network tags provided by GCP are default-allow-icmp, default-allow-internal, default-allow-rdp and default-allow-ssh. In this scenario, we are assigning a tag to the instance with no network rules so there would be no difference to behavior.

Ref: https://cloud.google.com/vpc/docs/add-remove-network-tags

Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag. is not right.

We are interested in enabling inbound traffic to our VM whereas egress firewall rules control outgoing connections from target instances in your VPC network.

Ref: https://cloud.google.com/vpc/docs/firewalls#egress\_cases

Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag. is the right answer.

This fits all our requirements. Ingress firewall rules control incoming connections from a source to target instances in your VPC network. We can create an ingress firewall rule to allow UDP port 636 for a network tag. And when we assign this network tag to the instance, the firewall rule applies to the instances so traffic is accepted on port 636 using UDP. Although not specified in this option, it has to be assumed that the source for the firewall rule is set to 0.0.0.0/0 i.e. all IP ranges so that external clients are allowed to connect to this VM.

Ref: https://cloud.google.com/vpc/docs/firewalls#ingress\_cases

Bottom of Form

Top of Form

Question 18: Incorrect

An external partner working on a production issue has asked you to share a list of all GCP APIs enabled for your GCP production project – production\_v1. How should you retrieve this information?

​

Run gcloud info to view the account value, and then run gcloud services list --account <Account>.

​

Run gcloud projects list to get the project ID, and then run gcloud services list --project <project ID>.

(Correct)

​

Run gcloud init to set the current project to my-project, and then run gcloud services list --available.

​

Run gcloud projects describe <project ID> to verify the project value, and then run gcloud services list --available.

(Incorrect)

Explanation

Run gcloud init to set the current project to my-project, and then run gcloud services list --available. is not right.

--available return the services available to the project to enable and not the services that are enabled. This list will include any services that the project has already enabled plus the services that the project can enable.

Ref: https://cloud.google.com/sdk/gcloud/reference/services/list

Also, to set the current project, you need to use gcloud config set project <project id>

Ref: https://cloud.google.com/sdk/gcloud/reference/config/set

gcloud init is used for initializing or reinitializing gcloud configurations.

https://cloud.google.com/sdk/gcloud/reference/init

Run gcloud info to view the account value, and then run gcloud services list --account <Account>. is not right.

We aren't passing any project id to the command so it would fail with the error shown below. (n.b. it is possible this command succeeds if you have an active gcloud configuration that has set the project so rather than accepting value from --project parameter, the command would obtain the project info from the gcloud configuration. The command shown below is run when no configuration is active).

gcloud services list --account <account\_id>

Errors with the following error.

ERROR: (gcloud.services.list) The project property is set to the empty string, which is invalid.

To set your project, run:

$ gcloud config set project PROJECT\_ID

or to unset it, run:

$ gcloud config unset project

Run gcloud projects describe <project ID> to verify the project value, and then run gcloud services list --available. is not right.

--available return the services available to the project to enable and not the services that are enabled. This list will include any services that the project has already enabled plus the services that the project can enable.

Ref: https://cloud.google.com/sdk/gcloud/reference/services/list

Run gcloud projects list to get the project ID, and then run gcloud services list --project <project ID>. is the right answer.

For the gcloud services list command, --enabled is the default.

So running

gcloud services list --project <project ID>

is the same as running

gcloud services list --project <project ID> --enabled

which would get all the enabled services for the project.

Bottom of Form

Top of Form

Question 19: Correct

EU GDPR requires you to archive all customer PII data indefinitely. The compliance department needs access to this data during the annual audit and is happy for the data to be archived after 30 days to save on storage costs. You want to design a cost-efficient solution for storing this data. What should you do?

​

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

​

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

​

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

​

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

(Correct)

Explanation

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

Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage. is not right.

When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region, moreover, this is expensive compared to standard Regional storage.

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

Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage. is not right.

When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region, moreover, this is expensive compared to standard Regional storage.

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

Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Nearline Storage. is not right.

While selecting Regional Storage is the right choice, archiving to Nearline is not the most optimal. We have a requirement to access data annually whereas Nearline Storage is ideal for data you plan to read or modify on average once per month or less. Nearline storage is more expensive than Coldline Storage which is more suitable for our requirements.

https://cloud.google.com/storage/docs/storage-classes#nearline

Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage. is the right answer.

Regional Storage is the right fit for our requirements (one geographic region) and archiving to Coldline storage is the most cost-efficient solution. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Since we have a requirement to access data once a quarter and want to go with the most cost-efficient option, we should select Coldline Storage.

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

Bottom of Form

Top of Form

Question 20: Incorrect

An image processing application running in your on-premises data centre requires 96 virtual CPUs to execute all processes. You colleague wants to migrate this application to Google Cloud Platform Compute Engine and has asked your suggestion for the instance size. What should you suggest?

​

Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs.

​

Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations.

(Incorrect)

​

When creating the VM, use Intel Skylake as the CPU platform.

​

When creating the VM, use machine type n1-standard-96.

(Correct)

Explanation

Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs. is not right.

You can't increase the vCPUs to 96 without changing the machine type. While it is possible to set machine type using gcloud, this would mean downtime for the mission-critical application while the upgrade happens which is undesirable.

Ref: https://cloud.google.com/compute/docs/instances/changing-machine-type-of-stopped-instance

Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations. is not right.

Since the application is mission-critical, we want to ensure that this application has all the required resources from the beginning. Starting with the default settings provisions a n1-standard-1 machine that has just 1 vCPU and our mission-critical application would be severely constrained for resources.

When creating the VM, use Intel Skylake as the CPU platform. is not right.

Intel Skylake is only offered in E2 machine types that are cost-optimized machine types and offer sizing between 2 to 16 vCPUs which is insufficient for our mission-critical application.

Ref: https://cloud.google.com/compute/docs/machine-types#e2\_machine\_types

When creating the VM, use machine type n1-standard-96. is the right answer.

n1-standard-96 offers 96 vCPUs and 624 GB of memory. This fits our requirements.

https://cloud.google.com/compute/docs/machine-types#n1\_machine\_type

Bottom of Form

Top of Form

Question 21: Correct

Your company has several business-critical applications running on its on-premises data centre, which is already at full capacity and wishes to expand to Google Cloud Platform to handle traffic bursts. You want to virtual machine instances in both on-premises data centre and Google Cloud Compute Engine to communicate securely via their internal IP addresses. What should you do?

​

In Google Cloud, configure the VPC for VPC Network Peering.

​

Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

(Correct)

​

Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses.

​

In Google Cloud, configure the VPC as a host for Shared VPC.

Explanation

In Google Cloud, configure the VPC as a host for Shared VPC. is not right.

Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. This in no way helps us connect to our on-premises network.

Ref: https://cloud.google.com/vpc/docs/shared-vpc

In Google Cloud, configure the VPC for VPC Network Peering. is not right.

Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization. VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally. Traffic stays within Google's network and doesn't traverse the public internet. This doesn't help us connect to our on-premises network.

Ref: https://cloud.google.com/vpc/docs/vpc-peering

Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses. is not right.

Bastion hosts provide an external facing point of entry into a network containing private network instances. Bastion hosts are primarily for end users so they can connect to an instance that does not have an external IP address through a bastion host.

Ref: https://cloud.google.com/compute/docs/instances/connecting-advanced

Set up Cloud VPN between the infrastructure on-premises and Google Cloud. is the right answer.

Cloud VPN securely connects your on-premises network to your Google Cloud (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection.

Ref: https://cloud.google.com/vpn/docs/concepts/overview

Bottom of Form

Top of Form

Question 22: Incorrect

You want to deploy an application to GKE cluster to enable the translation of mp3 files. The application uses an opensource translation library that is IOPS intensive. The organization backup strategy involves taking snapshots of all nodes at midnight. You want to estimate the cost of running this application in GKE cluster for the next month. In addition to the node pool size, instance type, location and usage duration, what else should you fill in the GCP pricing calculator when estimating the cost of running this application?

​

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

(Correct)

​

Select Add GPUs. Add estimated cost for cluster management.

​

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

(Incorrect)

​

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

Explanation

Fill in local SSD. Add estimated cost for cluster management. is not right.

You don't need to add an estimated cost for cluster management as the calculator automatically applies this. At the time of writing this, GKE clusters accrue a management fee of $0.10 per cluster per hour, irrespective of cluster size or topology. One zonal cluster per billing account is free. GKE cluster management fees do not apply to Anthos GKE clusters.

Ref: https://cloud.google.com/kubernetes-engine/pricing

Select Add GPUs. Add estimated cost for cluster management. is not right.

You don't need to add an estimated cost for cluster management as the calculator automatically applies this. At the time of writing this, GKE clusters accrue a management fee of $0.10 per cluster per hour, irrespective of cluster size or topology. One zonal cluster per billing account is free. GKE cluster management fees do not apply to Anthos GKE clusters.

Ref: https://cloud.google.com/kubernetes-engine/pricing

Select Add GPUs. Fill in persistent disk storage and snapshot storage. is not right.

GPUs don't help us with our requirement of high IOPS. Compute Engine provides graphics processing units (GPUs) that you can add to your virtual machine instances to accelerate specific workloads on your instances such as machine learning and data processing. But this doesn't help increase IOPS.

Ref: https://cloud.google.com/compute/docs/gpus

Fill in local SSD. Fill in persistent disk storage and snapshot storage. is the right answer.

The pricing calculator for Kubernetes Engine offers us the ability to add GPUs as well as specify Local SSD requirements for estimation. GPUs don't help us with our requirement of high IOPS but Local SSD does.

Ref: https://cloud.google.com/products/calculator

GKE offers always-encrypted local solid-state drive (SSD) block storage. Local SSDs are physically attached to the server that hosts the virtual machine instance for very high input/output operations per second (IOPS) and very low latency compared to persistent disks.

Ref: https://cloud.google.com/kubernetes-engine

Once you fill in the local SSD requirement, you can fill in persistent disk storage and snapshot storage.

Bottom of Form

Top of Form

Question 23: Correct

Your company stores terabytes of image thumbnails in Google Cloud Storage bucket with versioning enabled. You want to cut down the storage costs and you spoke to the image editing lab to understand their usage requirements. They inform you that they access noncurrent versions of images at most once a month and are happy for you to archive these objects after 30 days from the date of creation, however, there may be a need to retrieve some of these archived objects at the end of each month. What should you do?

​

Add a bucket lifecycle rule that archives objects from regional storage after 30 days to Coldline Storage.

​

Add a bucket lifecycle rule that archives objects from regional storage after 30 days to Nearline Storage.

​

Add a bucket lifecycle rule that archives noncurrent versions after 30 days to Coldline Storage.

​

Add a bucket lifecycle rule that archives noncurrent versions after 30 days to Nearline Storage.

(Correct)

Explanation

We don't know what the current storage class is. In the absence of this information and considering the 4 options provided, it is safe to assume that objects are currently in Regional or Multi-Regional buckets. We want to archive noncurrent versions after 30 days and you need to read and modify on average once per month

Add a bucket lifecycle rule that archives noncurrent versions after 30 days to Coldline Storage. is not right.

Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Our requirement states we need to read or modify every month so Coldline Storage is not an ideal storage class for our requirement.

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

Add a bucket lifecycle rule that archives objects from regional storage after 30 days to Coldline Storage. is not right.

Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Our requirement states we need to read or modify every month so Coldline Storage is not an ideal storage class for our requirement. Moreover, we don't want to archive live versions, we want to archive just the noncurrent versions.

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

Add a bucket lifecycle rule that archives objects from regional storage after 30 days to Nearline Storage. is not right.

While Nearline Storage is ideal for data you plan to read or modify on average once per month or less, we don't want to archive live versions, we want to archive just the noncurrent versions.

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

Add a bucket lifecycle rule that archives noncurrent versions after 30 days to Nearline Storage. is the right answer.

Nearline Storage is ideal for data you plan to read or modify on average once per month or less. And this option archives just the noncurrent versions which is what we want to do.

https://cloud.google.com/storage/docs/storage-classes#nearline

Bottom of Form

Top of Form

Question 24: Incorrect

Your company processes gigabytes of image thumbnails every day and stores them in your on-premises data centre. The development team at your company has developed an application that uses these image thumbnails with GCP services such as AutoML vision and pre-trained Vision API models to detect emotion, understand text and much more. The Cloud Security team has created a service account with the appropriate level of access, but the development team is unaware of how to authenticate to the GCP Services and APIs using the service account. What should they do?

​

Use service account credentials in your on-premises application.

​

Use gcloud to create a key file for the service account that has appropriate permissions.

(Correct)

​

Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.

​

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

(Incorrect)

Explanation

Use service account credentials in your on-premises application. is not right.

Service accounts do not have passwords

Ref: https://cloud.google.com/iam/docs/service-accounts

Go to the IAM & admin console, grant a user account permissions similar to the service account permissions, and use this user account for authentication from your data center. is not right.

While granting Users a similar set of permissions lets them impersonate service accounts and access all resources the service account has access to, you should use a service account to represent a non-human user that needs to authenticate and be authorized to access data in Google APIs. Typically, service accounts are used in scenarios such as:

Running workloads on virtual machines (VMs).

Running workloads on on-premises workstations or data centers that call Google APIs.

Running workloads that are not tied to the lifecycle of a human user.

Your application assumes the identity of the service account to call Google APIs so that the users aren't directly involved.

Ref: https://cloud.google.com/iam/docs/understanding-service-accounts

Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications. is not right.

While setting up interconnect provides a direct physical connection between your on-premises network and Google’s network, it doesn't directly help us authenticate our application running in the data center. You can configure Private Google Access for on-premises hosts by sending requests to restricted.googleapis.com and advertise a custom route on cloud router but this only lets you reach Google API and doesn't help with authentication.

Ref: https://cloud.google.com/interconnect/docs/support/faq

Use gcloud to create a key file for the service account that has appropriate permissions. is the right answer.

To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. You can create a service account key using the Cloud Console, the gcloud tool, the serviceAccounts.keys.create() method, or one of the client libraries.

Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys

Bottom of Form

Top of Form

Question 25: Incorrect

Your company has a requirement to persist logs from all compute engine instances in a single BigQuery dataset called pt-logs. Your colleague ran a script to install Cloud logging agent on all the virtual machines, but the logs from the VMs haven’t made their way to the BigQuery dataset. What should you do to fix this issue?

​

1. In Stackdriver Logging, create a logs export with a Cloud Pub/Sub topic called logs as a sink.

2. Create a Cloud Function that is triggered by messages in the logs topic.

3. Configure that Cloud Function to drop logs that are not from Compute Engine and to insert Compute Engine logs in the pt-logs dataset.

​

1. Create a Cloud Function that has the BigQuery User role on the pt-logs dataset.

2. Configure this Cloud Function to create a BigQuery Job that executes this query:

INSERT INTO dataset.pt-logs (timestamp, log)

SELECT timestamp, log FROM compute.logs

WHERE timestamp > DATE\_SUB(CURRENT\_DATE(), INTERVAL 1 DAY)

3. Use Cloud Scheduler to trigger this Cloud Function once a day.

​

1. Give the BigQuery Data Editor role on the pt-logs dataset to the service accounts used by your instances.

2. Update your instances' metadata to add the following value: logs-destination: bq://pt-logs.

(Incorrect)

​

1. In Stackdriver Logging, create a filter to view only Compute Engine logs.

2. Click Create Export.

3. Choose BigQuery as Sink Service, and the pt-logs dataset as Sink Destination.

(Correct)

Explanation

1. Give the BigQuery Data Editor role on the pt-logs dataset to the service accounts used by your instances.

2. Update your instances' metadata to add the following value: logs-destination: bq://pt-logs. is not right.

Among other things, roles/bigquery.dataEditor lets you Create, update, get, and delete the dataset's tables. However, setting a metadata tag logs-destination to bq://pt-logs has no effect on how the logs are generated or forwarded. The stack driver agent is already installed so the logs are forwarded to stack driver logging and not to the BigQuery dataset. Metadata entries are key-value pairs and do not influence this behavior.

Ref: https://cloud.google.com/compute/docs/storing-retrieving-metadata

1. In Stackdriver Logging, create a logs export with a Cloud Pub/Sub topic called logs as a sink.

2. Create a Cloud Function that is triggered by messages in the logs topic.

3. Configure that Cloud Function to drop logs that are not from Compute Engine and to insert Compute Engine logs in the pt-logs dataset. is not right.

While the end result meets our requirement, this option involves more steps, it is inefficient and expensive. Triggering a cloud function for each log message and then dropping messages that are not relevant (i.e. not compute engine logs) is inefficient. We are paying for cloud function execution for all log entries when we are only interested in compute engine logs. Secondly, triggering a cloud function and then have that insert into the BigQuery dataset is also inefficient and expensive when the same can be achieved directly by configuring BigQuery as the sink destination - we don't pay for cloud function executions. Using this option, we are unnecessarily paying for Cloud Pub/Sub and Cloud Functions.

Ref: https://cloud.google.com/logging/docs/export/configure\_export\_v2

Ref: https://cloud.google.com/logging/docs/view/advanced-queries

1. Create a Cloud Function that has the BigQuery User role on the pt-logs dataset.

2. Configure this Cloud Function to create a BigQuery Job that executes this query:

INSERT INTO dataset.pt-logs (timestamp, log)

SELECT timestamp, log FROM compute.logs

WHERE timestamp > DATE\_SUB(CURRENT\_DATE(), INTERVAL 1 DAY)

3. Use Cloud Scheduler to trigger this Cloud Function once a day. is not right.

The role roles/bigquery.user provides permissions to run jobs, including queries, within the project. A cloud function with this role can execute queries in BigQuery, however, the logs are not available in BigQuery in compute.logs so you can not query compute engine logs by running SELECT timestamp, log FROM compute.logs.

Ref: https://cloud.google.com/bigquery/docs/access-control

1. In Stack driver Logging, create a filter to view only Compute Engine logs.

2. Click Create Export.

3. Choose BigQuery as Sink Service, and the pt-logs dataset as Sink Destination. is the right answer.

In stack driver logging, it is possible to create a filter to just query the compute engine logs which is what we are interested in.

Ref: https://cloud.google.com/logging/docs/view/advanced-queries

You can then export these logs into a sink that has the BigQuery dataset configured as the destination.

https://cloud.google.com/logging/docs/export/configure\_export\_v2

This way, just the logs that we need are exported to BigQuery. This option is the most efficient of all options and uses features provided by GCP out of the box.

Bottom of Form

Top of Form

Question 26: Correct

To prevent accidental security breaches, the security team at your company has enabled Domain Restricted Sharing in the organization policies page in the Cloud Console to limit resource sharing in your GCP organization to just your cloud identity domain. The compliance department has engaged an external auditor to carry out the annual audit, and the auditor requires read access to all resources in the project to fill out specific sections in the audit report. How can you enable this access?

​

Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project.

​

Ask the auditor for their Google account, and give them the Viewer role on the project.

​

Ask the auditor for their Google account, and give them the Security Reviewer role on the project.

​

Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

(Correct)

Explanation

Ask the auditor for their Google account, and give them the Viewer role on the project. is not right.

Since the auditor's account is not part of your company's Cloud Identity domain, the auditor can not access resources from your GCP projects. Domain restriction constraint can be used in organization policies to limit resource sharing based on domain. This constraint allows you to restrict the set of identities that are allowed to be used in Cloud Identity and Access Management policies. In this scenario, since we are restricting based on the Cloud Identity domain, only the users in the Cloud Identity domain can access GCP services.

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

Ask the auditor for their Google account, and give them the Security Reviewer role on the project. is not right.

Since the auditor's account is not part of your company's Cloud Identity domain, the auditor can not access resources from your GCP projects. Domain restriction constraint can be used in organization policies to limit resource sharing based on domain. This constraint allows you to restrict the set of identities that are allowed to be used in Cloud Identity and Access Management policies. In this scenario, since we are restricting based on the Cloud Identity domain, only the users in the Cloud Identity domain can access GCP services.

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project. is not right.

Creating a temporary account for the auditor in your cloud identity is the right approach as this makes the auditor part of the Cloud identity domain and the organization policy in place lets the auditor access resources. However, the role granted here is not suitable, it provides permissions to list all resources and Cloud IAM policies. Note that list permissions only allow you to list but not view resources. You need to get permission to view the resources.

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

Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project. is the right answer.

The primitive viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data. This fits our requirements.

In addition, adding the auditor to Cloud Identity ensures that Organization Policy for Domain Restricted Sharing doesn't block them from accessing resources.

Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive\_role\_definitions

Bottom of Form

Top of Form

Question 27: Incorrect

You have developed a containerized application that performs video classification and recognition using Video AI, and you plan to deploy this application to the production GKE cluster. You want your customers to access this application on a public IP address on HTTPS protocol. What should you do?

​

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

(Correct)

​

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

​

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

​

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

(Incorrect)

Explanation

Create a Kubernetes Service of type ClusterIP for your application. Configure the public DNS name of your application using the IP of this Service. is not right.

Kubernetes Service of type ClusterIP exposes the Service on a cluster-internal IP. Choosing this value makes the Service only reachable from within the cluster so you can not route external traffic to this IP.

Ref: https://kubernetes.io/docs/concepts/services-networking/service/

Create a HAProxy pod in the cluster to load-balance the traffic to all the pods of the application. Forward the public traffic to HAProxy with an iptable rule. Configure the DNS name of your application using the public IP of the nodeHAProxy is running on. is not right.

HAProxy is a popular Kubernetes ingress controller. An Ingress object is an independent resource, apart from Service objects, that configures external access to a service’s pods. Ingress Controllers still need a way to receive external traffic. This can be done by exposing the Ingress Controller as a Kubernetes service with either NodePort or LoadBalancer type. You can't use public IP of the node the HAProxy is running on as this may be running in any node in the Kubernetes Cluster and in most cases, these nodes do not have public IPs. They are meant to be private and the pods/deployments are accessed through Service objects.

Ref: https://www.haproxy.com/blog/dissecting-the-haproxy-kubernetes-ingress-controller/

Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluster. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing. is not right.

Kubernetes Service of type NodePort uses a port in the range 30000-32767. Assuming that all the nodes have public IP addresses, enabling NodePort would expose a port such as 32000 so the application is accessible on https://IP:32000 which is not ideal. You want your application/website to be reachable directly on port 443. This also requires downstream clients to have awareness of all of your nodes’ IP addresses, since they will need to connect to those addresses directly. In other words, they won’t be able to connect to a single, proxied IP address. And this is against our requirement of "a public IP address".

Ref: https://kubernetes.io/docs/concepts/services-networking/service/

Ref: https://www.haproxy.com/blog/dissecting-the-haproxy-kubernetes-ingress-controller/

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

This meets all our requirements. With (Global) Cloud Load Balancing, a single anycast IP front-ends all your backend instances in regions around the world. It provides cross-region load balancing, including automatic multi-region failover, which gently moves traffic in fractions if backends become unhealthy.

Ref: https://cloud.google.com/load-balancing/

The ingress accepts traffic from the cloud load balancer and can distribute the traffic across the pods in the cluster.

Ref: https://kubernetes.io/docs/concepts/services-networking/ingress/

Bottom of Form

Top of Form

Question 28: Correct

Your data warehousing team executed an Apache Sqoop job to export data from Hive/Hbase and uploaded this data in AVRO file format to Cloud Storage. The business analysts at your company have years of experience using SQL and have asked you to identify if there is an easy way to query the information in AVRO files through SQL. What should you do?

​

Load data in Cloud Datastore and run a SQL query against it.

​

Create a BigQuery table and load data in BigQuery. Run a SQL query on this table and drop this table after you complete your request.

​

Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

(Correct)

​

Create a Hadoop cluster and copy the AVRO file to NDFS by compressing it. Load the file in a hive table and provide access to your analysts so that they can run SQL queries.

Explanation

Load data in Cloud Datastore and run a SQL query against it. is not right.

Datastore is a highly scalable NoSQL database and although it supports SQL like queries, it doesn't support SQL. Moreover, there is no out of the box way for transforming AVRO file from cloud storage into the Cloud Datastore entity. So we have to do in a bespoke way which adds to our cost and time.

Ref: https://cloud.google.com/datastore

Create a Hadoop cluster and copy the AVRO file to NDFS by compressing it. Load the file in a hive table and provide access to your analysts so that they can run SQL queries. is not right.

Like Cloud Datastore, Hive doesn't directly support SQL, it provides HiveQL (HQL) which is SQL like. In addition, the process of creating a Hadoop cluster and getting the data eventually into a hive table is time-consuming and adds to our cost and time.

Create a BigQuery table and load data in BigQuery. Run a SQL query on this table and drop this table after you complete your request. is not right.

Like the above two, while it is possible to build a solution that transforms and loads data into the target, BigQuery in this case, is not a trivial process and involves cost and time. GCP provides an out of the box way to query AVRO files from Cloud Storage and this should be preferred.

Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request. is the right answer.

BigQuery supports querying Cloud Storage data in a number of formats such as CSV, JSON, AVRO, etc. You do this by creating a Big Query external table that points to a Cloud Storage data source (bucket). This solution works out of the box, involves minimal effort, minimal cost, and is quick.

https://cloud.google.com/bigquery/external-data-cloud-storage

Bottom of Form

Top of Form

Question 29: Incorrect

Your company has a Citrix Licensing Server in a Windows VM in your on-premises data centre and needs to migrate this to Google Cloud Platform. You have provisioned a new Windows VM in a brand new Google project, and you want to RDP to the instance to install and register the licensing server. What should you do?

​

When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value.

(Incorrect)

​

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

​

After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM.

​

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

(Correct)

Explanation

When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value. is not right.

It is not possible to specify a windows password at the time of creating windows VM instance. You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. Alternatively, you can generate passwords programmatically with API commands but all these methods assume that you have an existing windows instance.

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

After the VM has been created, use your Google Account credentials to log in into the VM. is not right.

You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. Alternatively, you can generate passwords programmatically with API commands but you can't use your gcloud account credentials to log into the VM.

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

After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM. is not right.

This is not a supported method of authentication for logging into the VM. You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. Alternatively, you can generate passwords programmatically with API commands.

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

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

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

gcloud compute reset-windows-password windows-instance

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

Bottom of Form

Top of Form

Question 30: Incorrect

Your compliance officer has requested you to provide an external auditor view access to all project resources. What should you do?

​

Create a custom role with view-only service permissions. Add the user's account to the custom role.

​

Select the built-in IAM project Viewer role. Add the user's account to this role.

(Correct)

​

Select the built-in IAM service Viewer role. Add the user's account to this role.

​

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

(Incorrect)

Explanation

Select the built-in IAM project Viewer role. Add the user's account to this role. Is the right answer

The primitive role roles/viewer provides read access to all resources in the project. The permissions in this role are limited to Get and list access for all resources. As we have an out of the box role that exactly fits our requirement, we should use this.

Ref: https://cloud.google.com/resource-manager/docs/access-control-proj

It is advisable to use the existing GCP provided roles over creating custom roles with similar permissions as this becomes a maintenance overhead. If GCP modifies how permissions are handled or adds/removes permissions, the default GCP provided roles are automatically updated by Google whereas if they were custom roles, the responsibility is with us and this adds to the operational overhead and needs to be avoided.

Bottom of Form

Top of Form

Question 31: Incorrect

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

​

Modify the legacy application to use OAuth 2.0 and ask users to sign in through Gmail.

​

Modify the legacy application to use SAML and ask users to sign in through Gmail.

​

Use secure LDAP to authenticate the legacy application and ask users to sign in through Gmail.

(Correct)

​

Synchronize data within your LDAP server with Google Cloud Directory Sync.

(Incorrect)

Explanation

Modify the legacy application to use SAML and ask users to sign in through Gmail. is not right.

Modifying a legacy application to use SAML can be quite challenging. In any case, this is a time consuming and error-prone task and is very expensive.

Modify the legacy application to use OAuth 2.0 and ask users to sign in through Gmail. is not right.

Modifying a legacy application to use OAuth 2.0 can be quite challenging. In any case, this is a time consuming and error-prone task and is very expensive.

Synchronize data within your LDAP server with Google Cloud Directory Sync. is not right.

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

Use secure LDAP to authenticate the legacy application and ask users to sign in through Gmail. is the right answer.

Secure LDAP enables authentication, authorization, and user/group lookups for LDAP-based apps and IT infrastructure. Secure LDAP uses the same user directory for both SaaS and LDAP-based applications, so people can use the same Cloud Identity credentials they use to log in to services like G Suite and other SaaS apps as they do to log into traditional applications. Applications and IT infrastructure that use LDAP can be simply configured to leverage Cloud Identity’s secure LDAP service instead of an existing legacy identity system—end-users don't have to change how they access their apps.

Ref: https://cloud.google.com/blog/products/identity-security/cloud-identity-now-provides-access-to-traditional-apps-with-secure-ldap

Bottom of Form

Top of Form

Question 32: Correct

You have developed a python application to publish and consume messages from Cloud Pub/Sub. Your manager is a big fan of both serverless and containers and has asked you to containerize the application and deploy on Google Cloud Run. How should you do it?

​

1. Create a Cloud Function that uses a Cloud Pub/Sub trigger on that topic.

2. Call your application on Cloud Run from the Cloud Function for every message.

​

1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run.

2. Create a Cloud Pub/Sub subscription for that topic.

3. Make your application pull messages from that subscription.

​

1. Create a service account.

2. Give the Cloud Run Invoker role to that service account for your Cloud Run application.

3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

(Correct)

​

1. Deploy your application on Cloud Run on GKE with the connectivity set to Internal.

2. Create a Cloud Pub/Sub subscription for that topic.

3. In the same Google Kubernetes Engine cluster as your application, deploy a container that takes the messages and sends them to your application.

Explanation

1. Create a Cloud Function that uses a Cloud Pub/Sub trigger on that topic.

2. Call your application on Cloud Run from the Cloud Function for every message. is not right.

Both Cloud functions and Cloud Run are serverless offerings from GCP and they are both capable of integrating with Cloud Pub/Sub. It is pointless to invoking Cloud Function from Cloud Run.

1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run.

2. Create a Cloud Pub/Sub subscription for that topic.

3. Make your application pull messages from that subscription. is not right.

You need to provide Cloud Run Invoker role to that service account for your Cloud Run application.

Ref: https://cloud.google.com/run/docs/tutorials/pubsub

1. Deploy your application on Cloud Run on GKE with the connectivity set to Internal.

2. Create a Cloud Pub/Sub subscription for that topic.

3. In the same Google Kubernetes Engine cluster as your application, deploy a container that takes the messages and sends them to your application. is not right.

Like above, you need cloud Run Invoker role on the service account.

Ref: https://cloud.google.com/run/docs/tutorials/pubsub

Also, our question states the application on Cloud Run processes messages from a Cloud Pub/Sub topic; whereas in this option, we are utilizing a separate container to process messages from the topic. So this doesn't satisfy our requirements.

1. Create a service account.

2. Give the Cloud Run Invoker role to that service account for your Cloud Run application.

3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint. is the right answer.

This exact process is described in

https://cloud.google.com/run/docs/tutorials/pubsub

You create a service account.

gcloud iam service-accounts create cloud-run-pubsub-invoker \

--display-name "Cloud Run Pub/Sub Invoker"

You then give the invoker service account permission to invoke your service:

gcloud run services add-iam-policy-binding pubsub-tutorial \

--member=serviceAccount:cloud-run-pubsub-invoker@PROJECT\_ID.iam.gserviceaccount.com \

--role=roles/run.invoker

And finally, you create a Pub/Sub subscription with the service account:

gcloud pubsub subscriptions create myRunSubscription --topic myRunTopic \

--push-endpoint=SERVICE-URL/ \

--push-auth-service-account=cloud-run-pubsub-invoker@PROJECT\_ID.iam.gserviceaccount

Bottom of Form

Top of Form

Question 33: Incorrect

You want to provide your operations team access to all GCP production projects. Everyone at your company has G Suite accounts. How should you grant access to the operations team?

​

In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group.

(Incorrect)

​

Enable Cloud Identity in the GCP Console for your domain.

​

Grant them the required IAM roles using their G Suite email address.

(Correct)

​

Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.

Explanation

Grant them the required IAM roles using their G Suite email address. is the right answer.

You can use Cloud Identity or G Suite to create and manage users in GCP

Ref: https://cloud.google.com/iam/docs/faq

Since all users in organization already have a G Suite account, we should grant the roles to their G Suite email addresses for users that need access to GCP services.

Bottom of Form

Top of Form

Question 34: Correct

Your organization has several applications in the on-premises data centre that depend on Active Directory for user identification and authorization. Your organization is planning a migration to Google Cloud Platform and requires complete control over the Cloud Identity accounts used by staff to access Google Services and APIs. Where possible, you want to re-use Active Directory as the source of truth for identification and authorization. What should you do?

​

Ask each employee to create a Google account using self signup. Require that each employee use their company email address and password.

​

Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console.

​

Use the cloud Identity APIs and write a script to synchronize users to Cloud Identity.

​

Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

(Correct)

Explanation

Use the cloud Identity APIs and write a script to synchronize users to Cloud Identity. is not right.

You could do this, but this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console. is not right.

You could do this, but like above this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

Ask each employee to create a Google account using self signup. Require that each employee use their company email address and password. is not right.

If you let employees create accounts, your organization no longer has full control over the Google accounts used. This approach has several other issues with respect to creating/managing user accounts and should be avoided.

Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity. is the right answer.

Since we already have user identities in Active Directory, it makes sense to reuse this directory as the source of truth for identities. But for GCP, you need identities either in G Suite or Google Cloud Identity. Cloud Directory Sync is a tool that enables you to synchronize users, groups, and other data from an Active Directory/LDAP service to their Google Cloud domain directory. This performs a one-way synchronization and ensures Cloud Identity users match that of your Active Directory. This also helps with our requirement of the organization having full control over the accounts used by employees.

Ref: https://tools.google.com/dlpage/dirsync/

Ref: https://support.google.com/a/answer/106368?hl=en#:~:text=With%20Google%20Cloud%20Directory%20Sync,files)%20to%20your%20Google%20Account.

Bottom of Form

Top of Form

Question 35: Correct

The procurement department at your company is migration all their applications to Google Cloud, and one of their engineers have asked you to provide them IAM access to create and manage service accounts in all Cloud Projects. What should you do?

​

Add the user to roles/iam.securityAdmin role.

​

Add the user to roles/iam.roleAdmin role.

​

Add the user to roles/iam.serviceAccountUser role.

​

Add the user to roles/iam.serviceAccountAdmin role.

(Correct)

Explanation

Add the user to roles/iam.roleAdmin role. is not right.

roles/iam.roleAdmin is an administrator role that provides access to all custom roles in the project. This doesn't include permissions needed to manage service accounts.

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

Add the user to roles/iam.securityAdmin role. is not right.

roles/iam.securityAdmin role is a Security admin role, with permissions to get and set any IAM policy. This role is too broad i.e. includes too many permissions and goes against the principle of least privilege. Moreover, although this role provides iam.serviceAccounts.get/list, it doesn't provide iam.serviceAccounts.create, iam.serviceAccounts.delete and iam.serviceAccounts.update permissions that are needed for managing service accounts.

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

Add the user to roles/iam.serviceAccountUser role. is not right.

roles/iam.serviceAccountUser is a service Account User role which is used for running operations as the service account. This role does not provide the permissions iam.serviceAccounts.create, iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list which are required for managing service accounts.

Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

Add the user to roles/iam.serviceAccountAdmin role. is the right answer.

roles/iam.serviceAccountAdmin is a Service Account Admin role that lets you Create and manage service accounts. This grants all the required permissions for managing service accounts (iam.serviceAccounts.create iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list etc) and therefore fits our requirements.

Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

Bottom of Form

Top of Form

Question 36: Incorrect

The machine learning team at your company infrequently needs to use a GKE cluster with specific GPUs for processing a non-restartable job. You want to enable this while minimizing cost, what should you do?

​

Enable node auto-provisioning on the GKE cluster.

​

Create a node pool of instances with GPUs, and enable autoscaling on this node pool with a minimum size of 1.

(Correct)

​

Create a VerticalPodAutscaler for those workloads.

​

Create a node pool with preemptible VMs and GPUs attached to those VMs.

(Incorrect)

Explanation

Enable node auto-provisioning on the GKE cluster. is not right.

Node auto-provisioning automatically manages a set of node pools on the user's behalf. Without Node auto-provisioning, GKE considers starting new nodes only from the set of user-created node pools. With node auto-provisioning, new node pools can be created and deleted automatically. This in no way helps us with our requirements.

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

Create a VerticalPodAutscaler for those workloads. is not right.

Vertical pod autoscaling (VPA) frees you from having to think about what values to specify for a container's CPU and memory requests. The autoscaler can recommend values for CPU and memory requests and limits, or it can automatically update the values. This doesn't help us with the GPU requirement. Moreover, due to Kubernetes limitations, the only way to modify the resource requests of a running Pod is to recreate the Pod. This has the negative effect of killing the non-restartable jobs which is undesirable.

https://cloud.google.com/kubernetes-engine/docs/concepts/verticalpodautoscaler#overview

Create a node pool with preemptible VMs and GPUs attached to those VMs. is not right.

You can use preemptible VMs in your GKE clusters or node pools to run batch or fault-tolerant jobs that are less sensitive to the ephemeral, non-guaranteed nature of preemptible VMs. Whereas we have long-running and non-restartable jobs so preemptible VMs aren't suitable for our requirement.

Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/preemptible-vms

Create a node pool of instances with GPUs, and enable autoscaling on this node pool with a minimum size of 1. is the right answer.

A node pool is a group of nodes within a cluster that all have the same configuration. Our requirement is GPUs, so we create a node pool with GPU enabled and have the scientist's applications deployed to the cluster and use this node pool. At the same time, you want to minimize cost so you start with 1 instance and scale up as needed. It is important to note that the scale down needs to take into consideration if there are any running jobs otherwise the scale down may terminate the nonrestartable job.

Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools

Bottom of Form

Top of Form

Question 37: Correct

Your finance department has asked you to provide their team access to view billing reports for all projects. What should you do?

​

Add the group for the finance team to roles/billing.projectManager role.

​

Add the group for the finance team to roles/billing.user role.

​

Add the group for the finance team to roles/billing.viewer role.

(Correct)

​

Add the group for the finance team to roles/billing.admin role.

Explanation

Add the group for the finance team to roles/billing.user role. is not right.

This role has very restricted permissions, so you can grant it broadly, typically in combination with Project Creator. These two roles allow a user to create new projects linked to the billing account on which the role is granted.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.admin role. is not right.

This role is an owner role for a billing account. Use it to manage payment instruments, configure billing exports, view cost information, link and unlink projects, and manage other user roles on the billing account.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.projectManager role. is not right.

This role allows a user to attach the project to the billing account, but does not grant any rights over resources. Project Owners can use this role to allow someone else to manage the billing for the project without granting them resource access.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Add the group for the finance team to roles/billing.viewer role. is the right answer.

Billing Account Viewer access would usually be granted to finance teams, it provides access to spending information but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account.

Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Bottom of Form

Top of Form

Question 38: Incorrect

Your colleague is learning about docker images, containers and Kubernetes, and has recently deployed a sample application to a GKE cluster. Although the sample application is responding to requests, one of the pods is pending, and they are not sure why. They shared with you the following configuration files used for deploying the application and the output from their Cloud Shell instance.

apiVersion: apps/v1

kind: Deployment

metadata:

name: demo-deployment

spec:

selector:

matchLabels:

app: demo

replicas: 2

template:

metadata:

labels:

app: demo

spec:

containers:

- name: demo

image: demo:2.7

ports:

- containerPort: 8080

---

apiVersion: v1

kind: Service

metadata:

name: demo-service

spec:

ports:

- port: 80

targetPort: 8080

protocol: TCP

selector:

app: demo

kubectl get pods -l app=demo

NAME READY STATUS RESTART AGE

demo-deployment-8998dab376-brm68 0/1 Pending 0 29m

demo-deployment-8998dab376-kpg18 1/1 Running 0 29m

Your colleague has asked you to help them identify why the pod is in a pending state. How should you proceed with the investigation?

​

Review details of the demo-service Service object and check for error messages.

​

Review details of demo-deployment-8998dab376-brm68 Pod and check for warning messages.

(Correct)

​

Review details of the demo-deployment Deployment object and check for error messages.

​

View logs of the container in demo-deployment-8998dab376-brm68 pod and check for warning messages.

(Incorrect)

Explanation

Review details of the demo-service Service object and check for error messages. is not right.

The question states we have a problem with the deployment. Checking/Reviewing the status of the service object isn't of much use here.

View logs of the container in demo-deployment-8998dab376-brm68 pod and check for warning messages. is not right.

Since the pod hasn't moved to Running state, the logs of the container would be empty. So running

kubectl logs pod/demo-deployment-8998dab376-brm68

to check the logs of the pod isn't of much use.

Review details of the demo-deployment Deployment object and check for error messages. is not right.

Describing the details of the deployment shows us how many of the pods are available and unavailable but does not show errors/warnings related to a specific pod.

Here's a sample output of this use case.

kubectl describe deployment demo-deployment

Replicas: 3 desired | 3 updated | 3 total | 2 available | 1 unavailable

Events:

Type Reason Age From Message

---- ------ ---- ---- -------

Normal ScalingReplicaSet 4m54s deployment-controller Scaled up replica set demo-deployment-869d88c75f to 3

Review details of demo-deployment-8998dab376-brm68 Pod and check for warning messages. is the right answer.

Since the problem is with a specific pod, looking at the details of the pod is the best solution. When you have a deployment with some pods in running and other pods in Pending state, more often than not it is a problem with resources on the nodes. Here's a sample output of this use case. We see that the problem is with insufficient CPU on the Kubernetes nodes so we have to either enable auto-scaling or manually scale up the nodes.

kubectl describe pod demo-deployment-8998dab376-brm68

Events:

Type Reason Age From Message

---- ------ ---- ---- -------

Warning FailedScheduling 28s (x4 over 3m1s) default-scheduler 0/1 nodes are available: 1 Insufficient cpu.

Bottom of Form

Top of Form

Question 39: Correct

Your company has accumulated terabytes of analytics data from clickstream logs and stores this in BigQuery datasets. Several analytics teams at your company depend on querying this data to carry out their work. The costs for BigQuery job executions have recently shot up exponentially, and your finance team has asked your suggestions for controlling these spiralling costs. What should you do? (Select two)

​

Apply a user- or project-level custom query quota for BigQuery data warehouse.

(Correct)

​

Change your BigQuery query model from on-demand to flat rate. Apply the appropriate number of slots to each Project.

(Correct)

​

Split your BigQuery data warehouse into multiple data warehouses for each business unit.

​

Split the users from business units to multiple projects.

​

Create separate copies of your BigQuery data warehouse for each business unit.

Explanation

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

Ref: https://cloud.google.com/bigquery/pricing

Split the users from business units to multiple projects. is not right.

The bytes scanned is not expected to go down by splitting the users into multiple projects so this wouldn't reduce/control the costs.

Ref: https://cloud.google.com/bigquery/pricing

Split your BigQuery data warehouse into multiple data warehouses for each business unit. is not right.

The bytes scanned is not expected to go down by splitting the BigQuery warehouse into two so this wouldn't reduce/control the costs either.

Ref: https://cloud.google.com/bigquery/pricing

Create separate copies of your BigQuery data warehouse for each business unit. is not right.

Creating separate copies of the BigQuery data warehouse for each business unit is going to increase your costs. Not only is this expected to reduce the bytes scanned, but this is also going to increase the storage costs as we are now storing double the amount of data.

Ref: https://cloud.google.com/bigquery/pricing

Apply a user- or project-level custom query quota for BigQuery data warehouse. is the right answer.

BigQuery limits the maximum rate of incoming requests and enforces appropriate quotas on a per-project basis. You can set various limits to control costs such as Concurrent rate limit for interactive queries, Concurrent rate limit for interactive queries against Bigtable external data sources, Concurrent rate limit for legacy SQL queries that contain UDFs, Cross-region federated querying, Daily query size limit, etc.

https://cloud.google.com/bigquery/quotas

Change your BigQuery query model from on-demand to flat rate. Apply the appropriate number of slots to each Project. is the right answer.

This pricing option is best for customers who desire cost predictability. Flat-rate customers purchase dedicated resources for query processing and are not charged for individual queries. BigQuery offers flat-rate pricing for customers who prefer a stable cost for queries rather than paying the on-demand price per TB of data processed. You can choose to use flat-rate pricing using BigQuery Reservations. When you enroll in flat-rate pricing, you purchase slot commitments - dedicated query processing capacity, measured in BigQuery slots. Your queries consume this capacity, and you are not billed for bytes processed. If your capacity demands exceed your committed capacity, BigQuery will queue up slots, and you will not be charged additional fees.

Ref: https://cloud.google.com/bigquery/pricing#flat\_rate\_pricing

Bottom of Form

Top of Form

Question 40: Correct

Your production Compute workloads are running in a small subnet with a netmask 225.225.225.224. A recent surge in traffic has seen the production VMs struggle, but there are no free IP addresses for the Managed Instances Group (MIG) to autoscale. You anticipate requiring 30 IP addresses for new VMs. All VMs within the subnet need to communicate with each other. What should you do?

​

Delete the subnet, and recreate it using a wider range of IP addresses.

​

Create a new subnet with the same starting IP but a wider range to overwrite the current subnet.

​

Create a new project. Use Shared VPC to share the current network with the new project.

​

Use gcloud to expand the IP range of the current subnet.

(Correct)

Explanation

Use gcloud to expand the IP range of the current subnet. is the right answer.

Subnet mask of the existing subnet is 255.255.255.224 which means the max possible address in are 32. So the net prefix is /27 i.e. 5 bits free so 2 to the power of 5 is 32 IP Addresses.

As per IETF (Ref: https://tools.ietf.org/html/rfc1918), the supported internal IP Address ranges are

1. 24-bit block 10.0.0.0/8 (16777216 IP Addresses)

2. 20-bit block 172.16.0.0/12 (1048576 IP Addresses)

3. 16-bit block 192.168.0.0/16 (65536 IP Addresses)

A prefix of 27 is a very small subnet and could be in any of the ranges above; and all ranges have scope to accommodate a higher prefix.

A prefix of 26 gives you 64 IP Addresses i.e. 32 IP address more and we just need 30 more. So expanding the subnet to a prefix of 26 should give us the required capacity. And GCP lets you do exactly that running a gcloud command

https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range

gcloud compute networks subnets expand-ip-range <SUBNET NAME> --region=<REGION> --prefix-length=26

Bottom of Form

Top of Form

Question 41: Incorrect

You developed a python application that exposes an HTTP(s) endpoint and lets users retrieve 2-week weather forecast for a given location. You deployed the application in a single Google Cloud Compute Engine Virtual Machine, but the application is not as popular as you anticipated and has been receiving very few requests. To minimize costs, your colleague suggested containerizing the application and deploying on a suitable GCP compute service. Which GCP Compute service should you use?

​

Deploy the container on App Engine Flexible.

​

Deploy the container on Cloud Run on GKE.

(Incorrect)

​

Deploy the container on Cloud Run.

(Correct)

​

Deploy the container on Google Kubernetes Engine, with cluster autoscaling and horizontal pod autoscaling enabled.

Explanation

Deploy the container on Cloud Run on GKE. is not right.

Cloud Run on GKE can scale the number of pods to zero. The number of nodes per cluster cannot scale to zero and these nodes are billed in the absence of requests.

Ref: https://cloud.google.com/serverless-options

Deploy the container on Google Kubernetes Engine, with cluster autoscaling and horizontal pod autoscaling enabled. is not right.

Like above, while you can set up the pod autoscaler to scale back the pods to zero, the number of nodes per cluster cannot scale to zero and these nodes are billed in the absence of requests. If you specify the minimum node pool size of zero nodes, an idle node pool can scale down completely. However, at least one node must always be available in the cluster to run system Pods.

Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler

Deploy the container on App Engine Flexible. is not right.

App Engine flexible environment instances are Compute Engine virtual machines. This means you can't truly scale down to zero and compute instances are billed in the absence of requests.

Ref: https://cloud.google.com/appengine/docs/flexible

Deploy the container on Cloud Run. is the right answer.

Cloud Run is a fully managed compute platform that automatically scales your stateless containers. Cloud Run is serverless. Cloud Run abstracts away all infrastructure management. It automatically scales up and down from zero depending on traffic almost instantaneously. Cloud Run only charges you for the exact resources you use.

Ref: https://cloud.google.com/run

Bottom of Form

Top of Form

Question 42: Incorrect

Your analysts' team needs to run a BigQuery job to retrieve customer PII data. Security policies prohibit using Cloud Shell for retrieving with PII data. The security team has advised you to set up a Shielded VM with just the required IAM access permissions to run BigQuery jobs on the specific dataset. What is the most efficient way to let the analysts' team SSH to the VM?

​

Enable block project wide keys for the instance. Generate an SSH key and associate the key with that instance. Distribute the key to analyst users and direct them to use their third-party tools to connect.

​

Enable block project wide keys for the instance. Generate an SSH key for each user in the analyst group. Distribute the keys to analyst users and direct them to use their third-party tools to connect.

​

Set metadata to enable-oslogin=true for the instance. Grant the analyst group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

(Correct)

​

Set metadata to enable-oslogin=true for the instance. Set the service account to no service account for that instance. Direct them to use the Cloud Shell to ssh to that instance.

(Incorrect)

Explanation

You have multiple ways to connect to instances. More information can be found here: https://cloud.google.com/compute/docs/instances/access-overview

Enable block project wide keys for the instance. Generate an SSH key for each user in the analyst group. Distribute the keys to analyst users and direct them to use their third-party tools to connect. is not right.

Generating SSH keys for users is fine but unless the SSH keys are added to the instance, users would not be able to SSH to the server. If you need your instance to ignore project-wide public SSH keys and use only the instance-level keys, you can block project-wide public SSH keys from the instance. This allows only users whose public SSH key is stored in instance-level metadata to access the instance.

Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#edit-ssh-metadata

Enable block project wide keys for the instance. Generate an SSH key and associate the key with that instance. Distribute the key to analyst users and direct them to use their third-party tools to connect. is not right.

While this is possible, sharing SSH keys is a strict NO from a security point of view as this breaks auditing. Should one of the developers create a disaster (either accidental or malicious), your security admin would be unable to identify which of the users in analyst group caused the issue.

Set metadata to enable-oslogin=true for the instance. Set the service account to no service account for that instance. Direct them to use the Cloud Shell to ssh to that instance. is not right.

After you enable OS Login on one or more instances in your project, those VMs accept connections only from user accounts that have the necessary IAM roles in your project or organization. In this case, since we have not granted either of these roles - roles/compute.osLogin or roles/compute.osAdminLogin role, users of analyst group can't SSH to the server.

Ref: https://cloud.google.com/compute/docs/instances/managing-instance-access#configure\_users

Set metadata to enable-oslogin=true for the instance. Grant the analyst group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance. is the right answer.

After you enable OS Login on one or more instances in your project, those VMs accept connections only from user accounts that have the necessary IAM roles in your project or organization. In this case, we are granting the group compute.osLogin which lets them log in as non-administrator account. And since we are directing them to use Cloud Shell to ssh, we don't need to add their SSH keys to the instance metadata.

Ref: https://cloud.google.com/compute/docs/instances/managing-instance-access#configure\_users

Ref: https://cloud.google.com/compute/docs/instances/managing-instance-access#add\_oslogin\_keys

Bottom of Form

Top of Form

Question 43: Incorrect

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

​

Have a single person from the procurement team access document signing system with the service account credentials.

​

Ask the third-party provider to enable SAML for the application and set the credentials to the service account credentials.

(Incorrect)

​

Ask the third-party provider to enable OAuth 2.0 for the application and set the credentials to the service account credentials.

​

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

(Correct)

Explanation

Ask the third-party provider to enable SAML for the application and set the credentials to always use service account credentials. is not right.

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

Ask the third-party provider to enable OAuth 2.0 for the application and set the credentials to always use service account credentials. is not right.

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

Have a single person from the procurement team access document signing system with the service account credentials. is not right.

While this would prevent password reuse, it goes against our requirements and results in a single person dependency.

Register the application as a password vaulted app and set the credentials to the service account credentials. is the right answer.

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

Ref: https://support.google.com/cloudidentity/answer/9178974?hl=en

Bottom of Form

Top of Form

Question 44: Correct

Your company wants to move all its on-premises applications to Google Cloud. Most applications depend on Kubernetes orchestration, and you have chosen to deploy these applications in Google Kubernetes Engine (GKE) in your GCP project – app\_prod. The security team have requested you to store all container images in Google Container Registry (GCR) in a separate project – gcr\_proj - which has an automated vulnerability management scanning set up by a security partner. You are ready to push an image to GCR repo and want to tag it as tranquillity:v1. How should you do it?

​

Run gcloud builds submit --tag gcr.io/gcr\_proj/tranquillity

​

Run gcloud builds submit --tag gcr.io/app\_prod/tranquillity:v1

​

Run gcloud builds submit --tag gcr.io/gcr\_proj/tranquillity:v1

(Correct)

​

Run gcloud builds submit --tag gcr.io/app\_prod/tranquillity

Explanation

Run gcloud builds submit --tag gcr.io/gcr\_proj/tranquillity. is not right.

This command tags the image as tranquillity:latest but we want to tag the image as tranquillity:v1.

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Run gcloud builds submit --tag gcr.io/app\_prod/tranquillity. is not right.

This command tags the image as tranquillity:latest but we want to tag the image as tranquillity:v1. This command also upload the image to the wrong project.

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Run gcloud builds submit --tag gcr.io/app\_prod/tranquillity:v1. is not right.

This command also upload the image to the wrong project.

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Run gcloud builds submit --tag gcr.io/gcr\_proj/tranquillity:v1. is the right answer.

This command correctly tags the image as tranquillity:v1 and uploads the image to the gcr\_proj project.

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Bottom of Form

Top of Form

Question 45: Correct

Your company has chosen Okta, a third-party SSO identity provider, for all its IAM requirements because of the rich feature set it offers – support for over 6,500 pre-integrated apps for SSO and over 1,000 SAML integrations. How can your company users in Cloud Identity authenticate using Okta before accessing resources in your GCP project?

​

Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps.

​

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

​

In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

(Correct)

​

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

Explanation

In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps. is not right.

The question states that you want to use the company's existing Identity provider for SSO, not Google. Moreover, your users are in Cloud Identity and not in a GSuite domain so they don't have GSuite Gmail accounts and therefore can not sign in through Google.

Ref: https://cloud.google.com/identity/solutions/enable-sso

Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps. is not right.

OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow. See https://oauth.net/2/ for more information about OAuth 2.0 which is quite a popular protocol for SSO. When you sign in to a 3rd party website using Facebook/Twitter/Google, it uses OAuth 2.0 behind the scenes.

Ref: https://cloud.google.com/identity/solutions/enable-sso

Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications. is not right.

OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow. See https://oauth.net/2/ for more information about OAuth 2.0 which is quite a popular protocol for SSO. When you sign in to a 3rd party website using Facebook/Twitter/Google, it uses OAuth 2.0 behind the scenes.

Ref: https://cloud.google.com/identity/solutions/enable-sso

In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider. is the right answer.

This is the only possible option. You configure applications (service providers) to accept SAML assertions from the company's existing identity provider and users in Cloud Identity can sign in to various applications through the third-party single sign-on (SSO) identity provider. It is important to note that user authentication occurs in the third-party IdP so the absence of a Gmail login is not an issue for signing in.

Ref: https://cloud.google.com/identity/solutions/enable-sso

If you have a third-party IdP, you can still configure SSO for third-party apps in the Cloud Identity catalog. User authentication occurs in the third-party IdP, and Cloud Identity manages the cloud apps.

To use Cloud Identity for SSO, your users need Cloud Identity accounts. They sign in through your third-party IdP or using a password on their Cloud Identity accounts.

Bottom of Form

Top of Form

Question 46: Incorrect

You work for a multinational conglomerate that has thousands of GCP projects and a very complex resource hierarchy that includes over 100 folders. An external audit team has requested to view this hierarchy to fill out sections of a report. You want to enable them to view the hierarchy while ensuring they can’t do anything else. What should you do?

​

Add the users to roles/iam.roleViewer role.

​

Add the users to a group and add this group to roles/browser role.

(Correct)

​

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

(Incorrect)

​

Add the users to roles/browser role.

Explanation

Add the users to roles/iam.roleViewer role. is not right.

roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.

Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to a group and add this group to roles/iam.roleViewer role. is not right.

roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.

Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to roles/browser role. is not right.

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

Ref: https://cloud.google.com/iam/docs/understanding-roles

Add the users to a group and add this group to roles/browser role. is the right answer.

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

Ref: https://cloud.google.com/iam/docs/understanding-roles

Ref: https://cloud.google.com/iam/docs/overview

Bottom of Form

Top of Form

Question 47: Correct

Your colleague is learning about docker images, containers and Kubernetes, and has recently deployed a sample application to a GKE cluster. Although the sample application is responding to requests, one of the pods is pending, and they are not sure why. They shared with you the output from their Cloud Shell instance and asked you to identify why the pod is in pending state.

kubectl get pods -l app=demo

NAME READY STATUS RESTART AGE

demo-deployment-8998dab376-brm68 0/1 Pending 0 29m

demo-deployment-8998dab376-kpg18 1/1 Running 0 29m

What is the most likely explanation for this behaviour?

​

Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

(Correct)

​

The pending Pod's resource requests are too large to fit on a single node of the cluster.

​

The node pool is configured with a service account that does not have permission to pull the container image used by the pending Pod.

​

The pending Pod was originally scheduled on a node that has been preempted between the creation of the Deployment and your verification of the Pod status. It is currently being rescheduled on a new node.

Explanation

The pending Pod was originally scheduled on a node that has been preempted between the creation of the Deployment and your verification of the Pod status. It is currently being rescheduled on a new node. is not right.

Our question states that we provisioned a Google Kubernetes Engine cluster with a single preemptible node pool.

The node pool is configured with a service account that does not have permission to pull the container image used by the pending Pod. is not right.

If the node pool has permission issues when pulling the container image, the other pod would not be in Running status. And the status would have been ImagePullBackOff if there was a problem pulling the image.

The pending Pod's resource requests are too large to fit on a single node of the cluster. is not right.

If the resource requests in Pod specification are too large to fit on the node, the other pod would not be in Running status, i.e. both pods should have been in pending status if this was the case.

Ref: The pending Pod's resource requests are too large to fit on a single node of the cluster.

Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod. is the right answer.

When you have a deployment with some pods in running and other pods in the pending state, more often than not it is a problem with resources on the nodes. Here's a sample output of this use case. We see that the problem is with insufficient CPU on the Kubernetes nodes so we have to either enable auto-scaling or manually scale up the nodes.

kubectl describe pod myapp-deployment-58ddbbb995-lp86m

Events:

Type Reason Age From Message

---- ------ ---- ---- -------

Warning FailedScheduling 28s (x4 over 3m1s) default-scheduler 0/1 nodes are available: 1 Insufficient cpu.

Bottom of Form

Top of Form

Question 48: Incorrect

Your company migrated its data warehousing solution from its on-premises data centre to Google Cloud 3 years ago. Since then, several teams have worked on different data warehousing and analytics needs, and have created numerous BigQuery datasets. The proliferation in BigQuery datasets has resulted in increased storage costs, and your cost optimization manager has asked for your assistance in identifying all datasets that contain us\_social\_security\_number column to enable merging/deleting duplicate data. How can you most efficiently identify datasets that contain us\_social\_security\_number column?

​

Write a script that loops through all the projects in your organization and runs a query on INFORMATION\_SCHEMA.COLUMNS view to find the us\_social\_security\_number column.

​

Write a Cloud Dataflow job that loops through all the projects in your organization and runs a query on INFORMATION\_SCHEMA.COLUMNS view to find us\_social\_security\_number column.

(Incorrect)

​

Go to Data Catalog and search for us\_social\_security\_number in the search box.

(Correct)

​

Write a shell script that uses the bq command line tool to loop through all the projects in your organization.

Explanation

Go to Data Catalog and search for us\_social\_security\_number in the search box. is the right answer.

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

See https://cloud.google.com/data-catalog/docs/how-to/search for example.

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

Bottom of Form

Top of Form

Question 49: Incorrect

Your company has terabytes of audit logs and analytics data in multiple BigQuery datasets. Some of these data sets need to be retained long term for audit purposes. You want to ensure analysts querying data from these data sets do not accidentally delete them. What should you do?

​

Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role.

(Incorrect)

​

Add users to roles/bigquery.dataEditor role only, instead of roles/bigquery.dataOwner.

​

Create a custom role by removing delete permissions, and add users to that role only.

​

Add users to roles/bigquery.user role only, instead of roles/bigquery.dataOwner.

(Correct)

Explanation

Add users to roles/bigquery.dataEditor role only, instead of roles/bigquery.dataOwner. is not right.

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

Create a custom role by removing delete permissions, and add users to that role only. is not right.

This might work but this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role. is not right.

This might work but like above this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

Add users to roles/bigquery.user role only, instead of roles/bigquery.dataOwner. is the right answer.

roles/bigquery.user is a BigQuery User role which when applied to a project provides the ability to run jobs, including queries, within the project. A member with this role can enumerate their own jobs, cancel their own jobs, and enumerate datasets within a project.

Ref: https://cloud.google.com/iam/docs/understanding-roles#bigquery-roles

Bottom of Form

Top of Form

Question 50: Correct

All development teams at your company share the same GCP project, and this has previously resulted in some teams accidentally terminating other compute engine resources of other teams causing downtime and loss of productivity. You want to deploy a new application to the shared development GCP project, and you want to protect your instance from such downtime issues. What should you do?

​

Use a Preemptible VM.

​

Use a Shielded VM.

​

Use a sole-tenant node.

​

Enable deletion protection on the instance.

(Correct)

Explanation

Use a Shielded VM. is not right.

Shielded VMs are virtual machines (VMs) on Google Cloud hardened by a set of security controls that help defend against rootkits and boot kits. Using Shielded VMs helps protect enterprise workloads from threats like remote attacks, privilege escalation, and malicious insiders. But shielded VMs don't offer protection for accidental termination of the instance.

Ref: https://cloud.google.com/shielded-vm

Use a Preemptible VM. is not right.

A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage. Preemptible VMs don't offer protection for accidental termination of the instance.

Ref: https://cloud.google.com/compute/docs/instances/preemptible

Use a sole-tenant node. is not right.

Sole-tenancy lets you have exclusive access to a sole-tenant node, which is a physical Compute Engine server that is dedicated to hosting only your project's VMs. Use sole-tenant nodes to keep your VMs physically separated from VMs in other projects, or to group your VMs together on the same host hardware. Sole-tenant nodes don't offer protection for accidental termination of the instance.

Ref: https://cloud.google.com/compute/docs/nodes

Enable deletion protection on the instance. is the right answer.

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

Ref: https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion