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

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

​

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

(Incorrect)

​

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

​

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

​

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

(Correct)

Explanation

Setup the application using App Engine Standard environment with Cloud Router to connect to an on-premise database. is not right.

Cloud router by itself is not sufficient to connect VPC to an on-premise network. Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP).

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

Setup the application using App Engine Flexible environment with Cloud Router to connect to an on-premise database. is not right.

Cloud router by itself is not sufficient to connect VPC to an on-premise network. Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP).

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

Setup the application using App Engine Standard environment with Cloud VPN to connect to an on-premise database. is not right.

App Engine Standard can’t connect to the on-premise network with just Cloud VPN. Since App Engine is serverless, it can’t use Cloud VPN tunnels. In order to get App Engine to work with Cloud VPN, you need to connect it to the VPC using serverless VPC. You can configure the Serverless VPC by creating a connector: <https://cloud.google.com/vpc/docs/configure-serverless-vpc-access> and then you then update your app in App Engine Standard to use this connector <https://cloud.google.com/appengine/docs/standard/python/connecting-vpc>

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

You need Cloud VPN to connect VPC to an on-premise network.

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

Unlike App Engine Standard which is serverless, App Engine Flex instances are already within the VPC, so they can use Cloud VPN to connect to the on-premise network.

Bottom of Form

Top of Form

Question 2: Correct

A GKE cluster (test environment) in your test GCP project is experiencing issues with a sidecar container connecting to Cloud SQL. This issue has resulted in a massive amount of log entries in Cloud Logging and shot up your bill by 25%. Your manager has asked you to disable these logs as quickly as possible and using the least number of steps. You want to follow Google recommended practices. What should you do?

​

1. Go to the GKE console, and delete existing clusters.

2. Recreate a new cluster.

3. Clear the option to enable legacy Stackdriver Logging.

​

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

(Correct)

​

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

​

1. Go to the GKE console, and delete existing clusters.

2. Recreate a new cluster.

3. Clear the option to enable legacy Stackdriver Monitoring.

Explanation

1. Go to the GKE console, and delete existing clusters.

2. Recreate a new cluster.

3. Clear the option to enable legacy Stackdriver Logging. is not right.

Our requirement is to disable the logs ingested from the GKE container. We don't need to delete the existing cluster and create a new one.

1. Go to the GKE console, and delete existing clusters.

2. Recreate a new cluster.

3. Clear the option to enable legacy Stackdriver Monitoring. is not right.

Our requirement is to disable the logs ingested from the GKE container. We don't need to delete the existing cluster and create a new one.

Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE Cluster Operations resource. is not right.

Our requirement is to disable the logs ingested from GKE container, not the complete GKE Cluster Operations resource.

Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource. is the right answer.

We want to disable logs from a specific GKE container and this is the only option that does that.

More information about logs exclusions: https://cloud.google.com/logging/docs/exclusions

Bottom of Form

Top of Form

Question 3: Correct

Your company wants to migrate all applications from its on-premises data centre to Google Cloud Platform. The DevOps team currently use Jenkins extensively to automate configuration updates in applications. How should you migrate on-premises Jenkins application to Google Cloud while minimizing the number of steps needed?

​

Download and deploy the Jenkins Java WAR to App Engine Standard.

​

Use GCP Marketplace to launch the Jenkins solution.

(Correct)

​

Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image.

​

Create a new Compute Engine instance and install Jenkins through the command-line interface.

Explanation

Create a new Compute Engine instance and install Jenkins through the command line interface. is not right.

While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

Create a Kubernetes cluster on Compute Engine and create a deployment with the Jenkins Docker image. is not right.

While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

Download and deploy the Jenkins Java WAR to App Engine Standard. is not right.

While this is possible, we need to ensure App Engine is enabled, we then need to download the Java project/WAR, and run gcloud app deploy to set up a Jenkins server. This involves more steps than spinning up an instance from GCP Marketplace.

Ref: https://cloud.google.com/appengine/docs/standard/java/tools/uploadinganapp

Ref: https://cloud.google.com/solutions/using-jenkins-for-distributed-builds-on-compute-engine

Use GCP Marketplace to launch the Jenkins solution. is the right answer.

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

Bottom of Form

Top of Form

Question 4: Incorrect

You are exploring the possibility of migrating a mission-critical application from your on-premises data centre to Google Cloud Platform. You want to host this on a GKE cluster with autoscaling enabled, and you need to ensure each node can run a pod to push the application logs to Splunk Cloud. What should you use?

​

Deploy the monitoring pod in a StatefulSet object.

​

Reference the monitoring pod in a Deployment object.

​

Deploy the monitoring pod in a DaemonSet object.

(Correct)

​

Reference the monitoring pod in a cluster initializer at the GKE cluster creation time.

(Incorrect)

Explanation

Reference the monitoring pod in a Deployment object. is not right.

In our scenario, we need just 1 instance of the monitoring pod running on each node. Bundling the monitoring pod with a deployment object may result in multiple pod instances on the same node. In GKE, deployments represent a set of multiple, identical Pods with no unique identities. Deployment runs multiple replicas of your application and automatically replaces any instances that fail or become unresponsive. In this way, Deployments help ensure that one or more instances of your application are available to serve user requests.

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

Reference the monitoring pod in a cluster initializer at the GKE cluster creation time. is not right.

You can not use gcloud init to initialize a monitoring pod. gcloud initializer performs the following setup steps.

● Authorizes gcloud and other SDK tools to access Google Cloud Platform using your user account credentials, or from an account of your choosing whose credentials are already available.

● Sets up a new or existing configuration.

● Sets properties in that configuration, including the current project and optionally, the default Google Compute Engine region and zone you'd like to use.

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

Deploy the monitoring pod in a StatefulSet object. is not right.

In GKE, StatefulSets represents a set of Pods with unique, persistent identities and stable hostnames that GKE maintains regardless of where they are scheduled. The state information and other resilient data for any given StatefulSet Pod is maintained in persistent disk storage associated with the StatefulSet. The main purpose of StatefulSets is to set up persistent storage for pods that are deployed across multiple zones.

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

Although persistent volumes can be used, they are limited to two zones and you'd have to get into node affinity if you want to use a persistent volume with a pod on a zone that is not covered by the persistent volumes zones.

See this for more information https://kubernetes.io/docs/setup/best-practices/multiple-zones/

Deploy the monitoring pod in a DaemonSet object. is the right answer.

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

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

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

Bottom of Form

Top of Form

Question 5: Correct

You have three gcloud configurations - one for each of development, test and production projects. You want to list all the configurations and switch to a new configuration. With the fewest steps possible, what's the fastest way to switch to the correct configuration?

​

To list configurations - gcloud configurations list

To activate a configuration - gcloud config activate.

​

To list configurations - gcloud config configurations list

To activate a configuration - gcloud config configurations activate.

(Correct)

​

To list configurations - gcloud configurations list

To activate a configuration - gcloud configurations activate

​

To list configurations - gcloud config list

To activate a configuration - gcloud config activate.

Explanation

To list configurations - gcloud configurations list

To activate a configuration - gcloud configurations activate. is not right.

gcloud configurations list does not list configurations. To list existing configurations, you need to execute gcloud config configurations list.

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

gcloud configurations activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate

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

To list configurations - gcloud config list

To activate a configuration - gcloud config activate. is not right.

gcloud config list does not list configurations. It lists the properties of the existing configuration. To list existing configurations, you need to execute gcloud config configurations list.

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

gcloud config activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate

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

To list configurations - gcloud configurations list

To activate a configuration - gcloud config activate. is not right.

gcloud configurations list does not list configurations. To list existing configurations, you need to execute gcloud config configurations list.

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

gcloud config activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate

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

To list configurations - gcloud config configurations list

To activate a configuration - gcloud config configurations activate. is the right answer.

The two commands together achieve the intended outcome. gcloud config configurations list - lists existing named configurations and gcloud config configurations activate - activates an existing named configuration

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

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

See an example below

$ gcloud config configurations list

NAME IS\_ACTIVE ACCOUNT PROJECT DEFAULT\_ZONE DEFAULT\_REGION

dev-configuration False gcp-ace-lab-dev

prod-configuration False gcp-ace-lab-prod

test-configuration True gcp-ace-lab-test

$ gcloud config configurations activate prod-configuration

Activated [prod-configuration].

$ gcloud config configurations list

NAME IS\_ACTIVE ACCOUNT PROJECT DEFAULT\_ZONE DEFAULT\_REGION

dev-configuration False gcp-ace-lab-dev

prod-configuration True gcp-ace-lab-prod

test-configurationFalsegcp-ace-lab-test

Bottom of Form

Top of Form

Question 6: Correct

The Cloud Security team at your company has asked you, the operations manager, to review IAM users and their assigned roles in the production GCP project. You want to follow Google recommended practices. What should you do?

​

Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles.

(Correct)

​

Navigate to the project and then to the Roles section in the GCP Console. Review the roles and status.

​

Run gcloud iam service-accounts list. Review the output section.

​

Run gcloud iam roles list. Review the output section.

Explanation

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

Run gcloud iam roles list. Review the output section. is not right.

gcloud iam roles list lists the roles but does not list the users (i.e. IAM members)

Run gcloud iam service-accounts list. Review the output section. is not right.

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

Navigate to the project and then to the Roles section in the GCP Console. Review the roles and status. is not right.

This allows us to review the roles but not users. See the screenshot below.

Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles. is the right answer.

This is the only option that lets us view roles as well as users (members).

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

See the screenshot below.

A member can be a Google Account (for end-users), a service account (for apps and virtual machines), a Google group, or a G Suite or Cloud Identity domain that can access a resource. The identity of a member is an email address associated with a user, service account, or Google group; or a domain name associated with G Suite or Cloud Identity domains

Bottom of Form

Top of Form

Question 7: Correct

Your company is migrating a mission-critical application from the on-premises data centre to Google Cloud Platform. The application requires 12 Compute Engine VMs to handle traffic at peak usage times. Your operations team have asked you to ensure the VMs restart automatically (i.e. without manual intervention) if/when they crash, and the processing capacity of the application does not reduce down during system maintenance. What should you do?

​

Create an instance group for the instance.

Verify that the Advanced creation options setting for do not retry machine creation is set to off.

​

Create an instance template for the instances.

Set Automatic Restart to off.

Set On-host maintenance to Terminate VM instances.

Add the instance template to an instance group.

​

Create an instance group for the instances.

Set the Autohealing health check to healthy (HTTP).

​

Create an instance template for the instances.

Set the Automatic Restart to on.

Set the On-host maintenance to Migrate VM instance.

Add the instance template to an instance group.

(Correct)

Explanation

Requirements

1. 10 instances - indicates we need to look for MIG (Managed Instances Group) where we can configure healing/scaling settings. All options talk about creating an instance group so this point isn't of much use, unfortunately.

2. Highly available during system maintenance - indicates we need to look for Live Migration.

3. Automatically restart on crash - indicates we need to look for options that enable automatic restarts.

Create an instance template for the instances.

Set Automatic Restart to off.

Set On-host maintenance to Terminate VM instances.

Add the instance template to an instance group. is not right.

If Automatic Restart is off, then the compute engine instances are not automatically restarted. This results in loss of capacity and if GCP decides to start system maintenance on all instances at the same time, all instances are down and this does not meet our requirement "Highly available during system maintenance" so this option is not right.

Create an instance group for the instances.

Set the Autohealing health check to healthy (HTTP). is not right.

While auto-healing helps with the recreation of VM instances when needed, it doesn't Live-migrate the instances so our requirement of "highly available including during system maintenance" is not met. More info about Autohealing - Auto-healing allows the recreation of VM instances when needed. You can use a health check to recreate a VM instance if the health check finds it unresponsive. If you don't select a health check, Compute Engine will recreate VM instances only when they're not running.

Ref: https://cloud.google.com/compute/docs/instance-groups/?hl=en\_GB#managed\_instance\_groups\_and\_autohealing

Create an instance group for the instance.

Verify that the Advanced creation options setting for do not retry machine creation is set to off. is not right.

Like above - this option doesn't Live-migrate the instances so our requirement of "highly available including during system maintenance" is not met.

Create an instance template for the instances.

Set the Automatic Restart to on.

Set the On-host maintenance to Migrate VM instance.

Add the instance template to an instance group. is the right option.

Enabling automatic restart ensures that compute engine instances are automatically restarted when they crash. And Enabling "Migrate VM Instance" enables live migrates i.e. compute instances are migrated during system maintenance and remain running during the migration.

Automatic Restart - If your instance is set to terminate when there is a maintenance event, or if your instance crashes because of an underlying hardware issue, you can set up Compute Engine to automatically restart the instance by setting the automaticRestart field to true. This setting does not apply if the instance is taken offline through a user action, such as calling sudo shutdown, or during a zone outage.

Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#autorestart

Enabling the Migrate VM Instance option migrates your instance away from an infrastructure maintenance event, and your instance remains running during the migration. Your instance might experience a short period of decreased performance, although generally, most instances should not notice any difference. This is ideal for instances that require constant uptime and can tolerate a short period of decreased performance.

Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#live\_migrate

Bottom of Form

Top of Form

Question 8: Correct

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

​

Create a Failover replica in the same region but in a different zone.

​

Configure High Availability (HA) for Cloud SQL and Create a Failover replica in a different region

​

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

(Correct)

​

Create a Read replica in the same region but in a different zone.

Explanation

Create a Read replica in the same region but in a different zone. is not right.

Read replicas do not provide failover capability. To provide failover capability, you need to configure Cloud SQL Instance for High Availability.

Ref: https://cloud.google.com/sql/docs/mysql/replication

Create a Read replica in a different region. is not right.

Read replicas do not provide failover capability. To provide failover capability, you need to configure Cloud SQL Instance for High Availability.

Ref: https://cloud.google.com/sql/docs/mysql/replication

Configure High Availability (HA) for Cloud SQL and Create a Failover replica in a different region. is not right.

A Cloud SQL instance configured for HA is called a regional instance because it's primary and secondary instances are in the same region. They are located in different zones but within the same region. It is not possible to create a Failover replica in a different region.

Ref: https://cloud.google.com/sql/docs/mysql/high-availability

Configure High Availability (HA) for Cloud SQL and Create a Failover replica in the same region but in a different zone. is the right answer.

If a HA-configured instance becomes unresponsive, Cloud SQL automatically switches to serving data from the standby instance. The HA configuration provides data redundancy. A Cloud SQL instance configured for HA has instances in the primary zone (Master node) and secondary zone (standby/failover node) within the configured region. Through synchronous replication to each zone's persistent disk, all writes made to the primary instance are also made to the standby instance. If the primary goes down, the standby/failover node takes over and your data continues to be available to client applications.

Ref: https://cloud.google.com/sql/docs/mysql/high-availability

Bottom of Form

Top of Form

Question 9: Correct

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

$ kubectl get pods

NAME READY STATUS RESTARTS AGE

nginx-84748895c4-nqqmt 1/1 Running 0 9m41s

$ kubectl delete pod nginx-84748895c4-nqqmt

pod "nginx-84748895c4-nqqmt" deleted

$ kubectl get pods

NAME READY STATUS RESTARTS AGE

nginx-84748895c4-k6bzl 1/1 Running 0 25s

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

​

kubectl delete deployment nginx

(Correct)

​

kubectl delete nginx

​

kubectl delete pod nginx-84748895c4-k6bzl --no-restart

​

kubectl delete --deployment=nginx

Explanation

kubectl delete pod nginx-84748895c4-k6bzl --no-restart. is not right.

kubectl delete pod command does not support the flag --no-restart. The command fails to execute due to the presence of an invalid flag.

$ kubectl delete pod nginx-84748895c4-k6bzl --no-restart

Error: unknown flag: --no-restart

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

kubectl delete --deployment=nginx. is not right.

kubectl delete command does not support the parameter --deployment. The command fails to execute due to the presence of an invalid parameter.

$ kubectl delete --deployment=nginx

Error: unknown flag: --deployment

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

kubectl delete nginx. is not right.

We haven't provided the kubectl delete command information on what to delete, whether a pod, a service or a deployment. The command syntax is wrong and fails to execute.

$ kubectl delete nginx

error: resource(s) were provided, but no name, label selector, or --all flag specified

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

kubectl delete deployment nginx. is the right answer.

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

$ kubectl delete deployment nginx

deployment.apps "nginx" deleted

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

Bottom of Form

Top of Form

Question 10: Correct

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

​

Import data into Google Cloud Datastore.

​

Import data into Google Cloud SQL.

​

Import data into Google BigQuery.

(Correct)

​

Import flat files into Google Cloud Storage.

Explanation

Import data into Google Cloud SQL. is not right.

Cloud SQL is a fully-managed relational database service. It supports MySQL so the migration of data from your data center to cloud can be straightforward but Google Cloud SQL cannot handle petabyte-scale data. The current second-generation instances limit the storage to approximately 30TB.

Ref: <https://cloud.google.com/sql#overview>

Ref: https://cloud.google.com/sql/docs/quotas

Import flat files into Google Cloud Storage. is not right.

Cloud Storage is a service for storing objects in Google Cloud. You store objects in containers called buckets. You could export the MySQL data into files and import them into Google Cloud Storage, but it doesn't offer an SQL Interface to run queries/reports.

Ref: https://cloud.google.com/storage/docs/introduction

Import data into Google Cloud Datastore. is not right.

Your business analysts are already familiar with SQL Interface so we need a service that supports SQL. However, Cloud Datastore is a NoSQL document database. Cloud Datastore doesn't support SQL (it supports GQL which is similar to SQL, but not identical).

Ref: https://cloud.google.com/datastore/docs/reference/gql\_reference

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

Import data into Google BigQuery. is the right answer.

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

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

Bottom of Form

Top of Form

Question 11: Correct

You migrated an internal HR system from an on-premises database to Google Cloud Compute Engine Managed Instance Group (MIG). The networks team at your company has asked you to associate the internal DNS records of the compute engine instances in a custom DNS zone. How can this be achieved?

​

Create your Compute Engine instances with custom hostnames.

​

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

(Correct)

​

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

​

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

Explanation

Our requirements here are 1. Internal and 2. Custom Zone

Create your Compute Engine instances with custom hostnames. is not right.

This doesn’t put them in a custom zone.

Deploy the BIND DNS server in the VPC, and create a Cloud DNS forwarding zone to forward the DNS requests to BIND. Create records for each instance in the BIND DNS server. is not right.

This might be possible but not something Google recommends. The Cloud DNS service offering from Google already offers these features so it is pointless installing a custom DNS server to do that.

Create a new VPC, block all external traffic with a firewall rule and create 2 Cloud DNS zones - a first zone in the new VPC and a second zone in the main VPC that is forwarding requests to the first Cloud DNS zone. Create records for each instance in the first zone. is not right.

This doesn’t make any sense, moreover, the two VPCs can’t communicate without VPC peering.

Ref: https[://cloud.google.com/dns/docs/overview#concepts](https://cloud.google.com/dns/docs/overview#concepts)

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

You should absolutely do this when you want internal DNS records in a custom zone. Cloud DNS gives you the option of private zones and internal DNS names.

Ref: https[://cloud.google.com/dns/docs/overview#concepts](https://cloud.google.com/dns/docs/overview#concepts)

Bottom of Form

Top of Form

Question 12: Incorrect

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

​

gcloud compute instances create [INSTANCE\_NAME] --preemptible --boot-disk-auto-delete=no

(Incorrect)

​

gcloud compute instances create [INSTANCE\_NAME] --no-auto-delete

​

gcloud compute instances create [INSTANCE\_NAME] --preemptible --no-boot-disk-auto-delete

(Correct)

​

gcloud compute instances create [INSTANCE\_NAME] --preemptible. The flag --boot-disk-auto-delete is disabled by default.

Explanation

gcloud compute instances create [INSTANCE\_NAME] --preemptible --boot-disk-auto-delete=no. is not right.

gcloud compute instances create doesn't provide a parameter called boot-disk-auto-delete. It does have a flag by the same name. --boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use --no-boot-disk-auto-delete to disable.

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

gcloud compute instances create [INSTANCE\_NAME] --preemptible. --boot-disk-auto-delete flag is disabled by default. is not right.

--boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use --no-boot-disk-auto-delete to disable.

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

gcloud compute instances create [INSTANCE\_NAME] --no-auto-delete. is not right.

gcloud compute instances create doesn't provide a flag called no-auto-delete

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

gcloud compute instances create [INSTANCE\_NAME] --preemptible --no-boot-disk-auto-delete. is the right answer.

Use --no-boot-disk-auto-delete to disable automatic deletion of boot disks when the instances are deleted. --boot-disk-auto-delete flag is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. In order to prevent automatic deletion, we have to specify --no-boot-disk-auto-delete flag.

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

Bottom of Form

Top of Form

Question 13: Correct

You've created a Kubernetes engine cluster named "my-gcp-ace-proj-1", which has a cluster pool named my-gcp-ace-primary-node-pool. You want to increase the number of nodes within your cluster pool from 10 to 20 to meet capacity demands. What is the command to change the number of nodes in your pool?

​

gcloud container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20

​

kubectl container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20

​

gcloud container clusters resize my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --new-size 20

​

gcloud container clusters resize my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20

(Correct)

Explanation

kubectl container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20. is not right.

kubectl does not accept container as an operation.

Ref: https://kubernetes.io/docs/reference/kubectl/overview/#operations

gcloud container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20. is not right.

gcloud container clusters update can not be used to specify the number of nodes. It can be used to specify the node locations, but not the number of nodes.

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/update

gcloud container clusters resize my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --new-size 20. is not right.

gcloud container clusters resize command does not support the parameter new-size. While --size can be used to resize the cluster node pool, use of --size is discouraged as this is a deprecated parameter. "The --size flag is now deprecated. Please use --num-nodes instead."

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/resize

gcloud container clusters resize my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20. is the right answer

gcloud container clusters resize can be used to specify the number of nodes using the --num-nodes parameter which is the target number of nodes in the cluster.

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/resize

Bottom of Form

Top of Form

Question 14: Incorrect

You require a single VPC with 2 subnets in the same region. Each subnet has 2 Compute Engine VMs running different applications. You need all VMs to communicate with each other over the internal IP addresses. What should you do?

​

Create a single custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range.

(Correct)

​

Create a single custom VPC with 2 subnets. Create each subnet in the same region and with the same CIDR range.

(Incorrect)

​

Create 2 custom VPCs, each with a single subnet. Create each subnet in a different region and with a different CIDR range.

​

Create 2 custom VPCs, each with a single subnet. Create each subnet in the same region and with the same CIDR range.

Explanation

Create 2 custom VPCs, each with a single subnet. Create each subnet in a different region and with a different CIDR range. is not right.

We need to get our requirements working with 1 VPC, not 2 !!

Create 2 custom VPCs, each with a single subnet. Create each subnet in the same region and with the same CIDR range. is not right.

We need to get our requirements working with 1 VPC, not 2 !!

Create a single custom VPC with 2 subnets. Create each subnet in the same region and with the same CIDR range. is not right.

We can not create two subnets in one VPC with the same CIDR range. "Primary and secondary ranges for subnets cannot overlap with any allocated range, any primary or secondary range of another subnet in the same network, or any IP ranges of subnets in peered networks." Ref: https://cloud.google.com/vpc/docs/using-vpc#subnet-rules

Create a single custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range. is the right answer.

When we create subnets in the same VPC with different CIDR ranges, they can communicate automatically within VPC. "Resources within a VPC network can communicate with one another by using internal (private) IPv4 addresses, subject to applicable network firewall rules"

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

Bottom of Form

Top of Form

Question 15: Incorrect

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

​

Nearline storage class

​

Coldline storage class

(Incorrect)

​

Archive storage class

(Correct)

​

Standard storage class

Explanation

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

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

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

So the correct answer is Archive storage class.

Bottom of Form

Top of Form

Question 16: Correct

Your company has a centralized billing account for all development, test and production GCP projects. Your company has recently acquired another company that lets its developers pay for their projects using their company credit cards. You want to consolidate the billing of all GCP projects into a new billing account. You want to follow Google recommended practices. How should you do this?

​

Contact cloud-billing@google.com with your bank account details and request a corporate billing account for your company.

​

In the Google Platform Console, go to the Resource Manage and move all projects to the root Organization.

(Correct)

​

In the Google Cloud Platform Console, create a new billing account and set up a payment method.

​

Create a ticket with Google Support and wait for their call to share your credit card details over the phone.

Explanation

Contact cloud-billing@google.com with your bank account details and request a corporate billing account for your company. is not right.

That is not how we set up billing for the organization.

Ref: https://cloud.google.com/billing/docs/concepts

Create a ticket with Google Support and wait for their call to share your credit card details over the phone. is not right.

That is not how we set up billing for the organization.

Ref: https://cloud.google.com/billing/docs/concepts

In the Google Cloud Platform Console, create a new billing account and set up a payment method. is not right.

Unless all projects are modified to use the new billing account, this doesn't work.

Ref: https://cloud.google.com/billing/docs/concepts

In the Google Platform Console, go to the Resource Manage and move all projects to the root Organization. is the right answer.

If we move all projects under the root organization hierarchy, they still need to modified to use a billing account within the organization (same as the previous option).

Ref: https://cloud.google.com/resource-manager/docs/migrating-projects-billing#top\_of\_page

Note: The link between projects and billing accounts is preserved, irrespective of the hierarchy. When you move your existing projects into the organization they will continue to work and be billed as they used to before the migration, even if the corresponding billing account has not been migrated yet.

But in this option, all projects are in the organization resource hierarchy so the organization can uniformly apply organization policies to all its projects which is a Google recommended practice. So this is the better of the two options.

Ref: https://cloud.google.com/billing/docs/concepts

Bottom of Form

Top of Form

Question 17: Incorrect

Your company, which runs highly rated mobile games, has chosen to migrate its analytics backend to BigQuery. The analytics team of 7 analysts need access to perform queries against the data in BigQuery. How should you grant them access?

​

1. Create a dedicated Google group in Cloud Identity.

2. Add each analyst's user account to the group.

3. Assign the BigQuery jobUser role to the group.

(Incorrect)

​

1. Create an IAM entry for each analyst's user account.

2. Assign the BigQuery dataViewer user role to the group.

​

1. Create an IAM entry for each analyst's user account.

2. Assign the BigQuery jobUser role to the group.

​

1. Create a dedicated Google group in Cloud Identity.

2. Add each analyst's user account to the group.

3. Assign the BigQuery dataViewer user role to the group.

(Correct)

Explanation

1. Create an IAM entry for each analyst's user account.

2. Assign the BigQuery dataViewer user role to the group. is not right.

dataViewer provides permissions to Read data (i.e. query) and metadata from the table or view so this is the right role but given that our data science team changes frequently, we do not want to go through this lengthy provisioning and de-provisioning process. Instead, we should be using groups so that provisioning and de-provisioning is as simple as adding/removing the user to/from the group. Google Groups are a convenient way to apply an access policy to a collection of users

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

1. Create an IAM entry for each analyst's user account.

2. Assign the BigQuery jobUser role to the group. is not right.

Given that our data science team changes frequently, we do not want to go through this lengthy provisioning and de-provisioning process. Instead, we should be using groups so that provisioning and de-provisioning is as simple as adding/removing the user to/from the group. Google Groups are a convenient way to apply an access policy to a collection of users

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

Ref: https://cloud.google.com/iam/docs/overview#google\_group

1. Create a dedicated Google group in Cloud Identity.

2. Add each analyst's user account to the group.

3. Assign the BigQuery jobUser role to the group. is not right.

Since you want users to query the datasets, you need dataViewer role. jobUser provides the ability to run jobs, including "query jobs". The query job lets you query an authorized view. An authorized view lets you share query results with particular users and groups without giving them access to the underlying tables. You can also use the view's SQL query to restrict the columns (fields) the users are able to query.

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

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

1. Create a dedicated Google group in Cloud Identity.

2. Add each analyst's user account to the group.

3. Assign the BigQuery dataViewer user role to the group. is the right answer.

dataViewer provides permissions to Read data (i.e. query) and metadata from the table or view so this is the right role and this option also rightly uses groups instead of assigning permissions at the user level..

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

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

Bottom of Form

Top of Form

Question 18: Incorrect

Your networks team has set up Google compute network as shown below. In addition, firewall rules in the VPC network have been configured to allow egress to 0.0.0.0/0

[Larger image](javascript:void(0))

Which instances have access to Google APIs and Services such as Google Cloud Storage?

​

VM A1, VM A2, VM B1, VM B2

​

VM A1, VM A2, VM B2

(Correct)

​

VM A1, VM A2, VM B1

​

VM A1, VM A2

(Incorrect)

Explanation

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

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

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

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

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

Bottom of Form

Top of Form

Question 19: Correct

Your company is migrating an application from its on-premises data centre to Google Cloud. One of the applications uses a custom Linux distribution that is not available on Google Cloud. Your solution architect has suggested using VMWare tools to exporting the image and store it in a Cloud Storage bucket. The VM Image is a single compressed 64 GB tar file. You started copying this file using gsutil over a dedicated 1Gbps network, but the transfer is taking a very long time to complete. Your solution architect has suggested using all of the 1Gbps Network to transfer the file quickly. What should you do?

​

Use the GCP Console to transfer the file instead of gsutil.

​

Decrease the TCP window size on the machine initiating the transfer.

​

Change the storage class of the bucket from Nearline to Multi-Regional.

​

Enable parallel composite uploads using gsutil on the file transfer.

(Correct)

Explanation

Requirements - transfer the file rapidly, use as much of the rated 1 Gbps as possible

Use the GCP Console to transfer the file instead of gsutil. is not right.

GCP Console does not offer any specific features that help in improving the upload speed.

Decrease the TCP window size on the machine initiating the transfer. is not right.

By decreasing the TCP window size, you are reducing the chunks of data sent in the TCP window, and this has the effect of underutilizing your bandwidth and can slow down the upload.

Change the storage class of the bucket from Nearline to Multi-Regional. is not right.

Multi-Regional is not a storage class. It is a bucket location. You can transition between storage classes but that does not improve the upload speed.

https://cloud.google.com/storage/docs/locations

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

Enable parallel composite uploads using gsutil on the file transfer. is the right answer.

With cloud storage, Object composition can be used for uploading an object in parallel: you can divide your data into multiple chunks, upload each chunk to a distinct object in parallel, compose your final object, and delete any temporary source objects. This helps maximize your bandwidth usage and ensures the file is uploaded as fast as possible.

Ref: https://cloud.google.com/storage/docs/composite-objects#uploads

Bottom of Form

Top of Form

Question 20: Correct

You want to migrate an XML parser application from the on-premises data centre to Google Cloud Platform. You created a development project, set up the necessary IAM roles and deployed the application in a compute engine instance. The testing has succeeded, and you are ready to deploy the production instance. You want to create the same IAM roles in a new production project. How can you do this efficiently without compromising security?

​

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

​

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

(Correct)

​

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

​

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

Explanation

Our requirements are to create the same iam roles in a different (production) project with the fewest possible steps.

In the Google Cloud Platform Console, use the 'create role from role' functionality. is not right.

This creates a role in the same (development) project, not in the production project. So this doesn't meet our requirement to create same iam roles in production project

In the Google Cloud Platform Console, use the 'create role' functionality and select all applicable permissions. is not right.

This creates a role in the same (development) project, not in the production project. So this doesn't meet our requirement to create same iam roles in production project

Use gcloud iam roles copy and specify your organization as the destination organization. is not right.

We can optionally specify a destination organization but since our requirement is to copy the roles into "production project" (i.e. project, not organization), this option does not meet our requirement to create same iam roles in production project

Ref: https://cloud.google.com/sdk/gcloud/reference/iam/roles/copy

Use gcloud iam roles copy and specify the production project as the destination project. is the right answer.

This is the only option that fits our requirements. You copy the roles into the destination project using gcloud iam roles copy and by specifying the production project destination project.

$gcloud iam roles copy --source "<<role id to copy>>" --destination <<role id of the copied role in production project>> --dest-project <<id of production project>>

Ref: https://cloud.google.com/sdk/gcloud/reference/iam/roles/copy

Bottom of Form

Top of Form

Question 21: Correct

You are enhancing a production application currently running on an Ubuntu Linux VM on Google Compute Engine. The new enhancements require a connection to Cloud SQL to persist user addresses. Your colleague has created the Cloud SQL instance and an IAM service account with the correct permissions but doesn’t know how to configure the VM to use this service account, and has asked for your assistance. What should you do?

​

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

(Correct)

​

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

​

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

​

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

Explanation

When creating the VM via the web console, specify the service account under the ‘Identity and API Access’ section. is the right answer.

You can set the service account at the time of creating the compute instance. You can also update the service account used by the instance - this requires that you stop the instance first and then update the service account. Setting/Updating the service account can be done either via the web console or by executing gcloud command or by the REST API. See below an example for updating the service account through gcloud command.

gcloud compute instances set-service-account instance-1 --zone=us-central1-a --service-account=my-new-service-account@gcloud-gcp-ace-lab-266520.iam.gserviceaccount.com

Updated [https://www.googleapis.com/compute/v1/projects/gcloud-gcp-ace-lab-266520/zones/us-central1-a/instances/instance-1].

Download a JSON Private Key for the service account. On the Project Metadata, add that JSON as the value for the key compute-engine-serviceaccount is not right.

While updating the service account for a compute instance can be done through the console, gcloud or the REST API, they don't do it based on the JSON Private Key.

Download a JSON Private Key for the service account. On the Custom Metadata of the VM, add that JSON as the value for the key compute-engine-service-account. is not right.

While updating the service account for a compute instance can be done through the console, gcloud or the REST API, they don't do it based on the JSON Private Key.

Download a JSON Private Key for the service account. After creating the VM, ssh into the VM and save the JSON under ~/.gcloud/compute-engine-service-account.json is not right.

You can configure a VM to use a certain service account by providing the relevant JSON credentials file, but the procedure is different. Copying the JSON file to a specific path alone is not sufficient, moreover, the path mentioned is wrong as well. See below for a use case where a VM which is unable to list cloud storage buckets is updated to use a service account and it can then list the buckets.

Prior to using a service account. Use gsutil ls to list buckets and it fails.

$ gsutil ls

ServiceException: 401 Anonymous caller does not have storage.buckets.list access to project 393066724129.

Within the VM, execute the command below to use the service account. (Assumes that you have created a service account that provides the necessary permissions and have copied it over the VM)

gcloud auth activate-service-account admin-service-account@gcloud-gcp-ace-266520.iam.gserviceaccount.com --key-file=~/compute-engine-service-account.json

Activated service account credentials for: [admin-service-account@gcloud-gcp-ace-266520.iam.gserviceaccount.com]

The output above doesn't show this, but the credentials are written to the file

/home/gcloud\_gcp\_ace\_user/.config/gcloud/legacy\_credentials/admin-service-account@gcloud-gcp-ace-266520.iam.gserviceaccount.com/adc.json

Now, use gsutil ls again to list buckets and it works.

$ gsutil ls

gs://test-gcloud-gcp-ace-2020-bucket-1/

gs://test-gcloud-gcp-ace-2020-bucket-2/

Bottom of Form

Top of Form

Question 22: Correct

Your company runs several internal applications on bare metal Kubernetes servers in your on-premises data centre. One of the applications deployed in the Kubernetes cluster uses a NAS share to save files. In preparation for the upcoming migration to Google Cloud, you want to update the application to use Google Cloud Storage to save files, but the virtual machines do not have public IP addresses. What should you do?

​

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

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

In your on-premises network, configure your DNS server to resolve \*.googleapis.com as a CNAME to restricted.googleapis.com

(Correct)

​

Use nslookup to get the IP addresses for storage.googleapis.com

Negotiate with the security team to be able to give public IP addresses to the servers.

Only allow egress traffic from those servers to the IP addresses for storage.googleapis.com

​

Using Cloud VPN, create a VPN tunnel to a Virtual Private Cloud (VPC) in Google Cloud Platform (GCP)

In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance

Configure your servers to use that instance as a proxy to access cloud storage

​

Use Migrate for Compute Engine (formerly known as Velostrata) to migrate these servers to Compute Engine

Create an internal load balancer (ILB) that uses storage.googleapis.com as backend

Configure your new instances to use the ILB as a proxy

Explanation

Our requirement is to follow Google recommended practices to achieve the end result.

Configuring Private Google Access for On-Premises Hosts is best achieved by VPN/Interconnect + Advertise Routes + Use restricted Google IP Range.

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

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

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

Ref: https[://cloud.google.com/vpc/docs/configure-private-google-access-hybrid](https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid)

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

“You can use [Cloud Router Custom Route Advertisement](https://cloud.google.com/router/docs/how-to/advertising-custom-ip) to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network. The Restricted Google APIs IP range is 199.36.153.4/30. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection.”

Without having a public IP address or access to the internet, the only way you could connect to cloud storage is if you have an internal route to it. So Negotiate with the security team to be able to give public IP addresses to the servers is not right.

Following “Google recommended practices” is synonymous with “using Google’s services” (Not quite, but it is - at least for the exam !!). So In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance is not right.

Migrating the VM to Compute Engine is a bit drastic when Google says it is perfectly fine to have Hybrid Connectivity architectures <https://cloud.google.com/hybrid-connectivity>. So, Use Migrate for Compute Engine (formerly known as Velostrata) to migrate these servers to Compute Engine is not right.

Bottom of Form

Top of Form

Question 23: Correct

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

​

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Nearline Storage.

​

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage.

(Correct)

​

Use Google Cloud Regional Storage for the first 30 days, and then move videos to Google Persistent Disk.

​

Use Google Cloud Nearline Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage.

Explanation

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

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Nearline Storage. is not right.

Transitioning the data to Nearline Storage is a good idea as Nearline Storage costs less than standard storage, is highly durable for storing infrequently accessed data and a better choice than Standard Storage in scenarios where slightly lower availability is an acceptable trade-off for lower at-rest storage costs. Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

However, we do not have a requirement to access the data after 30 days; and there are storage classes that are cheaper than nearline storage, so it is not a suitable option.

Ref: https://cloud.google.com/storage/pricing#storage-pricing

Use Google Cloud Regional Storage for the first 30 days, and then move videos to Google Persistent Disk. is not right.

Persistent disk pricing is almost double that of standard storage class in Google Cloud Storage service. Plus the persistent disk can only be accessed when attached to another service such as compute engine, GKE, etc making this option very expensive.

Ref: https://cloud.google.com/storage/pricing#storage-pricing

Ref: https://cloud.google.com/compute/disks-image-pricing#persistentdisk

Use Google Cloud Nearline Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage. is not right.

Nearline storage class is suitable for storing infrequently accessed data and has costs associated with retrieval. Since the footage is processed regularly within the first 30 days, data retrieval costs may far outweigh the savings made by using nearline storage over standard storage class.

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

Ref: https://cloud.google.com/storage/pricing#archival-pricing

Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage. is the right answer.

We save the videos initially in Regional Storage (Standard) which does not have retrieval charges so we do not pay for accessing data within the first 30 days during which the videos are accessed frequently. We only pay for the standard storage costs. After 30 days, we transition the CCTV footage videos to Coldline storage which is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline storage class is cheaper than Nearline storage class.

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

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

Bottom of Form

Top of Form

Question 24: Correct

You are in the process of migrating a mission-critical application from your on-premises data centre to Google Kubernetes Engine (GKE). Your operations team do not want to take on the overhead for upgrading GKE cluster periodically to newer stable versions. What should you do?

​

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

​

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

(Correct)

​

Select the latest available cluster version for your GKE cluster.

​

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

Explanation

Enable the Node Auto-Repair feature for your GKE cluster. is not right.

GKE's node auto-repair feature helps you keep the nodes in your cluster in a healthy, running state. When enabled, GKE makes periodic checks on the health state of each node in your cluster. If a node fails consecutive health checks over an extended time period, GKE initiates a repair process for that node.

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

Select the latest available cluster version for your GKE cluster. is not right.

We can certainly select the latest available cluster version at the time of GKE cluster provisioning, however, this does not automatically upgrade the cluster if new versions become available.

Select "Container-Optimized OS (cos)" as a node image for your GKE cluster. is not right.

Container-Optimized OS comes with the Docker container runtime and all Kubernetes components pre-installed for out of the box deployment, management, and orchestration of your containers. But these do not help with automatically upgrading GKE cluster versions.

Ref: https://cloud.google.com/container-optimized-os

Enable the Node Auto-Upgrades feature for your GKE cluster. is the right answer.

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

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

Bottom of Form

Top of Form

Question 25: Incorrect

You are developing a simple application in App Engine Standard service. Unit testing and user acceptance testing has succeeded, and you want to build a new App Engine application to serve as your performance testing environment. What should you do?

​

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

(Correct)

​

Use gcloud to create the new project and to copy the deployed application to the new project.

​

Deploy your application again using gcloud and specify the project parameter with the new project name to create the new project.

​

Create a Deployment Manager configuration file that copies the current App Engine deployment into a new project.

(Incorrect)

Explanation

Use gcloud to create the new project and to copy the deployed application to the new project. is not right.

You can use gcloud to create a new project but you can not copy a deployed application from one project to another. This feature is not offered by Google App Engine.

Create a Deployment Manager configuration file that copies the current App Engine deployment into a new project. is not right.

The deployment manager configuration file contains configuration about the resources that need to be created in Google cloud, however, it does not offer the feature to copy app engine deployment into a new project.

Deploy your application again using gcloud and specify the project parameter with the new project name to create the new project. is not right.

You can deploy using gcloud app deploy and target it to a different project using --project flag. However, you can only deploy to an existing project as the gcloud app deploy command is unable to create a new project if it doesn't already exist.

Use gcloud to create the new project, and then deploy your application to the new project. is the right answer.

You can deploy to a different project by using --project flag.

By default, the service is deployed the current project configured via:

$ gcloud config set core/project PROJECT

To override this value for a single deployment, use the --project flag:

$ gcloud app deploy ~/my\_app/app.yaml --project=PROJECT

Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy

Bottom of Form

Top of Form

Question 26: Correct

Your team manages the game backend for a popular game with users all over the world. The current game backend runs on a fleet of VMs behind a Managed Instance Group (MIG) with autoscaling enabled. You have configured the scaling policy on the MIG to add more instances if the CPU utilization is consistently over 85% for 3 minutes, and to scale down when the CPU utilization is lower than 65%. You recently noticed the autoscaler adds more VMs than is necessary during the scale-up, and you suspect this might be down to an incorrect configuration in the health check – the initial delay on the health check is 30 seconds. Each VM takes just under 3 minutes before it is ready to process the requests from the web application and mobile app. What should you do to fix the scaling issue?

​

Set the maximum number of instances to 1.

​

Decrease the maximum number of instances to 3.

​

Increase the initial delay of the HTTP health check to 200 seconds.

(Correct)

​

Use a TCP health check instead of an HTTP health check.

Explanation

Scenario

● Autoscaling is enabled and kicks off the scale-up

● Scaling policy is based on target CPU utilization of 80%

● The initial delay is 30 seconds

● VM startup time is 3 minutes.

● Auto-scaling creates more instances than necessary.

Set the maximum number of instances to 1. is not right.

Setting the maximum number of instances to 1 effectively limits the scale up to 1 instance which is undesirable as in this case we may still be struggling with the CPU usage but we can't scale up. Therefore this is not the right answer.

Decrease the maximum number of instances to 3. is not right.

Setting the maximum number of instances to 3 effectively limits the scale up to 3 instances which is undesirable as in this case we may still be struggling with the CPU usage but we can't scale up. Therefore this is not the right answer.

Use a TCP health check instead of an HTTP health check. is not right.

TCP health check is a legacy health check, whereas HTTP health check is more advanced and "non-legacy". It is possible a TCP health check might say the application is UP when it is not as it only listens on application servers TCP port and doesn't validate the application health through a HTTP check on its health endpoint. This results in the load balancer sending requests to the application server when it is still loading the application resulting in failures.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/health-checks/create/tcp

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/health-checks/create/http

Increase the initial delay of the HTTP health check to 200 seconds. is the right answer.

The reason why our autoscaling is adding more instances than needed is that it checks 30 seconds after launching the instance and at this point, the instance isn't up and isn't ready to serve traffic. So our autoscaling policy starts another instance - again checks this after 30 seconds and the cycle repeats until it gets to the maximum instances or the instances launched earlier are healthy and start processing traffic - which happens after 180 seconds (3 minutes). This can be easily rectified by adjusting the initial delay to be higher than the time it takes for the instance to become available for processing traffic.

So setting this to 200 ensures that it waits until the instance is up (around 180-second mark) and then starts forwarding traffic to this instance. Even after a cool out period, if the CPU utilization is still high, the autoscaler can again scale up but this scale-up is genuine and is based on the actual load.

"Initial Delay Seconds" - This setting delays autohealing from potentially prematurely recreating the instance if the instance is in the process of starting up. The initial delay timer starts when the currentAction of the instance is VERIFYING.

Ref: https://cloud.google.com/compute/docs/instance-groups/autohealing-instances-in-migs

Bottom of Form

Top of Form

Question 27: Incorrect

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

​

In the bucket advanced settings, select the Customer-supplied key and then select a Cloud KMS encryption key.

​

Modify .boto configuration to include encryption\_key = [KEY\_RESOURCE] when uploading objects to bucket.

(Correct)

​

In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key.

(Correct)

​

Use gsutil with --encryption-key=[ENCRYPTION\_KEY] when uploading objects to the bucket.

(Incorrect)

​

Use gsutil with -o "GSUtil:encryption\_key=[KEY\_RESOURCE]" when uploading objects to the bucket.

(Correct)

Explanation

In the bucket advanced settings, select the Customer-supplied key and then select a Cloud KMS encryption key. is not right.

The customer-supplied key is not an option when selecting the encryption method in the console.

Use gsutil with --encryption-key=[ENCRYPTION\_KEY] when uploading objects to the bucket. is not right.

gsutil doesn't accept the flag --encryption-key. gsutil can be set up to use an encryption key by modifying boto configuration or by specifying a top-level -o flag but neither of these is included in this option.

Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

In the bucket advanced settings, select the Customer-managed key and then select a Cloud KMS encryption key. is the right answer.

Our compliance department wants us to use customer-managed encryption keys. We can select Customer-Managed radio and provide a cloud KMS encryption key to encrypt objects with the customer-managed key. This fit our requirements.

Use gsutil with -o "GSUtil:encryption\_key=[KEY\_RESOURCE]" when uploading objects to the bucket. is the right answer.

We can have gsutil use an encryption key by using the -o top-level flag: -o "GSUtil:encryption\_key=[KEY\_RESOURCE]".

Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

Modify .boto configuration to include encryption\_key = [KEY\_RESOURCE] when uploading objects to bucket. is the right answer.

As an alternative to the -o top-level flag, gsutil can also use an encryption key if .boto configuration is modified to specify the encryption key.

encryption\_key = [KEY\_RESOURCE]

Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

Bottom of Form

Top of Form

Question 28: Correct

You created a cluster.YAML file containing

resources:

- name: cluster

type: container.v1.cluster

properties:

zone: europe-west1-b

cluster:

description: "My GCP ACE cluster"

initialNodeCount: 2

You want to use Cloud Deployment Manager to create this cluster in GKE. What should you do?

​

gcloud deployment-manager deployments create my-gcp-ace-cluster --config cluster.yaml

(Correct)

​

gcloud deployment-manager deployments apply my-gcp-ace-cluster --config cluster.yaml

​

gcloud deployment-manager deployments create my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml

​

gcloud deployment-manager deployments apply my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml

Explanation

gcloud deployment-manager deployments apply my-gcp-ace-cluster --config cluster.yaml. is not right.

"gcloud deployment-manager deployments" doesn't support action apply. With Google cloud in general, the action for creating is create and the action for retrieving is list. With Kubernetes resources, the corresponding actions are apply and get respectively.

Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create

gcloud deployment-manager deployments apply my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml. is not right.

"gcloud deployment-manager deployments" doesn't support action apply. With Google cloud in general, the action for creating is create and the action for retrieving is list. With Kubernetes resources, the corresponding actions are apply and get respectively.

Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create

gcloud deployment-manager deployments create my-gcp-ace-cluster --type container.v1.cluster --config cluster.yaml. is not right.

"gcloud deployment-manager deployments create" creates deployments based on the configuration file. (Infrastructure as code). It doesn't expect the parameter type passed to it directly and fails when executed with the type parameter.

Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create

gcloud deployment-manager deployments create my-gcp-ace-cluster --config cluster.yaml. is the right answer.

"gcloud deployment-manager deployments create" creates deployments based on the configuration file. (Infrastructure as code). All the configuration related to the artifacts is in the configuration file. This command correctly creates a cluster based on the provided cluster.yaml configuration file.

Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create

Bottom of Form

Top of Form

Question 29: Correct

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

​

Cloud Run

​

Cloud Run for Anthos

​

Cloud Functions

(Correct)

​

App Engine Standard

Explanation

GCP serverless compute portfolio includes 4 services, which are all listed in the answer options. Our requirements are to identify a GCP serverless service that

1. Lets us scale down to 0

2. Integrates with Cloud Pub/Sub seamlessly

Cloud Run for Anthos. is not right.

Among the four options, App Engine Standard, Cloud Functions and Cloud Run can all scale down to zero. Cloud Run for Anthos can scale the pods down the zero but the number of nodes per cluster can not scale to zero so these nodes are billed in the absence of requests. This rules out Cloud Run for Anthos.

App Engine Standard. is not right.

App Engine Standard doesn’t offer an out of the box integration with Cloud Pub/Sub. We can use the Cloud Client Library to send and receive Pub/Sub messages as described in the note below but the key point to note is the absence of out of the box integration with Cloud Pub/Sub so this rules out App Engine Standard

Ref: <https://cloud.google.com/appengine/docs/standard/nodejs/writing-and-responding-to-pub-sub-messages>

Cloud Run. is not right.

Cloud Run is an excellent product and integrates with Cloud Pub/Sub for several use cases. For example, every time a new .csv file is created inside a Cloud Storage bucket, an event is fired and delivered via a Pub/Sub subscription to a Cloud Run service. The Cloud Run service extracts data from the file and stores it as structured data into a BigQuery table.

Ref: <https://cloud.google.com/run#section-7>

At the same time, we want to follow Google recommended practices. Google doesn’t list integration with Cloud Pub/Sub as a key feature of Cloud Run. Contrary to this, Google says “If you’re building a simple API (a small set of functions to be accessed via HTTP or Cloud Pub/Sub), we recommend using [Cloud Functions](https://cloud.google.com/functions/docs).”

Cloud Functions. is the right answer.

Cloud Functions is Google Cloud’s event-driven serverless compute platform that lets you run your code locally or in the cloud without having to provision servers. Cloud Functions scales up or down, so you pay only for compute resources you use. Cloud Functions have excellent integration with Cloud Pub/Sub, lets you scale down to zero and is recommended by Google as the ideal serverless platform to use when dependent on Cloud Pub/Sub.

“If you’re building a simple API (a small set of functions to be accessed via HTTP or Cloud Pub/Sub), we recommend using Cloud Functions.”

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

Bottom of Form

Top of Form

Question 30: Incorrect

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

​

Export audit logs to Cloud Storage via an export sink.

(Correct)

​

Create an account for auditors to have view access to Stackdriver Logging.

(Incorrect)

​

Generate a signed URL to the Stackdriver export destination for auditors to access.

(Correct)

​

Export audit logs to BigQuery via an export sink.

​

Export audit logs to Splunk via a Pub/Sub export sink.

Explanation

Create an account for auditors to have view access to Stackdriver Logging. is not right.

While it is possible to configure a custom retention period of 10 years in Stackdriver logging, storing logs in Stackdriver is expensive compared to Cloud Storage. Stackdriver charges $0.01 per GB per month, whereas something like Cloud Storage Coldline Storage costs $0.007 per GB per month (30% cheaper) and Cloud Storage Archive Storage costs 0.004 per GB per month (60% cheaper than Stackdriver)

Ref: https://cloud.google.com/logging/docs/storage#pricing

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

Export audit logs to BigQuery via an export sink. is not right.

Storing logs in BigQuery is expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.

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

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

Export audit logs to Cloud Filestore via a Pub/Sub export sink. is not right.

Storing logs in Cloud Filestore is expensive. In Cloud Filestore, Standard Tier pricing costs $0.2 per GB per month and Premium Tier pricing costs $0.3 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.

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

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

Export audit logs to Cloud Storage via an export sink. is the right answer.

Among all the storage solutions offered by Google Cloud Platform, Cloud storage offers the best pricing for long term storage of logs. Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.

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

Generate a signed URL to the Stackdriver export destination for auditors to access. is the right answer.

In Google Cloud Storage, you can generate a signed URL to provide limited permission and time to make a request. Anyone who possesses it can use the signed URL to perform specified actions, such as reading an object, within a specified period of time.

In our scenario, we do not need to create accounts for our auditors to provide access to logs in Cloud Storage. Instead, we can generate them signed URLs which are time-bound and lets them access/download log files.

Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

Bottom of Form

Top of Form

Question 31: Incorrect

Your company’s auditors carry out an annual audit every year and have asked you to provide them with all the IAM policy changes in Google Cloud since the last audit. You do not want to compromise on the security, and you want to streamline and expedite the analysis for audit. How should you share the information requested by auditors?

​

Enable Logging export to Google Cloud Storage (GCS) bucket and delegate access to the bucket

​

Enable Logging export to Google BigQuery and use ACLs and views to scope the data shared with the auditor

(Correct)

​

Create custom Google Stackdriver alerts and send them to the auditor

​

Use Cloud Functions to transfer log entries to Google Cloud SQL and use ACLs and views to limit an auditor's view

(Incorrect)

Explanation

Create custom Google Stackdriver alerts and send them in an email to the auditor. is not right.

Stackdriver Alerting gives timely awareness to problems in your cloud applications so you can resolve the problems quickly. Sending alerts to your auditor is not of much use during audits.

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

Use Cloud Functions to transfer log entries to Google Cloud SQL and use ACLs and views to limit an auditor's view. is not right.

Using Cloud Functions to transfer log entries to Google Cloud SQL is expensive in comparison to audit logs export feature which exports logs to various destinations with minimal configuration.

Ref: https://cloud.google.com/logging/docs/export/

Auditors spend a lot of time reviewing log messages. And you want to expedite the audit process!! So you want to make it easier for the auditor to extract the information easily from the logs.

Between the two remaining options, the only difference is the log export sink destination

Ref: https://cloud.google.com/logging/docs/export/

One option exports to Google Cloud Storage (GCS) bucket whereas other exports to BigQuery. Querying information out of files in a bucket is much harder compared to querying information from BigQuery Dataset where it is as simple as running a job or set of jobs to extract just the required information and in the format required. By enabling the auditor to run jobs in Big Queries, you streamline the log extraction process and the auditor can review the extracted logs much quicker. While as good as the other option (bucket) is, Enable Logging export to Google BigQuery and use ACLs and views to scope the data shared with the auditor is the right answer.

You need to configure log sinks before you can receive any logs, and you can’t retroactively export logs that were written before the sink was created.

Bottom of Form

Top of Form

Question 32: Incorrect

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

​

Create a Service of type ClusterIP for dispatch-order. Have create-order use the Service IP address.

(Correct)

​

Create a Service of type NodePort for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address.

​

Create a Service of type LoadBalancer for dispatch-order. Have create-order use the Service IP address.

​

Create a Service of type LoadBalancer for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address.

(Incorrect)

Explanation

Create a Service of type LoadBalancer for dispatch-order. Have create-order use the Service IP address. is not right.

When you create a Service of type LoadBalancer, the Google Cloud controller configures a network load balancer that is publicly available. Since we don't want our service to be publicly available, we shouldn't create a Service of type LoadBalancer

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

Create a Service of type LoadBalancer for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address. is not right.

When you create a Service of type LoadBalancer, the Google Cloud controller configures a network load balancer that is publicly available. Since we don't want our service to be publicly available, we shouldn't create a Service of type LoadBalancer

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

Create a Service of type NodePort for dispatch-order and an Ingress Resource for that Service. Have create-order use the Ingress IP address. is not right.

Exposes the Service on each Node’s IP at a static port (the NodePort). If the compute instance has public connectivity, the dispatch-order can be accessed publicly which is undesirable. Secondly, dispatch-order has auto-scaling enabled so we shouldn't create a service of NodePort. If autoscaler spins up another pod on the node, it fails to initialize as the port on the node is already taken by an existing pod on the same node.

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

Create a Service of type ClusterIP for dispatch-order. Have create-order use the Service IP address. is the right answer.

ClusterIP exposes the Service on a cluster-internal IP that is only reachable within the cluster. This satisfies our requirement that dispatch-order shouldn't be publicly accessible. create-order which is also located in the same GKE cluster can now access the ClusterIP of the service to reach dispatch-order.

Ref: https[://kubernetes.io/docs/concepts/services-networking/service/](https://kubernetes.io/docs/concepts/services-networking/service/)

Bottom of Form

Top of Form

Question 33: Incorrect

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

​

Cloud Pub/Sub, Cloud Dataflow, Cloud Dataproc

​

Cloud Pub/Sub, Cloud Dataflow, BigQuery

(Correct)

​

Cloud Pub/Sub, Cloud Dataflow, Cloud Dataprep

(Incorrect)

​

Stackdriver, Cloud Dataflow, BigQuery

Explanation

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

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

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

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

Next, you want to store these results. BigQuery is an ideal place to store these results as BigQuery supports the querying of streaming data in real-time. This assists in real-time predictive analytics.

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

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

Here’s more information from Google docs about the Stream analytics use case. Google recommends we use Dataflow along with Pub/Sub and BigQuery.

<https://cloud.google.com/dataflow#section-6>

Google’s [stream analytics](https://cloud.google.com/solutions/stream-analytics) makes data more organized, useful, and accessible from the instant it’s generated. Built on Dataflow along with Pub/Sub and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights. This abstracted provisioning reduces complexity and makes stream analytics accessible to both data analysts and data engineers.

and

<https://cloud.google.com/solutions/stream-analytics>

Ingest, process, and analyze event streams in real time. Stream analytics from Google Cloud makes data more organized, useful, and accessible from the instant it’s generated. Built on the autoscaling infrastructure of Pub/Sub, Dataflow, and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights.

Bottom of Form

Top of Form

Question 34: Correct

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

​

Cloud Functions

(Correct)

​

Google Compute Engine

​

Google App Engine

​

Google Kubernetes Engine

Explanation

Cloud Functions. is the right answer.

Cloud Functions is Google Cloud’s event-driven serverless compute platform. It automatically scales based on the load and requires no additional configuration. You pay only for the resources used.

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

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

Bottom of Form

Top of Form

Question 35: Correct

An application that you are migration to Google Cloud relies on overnight batch jobs that take between 2 to 3 hours to complete. You want to do this at a minimal cost. Where should you run these batch jobs?

​

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

(Correct)

​

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

​

Select GKE. Use a single node cluster with a small instance type

​

Select GKE. Use a three-node cluster with micro instance types.

Explanation

Requirements - achieve end goal while minimizing service costs.

Select GKE. Use a single node cluster with a small instance type is not right.

We do not know if a small instance is capable of handling all the batch volume. Plus this is not the most cost-effective of the options.

Select GKE. Use a three-node cluster with micro instance types is not right.

We do not know if three micro instances are capable of handling all the batch volume. Plus this is not the most cost-effective of the options.

Select Compute Engine. Use VM instance types that support micro bursting is not right.

We can use an instance that supports micro bursting but we have a job that runs for 2 hours. Bursting is suitable for short periods.

Select Compute Engine. Use preemptible VM instances of the appropriate standard machine types is the right answer.

We minimize the cost by selecting a preemptible instance of the appropriate type. If the preemptible instance is terminated, the next nightly run picks up the unprocessed volume.

Bottom of Form

Top of Form

Question 36: Correct

Your compliance department has asked you to share a compressed zip of sensitive audit logs with an external auditor. The external auditor does not have a Google account, and you want to remove the access after 4 hours. How can you do this with the least number of steps?

​

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

(Correct)

​

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

​

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

​

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

Explanation

Set object access to 'public' and use object lifecycle management to remove the object after four hours. is not right.

While the external company can access the public objects from the bucket, it doesn't stop bad actors from accessing the data as well. Since the data is "sensitive" and we want to follow a "secure method", we shouldn't do this.

Configure the storage bucket as a static website and furnish the object's URL to the company. Delete the object from the storage bucket after four hours. is not right.

The static website is public by default. While the external company can access the objects from the static website, it doesn't stop bad actors from accessing the data as well. Since the data is "sensitive" and we want to follow a "secure method", we shouldn't do this.

Create a new Cloud Storage bucket specifically for the external company to access. Copy the object to that bucket. Delete the bucket after four hours have passed. is not right.

Even if we were to create a separate bucket for the external company to access, since the company does not have a google account, the only way to have them access this separate bucket is by enabling public access which we can't because of the nature of data (sensitive) and is against standard security practices.

Create a signed URL with a four-hour expiration and share the URL with the company. is the right answer.

This is the only option that fits all requirements. When we generate a signed URL, we can specify an expiry and only users with the signed URL can view/download the objects, and they don't need a google account.

Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

This page provides an overview of signed URLs, which you use to give time-limited resource access to anyone in possession of the URL, regardless of whether they have a Google account.

Bottom of Form

Top of Form

Question 37: Correct

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

​

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

​

Use the gcloud compute ssh command.

(Correct)

​

Create a key with the ssh-keygen command. Then use the gcloud compute ssh command.

​

Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.

Explanation

Create a key with the ssh-keygen command. Upload the key to the instance. Run gcloud compute instances list to get the IP address of the instance, then use the ssh command. is not right.

This approach certainly works. You can create a key pair with ssh-keygen, update the instance metadata with the public key and SSH to the instance. But is it the easiest way to SSH to the instance with the fewest possible steps? Let’s explore other options to decide (you will see that there is another option that does the same with less effort). You can find more information about this option here: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#block-project-keys

Create a key with the ssh-keygen command. Then use the gcloud compute ssh command. is not right.

This works but is more work (having to create the key) than the answer. gcloud compute ssh ensures that the user's public SSH key is present in the project's metadata. If the user does not have a public SSH key, one is generated using ssh-keygen and added to the project’s metadata.

Run gcloud compute instances list to get the IP address of the instance, then use the ssh command. is not right.

We can get the IP of the instance by executing the gcloud compute instances list but unless an SSH is generated and updated in project metadata, you would not be able to SSH to the instance. User access to a Linux instance through third-party tools is determined by which public SSH keys are available to the instance. You can control the public SSH keys that are available to a Linux instance by editing metadata, which is where your public SSH keys and related information are stored.

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

Use the gcloud compute ssh command. is the right answer.

gcloud compute ssh ensures that the user's public SSH key is present in the project's metadata. If the user does not have a public SSH key, one is generated using ssh-keygen and added to the project’s metadata. This is similar to the other option where we copy the key explicitly to the project’s metadata but here it is done automatically for us. There are also security benefits with this approach. When we use gcloud compute ssh to connect to Linux instances, we are adding a layer of security by storing your host keys as guest attributes. Storing SSH host keys as guest attributes improve the security of your connections by helping to protect against vulnerabilities such as man-in-the-middle (MITM) attacks. On the initial boot of a VM instance, if guest attributes are enabled, Compute Engine stores your generated host keys as guest attributes. Compute Engine then uses these host keys that were stored during the initial boot to verify all subsequent connections to the VM instance.

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

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

Bottom of Form

Top of Form

Question 38: Correct

You work at a large organization where each team has a distinct role. The development team can create Google Cloud projects but can’t link them to a billing account – this role is reserved for the finance team, and the development team do not want finance team to make changes to their project resources. How should you configure IAM access controls to enable this?

​

Assign the finance team the Billing Account User role on the billing account and the Project Billing Manager role on the organization.

(Correct)

​

Assign the engineering team only the Billing Account User role on the billing account.

​

Assign the finance team only the Billing Account User role on the billing account.

​

Assign the engineering team the Billing Account User role on the billing account and the Project Billing Manager role on the organization.

Explanation

Assign the finance team only the Billing Account User role on the billing account. is not right.

In order to link a project to a billing account, you need the necessary roles at the project level as well as at the billing account level. In this scenario, we are granting just the Billing Account User role on the billing account to the Finance team which allows them to link projects to the billing account on which the role is granted. But we haven't granted them any role at the project level. So they would not be unable to link projects.

Assign the engineering team only the Billing Account User role on the billing account. is not right.

In order to link a project to a billing account, you need the necessary roles at the project level as well as at the billing account level. In this scenario, we are granting just the Billing Account User role on the billing account to the Engineering team which allows them to link projects to the billing account and our question clearly states we do not want to do that.

Assign the engineering team the Billing Account User role on the billing account and the Project Billing Manager role on the organization. is not right.

In order to link a project to a billing account, you need the necessary roles at the project level as well as at the billing account level. In this scenario, we are assigning the engineering team the Billing Account User role on the billing account which allows them to create new projects linked to the billing account on which the role is granted. We are also assigning them the Project Billing Manager role on the organization (trickles down to the project as well) which lets them attach the project to the billing account. But we don't want the engineering team to link projects to the billing account.

Assign the finance team the Billing Account User role on the billing account and the Project Billing Manager role on the organization. is the right answer.

In order to link a project to a billing account, you need the necessary roles at the project level as well as at the billing account level. In this scenario, we are assigning the finance team the Billing Account User role on the billing account which allows them to create new projects linked to the billing account on which the role is granted. We are also assigning them the Project Billing Manager role on the organization (trickles down to the project as well) which lets them attach the project to the billing account, but does not grant any rights over resources. This is exactly what we want.

Bottom of Form

Top of Form

Question 39: Incorrect

Your team is responsible for migration all legacy on-premises to Google Cloud. Your team is a big admirer of serverless and has chosen App Engine Standard as the preferred choice for compute workloads. Your manager asked you to migrate a legacy accounting application built in C++, but you realized C++ isn’t supported. What GCP compute services should you use instead? (Choose two answers)

​

Split your application into different functions. Deploy your application as separate cloud functions in Google Cloud Functions (GCP) environment.

​

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

(Correct)

​

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

(Correct)

​

Containerize your new application and deploy it to a App Engine flexible environment.

(Incorrect)

​

Containerize your new application and deploy it to a Google Kubernetes Engine environment.

Explanation

App engine standard currently supports Python, Java, Node.js, PHP, Ruby and Go.

Ref: https[://cloud.google.com/appengine/docs/standard/](https://cloud.google.com/appengine/docs/standard/)

The question already states C# isn’t supported by App Engine. Our requirement is to ensure we maintain the serverless aspect of our application.

Split your application into different functions. Deploy your application as separate cloud functions in Google Cloud Functions (GCP) environment is not right.

Cloud Functions is a serverless platform where you can run the code in the cloud without having to provision servers. You split your application functionality into multiple functions, and each of these is defined as a cloud function. Cloud Functions don’t support C#. Supported runtimes are Python, Node.js and Go.

Ref: https[://cloud.google.com/functions](https://cloud.google.com/functions)

Containerize your new application and deploy it to a App Engine flexible environment is not right.

While App Engine flexible lets us customize runtimes or provide our own runtime by supplying a custom Docker image or Dockerfile from the open-source community, it uses compute engine virtual machines so it is not serverless. Ref: https[://cloud.google.com/appengine/docs/flexible/](https://cloud.google.com/appengine/docs/flexible/)

Containerize your new application and deploy it to a Google Kubernetes Engine environment. is not right.

GKE i.e. Google Kubernetes Clusters uses compute engine virtual machines so it is not serverless.

Ref: https[://cloud.google.com/kubernetes-engine](https://cloud.google.com/kubernetes-engine)

Containerize your new application and deploy it to a Cloud Run environment. is the right answer.

Cloud Run is a fully managed compute platform that automatically scales your stateless containers. Cloud Run is serverless: it abstracts away all infrastructure management, so you can focus on what matters most—building great applications. Run your containers in fully managed Cloud Run or on [Anthos](https://cloud.google.com/anthos), which supports both Google Cloud and on‐premises environments. Cloud Run is built upon an open standard, [Knative](https://knative.dev/), enabling the portability of your applications.

Ref: https[://cloud.google.com/run](https://cloud.google.com/run)

Containerize your new application and deploy it to a Cloud Run on GKE environment. is the right answer.

Cloud Run implements the [Knative serving API](https://github.com/knative/serving/blob/master/docs/spec/spec.md), an open-source project to run serverless workloads on top of Kubernetes. That means you can deploy Cloud Run services anywhere Kubernetes runs. And if you need more control over your services (like access to GPU or more memory), you can also deploy these serverless containers in your own GKE cluster instead of using the fully managed environment. When using the fully managed environment, Cloud Run on GKE is serverless.

Ref: <https://cloud.google.com/blog/products/serverless/cloud-run-bringing-serverless-to-containers>

Bottom of Form

Top of Form

Question 40: Correct

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

​

1. Set env: flex in app.yaml

2. gcloud app deploy --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions migrate [NEW\_VERSION]

​

1. Set env: flex in app.yaml

2. gcloud app deploy --no-promote --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions migrate [NEW\_VERSION]

(Correct)

​

1. Set env: app-engine-flex in app.yaml

2. gcloud app deploy --no-promote --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions start [NEW\_VERSION]

​

1. Set env: app-engine-flex in app.yaml

2. gcloud app deploy --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions start [NEW\_VERSION]

Explanation

1. Set env: flex in app.yaml

2. gcloud app deploy --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions migrate [NEW\_VERSION]. is not right.

Executing gcloud app deploy --version=[NEW\_VERSION] without --no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.

Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

1. Set env: app-engine-flex in app.yaml

2. gcloud app deploy --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions start [NEW\_VERSION] is not right.

env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex. Also, Executing gcloud app deploy --version=[NEW\_VERSION] without --no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.

Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

1. Set env: app-engine-flex in app.yaml

2. gcloud app deploy --no-promote --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions start [NEW\_VERSION] is not right.

env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex.

Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

1. Set env: flex in app.yaml

2. gcloud app deploy --no-promote --version=[NEW\_VERSION]

3. Validate [NEW\_VERSION] in App Engine Flex

4. gcloud app versions migrate [NEW\_VERSION] is the right answer.

These commands together achieve the end goal while satisfying our requirements. Setting env: flex in app.yaml and executing gcloud app deploy --no-promote --version=[NEW\_VERSION] results in a new version deployed to flex engine. but the new version is not configured to serve traffic. We take the opportunity to review this version before migrating it to serve live traffic by running gcloud app versions migrate [NEW\_VERSION]

Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy

Bottom of Form

Top of Form

Question 41: Correct

You created a compute instance by running gcloud compute instances create instance1. You intended to create the instance in project gcp-ace-proj-266520 but the instance got created in a different project. Your cloud shell gcloud configuration is as shown.

$ gcloud config list

[component\_manager]

disable\_update\_check = True

[compute]

gce\_metadata\_read\_timeout\_sec = 5

zone = europe-west2-a

[core]

account = gcp-ace-lab-user@gmail.com

disable\_usage\_reporting = False

project = gcp-ace-lab-266520

[metrics]

environment = devshell

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

​

gcloud compute instances delete instance1

gcloud compute instances create instance1

​

gcloud compute instances delete instance1

gcloud config set compute/project gcp-ace-proj-266520

gcloud compute instances create instance1

​

gcloud config set project gcp-ace-proj-266520

gcloud compute instances recreate instance1 --previous-project gcp-ace-lab-266520

​

gcloud compute instances delete instance1

gcloud config set project gcp-ace-proj-266520

gcloud compute instances create instance1

(Correct)

Explanation

gcloud compute instances delete instance1

gcloud compute instances create instance1. is not right.

The default core/project property is set to gcp-ace-lab-266520 in our current configuration so the instance would have been created in this project. Running the first command to delete the instance correctly deletes it from this project but we haven't modified the core/project property before executing the second command so the instance is recreated in the same project which is not what we want.

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

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

gcloud config set project gcp-ace-proj-266520

gcloud compute instances recreate instance1 --previous-project gcp-ace-lab-266520. is not right.

gcloud compute instances command doesn't support recreate action. It supports create/delete which is what we are supposed to use for this requirement.

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

gcloud compute instances delete instance1

gcloud config set compute/project gcp-ace-proj-266520

gcloud compute instances create instance1. is not right.

The approach is right but the syntax is wrong. gcloud config does not have a compute/project property. The project property is part of the core/ section as seen in the output of gcloud configuration list in the question. In this scenario, we are trying to set compute/project property that doesn't exist in the compute section so the command fails.

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

gcloud compute instances delete instance1

gcloud config set project gcp-ace-proj-266520

gcloud compute instances create instance1. is the right answer.

This sequence of commands correctly deletes the instance from gcp-ace-lab-266520 which is the default project in the active gcloud configuration, then modifies the current configuration to set the default project to gcp-ace-proj-266520, and finally creates the instance in the project gcp-ace-proj-266520 which is the default project in active gcloud configuration at the time of running the command. This produces the intended outcome of deleting the instance from gcp-ace-lab-266520 project and recreating it in gcp-ace-prod-266520

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

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

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

Bottom of Form

Top of Form

Question 42: Incorrect

You have two Kubernetes resource configuration files.

deployments.yaml - creates a deployment

service.yaml - sets up a LoadBalancer service to expose the pods.

You don't have a GKE cluster in the development project and you need to provision one. Which of the commands fail with an error in Cloud Shell when you are attempting to create a GKE cluster and deploy the YAML configuration files to create a deployment and service. (Select Two)

​

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml,service.yaml

(Incorrect)

​

gcloud config set compute/zone us-central1-a

gcloud container clusters create cluster-1

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml

kubectl apply -f service.yaml

​

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f [deployment.yaml,service.yaml]

(Correct)

​

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml

kubectl apply -f service.yaml

​

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml&&service.yaml

(Correct)

Explanation

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml

kubectl apply -f service.yaml. is not right (i.e. commands executes successfully)

You create a cluster by running gcloud container clusters create command. You then fetch credentials for a running cluster by running gcloud container clusters get-credentials command. Finally, you apply the kubernetes resource configuration by running kubectl apply -f

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/create

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/get-credentials

Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml,service.yaml. is not right (i.e. commands executes successfully)

Like above, but the only difference is that both configurations are applied in the same statement. With kubectl apply, you can apply the configuration from a single file or multiple files or even a complete directory.

Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

gcloud config set compute/zone us-central1-a

gcloud container clusters create cluster-1

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.YAML

kubectl apply -f service.yaml. is not right (i.e. commands executes successfully)

Like above, but the only difference is in how the compute zone is set. In this scenario, you set the zone us-central1-a as the default zone so when you don't pass a zone property to the gcloud container clusters create command, it takes the default zone which is us-central1-a.

Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f [deployment.yaml,service.yaml]. is the right answer (i.e. commands fail)

kubectl apply can apply the configuration from a single file or multiple files or even a complete directory. When applying configuration from multiple files, the file names need to be separated by a comma. In this scenario, the filenames are passed as a list and Kubernetes treats the list as literal so looks for files "[deployment.yaml" and "service.yaml]" which it doesn't find.

Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

gcloud container clusters create cluster-1 --zone=us-central1-a

gcloud container clusters get-credentials cluster-1 --zone=us-central1-a

kubectl apply -f deployment.yaml&&service.yaml. is the right answer (i.e. commands fail)

kubectl apply can apply the configuration from a single file or multiple files or even a complete directory. When applying configuration from multiple files, the file names need to be separated by a comma. In this scenario, the filenames are separated by && and kubernetes treats the && as literal so it looks for the file "deployment.yaml&&service.yaml" which it doesn't find.

Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

Bottom of Form

Top of Form

Question 43: Correct

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

​

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

(Correct)

​

The internal IP address is disabled.

​

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

​

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

Explanation

The compute instances have a static IP for their internal IP. is not right.

Static internal IPs shouldn't be a reason for failed SSH connections. With all networking set up correctly, SSH works fine on Static internal IPs.

Ref: https://cloud.google.com/compute/docs/ip-addresses#networkaddresses

The internal IP address is disabled. is not right.

Every compute instance has one or more internal IP addresses so this option is not correct.

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

There is no such thing as cross region SSH IAM permissions.

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

The combination of compute instance network tags and VPC firewall rules can certainly result in SSH traffic being allowed on the external IP range but disabled from subnets IP range. The firewall rule can be configured to allow SSH traffic from 0.0.0.0/0 but deny traffic from the VPC range e.g. 10.0.0.0/8. In this case, all SSH traffic from within the VPC is denied but external SSH traffic (i.e. on external IP) is allowed.

Ref: https://cloud.google.com/vpc/docs/using-firewalls

Bottom of Form

Top of Form

Question 44: Correct

Your team is working towards using the desired state configuration for your application deployed on the GKE cluster. You have YAML files for the Kubernetes Deployment and Service objects. Your application is designed to have 2 pods, which is defined by the replicas parameter in app-deployment.yaml. Your service uses GKE Load Balancer which is defined in app-service.yaml

You created the Kubernetes resources by running

kubectl apply -f app-deployment.yaml

kubectl apply -f app-service.yaml

Your deployment is now serving live traffic but is suffering from performance issues. You want to increase the number of replicas to 5. What should you do in order to update the replicas in existing Kubernetes deployment objects?

​

Disregard the YAML file. Enable autoscaling on the deployment to trigger on CPU usage and set max pods to 5. kubectl autoscale myapp --max=5 --cpu-percent=80

​

Edit the number of replicas in the YAML file and rerun the kubectl apply. kubectl apply -f app-deployment.yaml

(Correct)

​

Modify the current configuration of the deployment by using kubectl edit to open the YAML file of the current configuration, modify and save the configuration. kubectl edit deployment/app-deployment -o yaml --save-config

​

Disregard the YAML file. Use the kubectl scale command to scale the replicas to 5. kubectl scale --replicas=5 -f app-deployment.yaml

Explanation

Disregard the YAML file. Use the kubectl scale command to scale the replicas to 5. kubectl scale --replicas=5 -f app-deployment.yaml. is not right.

While the outcome is the same, this approach doesn't update the change in the desired state configuration (YAML file). If you were to make some changes in your app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.

Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#scaling-a-deployment

Disregard the YAML file. Enable autoscaling on the deployment to trigger on CPU usage and set minimum pods as well as maximum pods to 5. kubectl autoscale myapp --min=5 --max=5 --cpu-percent=80. is not right.

While the outcome is the same, this approach doesn't update the change in the desired state configuration (YAML file). If you were to make some changes in your app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.

Ref: https://kubernetes.io/blog/2016/07/autoscaling-in-kubernetes/

Modify the current configuration of the deployment by using kubectl edit to open the YAML file of the current configuration, modify and save the configuration. kubectl edit deployment/app-deployment -o yaml --save-config. is not right.

Like the above, the outcome is the same. This is equivalent to first getting the resource, editing it in a text editor, and then applying the resource with the updated version. This approach doesn't update the replicas change in our local YAML file. If you were to make some changes in your local app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.

Ref: https://kubernetes.io/docs/concepts/cluster-administration/manage-deployment/#in-place-updates-of-resources

Edit the number of replicas in the YAML file and rerun the kubectl apply. kubectl apply -f app-deployment.yaml. is the right answer.

This is the only approach that guarantees that you use desired state configuration. By updating the YAML file to have 5 replicas and applying it using kubectl apply, you are preserving the intended state of Kubernetes cluster in the YAML file.

Ref: https://kubernetes.io/docs/concepts/cluster-administration/manage-deployment/#in-place-updates-of-resources

Bottom of Form

Top of Form

Question 45: Correct

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

​

Perform a rolling update to modify machine type from n1-standard-2 to n1-standard-4.

​

Enable autoscaling on Kubernetes Engine.

(Correct)

​

Enable Horizontal Pod Autoscaling for the Kubernetes deployment.

​

Create another identical Kubernetes workload and split traffic between the two workloads.

Explanation

Enable Horizontal Pod Autoscaling for the Kubernetes deployment. is not right.

Horizontal Pod Autoscaling can not be enabled for Daemon Sets, this is because there is only one instance of a pod per node in the cluster. In a replica deployment, when Horizontal Pod Autoscaling scales up, it can add pods to the same node or another node within the cluster. Since there can only be one pod per node in the Daemon Set workload, Horizontal Pod Autoscaling is not supported with Daemon Sets.

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

Create another identical Kubernetes cluster and split traffic between the two workloads. is not right.

Creating another identical Kubernetes cluster is going to double your costs; at the same time, there is no guarantee that this is enough to handle all the traffic. Finally, it doesn't satisfy our requirement of "cluster scales up and scales down automatically"

Perform a rolling update to modify machine type from n1-standard-2 to n1-standard-4. is not right.

While increasing the machine type from n1-standard-2 to n1-standard-4 gives the existing nodes more resources and processing power, we don't know if that would be enough to handle the increased volume of traffic. Also, it doesn't satisfy our requirement of "cluster scales up and scales down automatically"

Ref: https://cloud.google.com/compute/docs/machine-types

Enable autoscaling on Kubernetes Engine. is the right answer.

GKE's cluster autoscaler automatically resizes the number of nodes in a given node pool, based on the demands of your workloads. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed. DaemonSets attempt to adhere to a one-Pod-per-node model.

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

Bottom of Form

Top of Form

Question 46: Incorrect

You are enhancing a production application currently running on an Ubuntu Linux VM on Google Compute Engine. The new enhancements require a connection to SQL Server instance to persist user appointments. Your colleague has provisioned an SQL Server instance in a Google Compute Engine VM in US-Central region and has asked for your assistance to RDP to the VM in the least number of steps. What should you suggest?

​

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

(Correct)

​

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

(Incorrect)

​

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

​

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

Explanation

Requirements - Connect to compute instance using fewest steps. The presence of SQL Server 2017 on the instance is a red herring and should be ignored as none of the options provided say anything about the database and all seem to revolve around RDP.

Install a RDP client on your desktop. Verify that a firewall rule for port 3389 exists. is not right.

Although opening port 3389 is essential for serving RDP traffic, we do not have the credentials to RDP so this isn’t going to work.

Set a Windows password in the GCP Console. Verify that a firewall rule for port 22 exists. Click the RDP button in the GCP Console and supply the credentials to log in. is not right.

RDP uses port 3389 and not 22.

Ref: https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-rdp

Set a Windows username and password in the GCP Console. Verify that a firewall rule for port 3389 exists. Click the RDP button in the GCP Console, and supply the credentials to log in. is not right.

While this option correctly sets the username and password on the console and verifies a firewall rule is set on port 3389 to allow RDP traffic, you can RDP from console unless you install Chrome RDP for Google Cloud Platform extension in order to RDP from the console. (See Chrome Desktop for GCP tab in <https://cloud.google.com/compute/docs/instances/connecting-to-instance#windows>). If we assume that installing Chrome RDP for Google Cloud Platform extension is carried out (even though not specified in the option), we end up executing more steps in this option to successfully RDP compare to the correct answer (below)

Install an RDP client on your desktop. Set a Windows username and password in the GCP Console. Use the credentials to log in to the instance. is the right answer.

This option correctly sets the username/password which is essential. In addition, the default VPC comes with port 3389 open to the public. The question doesn’t explicitly state the compute engine is in a custom VPC so it is safe to assume we are using default VPC which has default RDP access open to the public. Finally, you install an RDP client on the desktop and use the credentials set up earlier to RDP to the server.

Bottom of Form

Top of Form

Question 47: Incorrect

Your manager asked you to write a script to upload objects to a Cloud Storage bucket. What IAM access do you need to set up in Google Cloud Platform to enable the shell script upload objects to Cloud Storage?

​

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

(Incorrect)

​

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

​

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

(Correct)

​

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

Explanation

Our requirements are

1. Google recommended practices

2. Multiple compute engine instances to write data to a bucket.

Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/devstorage.write\_only'. is not right.

You can't attach scope when creating service account.

Ref: https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/create

Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/cloud-platform'. is not right.

You can't attach scope when creating service account.

Ref: https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/create

Create a service account and add it to the IAM role 'storage.objectAdmin' for that bucket. is not right.

You need to provide Compute Engine instances permissions to write data into a particular Cloud Storage bucket. Storage Object Admin (roles/storage.objectAdmin) grants full control over objects, including listing, creating, viewing, and deleting objects. This falls foul of the principle of least privilege.

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

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

You need to provide Compute Engine instances permissions to write data into a particular Cloud Storage bucket. Storage Object Creator (roles/storage.objectCreator) allows users to create objects. Does not give permission to view, delete, or overwrite objects. This is the precise permission the VM instances need to write data to bucket. So we create a service account, add this IAM role and let the compute engine instances use this service account to write objects to the bucket.

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

Bottom of Form

Top of Form

Question 48: Correct

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

​

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

​

Add the finance team to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only.

​

Add the finance team to the Billing Account Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the Project.

(Correct)

​

Add the finance team to the Viewer role for the Project. Add the developers to the Security Reviewer role for each of the billing accounts.

Explanation

Add the finance team to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only. is not right.

Granting your finance team the default IAM role provides them permissions to manage roles and permissions for a project and subsequently use that to assign them the permissions to view/edit resources in all projects. This is against our requirements. Also, you can write a custom role that lets developers view their project spend but they are missing permissions to view project resources.

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

Add the developers and finance managers to the Viewer role for the Project. is not right.

Granting your finance team the Project viewer role lets them view resources in all projects and doesn’t let them set budgets - both are against our requirements.

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

Add the finance team to the Viewer role on all projects. Add the developers to the Security Reviewer role for each of the billing accounts. is not right.

Granting your finance team the Project viewer role lets them view resources in all projects which is against our requirements. Also, the security Reviewer role enables the developers to view custom roles but doesn’t let them view the project's costs or project resources.

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

Add the finance team to the Billing Account Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the Project. is the right answer.

Billing Account Administrator role is an owner role for a billing account. It provides permissions to manage payment instruments, configure billing exports, view cost information, set budgets, link and unlink projects and manage other user roles on the billing account.

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

Project viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data; including viewing the billing charges for the project.

https://cloud.google.com/iam/docs/understanding-roles#primitive\_roles

Bottom of Form

Top of Form

Question 49: Correct

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

​

Create JSON keys for the service account and execute gcloud authenticate service-account --key-file [KEY\_FILE]

​

Create JSON keys for the service account and execute gcloud auth activate-service-account --key-file [KEY\_FILE]

(Correct)

​

Create JSON keys for the service account and execute gcloud authenticate activate-service-account --key-file [KEY\_FILE]

​

Create JSON keys for the service account and execute gcloud auth service-account --key-file [KEY\_FILE]

Explanation

Create JSON keys for the service account and execute gcloud authenticate activate-service-account --key-file [KEY\_FILE]. is not right.

gcloud doesn't support using "authenticate" to grant/revoke credentials for Cloud SDK. The correct service is "auth".

Ref: https[://cloud.google.com/sdk/gcloud/reference/auth](https://cloud.google.com/sdk/gcloud/reference/auth)

Create JSON keys for the service account and execute gcloud authenticate service-account --key-file [KEY\_FILE]. is not right.

gcloud doesn't support using "authenticate" to grant/revoke credentials for Cloud SDK. The correct service is "auth".

Ref: https://cloud.google.com/sdk/gcloud/reference/auth

Create JSON keys for the service account and execute gcloud auth service-account --key-file [KEY\_FILE]. is not right.

gcloud auth does not support service-account action. The correct action to authenticate a service account is activate-service-account.

Ref: https://cloud.google.com/sdk/gcloud/reference/auth/activate-service-account

Create JSON keys for the service account and execute gcloud auth activate-service-account --key-file [KEY\_FILE]. is the right answer.

This command correctly authenticates access to Google Cloud Platform with a service account using its JSON key file. To allow gcloud (and other tools in Cloud SDK) to use service account credentials to make requests, use this command to import these credentials from a file that contains a private authorization key, and activate them for use in gcloud

Ref: <https://cloud.google.com/sdk/gcloud/reference/auth/activate-service-account>

Bottom of Form

Top of Form

Question 50: Correct

You deployed a Java application on four Google Cloud Compute Engine VMs in two zones behind a network load balancer. During peak usage, the application has stuck threads. This issue ultimately takes down the whole system and requires a reboot of all VMs. Your operations team have recently heard about self-healing mechanisms in Google Cloud and have asked you to identify if it is possible to automatically recreate the VMs if they remain unresponsive to requests for 2 minutes. What should you do?

​

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

(Correct)

​

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

​

Create a managed instance group. Verify that the auto-scaling setting is on.

​

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

Explanation

Create a managed instance group. Verify that the auto-scaling setting is on. is not right.

While auto-scaling capabilities of Managed instance groups let you automatically add or delete instances from a managed instance group based on increases or decreases in load, they don't help you with re-creation should the VMs go unresponsive.

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

Create a HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10 is not right.

You set RPS (Requests per Second) on load balancer when using RATE balancing mode. This has no effect on auto-healing.

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

Create a HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP) is not right.

The health checks defined on the load balancer determine whether VM instances respond properly to traffic. This has no impact on auto-healing. It is important to note that the health checks defined on the load balancer are different to the health checks defined on the auto-healing for managed instances group - see the explanation in the right answer for more information.

Ref: https://cloud.google.com/load-balancing/docs/health-checks#create\_a\_health\_check

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

In order to enable auto-healing, you need to group the instances into a managed instance group. Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An auto-healing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.

It is important to use separate health checks for load balancing and for auto-healing. Health checks for load balancing can and should be more aggressive because these health checks determine whether an instance receives user traffic. You want to catch non-responsive instances quickly, so you can redirect traffic if necessary. In contrast, health checking for auto-healing causes Compute Engine to proactively replace failing instances, so this health check should be more conservative than a load balancing health check.