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

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

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

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

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

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

Premium Practice Test 3 (Updated October 2020) - Results

Return to review

Created with Highcharts 6.1.0

Attempt 1

All questions

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

[Correct](javascript:void(0))

[Incorrect](javascript:void(0))

[Skipped](javascript:void(0))

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

Top of Form

Question 1: Incorrect

You have developed an enhancement to a production application deployed in App Engine Standard service. Unit testing and user acceptance testing has succeeded, and you deployed the new version to production. Users have started complaining of slow performance after the recent update, and you need to revert to the previous version immediately. How can you do this?

​

On the App Engine page of the GCP Console, select the application that needs to be reverted and click Revert.

​

Deploy the original version as a separate application. Then go to App Engine settings and split traffic between applications so that the original version serves 100% of the requests.

(Incorrect)

​

On the App Engine Versions page of the GCP Console, route 100% of the traffic to the previous version.

(Correct)

​

Run gcloud app restore.

Explanation

Run gcloud app restore. is not right.

restore action is not supported by gcloud app command.

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

On the App Engine page of the GCP Console, select the application that needs to be reverted and click Revert. is not right.

Revert option is not present on the App Engine page of the GCP Console.

Deploy the original version as a separate application. Then go to App Engine settings and split traffic between applications so that the original version serves 100% of the requests. is not right.

Each application in the app engine is different and it is not possible to split traffic between applications in App Engine. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service but not across applications.

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

On the App Engine Versions page of the GCP Console, route 100% of the traffic to the previous version. is the right answer

You can roll back to a previous version in the app engine GCP console. Go back to the list of versions and check the box next to the version that you want to receive all traffic and click the MAKE DEFAULT button located above the list. Traffic immediately switches over to the selected version.

Ref: https://cloud.google.com/community/tutorials/how-to-roll-your-app-engine-managed-vms-app-back-to-a-previous-version-part-1

Bottom of Form

Top of Form

Question 2: Correct

Your company has an App Engine application that needs to store stateful data in a proper storage service. Your data is non-relational data. You do not expect the database size to grow beyond 10 GB and you need to have the ability to scale down to zero to avoid unnecessary costs. Which storage service should you use?

​

Cloud SQL

​

Cloud Datastore

(Correct)

​

Cloud Bigtable

​

Cloud Dataproc

Explanation

Cloud SQL. is not right.

Cloud SQL is not suitable for non-relational data. Cloud SQL is a fully-managed database service that makes it easy to set up, maintain, manage, and administer your relational databases on Google Cloud Platform

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

Cloud Dataproc. is not right.

Cloud Dataproc is a fast, easy-to-use, fully managed cloud service for running Apache Spark and Apache Hadoop clusters in a simple, cost-efficient way. It is not a database.

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

Cloud Bigtable. is not right.

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

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

Cloud Datastore. is the right answer.

Cloud Datastore is a highly-scalable NoSQL database. Cloud Datastore scales seamlessly and automatically with your data, allowing applications to maintain high performance as they receive more traffic; automatically scales back when the traffic reduces.

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

Bottom of Form

Top of Form

Question 3: Correct

You want to find a list of regions and the prebuilt images offered by Google Compute Engine. Which commands should you execute to retrieve this information?

​

gcloud compute regions list

gcloud images list

​

gcloud compute regions list

gcloud compute images list

(Correct)

​

gcloud regions list

gcloud compute images list

​

gcloud regions list

gcloud images list

Explanation

gcloud regions list.

gcloud images list. is not right.

The correct command to list compute regions is gcloud compute regions list.

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

The correct command to list compute images is gcloud compute images list.

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

gcloud compute regions list

gcloud images list. is not right.

The correct command to list compute images is gcloud compute images list.

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

gcloud regions list

gcloud compute images list. is not right.

The correct command to list compute regions is gcloud compute regions list.

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

gcloud compute regions list

gcloud compute images list. is the right answer.

Both the commands correctly retrieve images and regions offered by Google Compute Engine

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

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

Bottom of Form

Top of Form

Question 4: Incorrect

Your operations team have deployed an update to a production application running in Google Cloud App Engine Standard service. The deployment was successful, but your operations are unable to find this deployment in the production GCP project. What should you do?

​

Check the web application XML file for your application and check project settings

​

Go to Cloud Shell and run gcloud config list to review the Google Cloud configurations used for deployment.

(Correct)

​

Check the app YAML file for your application and check the project settings.

(Incorrect)

​

Go to Deployment Manager and review settings for the deployment of application

Explanation

Check the app YAML file for your application and check the project settings. is not right.

The Yaml file of application does not hold Google project information.

Check the web application XML file for your application and check project settings. is not right.

The web application file of the application does not hold Google project information.

Go to Deployment Manager and review settings for the deployment of the application. is not right.

Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format using yaml. In this scenario, we haven't used Cloud Deployment Manager to deploy. The app was deployed using gcloud app deploy so this option is not right.

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

Go to Cloud Shell and run gcloud config list to review the Google Cloud configurations used for deployment. is the right answer.

If the deployment was successful but it did not deploy to the intended project, it is likely that the gcloud app deploy command deployed the application to a different project. In the same gcloud shell, you can identify the current properties of the configuration by executing gcloud config list. This returns config properties such as project, account etc, as well as app-specific properties such as app/promote\_by\_default, app/stop\_previous\_version.

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

Bottom of Form

Top of Form

Question 5: Skipped

Your company is migration all applications from the on-premises data centre to Google Cloud, and one of the applications is dependent on Websockets protocol. You want to ensure this application can be migrated to Google Cloud platform and continue serving requests without issues. What should you do?

​

Redesign the application to use a distributed user session service that does not rely on WebSockets and HTTP sessions.

​

Convert the WebSocket code to use HTTP streaming.

​

Meet with the cloud enablement team to discuss load balancer options.

(Correct)

​

Review the encryption requirements for WebSocket connections with the security team.

Explanation

Google HTTP(S) Load Balancing has native support for the WebSocket protocol when you use HTTP or HTTPS, not HTTP/2, as the protocol to the backend.

Ref: https://cloud.google.com/load-balancing/docs/https#websocket\_proxy\_support

So the next possible step is to Meet with the cloud enablement team to discuss load balancer options.

We don't need to convert WebSocket code to use HTTP streaming or Redesign the application, as WebSocket support is offered by Google HTTP(S) Load Balancing. Reviewing the encryption requirements is a good idea but it has nothing to do with WebSockets.

Bottom of Form

Top of Form

Question 6: Incorrect

The application development team at your company wants to know the biggest CIDR range possible for a VPC and has asked for your suggestion. Your operations team is averse to using any beta features. What should you suggest?

​

10.0.0.0/8

(Correct)

​

0.0.0.0/0

​

172.16.0.0/12

​

192.168.0.0/16

(Incorrect)

Explanation

The private network range is defined by IETF (Ref: https[://tools.ietf.org/html/rfc1918](https://tools.ietf.org/html/rfc1918)) and adhered to by all cloud providers. The supported internal IP Address ranges are

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

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

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

10.0.0.0/8 gives you the largest range - 16777216 IP Addresses.

Bottom of Form

Top of Form

Question 7: Incorrect

You want to use Google Cloud Storage to host a static website on www.example.com for your staff. You created a bucket example-static-website and uploaded index.html and css files to it. You turned on static website hosting on the bucket and set up a CNAME record on www.example.com to point to c.storage.googleapis.com. You access the static website by navigating to www.example.com in the browser but your index page is not displayed. What should you do?

​

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

(Correct)

​

In example.com zone, modify the CNAME record to c.storage.googleapis.com/example-static-website.

​

In example.com zone, delete the existing CNAME record and set up an A record instead to point to c.storage.googleapis.com.

(Incorrect)

​

Reload the Cloud Storage static website server to load the objects.

Explanation

In example.com zone, modify the CNAME record to c.storage.googleapis.com/example-static-website. is not right.

CNAME records cannot contain paths. There is nothing wrong with the current CNAME record.

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

A records cannot use hostnames. A records use IP Addresses.

Reload the Cloud Storage static website server to load the objects. is not right.

There is no such thing as a Cloud Storage static website server. All infrastructure that underpins the static websites is handled by Google Cloud Platform.

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

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

NAME TYPE DATA

www.example.com CNAME c.storage.googleapis.com.

Ref: https://cloud.google.com/storage/docs/hosting-static-website

Bottom of Form

Top of Form

Question 8: Incorrect

You plan to deploy an application on an autoscaled managed instances group. The application uses a tomcat server and runs on port 8080. You want to access the application on https://www.example.com. You want to follow Google recommended practices. What services would you use?

​

Google Domains, Cloud DNS, HTTP(S) Load Balancer

(Correct)

​

Google Domains, Cloud DNS private zone, SSL Proxy Load Balancer

​

Google DNS, Google CDN, SSL Proxy Load Balancer

​

Google Domains, Cloud DNS private zone, HTTP(S) Load Balancer

(Incorrect)

Explanation

To serve traffic on https://www.example.com, we have to first own the domain example.com. We can use Google Domains service to register a domain.

Ref: <https://domains.google/>

Once we own example.com domain, we need to create a zone www.example.com. We can use Cloud DNS, which is a scalable, reliable, and managed authoritative Domain Name System (DNS) to create a DNS zone.

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

Once the www.example.com zone is set up, we need to create a DNS (A) record to point to the public IP of the Load Balancer. This is also carried out in Cloud DNS.

Finally, we need a load balancer to front the autoscaled managed instances group. Google recommends we use HTTP(S) Load Balancer for this requirement as "SSL Proxy Load Balancing is intended for non-HTTP(S) traffic. For HTTP(S) traffic, we recommend that you use HTTP(S) Load Balancing."

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

So the correct answer is Google Domains, Cloud DNS, HTTP(S) Load Balancer

Bottom of Form

Top of Form

Question 9: Correct

The deployment team currently spends a lot of time creating and configuring resources in Google Cloud Console, and feel they could be more productive and consistent if they can achieve the same result using Infrastructure as Code. You want to help them identify a suitable service. What should you recommend?

​

Cloud Composer

​

Unmanaged Instance Group

​

Managed Instance Group

​

Deployment Manager

(Correct)

Explanation

Unmanaged Instance Group. is not right.

Unmanaged instance groups let you load balance across a fleet of VMs that you manage yourself. But it doesn't help with dynamically provisioning VMs.

Ref: https://cloud.google.com/compute/docs/instance-groups#unmanaged\_instance\_groups

Cloud Composer. is not right.

Cloud Composer is a fully managed workflow orchestration service that empowers you to author, schedule, and monitor pipelines that span across clouds and on-premises data centers. Cloud Composer is deeply integrated within the Google Cloud Platform, giving users the ability to orchestrate their full pipeline. Cloud Composer has robust, built-in integration with many products, including BigQuery, Cloud Dataflow, Cloud Dataproc, Cloud Datastore, Cloud Storage, Cloud Pub/Sub, and AI Platform.

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

Managed Instance Group. is not right.

Managed instance groups (MIGs) let you operate apps on multiple identical VMs. You can make your workloads scalable and highly available by taking advantage of automated MIG services, including autoscaling, autohealing, regional (multiple zones) deployment, and automatic updating. While MIG dynamically provisions virtual machines based on scaling policy, it doesn't satisfy our requirement of "dedicated configuration file"

Ref: https://cloud.google.com/compute/docs/instance-groups#managed\_instance\_groups

Deployment Manager. is the right answer.

Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format using YAML. You can also use Python or Jinja2 templates to parameterize the configuration and allow reuse of common deployment paradigms such as a load-balanced, auto-scaled instance group. You can deploy many resources at one time, in parallel. Using the deployment manager, you can apply a Python/Jinja2 template to create a MIG/auto-scaling policy that dynamically provisions VM. And our other requirement of "dedicated configuration file" is also met. Using the deployment manager for provisioning results in a repeatable deployment process. By creating configuration files that define the resources, the process of creating those resources can be repeated over and over with consistent results. Google recommends we script our infrastructure and deploy using Deployment Manager

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

Bottom of Form

Top of Form

Question 10: Correct

You are the operations manager at your company, and you have been requested to provide administrative access to the virtual machines in the development GCP project for all members of the development team. There are over a hundred VM instances, and everyone at your company has a Google account. How can you simplify this access request while ensuring you can audit logins if needed?

​

Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key in the metadata of each instance.

​

Ask each member of the team to generate a new SSH key pair and to send you their public key. Use a configuration management tool to deploy those keys on each instance.

​

Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key as a project-wide public SSH key in your Cloud Platform project and allow project-wide public SSH keys on each instance.

​

Ask each member of the team to generate a new SSH key pair and to add the public key to their Google account. Grant the "compute.osAdminLogin" role to the Google group corresponding to this team.

(Correct)

Explanation

Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key in the metadata of each instance. is not right.

Reuse of a single SSH key pair by all employees is a very bad security practice as auditing becomes very impossible.

Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key as a project-wide public SSH key in your Cloud Platform project and allow project-wide public SSH keys on each instance. is not right.

Reuse of a single SSH key pair by all employees is a very bad security practice as auditing becomes very impossible.

Ask each member of the team to generate a new SSH key pair and to send you their public key. Use a configuration management tool to deploy those keys on each instance. is not right.

While this can be done, it is not operationally efficient. Let's say a user leaves the company, you then have to remove their SSH key from all instances where it has been added (can't be removed at a single place). Similarly, when a user joins the company, you have to add their SSH key to all the instances. This is very tedious and not operationally efficient.

Ask each member of the team to generate a new SSH key pair and to add the public key to their Google account. Grant the "compute.osAdminLogin" role to the Google group corresponding to this team. is the right answer.

By letting users manage their own SSH key pair (and it's rotation etc), you delete the operational burden of managing SSH keys to individual users. Secondly, granting compute.osAdminLogin grants the group administrator permissions (as opposed to granting compute.osLogin, which does not grant administrator permissions). Finally, managing provisioning and de-provisioning is as simple as adding or removing the user from the group.

OS Login lets you use Compute Engine IAM roles to efficiently manage SSH access to Linux instances and is an alternative to manually managing instance access by adding and removing SSH keys in the metadata. Before you can manage instance access using IAM roles, you must enable the OS Login feature by setting a metadata key-value pair in your project or in your instance's metadata: enable-oslogin=TRUE. After you enable OS Login on one or more instances in your project, those instances accept connections only from user accounts that have the necessary IAM roles in your project or organization. There are two predefined roles.

● roles/compute.osLogin, which does not grant administrator permissions

● roles/compute.osAdminLogin, which grants administrator permissions

At any point, to revoke user access to instances that are enabled to use OS Login, remove the user roles from that user account

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

Bottom of Form

Top of Form

Question 11: Correct

You deployed your application to a default node pool on the GKE cluster and you want to configure cluster autoscaling for this GKE cluster. For your application to be profitable, you must limit the number of Kubernetes nodes to 10. You want to start small and scale up as traffic increases and scale down when the traffic goes down. What should you do?

​

To enable autoscaling, add a tag to the instances in the cluster by running the command gcloud compute instances add-tags [INSTANCE] --tags=enable-autoscaling,min-nodes=1,max-nodes=10

​

Create a new GKE cluster by running the command gcloud container clusters create [CLUSTER\_NAME] --enable-autoscaling --min-nodes=1 --max-nodes=10. Redeploy your application

​

Update existing GKE cluster to enable autoscaling by running the command gcloud container clusters update [CLUSTER\_NAME] --enable-autoscaling --min-nodes=1 --max-nodes=10

(Correct)

​

Set up a stack driver alert to detect slowness in the application. When the alert is triggered, increase nodes in the cluster by running the command gcloud container clusters resize CLUSTER\_Name --size <new size>.

Explanation

Set up a stack driver alert to detect slowness in the application. When the alert is triggered, increase nodes in the cluster by running the command gcloud container clusters resize CLUSTER\_Name --size <new size>. is not right.

The command gcloud container clusters resize command resizes an existing cluster for running containers. While it is possible to manually increase the number of nodes in the cluster by running the command, the scale-up is not automatic, it is a manual process. Also, there is no scale down so it doesn’t fit our requirement of "scale up as traffic increases and scale down when the traffic goes down".

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

To enable autoscaling, add a tag to the instances in the cluster by running the command gcloud compute instances add-tags [INSTANCE] --tags=enable-autoscaling,min-nodes=1,max-nodes=10. is not right.

Autoscaling can not be enabled on the GKE cluster by adding tags on compute instances. Autoscaling can be enabled at the time of creating the cluster and can also be enabled for existing clusters by running one of the gcloud container clusters to create/update commands.

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

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

Create a new GKE cluster by running the command gcloud container clusters create [CLUSTER\_NAME] --enable-autoscaling --min-nodes=1 --max-nodes=10. Redeploy your application. is not right.

The command gcloud container clusters create - creates a GKE cluster and the flag --enable-autoscaling enables autoscaling and the parameters --min-nodes=1 --max-nodes=10 define the minimum and maximum number of nodes in the node pool. However, we want to configure cluster autoscaling for the existing GKE cluster; not create a new GKE cluster.

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

Update existing GKE cluster to enable autoscaling by running the command gcloud container clusters update [CLUSTER\_NAME] --enable-autoscaling --min-nodes=1 --max-nodes=10. is the right answer.

The command gcloud container clusters update - updates an existing GKE cluster. The flag --enable-autoscaling enables autoscaling and the parameters --min-nodes=1 --max-nodes=10 define the minimum and maximum number of nodes in the node pool. This enables cluster autoscaling which scales up and scales down the nodes automatically between 1 and 10 nodes in the node pool.

Bottom of Form

Top of Form

Question 12: Correct

You work for a leading retail platform that enables its retailers to sell their items to over 200 million users worldwide. You persist all analytics data captured during user navigation to BigQuery. A business analyst wants to run a query to identify products that were popular with buyers in the recent thanksgiving sale. The analyst understands the query needs to iterate through billions of rows to fetch the required information but is not sure of the costs involved in the on-demand pricing model, and has asked you to help estimate the query cost. What should you do?

​

Run a select count (\*) to get an idea of how many records your query will look through. Then convert that number of rows to dollars using the Pricing Calculator.

​

Use the command line to run a dry run query to estimate the number of bytes read. Then convert that bytes estimate to dollars using the Pricing Calculator.

(Correct)

​

Use the command line to run a dry run query to estimate the number of bytes returned. Then convert that bytes estimate to dollars using the Pricing Calculator.

​

Arrange to switch to Flat-Rate pricing for this query, then move back to on-demand.

Explanation

Arrange to switch to Flat-Rate pricing for this query, then move back to on-demand. is not right.

The cost of acquiring a big query slot (associated with flat-rate pricing) is significantly higher than our requirement here to run a single important query or just to know how much it would cost to run that query. BigQuery offers flat-rate pricing for customers who prefer a stable monthly cost for queries rather than paying the on-demand price per TB of data processed. You enroll in flat-rate pricing by purchasing slot commitments, measured in BigQuery slots. Slot commitments start at 500 slots and the price starts from $10000. Your queries consume this slot capacity, and you are not billed for bytes processed.

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

Use the command line to run a dry run query to estimate the number of bytes returned. Then convert that bytes estimate to dollars using the Pricing Calculator. is not right.

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

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

Run a select count (\*) to get an idea of how many records your query will look through. Then convert that number of rows to dollars using the Pricing Calculator. is not right.

This is not as practical as identifying the number of records your query will look through (i.e. scan/process) is not straightforward. Plus BigQuery supports external data sources such as Cloud Storage, Google Drive, or Cloud Bigtable; and the developer cost associated with identifying this information from various data sources is significant, not practical and sometimes not possible.

Use the command line to run a dry run query to estimate the number of bytes read. Then convert that bytes estimate to dollars using the Pricing Calculator. is the right answer.

BigQuery pricing is based on the number of bytes processed/read. Under on-demand pricing, BigQuery charges for queries by using one metric: the number of bytes processed (also referred to as bytes read). You are charged for the number of bytes processed whether the data is stored in BigQuery or in an external data source such as Cloud Storage, Google Drive, or Cloud Bigtable. On-demand pricing is based solely on usage.

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

Bottom of Form

Top of Form

Question 13: Correct

Your company has migrated most of the data center VMs to Google Compute Engine. The remaining VMs in the data center host legacy applications that are due to be decommissioned soon and your company has decided to retain them in the datacenter. Due to a change in the business operational model, you need to introduce changes to one of the legacy applications to read files from Google Cloud Storage. However, your data center does not have access to the internet and your company doesn't want to invest in setting up internet access as the data center is due to be turned off soon. Your data center has a partner interconnect to GCP. You wish to route traffic from your datacenter to Google Storage through partner interconnect. What should you do?

​

1. In on-premises DNS configuration, map storage.cloud.google.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel.

3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway.

4. Created a Cloud DNS managed private zone for storage.cloud.google.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

​

1. In on-premises DNS configuration, map storage.cloud.google.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel.

3. Created a Cloud DNS managed public zone for storage.cloud.google.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

​

1. In on-premises DNS configuration, map \*.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel.

3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway.

4. Created a Cloud DNS managed private zone for \*.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

(Correct)

​

1. In on-premises DNS configuration, map \*.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel.

3. Created a Cloud DNS managed public zone for \*.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

Explanation

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

Ref: <https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity>

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

The main differences between the remaining two options are

1. Static route in the VPC network.

2. Public/Private zone.

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

So, the right answer is

1. In on-premises DNS configuration, map \*.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

2. Configure Cloud Router to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel.

3. Add a custom static route to the VPC network to direct traffic with the destination 199.36.153.4/30 to the default internet gateway.

4. Created a Cloud DNS managed private zone for \*.googleapis.com that maps to 199.36.153.4/30 and authorize the zone for use by VPC network

Here’s more information about how to set up private connectivity to Google’s services through VPC.

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

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

● The on-premises DNS configuration maps \*.googleapis.com requests to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

● Cloud Router has been configured to advertise the 199.36.153.4/30 IP address range through the Cloud VPN tunnel by using a custom route advertisement. Traffic going to Google APIs is routed through the tunnel to the VPC network.

● A custom static route was added to the VPC network that directs traffic with the destination 199.36.153.4/30 to the default internet gateway (as the next hop). Google then routes traffic to the appropriate API or service.

If you created a Cloud DNS managed private zone for \*.googleapis.com that maps to 199.36.153.4/30 and have authorized that zone for use by your VPC network, requests to anything in the googleapis.com domain are sent to the IP addresses that are used by restricted.googleapis.com

Bottom of Form

Top of Form

Question 14: Incorrect

Your company recently migrated all infrastructure to Google Cloud Platform (GCP) and you want to use Google Cloud Build to build all container images. You want to store the build logs in Google Cloud Storage. You also have a requirement to push the images to Google Container Registry. You wrote a cloud build YAML configuration file with the following contents.

steps:

- name: 'gcr.io/cloud-builders/docker'

args: ['build', '-t', 'gcr.io/[PROJECT\_ID]/[IMAGE\_NAME]', '.']

images: ['gcr.io/[PROJECT\_ID]/[IMAGE\_NAME]']

How should you execute Cloud build to satisfy these requirements?

​

Execute gcloud builds run --config=[CONFIG\_FILE\_PATH] --gcs-log-dir=[GCS\_LOG\_DIR] [SOURCE]

​

Execute gcloud builds push --config=[CONFIG\_FILE\_PATH] [SOURCE]

​

Execute gcloud builds submit --config=[CONFIG\_FILE\_PATH] [SOURCE]

(Incorrect)

​

Execute gcloud builds submit --config=[CONFIG\_FILE\_PATH] --gcs-log-dir=[GCS\_LOG\_DIR] [SOURCE]

(Correct)

Explanation

Execute gcloud builds push --config=[CONFIG\_FILE\_PATH] [SOURCE]. is not right.

gcloud builds command does not support push operation. The correct operation to build images and push them to gcr is submit.

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

Execute gcloud builds run --config=[CONFIG\_FILE\_PATH] --gcs-log-dir=[GCS\_LOG\_DIR] [SOURCE]. is not right.

gcloud builds command does not support run operation. The correct operation to build images and push them to gcr is submit.

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

Execute gcloud builds submit --config=[CONFIG\_FILE\_PATH] [SOURCE]. is not right.

This command correctly builds the container image and pushes the image to GCR (Google Container Registry) but doesn’t upload the build logs to Google Cloud Storage which is one of our requirements.

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

Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

Execute gcloud builds submit --config=[CONFIG\_FILE\_PATH] --gcs-log-dir=[GCS\_LOG\_DIR] [SOURCE]. is the right answer.

This command correctly builds the container image, pushes the image to GCR (Google Container Registry) and uploads the build logs to Google Cloud Storage.

--config flag specifies the YAML or JSON file to use as the build configuration file.

--gcs-log-dir specifies the directory in Google Cloud Storage to hold build logs.

[SOURCE] is the location of the source to build. The location can be a directory on a local disk or a gzipped archive file (.tar.gz) in Google Cloud Storage.

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

Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

Bottom of Form

Top of Form

Question 15: Correct

Your company produces documentary videos for a reputed television channel and stores its videos in Google Cloud Storage for long term archival. Videos older than 90 days are accessed only in exceptional circumstances and videos older than one year are no longer needed. How should you optimise the storage to reduce costs?

​

Use gsutil rewrite and set the Delete action to 365 days.

​

Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days.

(Correct)

​

Use gsutil rewrite and set the Delete action to 275 days (365-90).

​

Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 275 days (365 - 90)

Explanation

Use gsutil rewrite and set the Delete action to 275 days (365-90). is not right.

gsutil rewrite is used to change the storage class of objects within a bucket through overwriting the object. It does not support Delete action.

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

Use gsutil rewrite and set the Delete action to 365 days. is not right.

gsutil rewrite is used to change the storage class of objects within a bucket through overwriting the object. It does not support Delete action.

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

Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 275 days (365 - 90). is not right.

Object Lifecycle Management does not rewrite an object when changing its storage class. This means that when an object is transitioned to Nearline Storage, Coldline Storage, or Archive Storage using the SetStorageClass feature, any subsequent early deletion and associated charges are based on the original creation time of the object, regardless of when the storage class changed.

If however, the change of storage class is done manually using a rewrite, the creation time of the objects is the new creation time since they are rewritten. In such a case, you would need to apply a lifecycle delete action of 275 days.

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

Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days. is the right answer.

Object Lifecycle Management does not rewrite an object when changing its storage class. This means that when an object is transitioned to Nearline Storage, Coldline Storage, or Archive Storage using the SetStorageClass feature, any subsequent early deletion and associated charges are based on the original creation time of the object, regardless of when the storage class changed.

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

Bottom of Form

Top of Form

Question 16: Correct

You are designing an application that lets users upload and share photos. You expect your application to grow really fast and you are targeting a worldwide audience. You want to delete uploaded photos after 30 days. You want to minimize costs while ensuring your application is highly available. Which GCP storage solution should you choose?

​

Cloud Datastore database.

​

Persistent SSD on VM instances.

​

Multiregional Cloud Storage bucket.

(Correct)

​

Cloud Filestore.

Explanation

Cloud Datastore database. is not right.

Cloud Datastore is a NoSQL document database built for automatic scaling, high performance, and ease of application development. We want to store objects/files and Cloud Datastore is not a suitable storage option for such data.

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

Cloud Filestore. is not right.

Cloud Filestore is a managed file storage service based on NFSv3 protocol. While Cloud Filestore can be used to store images, Cloud Filestore is a zonal service and can not scale easily to support a worldwide audience. Also, Cloud Filestore costs a lot (10 times) more than some of the storage classes offered by Google Cloud Storage.

Ref: https[://cloud.google.com/filestore](https://cloud.google.com/filestore), Ref: https://cloud.google.com/storage/pricing

Persistent SSD on VM instances. is not right.

Persistent SSD is a regional service and doesn't automatically scale to other regions to support a worldwide user base. Moreover, Persistent SSD disks are very expensive. A regional persistent SSD costs $0.34 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.

Ref: https://cloud.google.com/persistent-disk

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

Multiregional Cloud Storage bucket. is the right answer.

Cloud Storage allows world-wide storage and retrieval of any amount of data at any time. We don't need to set up auto-scaling ourselves. Cloud Storage autoscaling is managed by GCP. Cloud Storage is an object store so it is suitable for storing photos. Cloud Storage allows world-wide storage and retrieval so cater well to our worldwide audience. Cloud storage provides us lifecycle rules that can be configured to automatically delete objects older than 30 days. This also fits our requirements. Finally, 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 any of the options above.

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

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

Bottom of Form

Top of Form

Question 17: Correct

You want to deploy a python application to an autoscaled managed instance group on Compute Engine. You want to use GCP deployment manager to do this. What is the fastest way to get the application onto the instances without introducing undue complexity?

​

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

​

Include a startup script to bootstrap the python application when creating an instance template by running

gcloud compute instance-templates create app-template --startup-script=/scripts/install\_app.sh

​

Include a startup script to bootstrap the python application when creating an instance template by running

gcloud compute instance-templates create app-template --metadata-from-file startup-script=/scripts/install\_app.sh

(Correct)

​

Include a startup script to bootstrap the python application when creating an instance template by running

gcloud compute instance-templates create app-template --metadata-from-file startup-script-url=/scripts/install\_app.sh

Explanation

Include a startup script to bootstrap the python application when creating instance template by running

gcloud compute instance-templates create app-template --startup-script=/scripts/install\_app.sh. is not right.

gcloud compute instance-templates create command does not accept a flag called --startup-script. While creating compute engine images, the startup script can be provided through a special metadata key called startup-script which specifies a script that will be executed by the instances once they start running. For convenience, --metadata-from-file can be used to pull the value from a file.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instance-templates/create

Include a startup script to bootstrap the python application when creating instance template by running

gcloud compute instance-templates create app-template --metadata-from-file startup-script-url=/scripts/install\_app.sh. is not right.

startup-script-url is to be used when contents of the script need to be pulled from a publicly-accessible location on the web. But in this scenario, we are passing the location of the script on the filesystem which doesn't work and the command errors out.

$ gcloud compute instance-templates create app-template --metadata-from-file startup-script-url=/scripts/install\_app.sh

ERROR: (gcloud.compute.instance-templates.create) Unable to read file [/scripts/install\_app.sh]: [Errno 2] No such file or directory: '/scripts/install\_app.sh'

Once the instance starts up, connect over SSH and install the application. is not right.

The managed instances group has auto-scaling enabled. If we are to connect over SSH and install the application, we have to repeat this task on all current instances and on future instances the autoscaler adds to the group. This process is manual, error-prone, time consuming and should be avoided.

Include a startup script to bootstrap the python application when creating instance template by running

gcloud compute instance-templates create app-template --metadata-from-file startup-script=/scripts/install\_app.sh. is the right answer.

This command correctly provides the startup script using the flag metadata-from-file and providing a valid startup-script value. When creating compute engine images, the startup script can be provided through a special metadata key called startup-script which specifies a script that will be executed by the instances once they start running. For convenience, --metadata-from-file can be used to pull the value from a file.

Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instance-templates/create

Bottom of Form

Top of Form

Question 18: Correct

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

​

Deploy the new version in the same application and use the --splits option to give a weight of 99 to the current version and a weight of 1 to the new version.

(Correct)

​

Create a new App Engine application in the same project. Deploy the new version in that application. Configure your network load balancer to send 1% of the traffic to that new application.

​

Create a new App Engine application in the same project. Deploy the new version in that application. Use the App Engine library to proxy 1% of the requests to the new version.

​

Deploy the new version in the same application and use the --migrate option.

Explanation

Deploy the new version in the same application and use the --migrate option. is not right.

migrate is not a valid flag for the gcloud app deploy command.

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

Also, gcloud app versions migrate, which is a valid command to migrate traffic from one version to another for a set of services, is not suitable either as we only want to send 1% traffic.

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

Create a new App Engine application in the same project. Deploy the new version in that application. Use the App Engine library to proxy 1% of the requests to the new version. is not right.

While this can be done, we are increasing complexity and do not meet our requirement "minimize complexity". There is an out of the box option in the app engine to split traffic in a seamless way.

Create a new App Engine application in the same project. Deploy the new version in that application. Configure your network load balancer to send 1% of the traffic to that new application. is not right.

Instances that participate as backend VMs for network load balancers must be running the appropriate [Linux guest environment](https://cloud.google.com/compute/docs/instances/linux-guest-environment), [Windows guest environment](https://github.com/GoogleCloudPlatform/compute-image-windows), or other processes that provide equivalent functionality. Network load balancer is not suitable for App Engine standard environment which is container-based and provide us specific runtimes without any promise on the underlying guest environments.

Deploy the new version in the same application and use the --splits option to give a weight of 99 to the current version and a weight of 1 to the new version. is the right answer.

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

For this scenario, we can split the traffic as shown below, sending 1% to v2 and 99% to v1

by executing the command gcloud app services set-traffic service1 --splits v2=1,v1=99

Ref: https://cloud.google.com/sdk/gcloud/reference/app/services/set-traffic

Bottom of Form

Top of Form

Question 19: Correct

You are migrating a Python application from your on-premises data centre to Google Cloud. You modified the python application to use Cloud Pub/Sub instead of RabbitMQ. The application uses a specific service account which has the necessary publish and subscribe permissions on Cloud Pub/Sub, but the operations team have not enabled the Cloud Pub/Sub API yet. What should you do?

​

Use the Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed.

​

Enable the Cloud Pub/Sub API in the API Library on the GCP Console.

(Correct)

​

Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it.

​

Grant the App Engine default service account the role of Cloud Pub/Sub Admin. Have your application enable the API on the first connection to Cloud Pub/Sub.

Explanation

Requirements

1. We need to enable Cloud Pub/Sub API

2. Get our application to use the service account.

Grant the App Engine default service account the role of Cloud Pub/Sub Admin. Have your application enable the API on the first connection to Cloud Pub/Sub. is not right.

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

Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it. is not right.

There is no such thing as automatic enablement of the APIs when the service (Cloud Pub/Sub in this scenario) is accessed. APIs can be enabled through Google Cloud Console, gcloud command-line and REST API. See https://cloud.google.com/service-usage/docs/enable-disable for more information.

Use the Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed. is not right.

There is no such thing as automatic enablement of the APIs (Cloud Pub/Sub in this scenario) is accessed. APIs can be enabled through Google Cloud Console, gcloud command-line and REST API. See https://cloud.google.com/service-usage/docs/enable-disable for more information.

Enable the Cloud Pub/Sub API in the API Library on the GCP Console. is the right answer.

For most operational use cases, the simplest way to enable and disable services is to use the Google Cloud Console. you need to create scripts, you can also use the gcloud command-line interface. If you need to program against the Service Usage API, we recommend that you use one of our provided client libraries

Ref: https://cloud.google.com/service-usage/docs/enable-disable

Secondly, after you create an App Engine application, the App Engine default service account is created and used as the identity of the App Engine service. The App Engine default service account is associated with your Cloud project and executes tasks on behalf of your apps running in App Engine. By default, the App Engine default service account has the Editor role in the project so this already has the permissions to push/pull/receive messages from Cloud Pub/Sub

Bottom of Form

Top of Form

Question 20: Incorrect

You work for a multinational consumer credit reporting company that collects and aggregates financial information and provides a credit report for over 100 million individuals and businesses. The company wants to trial a new application for a small geography and requires a relational database for storing important user information. Your company places a high value on reliability and requires point-in-time recovery while minimizing operational cost. What should you select?

​

Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.

(Correct)

​

Select Cloud Spanner. Set up your instance as multi-regional.

​

Select Cloud Spanner. Set up your instance with 2 nodes.

​

Select Cloud SQL (MySQL). Select the create failover replicas option.

(Incorrect)

Explanation

Requirements

1. Cost effective

2. Relational Data

3. Small set of data

4. One location

5. Point in time recovery

Select Cloud Spanner. Set up your instance with 2 nodes. is not right.

Cloud spanner is a massively scalable, fully managed, relational database service for regional and global application data. Cloud spanner is expensive compared to Cloud SQL. We have a small set of data and we want to be cost-effective, so Cloud Spanner doesn't fit these requirements. Furthermore, Cloud Spanner does not offer a "Point in time" recovery feature.

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

Select Cloud Spanner. Set up your instance as multi-regional. is not right.

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

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

Select Cloud SQL (MySQL). Select the create failover replicas option. is not right.

Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. But This option does not enable point in time recovery so our requirement to support point-in-time recovery is not met.

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

Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected. is the right answer

Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. And by enabling binary logging, we can enable point-in-time recovery which fits our requirement.

You must enable binary logging to use point-in-time recovery. Point-in-time recovery helps you recover an instance to a specific point in time. For example, if an error causes a loss of data, you can recover a database to its state before the error occurred.

Ref: https://cloud.google.com/sql/docs/mysql/backup-recovery/backups#tips-pitr

Bottom of Form

Top of Form

Question 21: Incorrect

You deployed a workload to your GKE cluster by running the command kubectl apply -f app.yaml. You also enabled a LoadBalancer service to expose the deployment by running kubectl apply -f service.yaml. Your pods are struggling due to increased load so you decided to enable horizontal pod autoscaler by running kubectl autoscale deployment [YOUR DEPLOYMENT] --cpu-percent=50 --min=1 --max=10. You noticed the autoscaler has launched several new pods but the new pods have failed with the message "Insufficient cpu". What should you do to resolve this issue?

​

Use "kubectl container clusters resize" to add more nodes to the node pool.

​

Use "gcloud container clusters resize" to add more nodes to the node pool.

(Correct)

​

Edit the managed instance group of the cluster and enable autoscaling.

(Incorrect)

​

Edit the managed instance group of the cluster and increase the number of VMs by 1.

Explanation

Use "kubectl container clusters resize" to add more nodes to the node pool. is not right.

kubectl doesn't support the command kubectl container clusters resize. You have to use gcloud container clusters resize to resize a cluster.

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

Edit the managed instance group of the cluster and increase the number of VMs by 1. is not right.

GKE Cluster does not use a managed instance group. Instead, the cluster master (control plan) handles the lifecycle of nodes in the node pools. The cluster master is responsible for managing the workloads' lifecycle, scaling, and upgrades. The master also manages network and storage resources for those workloads.

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

Edit the managed instance group of the cluster and enable autoscaling. is not right.

GKE Cluster does not use a managed instance group. Instead, the cluster master (control plan) handles the lifecycle of nodes in the node pools. The cluster master is responsible for managing the workloads' lifecycle, scaling, and upgrades. The master also manages network and storage resources for those workloads.

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

Use "gcloud container clusters resize" to add more nodes to the node pool. is the right answer.

Your pods are failing with "Insufficient cpu". This is because the existing nodes in the node pool are maxed out, therefore, you need to add more nodes to your node pool. For such scenarios, enabling cluster autoscaling is ideal, however, this is not in any of the answer options. In the absence of cluster autoscaling, the next best approach is to add more nodes to the cluster manually. This is achieved by running the command gcloud container clusters resize which resizes an existing cluster for running containers.

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

Bottom of Form

Top of Form

Question 22: Correct

You have a Cloud Function that is triggered every night by Cloud Scheduler. When triggered by the scheduler, the Cloud function creates a snapshot of VMs running in all projects in the department. Your team created a new project ptech-vm under the department hierarchy, and you now need to provide IAM access to the service account used by the Cloud Function so that it can create snapshots of VMs in ptech-vm project. You want to follow Google recommended practices. What should you do?

​

Download the private key from the service account, and add the private key to each VM's SSH keys.

​

Grant the service account the IAM Role of Compute Storage Admin in the project called ptech-vm.

(Correct)

​

Download the private key from the service account, and add it to each VMs custom metadata.

​

When creating the VMs, set the service account's API scope for Compute Engine to read/write.

Explanation

Download the private key from the service account, and add it to each VMs custom metadata. is not right.

Adding service accounts private key (JSON file) to VMs custom metadata has no effect. Metadata entries are key-value pairs and do not influence any other behavior.

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

Download the private key from the service account, and add the private key to each VM's SSH keys. is not right.

Adding service accounts private key to the VMs SSH keys does not influence any other behavior. SSH keys are used for SSHing to the instance.

https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys

When creating the VMs, set the service account's API scope for Compute Engine to read/write. is not right.

The scopes can be modified only when using compute engine default service account.

Ref: https://cloud.google.com/compute/docs/access/service-accounts#default\_service\_account

See the screenshot below.

The scopes can not be modified when using a non-default service account. See the screenshot below.

Since we want to use service accounts from another project, it is safe to say they are not the default compute service accounts of this project and hence it is not possible to customize the scopes.

Grant the service account the IAM Role of Compute Storage Admin in the project called ptech-vm. is the right answer.

Compute Storage Admin role provides permissions to create, modify, and delete disks, images, and snapshots. If the service account in ptech-sa is granted the IAM Role of Compute Storage Admin in the project called ptech-vm, it can take snapshots and carry out other activities as defined by the role.

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

Bottom of Form

Top of Form

Question 23: Correct

Your company plans to store sensitive PII data in a cloud storage bucket. Your compliance department has asked you to ensure the objects in this bucket are encrypted by customer-managed encryption keys. What should you do?

​

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

​

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

​

Recreate the bucket to use a Customer-managed key. Encryption can only be specified at the time of bucket creation.

​

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

(Correct)

Explanation

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

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

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

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

Recreate the bucket to use a Customer-managed key. Encryption can only be specified at the time of bucket creation. is not right.

Bucket encryption can be changed at any time. The bucket doesn't have to be recreated to change encryption.

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

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

This option correctly selects the Customer-managed key and then the key to use which satisfies our requirement. See the screenshot below for reference.

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

Bottom of Form

Top of Form

Question 24: Correct

You have files in a Cloud Storage bucket that you need to share with your suppliers. You want to restrict the time that the files are available to your suppliers to 1 hour. You want to follow Google recommended practices. What should you do?

​

Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -t 60m <JSON Key File> gs://<bucket>/\*.\* .

​

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 1h <JSON Key File> gs://<bucket>/\*\*.

(Correct)

​

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m 1h <JSON Key File> gs://<bucket>/\*.

​

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -p 60m <JSON Key File> gs://<bucket>/.

Explanation

Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -t 60m <JSON Key File> gs://<bucket>/\*.\* is not right.

gsutil signurl does not support -t flag. Executing the command with -t flag fails as shown.

$ gsutil signurl -t 60m keys.json gs://gcp-ace-lab-255520/\*.\*

CommandException: Incorrect option(s) specified. Usage:

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

Also, using the default compute engine service account violates the principle of least privilege. The recommended approach is to create a service account with just the right permissions needed and create JSON keys for this service account to use with gsutil signurl command.

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -p 60m <JSON Key File> gs://<bucket>/. is not right.

With gsutil signurl, -p is used to specify the key store password instead of prompting for the password. It can not be used to pass a time value. Executing the command with -p flag fails as shown.

$ gsutil signurl -p 60m keys.json gs://gcp-ace-lab-255520/\*.\*

TypeError: Last argument must be a byte string or a callable.

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

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m 1h <JSON Key File> gs://<bucket>/\*. is not right.

With gsutil signurl, -m is used to specify the operation e.g. PUT/GET etc. Executing the command with -m flag fails as shown.

$ gsutil signurl -m 1h keys.json gs://gcp-ace-lab-255520/\*.\*

CommandException: HTTP method must be one of[GET|HEAD|PUT|DELETE|RESUMABLE]

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

Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 1h <JSON Key File> gs://<bucket>/\*\*. is the right answer.

This command correctly specifies the duration that the signed url should be valid for by using the -d flag. The default is 1 hour so omitting the -d flag would have also resulted in the same outcome. Times may be specified with no suffix (default hours), or with s = seconds, m = minutes, h = hours, d = days. The max duration allowed is 7d.

Ref: https[://cloud.google.com/storage/docs/gsutil/commands/signurl](https://cloud.google.com/storage/docs/gsutil/commands/signurl)

Bottom of Form

Top of Form

Question 25: Incorrect

You deployed a java application in a single Google Cloud Compute Engine VM. During peak usage, the application CPU is maxed out and results in stuck threads which ultimately make the system unresponsive, and requires a reboot. Your operations team want to receive an email alert when the CPU utilization is greater than 95% for more than 10 minutes so they can manually change the instance type to another instance that offers more CPU. What should you do?

​

1. In Stackdriver logging, create a logs based metric to extract the CPU usage by using a regular expression.

2. In Stackdriver Monitoring, create an Alerting Policy based on this metric

3. Configure your email address in the notification channel.

(Incorrect)

​

1. Create a Stackdriver Workspace and associate your Google Cloud Platform (GCP) project with it

2. Create an Alerting Policy in Stackdriver that uses the threshold as a trigger condition.

3. Configure your email address in the notification channel.

(Correct)

​

1. Create a Stackdriver Workspace and associate your GCP project with it.

2. Write a script that monitors the CPU usage and sends it as a custom metric to Stackdriver

3. Create an uptime check for the instance in Stackdriver.

​

1. Create a consumer Gmail Account

2. Write a script that monitors the CPU usage.

3. When the CPU usage exceeds the threshold, have the script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.

Explanation

We want to use Google services. So that eliminates the two options where we Write a script. Why would we want to write a script when there is a Google service that does exactly that - with minimal configuration!!

Stackdriver logging does not log CPU usage. (Stackdriver monitoring does that) So that rules out the option In Stackdriver logging, create a logs based metric to extract the CPU usage by using a regular expression.

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

1. Create a Stackdriver Workspace and associate your Google Cloud Platform (GCP) project with it

2. Create an Alerting Policy in Stackdriver that uses the threshold as a trigger condition.

3. Configure your email address in the notification channel.

is the right answer.

A Workspace is a tool for monitoring resources contained in one or more Google Cloud projects or AWS accounts. In our case, we create a Stackdriver workspace and link our project to this workspace.

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

Stackdriver monitoring captures the CPU usage. By default, the Monitoring agent collects disk, CPU, network, and process metrics. You can also have the agent send custom metrics to Stackdriver monitoring.

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

You can then set up an alerting policy to alert with CPU utilization exceeds 90% for 15 minutes.

Ref: https[://cloud.google.com/monitoring/alerts/](https://cloud.google.com/monitoring/alerts/). See here for an example of setting up an alerting policy on CPU load. In our case, we’d have to substitute the CPU load for the CPU utilization metric. <https://cloud.google.com/monitoring/quickstart-lamp>

Stack driver monitoring supports multiple notification options for triggering alerts; email is one of them. Ref: https[://cloud.google.com/monitoring/support/notification-options](https://cloud.google.com/monitoring/support/notification-options)

Bottom of Form

Top of Form

Question 26: Correct

You work for a big multinational financial company that has several hundreds of Google Cloud Projects for various development, test and production workloads. Financial regulations require your company to store all audit files for three years. What should you do to implement a log retention solution while minimizing storage cost?

​

Write a custom script that uses logging API to copy the logs from Stackdriver logs to BigQuery.

​

Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket.

(Correct)

​

Export these logs to Cloud Pub/Sub and write a Cloud Dataflow pipeline to store logs to Cloud SQL.

​

Create an export to the sink that saves logs from Cloud Audit to BigQuery.

Explanation

Create an export to the sink that saves logs from Cloud Audit to BigQuery. is not right.

You can export logs into BigQuery by creating one or more sinks that include a logs query and an export destination (big query). However, this option is very expensive compared to the cost of Cloud Storage.

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

Write a custom script that uses logging API to copy the logs from Stackdriver logs to BigQuery. is not right.

Stackdriver already offers sink exports that let you copy logs from Stackdriver logs to BigQuery. While BigQuery is already quite expensive compared to Cloud Storage, coming up with a custom script and maintaining it to copy the logs from Stackdriver logs to BigQuery is going to add to the cost. This option is very inefficient and expensive.

Export these logs to Cloud Pub/Sub and write a Cloud Dataflow pipeline to store logs to Cloud SQL. is not right.

Cloud SQL is primarily used for storing relational data. Storing huge quantities of logs in Cloud SQL is very expensive compared to Cloud Storage. And add to it the fact that you also need to pay for Cloud Pub/Sub and Cloud Dataflow pipeline, and this option gets very expensive very soon.

Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket. is the right answer.

Coldline Storage is the perfect service to store audit logs from all the projects and is very cost-efficient as well. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline Storage is ideal for data you plan to read or modify at most once a quarter.

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

Bottom of Form

Top of Form

Question 27: Correct

You want to list all the internal and external IP addresses of all compute instances. Which of the commands below should you run to retrieve this information?

​

gcloud compute networks list.

​

gcloud compute networks list-ip.

​

gcloud compute instances list-ip.

​

gcloud compute instances list.

(Correct)

Explanation

gcloud compute instances list-ip. is not right.

"gcloud compute instances" doesn't support the action list-ip.

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

gcloud compute networks list-ip. is not right.

"gcloud compute networks" doesn't support the action list-ip.

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

gcloud compute networks list. is not right.

"gcloud compute networks list" doesn't list the IP addresses. It is used for listing Google Compute Engine networks (i.e. VPCs)

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

Here's a sample output of the command.

$ gcloud compute networks list

NAME SUBNET\_MODE BGP\_ROUTING\_MODE IPV4\_RANGE GATEWAY\_IPV4

default AUTO REGIONAL

test-vpc CUSTOM REGIONAL

gcloud compute instances list. is the right answer

gcloud compute instances list - lists Google Compute Engine instances. The output includes internal as well as external IP addresses.

Ref: https[://cloud.google.com/sdk/gcloud/reference/compute/instances/list](https://cloud.google.com/sdk/gcloud/reference/compute/instances/list)

Here's a sample output of the command.

$ gcloud compute instances list

NAME ZONE MACHINE\_TYPE PREEMPTIBLE INTERNAL\_IP EXTERNAL\_IP STATUS

gke-cluster-1-default-pool-8c599c87-16g9 us-central1-a n1-standard-1 10.128.0.8 35.184.212.227 RUNNING

gke-cluster-1-default-pool-8c599c87-36xh us-central1-a n1-standard-1 10.128.0.6 34.68.254.220 RUNNING

gke-cluster-1-default-pool-8c599c87-lprq us-central1-a n1-standard-1 10.128.0.7 35.224.96.151 RUNNING

Bottom of Form

Top of Form

Question 28: Correct

Your company has deployed several production applications across many Google Cloud Projects. Your operations team requires a consolidated monitoring dashboard for all the projects. What should you do?

​

Configure a single Stackdriver account, and link all projects to the same account.

(Correct)

​

For each project, create a Stackdriver account. In each project, create a service account for that project and grant it the role of Stackdriver Account Editor in all other projects.

​

Use Shared VPC to connect all projects, and link Stackdriver to one of the projects.

​

Configure a single Stackdriver account for one of the projects. In Stackdriver, create a Group and add the other project names as criteria for that Group.

Explanation

Use Shared VPC to connect all projects, and link Stackdriver to one of the projects. is not right.

Linking Stackdriver to one project brings metrics from that project alone. A Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network so that they can communicate with each other securely and efficiently using internal IPs from that network. But it does not help in linking all projects to a single Stackdriver workspace/account. Ref: https://cloud.google.com/vpc/docs/shared-vpc

For each project, create a Stackdriver account. In each project, create a service account for that project and grant it the role of Stackdriver Account Editor in all other projects. is not right.

Stackdriver monitoring does not use roles to gather monitoring information from the project. Instead, the Stackdriver Monitoring agent, which is a collectd-based daemon, gathers system and application metrics from virtual machine instances and sends them to Monitoring. In this case, as each project is linked to a separate Stackdriver account, it is not possible to have a consolidated view of all monitoring. Ref: https://cloud.google.com/monitoring/agent

Configure a single Stackdriver account for one of the projects. In Stackdriver, create a Group and add the other project names as criteria for that Group. is not right.

As the other projects are not linked to the stack driver, they can't be monitored. Moreover, you can not add projects to Stackdriver groups. Groups provide a mechanism for alerting on the behavior of a set of resources, rather than on individual resources. For example, you can create an alerting policy that is triggered if some number of resources in the group violates a particular condition (for example, CPU load), rather than having each resource inform you of violations individually.

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

Configure a single Stackdriver account, and link all projects to the same account. is the right answer.

You can monitor resources of different projects in a single Stackdriver account by creating a Stackdriver workspace. A Stackdriver workspace is a tool for monitoring resources contained in one or more Google Cloud projects or AWS accounts. Each Workspace can have between 1 and 100 monitored projects, including Google Cloud projects and AWS accounts. A Workspace accesses metric data from its monitored projects, but the metric data and log entries remain in the individual projects. Ref: https://cloud.google.com/monitoring/workspaces

Bottom of Form

Top of Form

Question 29: Correct

An intern joined your team recently and needs access to Google Compute Engine in your sandbox project to explore various settings and spin up compute instances to test features. You have been asked to facilitate this. How should you give your intern access to compute engine without giving more permissions than is necessary?

​

Grant Project Editor IAM role for sandbox project.

​

Grant Compute Engine Admin Role for sandbox project.

​

Create a shared VPC to enable the intern access Compute resources.

​

Grant Compute Engine Instance Admin Role for the sandbox project.

(Correct)

Explanation

Create a shared VPC to enable the intern access Compute resources. is not right.

Creating a shared VPC is not sufficient to grant intern access to compute resources. Shared VPCs are primarily used by organizations to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, so that they can communicate with each other securely and efficiently using internal IPs from that network.

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

Grant Project Editor IAM role for sandbox project. is not right.

Project editor role grants all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. While this role lets the intern explore compute engine settings and spin up compute instances, it grants more permissions than what is needed. Our intern can modify any resource in the project.

https://cloud.google.com/iam/docs/understanding-roles#primitive\_roles

Grant Compute Engine Admin Role for sandbox project. is not right.

Compute Engine Admin Role grants full control of all Compute Engine resources; including networks, load balancing, service accounts etc. While this role lets the intern explore compute engine settings and spin up compute instances, it grants more permissions than what is needed.

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

Grant Compute Engine Instance Admin Role for the sandbox project. is the right answer.

Compute Engine Instance Admin Role grants full control of Compute Engine instances, instance groups, disks, snapshots, and images. It also provides read access to all Compute Engine networking resources. This provides just the required permissions to the intern.

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

Bottom of Form

Top of Form

Question 30: Correct

Your company owns a web application that lets users post travel stories. You began noticing errors in logs for a specific Deployment. The deployment is responsible for translating a post from one language to another. You've narrowed the issue down to a specific container named "msg-translator-22" that is throwing the errors. You are unable to reproduce the error in any other environment, and none of the other containers serving the deployment have this issue. You would like to connect to this container to figure out the root cause. What steps would allow you to run commands against the msg-translator-22?

​

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

​

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

​

Use the kubectl run command to run a shell on that container.

​

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

(Correct)

Explanation

Use the kubectl run command to run a shell on that container. is not right.

kubectl run creates and runs a deployment. It creates a deployment or a job to manage the created container(s). It is not possible to use kubectl run to connect to an existing container.

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

Use the kubectl run msg-translator-22 /bin/ bash command to run a shell on that container. is not right.

kubectl run creates and runs a deployment. It creates a deployment or a job to manage the created container(s). It is not possible to use kubectl run to connect to an existing container.

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

Use the kubectl exec -it -- /bin/bash command to run a shell on that container. is not right.

While kubectl exec is used to execute a command in a container, the command above doesn't quite work because we haven't passed to it the identifier of the container.

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

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

kubectl exec is used to execute a command in a container. We pass the container name msg-translator-22 so kubectl exec knows which container to connect to. And we pass the command /bin/bash to it, so it starts a shell on the container and we can then run custom commands and identify the root cause of the issue.

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

Bottom of Form

Top of Form

Question 31: Incorrect

Your team uses Splunk for centralized logging and you have a number of reports and dashboards based on the logs in Splunk. You want to install Splunk forwarder on all nodes of your new Kubernetes Engine Autoscaled Cluster. The Splunk forwarder forwards the logs to a centralized Splunk Server. You want to minimize operational overhead. What is the best way to install Splunk Forwarder on all nodes in the cluster?

​

SSH to each node and run a script to install the forwarder agent.

​

Include the forwarder agent in a StatefulSet deployment.

​

Include the forwarder agent in a DaemonSet deployment.

(Correct)

​

Use Deployment Manager to orchestrate the deployment of forwarder agents on all nodes.

(Incorrect)

Explanation

SSH to each node and run a script to install the forwarder agent. is not right.

While this can be done, this approach does not scale. Every time the Kubernetes cluster autoscaling adds a new node, we have to SSH to the instance and run the script which is manual, possibly error-prone and adds operational overhead. We need to look for a solution that automates this task.

Include the forwarder agent in a StatefulSet deployment. 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 main purpose of StatefulSets is to set up persistent storage for pods that are deployed across multiple zones. StatefulSets are not suitable for installing the forwarder agent nor do they provide us the ability to install forwarder agents.

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

Use Deployment Manager to orchestrate the deployment of forwarder agents on all nodes. is not right.

You can use a deployment manager to create a number of GCP resources including GKE Cluster but you can not use it to create Kubernetes deployments or apply configuration files.

Ref: https://cloud.google.com/deployment-manager/docs/fundamentals

Include the forwarder agent in a DaemonSet deployment. 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. So by configuring the pod to use Splunk forwarder agent image and with some minimal configuration (e.g. identifying which logs need to be forwarded), you can automate the installation and configuration of Splunk forwarder agent on each GKE cluster node.

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

Bottom of Form

Top of Form

Question 32: Skipped

You developed an application that lets users upload statistical files and subsequently run analytics on this data. You chose to use Google Cloud Storage and BigQuery respectively for these requirements as they are highly available and scalable. You have a docker image for your application code, and you plan to deploy on your on-premises Kubernetes clusters. Your on-prem Kubernetes cluster needs to connect to Google Cloud Storage and BigQuery and you want to do this in a secure way following Google recommended practices. What should you do?

​

Use the default service account for App Engine, which already has the required permissions.

​

Use the default service account for Compute Engine, which already has the required permissions.

​

Create a new service account, grant it the least viable privileges to the required services, generate and download a JSON key. Use the JSON key to authenticate inside the application.

(Correct)

​

Create a new service account, with editor permissions, generate and download a key. Use the key to authenticate inside the application.

Explanation

Use the default service account for Compute Engine, which already has the required permissions. is not right.

The Compute Engine default service account is created with the Cloud IAM project editor role

Ref: https://cloud.google.com/compute/docs/access/service-accounts#default\_service\_account

The project editor role includes all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. Using a service account that is over-privileged falls foul of the principle of least privilege. Google recommends you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need.

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

Use the default service account for App Engine, which already has the required permissions. is not right.

App Engine default service account has the Editor role in the project (Same as the default service account for Compute Engine).

Ref: https://cloud.google.com/appengine/docs/standard/python/service-account

The project editor role includes all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. Using a service account that is over-privileged falls foul of the principle of least privilege. Google recommends you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need.

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

Create a new service account, with editor permissions, generate and download a key. Use the key to authenticate inside the application. is not right.

The project editor role includes all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. Using a service account that is over-privileged falls foul of the principle of least privilege. Google recommends you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need.

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

Create a new service account, grant it the least viable privileges to the required services, generate and download a JSON key. Use the JSON key to authenticate inside the application. is the right answer.

Using a new service account with just the least viable privileges for the required services follows the principle of least privilege. To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. Once you have the key, you can use it in your application to authenticate connections to Cloud Storage and BigQuery.

Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys#creating\_service\_account\_keys

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

Bottom of Form

Top of Form

Question 33: Correct

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

​

gcloud list gke-deployments --filter={ pod }

​

gcloud get pods --selector="app=prod"

​

kubectl get pods -l "app=prod"

(Correct)

​

kubectl get deployments --output=pods

Explanation

gcloud get pods --selector="app=prod". is not right.

You can not retrieve pods from the Kubernetes cluster by using gcloud. You can list pods by using Kubernetes CLI - kubectl get pods.

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

gcloud list gke-deployments --filter={ pod }. is not right.

You can not retrieve pods from the Kubernetes cluster by using gcloud. You can list pods by using Kubernetes CLI - kubectl get pods.

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

kubectl get deployments --output=pods. is not right.

You can not list pods by listing Kubernetes deployments. You can list pods by using Kubernetes CLI - kubectl get pods.

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

kubectl get pods -l "app=prod". is the right answer.

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

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

Ref: https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/#list-containers-filtering-by-pod-label

Bottom of Form

Top of Form

Question 34: Incorrect

Your company is a leading multinational news media organization and runs its online news website in Google Cloud on a 3-tier architecture as described below.

1. Web tier in Subnet 1 with a CIDR range 192.168.56.0/24. All instances in this tier use serviceAccount\_subnet1

2. App tier in Subnet 2 with a CIDR range 192.168.57.0/24. All instances in this tier use serviceAccount\_subnet2

3. DB tier in Subnet 3 with a CIDR range 192.168.58.0/24. All instances in this tier use serviceAccount\_subnet3

Your security team has asked you to disable all but essential communication between the tiers. Your application requires instances in the Web tier to communicate with the instances in App tier on port 80, and the instances in App tier to communicate with the instances in DB tier on port 3306.

How should you design the firewall rules?

​

1. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet2

- Source filter: all instances with serviceAccount\_subnet1

- Protocols: allow all

2. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet3

- Source filter: all instances with serviceAccount\_subnet2

- Protocols: allow all

​

1. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet2

- Source filter: all instances with serviceAccount\_subnet1

- Protocols: allow TCP:80

2. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet3

- Source filter: all instances with serviceAccount\_subnet2

- Protocols: allow TCP: 3306

(Correct)

​

1. Create an egress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.57.0/24)

- Protocols: allow TCP: 80

2. Create an egress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.56.0/24)

- Protocols: allow TCP: 3306

(Incorrect)

​

1. Create an ingress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.57.0/24)

- Protocols: allow all

2. Create an ingress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.56.0/24)- Protocols: allow all

Explanation

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

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

1. Create an egress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.57.0/24)

- Protocols: allow TCP: 80

2. Create an egress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.56.0/24)

- Protocols: allow TCP: 3306.

is not right.

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

1. Create an ingress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.57.0/24)

- Protocols: allow all

2. Create an ingress firewall rule with the following settings:

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.56.0/24)

- Protocols: allow all.

is not right.

If we create an ingress firewall rule with the settings

- Targets: all instances

- Source filter: IP ranges (with the range set to 192.168.56.0/24)

- Protocols: allow all.

then, we are allowing Tier 1 (192.168.56.0/24) access to all instances - including Tier 3 (192.168.58.0/24) which is not desirable.

1. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet2

- Source filter: all instances with serviceAccount\_subnet1

- Protocols: allow all

2. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet3

- Source filter: all instances with serviceAccount\_subnet2

- Protocols: allow all.

is not right.

The first firewall rule ensures that all instances with serviceAccount\_subnet2 i.e. all instances in Subnet Tier #2 (192.168.57.0/24) can be reached from all instances with serviceAccount\_subnet1 i.e. all instances in Subnet Tier #1 (192.168.56.0/24), on all ports. Similarly, the second firewall rule ensures that all instances with serviceAccount\_subnet3 i.e. all instances in Subnet Tier #3 (192.168.58.0/24) can be reached from all instances with serviceAccount\_subnet2 i.e. all instances in Subnet Tier #2 (192.168.57.0/24), on all ports. Though this matches our requirements, we are opening all ports instead of the specified ports which is our requirement. While this solution works, it is not as secure as the other option (see below)

1. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet2

- Source filter: all instances with serviceAccount\_subnet1

- Protocols: allow TCP:80

2. Create an ingress firewall rule with the following settings:

- Targets: all instances with serviceAccount\_subnet3

- Source filter: all instances with serviceAccount\_subnet2

- Protocols: allow TCP: 3306.

is the right answer.

The first firewall rule ensures that all instances with serviceAccount\_subnet2 i.e. all instances in Subnet Tier #2 (192.168.57.0/24) can be reached from all instances with serviceAccount\_subnet1 i.e. all instances in Subnet Tier #1 (192.168.56.0/24), on port 80. Similarly, the second firewall rule ensures that all instances with serviceAccount\_subnet3 i.e. all instances in Subnet Tier #3 (192.168.58.0/24) can be reached from all instances with serviceAccount\_subnet2 i.e. all instances in Subnet Tier #2 (192.168.57.0/24), on port 3306. This matches our requirements.

Bottom of Form

Top of Form

Question 35: Correct

Your operations team has configured a lifecycle management rule on a bucket. The bucket is multi-regional and has versioning enabled. Which of the following statement accurately reflects the following lifecycle config?

{

"rule":[

{

"action":{

"type":"Delete"

},

"condition":{

"age":60,

"isLive":false

}

},

{

"action":{

"type":"SetStorageClass",

"storageClass":"NEARLINE"

},

"condition":{

"age":366,

"matchesStorageClass":"MULTI\_REGIONAL"

}

}

]

}

​

Delete objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class in Multi-regional.

​

Move objects to Nearline Storage after 366 days if the storage class in Multi-regional First rule has no effect on the bucket.

​

Delete archived objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class is Multi-regional.

(Correct)

​

Archive objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class in Multi-regional.

Explanation

Archive objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class in Multi-regional. is not right.

The action has "type":"Delete" which means we want to Delete, not archive.

Ref: https://cloud.google.com/storage/docs/managing-lifecycles

Delete objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class in Multi-regional. is not right.

We want to delete objects as indicated by the action, however, we don't want to delete all objects older than 60 days. We only want to delete archived objects as indicated by "isLive":false condition

Ref: https://cloud.google.com/storage/docs/managing-lifecycles

Move objects to Nearline Storage after 366 days if the storage class in Multi-regional. First rule has no effect on the bucket. is not right.

The first rule certainly has an effect. It deletes archived objects older than 60 days.

Delete archived objects older than 60 days and move objects to Nearline Storage after 366 days if the storage class is Multi-regional. is the right answer.

The first part of the rule: The action has "type":"Delete" which means we want to Delete. "isLive":false condition means we are looking for objects that are not Live i.e. objects that are archived. Together, it means we want to delete archived objects older than 60 days. Note that if an object is deleted, it cannot be undeleted. Take care in setting up your lifecycle rules so that you do not cause more data to be deleted than you intend.

Ref: https://cloud.google.com/storage/docs/managing-lifecycles

The second part of the rule: The action indicates we want to set storage class to Nearline. The condition is true if the existing storage class is multi-regional and the age of the object is 366 days or over. Together it means we want to set the storage class to Nearline if existing storage class is multi-regional and age of the object is 366 days or over

Bottom of Form

Top of Form

Question 36: Incorrect

A recent reorganization in your company has seen the creation of a new data custodian team – responsible for managing data in all storage locations. Your production GCP project uses buckets in Cloud Storage, and you need to delegate control to the new team to Manage objects and buckets in your GCP project. What role should you grant them?

​

Storage Admin

(Correct)

​

Storage Object Admin

(Incorrect)

​

Storage Object Creator

​

Project Editor

Explanation

Project Editor is not right. is not right.

Project editor is a primitive role that grants a lot more than what we need here. Google doesn't recommend using Primitive roles.

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

All viewer permissions, plus permissions for actions that modify state, such as changing existing resources.

Storage Object Admin. is not right.

While this role grants full access to the objects, it does not grant access to the buckets so users of this role can not "manage buckets".

This role grants full control over objects, including listing, creating, viewing, and deleting objects.

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

Storage Object Creator. is not right.

This role allows users to create objects. It does not give permission to view, delete, or overwrite objects.

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

Storage Admin. is the right answer.

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

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

Bottom of Form

Top of Form

Question 37: Incorrect

Your company has multiple GCP projects in several regions, and your operations team have created numerous gcloud configurations for most common operational needs. They have asked your help to retrieve an inactive gcloud configuration and the GKE clusters that use it, using the least number of steps. How should you do this?

​

Use kubectl config get-contexts to review the output.

(Correct)

​

Use kubectl config use-context and kubectl config view to review the output.

​

Use gcloud config configurations describe to review the output.

(Incorrect)

​

Use gcloud config configurations activate and gcloud config list to review the output.

Explanation

Our requirement is to get to the end goal with the fewest possible steps.

Use gcloud config configurations describe to review the output. is not right.

gcloud config configurations describe - describes a named configuration by listing its properties. This does not return any Kubernetes cluster details.

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

Use gcloud config configurations activate and gcloud config list to review the output. is not right.

gcloud config configurations activate - activates an existing named configuration. This does not return any Kubernetes cluster details.

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

Use kubectl config get-contexts to review the output. is the right answer.

kubectl config get-contexts displays a list of contexts as well as the clusters that use them. Here's a sample output.

$ kubectl config get-contexts

CURRENT NAME CLUSTER

gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1 gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1 gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

\* gke\_kubernetes-260922\_us-central1\_standard-cluster-1 gke\_kubernetes-260922\_us-central1\_standard-cluster-1

The output shows the clusters and the configurations they use. Using this information, it is possible to find out the cluster using the inactive configuration with just 1 step.

Use kubectl config use-context and kubectl config view to review the output. is not right.

kubectl config use-context [my-cluster-name] is used to set the default context to [my-cluster-name]. But in order to do this, we first need a list of contexts and if you have multiple contexts, you'd need to execute kubectl config use-context [my-cluster-name] against each context. So that is at least 2+ steps. Further to that, the kubectl config view is used to get a full list of config. The output of the kubectl config view can be used to verify which clusters use what configuration but that is one additional step. Moreover, the output of the kubectl config view doesn't change much from one context to other - other than the current-context field. So our earlier steps of determining the contexts and using each context are of not much use. Though this can be used to achieve the same outcome, it involves more steps than the other option.

Here’s a sample execution

Step 1: First get a list of contexts

kubectl config get-contexts -o=name

gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

gke\_kubernetes-260922\_us-central1\_standard-cluster-1

Step 2: Use each context and view the config.

kubectl config use-context gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

Switched to context "gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1".

kubectl config view > 1.out (this saves the output in of config view in 1.out)

kubectl config use-context gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

Switched to context "gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1".

kubectl config view > 2.out (this saves the output in of config view in 2.out)

kubectl config use-context gke\_kubernetes-260922\_us-central1\_standard-cluster-1

Switched to context "gke\_kubernetes-260922\_us-central1\_standard-cluster-1".

kubectl config view > 3.out (this saves the output in of config view in 3.out)

diff 1.out 2.out

28c28

< current-context: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

---

> current-context: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

diff 2.out 3.out

28c28

< current-context: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

---

> current-context: gke\_kubernetes-260922\_us-central1\_standard-cluster-1

Step 3: Determine the inactive configuration and the cluster using that configuration.

The config itself has details about the clusters and contexts as shown below.

$ kubectl config view

apiVersion: v1

clusters:

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://35.222.130.166

name: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://35.225.14.172

name: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://34.69.212.109

name: gke\_kubernetes-260922\_us-central1\_standard-cluster-1

contexts:

- context:

cluster: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

user: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

name: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

- context:

cluster: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

user: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

name: gke\_kubernetes-260922\_us-central1-a\_your-first-cluster-1

- context:

cluster: gke\_kubernetes-260922\_us-central1\_standard-cluster-1

user: gke\_kubernetes-260922\_us-central1\_standard-cluster-1

name: gke\_kubernetes-260922\_us-central1\_standard-cluster-1

current-context: gke\_kubernetes-260922\_us-central1-a\_standard-cluster-1

Bottom of Form

Top of Form

Question 38: Correct

The storage costs for your application logs have far exceeded the project budget. The logs are currently being retained indefinitely in the Cloud Storage bucket myapp-gcp-ace-logs. You have been asked to remove logs older than 90 days from your Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend. What should you do?

​

Write a script that runs gsutil ls -l gs://myapp-gcp-ace-logs/\*\* to find and remove items older than 90 days. Schedule the script with cron.

​

Write a script that runs gsutil ls -lr gs://myapp-gcp-ace-logs/\*\* to find and remove items older than 90 days. Repeat this process every morning.

​

Write a lifecycle management rule in XML and push it to the bucket with gsutil lifecycle set config-xml-file.

​

Write a lifecycle management rule in JSON and push it to the bucket with gsutil lifecycle set config-json-file.

(Correct)

Explanation

You write a lifecycle management rule in XML and push it to the bucket with gsutil lifecycle set config-xml-file. is not right.

gsutil lifecycle set enables you to set the lifecycle configuration on one or more buckets based on the configuration file provided. However, XML is not a valid supported type for the configuration file.

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

Write a script that runs gsutil ls -lr gs://myapp-gcp-ace-logs/\*\* to find and remove items older than 90 days. Repeat this process every morning. is not right.

This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

Write a script that runs gsutil ls -l gs://myapp-gcp-ace-logs/\*\* to find and remove items older than 90 days. Schedule the script with cron. is not right.

This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

Write a lifecycle management rule in JSON and push it to the bucket with gsutil lifecycle set config-json-file. is the right answer.

You can assign a lifecycle management configuration to a bucket. The configuration contains a set of rules which apply to current and future objects in the bucket. When an object meets the criteria of one of the rules, Cloud Storage automatically performs a specified action on the object. One of the supported actions is to Delete objects. You can set up a lifecycle management to delete objects older than 90 days. "gsutil lifecycle set" enables you to set the lifecycle configuration on the bucket based on the configuration file. JSON is the only supported type for the configuration file. The config-json-file specified on the command line should be a path to a local file containing the lifecycle configuration JSON document.

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

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

Bottom of Form

Top of Form

Question 39: Correct

Your company wants to migrate a mission-critical application to Google Cloud Platform. The application is currently hosted in your on-premises data centre and runs off several VMs. Your migration manager has suggested a “lift and shift” to Google Compute Engine Virtual Machines while ensuring that the application scales quickly, automatically and efficiently based on the CPU utilization. You want to follow Google recommended practices. What should you do?

​

Use a set of third-party tools to build automation around scaling the application up and down, based on Stackdriver CPU usage monitoring

​

Create an instance template, and use the template in a managed instance group with autoscaling configured.

(Correct)

​

Create an instance template, and use the template in a managed instance group that scales up and down based on the time of day.

​

Create a Google Kubernetes Engine cluster, and use horizontal pod autoscaling to scale the application.

Explanation

Our requirements are

1. Use Virtual Machines directly (i.e. not container-based)

2. Scale Automatically

3. Scaling is efficient & is quick

Create a Google Kubernetes Engine cluster, and use horizontal pod autoscaling to scale the application. is not right.

We want to use virtual machines directly. And although GKE uses virtual machines under the hood for its GKE cluster, the autoscaling is totally different - it uses scaling at VMs (cluster auto-scaling) as well as at pod level (horizontal and vertical pod autoscaling).

Create an instance template, and use the template in a managed instance group that scales up and down based on the time of day. is not right.

Scaling based on time of the day may be insufficient especially when there is a sudden surge of requests (causing high CPU utilization) or if the requests go down suddenly (resulting in low CPU usage). Our requirements state we need to scale automatically i.e. we need autoscaling solution that scales up and down based on CPU usage which is indicative of the volume of requests processed but scaling based on time of the day is not indicative of the load (CPU) on the system and is therefore not right.

Use a set of third-party tools to build automation around scaling the application up and down, based on Stackdriver CPU usage monitoring. is not right.

While this can be done, it is not the most efficient solution when Google's own services offer this functionality and can do it more efficiently as they are all natively integrated.

Create an instance template, and use the template in a managed instance group with autoscaling configured. is the right answer.

Managed instance groups offer autoscaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load (CPU Utilization in this case). Autoscaling helps your apps gracefully handle increases in traffic and reduce costs when the need for resources is lower. You define the autoscaling policy and the autoscaler performs automatic scaling based on the measured load (CPU Utilization in this case). Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).

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

Bottom of Form

Top of Form

Question 40: Correct

An engineer from your team accidentally deployed several new versions of NodeJS application on Google App Engine Standard. You are concerned the new versions are serving traffic. You have been asked to produce a list of all the versions of the application that are receiving traffic as well the percent traffic split between them. What should you do?

​

gcloud app versions list --show-traffic

​

gcloud app versions list

​

gcloud app versions list --traffic

​

gcloud app versions list --hide-no-traffic

(Correct)

Explanation

gcloud app versions list. is not right

This command lists all the versions of all services that are currently deployed to the App Engine server. While this list includes all versions that are receiving traffic, it also includes versions that are not receiving traffic.

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

gcloud app versions list --traffic. is not right

gcloud app versions list command does not support --traffic flag.

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

gcloud app versions list --show-traffic. is not right

gcloud app versions list command does not support --show-traffic flag.

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

gcloud app versions list --hide-no-traffic. is the right answer.

This command correctly lists just the versions that are receiving traffic by hiding versions that do not receive traffic. This is the only command that fits our requirements.

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

Bottom of Form

Top of Form

Question 41: Incorrect

Your company owns a mobile game that is popular with users all over the world. The mobile game backend uses Cloud Spanner to store user state. An overnight job exports user state to a Cloud Storage bucket. Your operations team needs access to manage the spanner instance but not the user data. What should you do to streamline their IAM access?

​

Add the support team group to the roles/monitoring.viewer role

(Correct)

​

Add the support team group to the roles/stackdriver.accounts.viewer role

​

Add the support team group to the roles/spanner.database.user role

​

Add the support team group to the roles/spanner.database.reader role

(Incorrect)

Explanation

Requirements -

1. Monitoring access but no data access

2. Streamlined solution

3. Google recommended practices (i.e. look for something out of the box).

roles/spanner.databaseReader provides permission to read from the Spanner database, execute SQL queries on the database, and view the schema. Since this provides read access to data, roles/spanner.databaseReader. is not right.

roles/spanner.databaseUser provides permission to read from and write to the Spanner database, execute SQL queries on the database, and view and update the schema. Since this provides both read and write access to data, roles/spanner.databaseUser. is not right.

roles/stackdriver.accounts.viewer read-only access to get and list information about Stackdriver account structure. Since this does not provide monitor access to Cloud Spanner, roles/stackdriver.accounts.viewer. is not right.

roles/monitoring.viewer provides read-only access to get and list information about all monitoring data and configurations. This role provides monitoring access and fits our requirements. roles/monitoring.viewer. is the right answer.

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

Bottom of Form

Top of Form

Question 42: Correct

Your company has three GCP projects – for development, test and production environments. The budgeting team in the finance department needs to know the cost estimates for the next financial year to include it in budget planning. They have years of experience using SQL and need to group service costs by parameters such as duration (day/week/month/quarter), service type, region etc. for various subsections in the budget plan. How can you enable this?

​

Export your transactions to a local file and perform analysis with a suitable desktop tool.

​

Export your bill to a BigQuery dataset and then write time window based SQL queries for analysis.

(Correct)

​

Export your bill to a Cloud Storage bucket and then import into Google Sheets for analysis

​

Export your bill to a Cloud Storage bucket and then import into Cloud Bigtable for analysis.

Explanation

Requirements

1. use query syntax

2. need the billing data of all three projects

Export your bill to a Cloud Storage bucket and then import into Cloud Bigtable for analysis. is not right.

BigTable is a NoSQL database and doesn't offer query syntax support.

Export your bill to a Cloud Storage bucket and then import into Google Sheets for analysis. is not right.

Google Sheets don't offer full support for query syntax. Moreover, export to Cloud Storage bucket captures a smaller dataset than export to BigQuery. For example, the exported billing data does not include resource labels or any invoice-level charges such as taxes accrued or adjustment memos.

Export your transactions to a local file and perform analysis with a suitable desktop tool. is not right.

Billing data can't be exported to a local file, it can only be exported to a BigQuery Dataset or Cloud Storage bucket.

Export your bill to a BigQuery dataset and then write time window based SQL queries for analysis. is the right answer.

You can export billing information from multiple projects into a BigQuery dataset. Unlike the export to Cloud Storage bucket, export to BigQuery dataset includes all information making it easy and straightforward to construct queries in BigQuery to estimate the cost. BigQuery supports Standard SQL so you can join tables and group by fields (labels in this case) as needed

Ref: https[://cloud.google.com/billing/docs/how-to/export-data-bigquery](https://cloud.google.com/billing/docs/how-to/export-data-bigquery).

Bottom of Form

Top of Form

Question 43: Correct

You defined an instance template for a Python web application. When you deploy this application in Google Compute Engine, you want to ensure the service scales up and scales down automatically based on the number of HTTP requests. What should you do?

​

1. Create the necessary number of instances based on the instance template to handle peak user traffic.

2. Group the instances together in an unmanaged instance group.

3. Configure the instance group as the Backend Service of an External HTTP(S) load balancer.

​

1. Create an instance from the instance template.

2. Create an image from the instance's disk and export it to Cloud Storage.

3. Create an External HTTP(s) load balancer and add the Cloud Storage bucket as its backend service.

​

1. Deploy your Python web application instance template to Google Cloud App Engine.

2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.

​

1. Create a managed instance group from the instance template.

2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.

3. Configure the instance group as the backend service of an External HTTP(S) load balancer.

(Correct)

​

1. Create an unmanaged instance group from the instance template.

2. Configure autoscaling on the unmanaged instance group with a scaling policy based on HTTP traffic.

3. Configure the unmanaged instance group as the backend service of an Internal HTTP(S) load balancer.

Explanation

1. Create an instance from the instance template.

2. Create an image from the instance's disk and export it to Cloud Storage.

3. Create an External HTTP(s) load balancer and add the Cloud Storage bucket as its backend service. is not right.

You can upload a custom image from instance's boot disk and export it to cloud storage.

https://cloud.google.com/compute/docs/images/export-image

However, this image in the Cloud Storage bucket is unable to handle traffic as it is not a running application. Cloud Storage can not serve requests of the custom image.

1. Create an unmanaged instance group from the instance template.

2. Configure autoscaling on the unmanaged instance group with a scaling policy based on HTTP traffic.

3. Configure the unmanaged instance group as the backend service of an Internal HTTP(S) load balancer. is not right.

An unmanaged instance group does not autoscale. An unmanaged instance group is a collection of virtual machines (VMs) that reside in a single zone, VPC network, and subnet. An unmanaged instance group is useful for grouping together VMs that require individual configuration settings or tuning.

Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

1. Create the necessary number of instances based on the instance template to handle peak user traffic.

2. Group the instances together in an unmanaged instance group.

3. Configure the instance group as the Backend Service of an External HTTP(S) load balancer. is not right.

An unmanaged instance group does not autoscale. Although we may have enough compute power to handle peak user traffic, it does not automatically scale down when the traffic goes down so it doesn't meet our requirements.

Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

1. Deploy your Python web application instance template to Google Cloud App Engine.

2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic. is not right.

You can not use compute engine instance templates to deploy applications to Google Cloud App Engine. Google App Engine lets you deploy applications quickly by providing run time environments for many of the popular languages like Java, PHP, Node.js, Python, C#, .Net, Ruby, and Go. You have an option of using custom runtimes but using compute engine instance templates is not an option.

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

1. Create a managed instance group from the instance template.

2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.

3. Configure the instance group as the backend service of an External HTTP(S) load balancer. is the right answer.

The 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 - this can be set up by configuring scaling policies. In addition, you can configure External HTTP(S) load balancer to send traffic to the managed instance group. The External HTTP(S) load balancer tries to balance requests by using a round-robin algorithm and when the load increases beyond the threshold defined in the scaling policy, autoscaling kicks in and adds more nodes.

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

Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances

Bottom of Form

Top of Form

Question 44: Correct

You have a web application deployed as a managed instance group. You noticed some of the compute instances are running low on memory. You suspect this is due to JVM memory leak and you want to restart the compute instances to reclaim the leaked memory. Your web application is currently serving live web traffic. You want to ensure that the available capacity does not go below 80% at any time during the restarts and you want to do this at the earliest. What would you do?

​

Perform a rolling-action restart with max-unavailable set to 20%.

(Correct)

​

Perform a rolling-action reboot with max-surge set to 20%.

​

Stop instances in the managed instance group (MIG) one at a time and rely on autohealing to bring them back up.

​

Perform a rolling-action replace with max-unavailable set to 20%.

Explanation

Perform a rolling-action reboot with max-surge set to 20%. is not right.

reboot is not a supported action for rolling updates. The supported actions are replace, restart, start-update and stop-proactive-update.

Ref: https://cloud.google.com/sdk/gcloud/reference/beta/compute/instance-groups/managed/rolling-action

Perform a rolling-action replace with max-unavailable set to 20%. is not right.

Performing a rolling-action replace - Replaces instances in a managed instance group. While this resolves the JVM memory leak issue, recreating the instances is a little drastic when the same result can be achieved with the simple restart action. One of our requirements is to "do this at the earliest '' but recreating instances might take a lot of time depending on the number of instances and startup scripts; certainly more time than restart action.

Ref: https://cloud.google.com/sdk/gcloud/reference/beta/compute/instance-groups/managed/rolling-action

Stop instances in the managed instance group (MIG) one at a time and rely on autohealing to bring them back up. is not right.

While this would result in the same eventual outcome, it is manual, error-prone and time-consuming. One of our requirements is to "do this at the earliest" but stopping instances manually is time-consuming and could take a lot of time depending on the number of instances in the MIG. Also, relying on autohealing health checks to detect the failure and spin up the instance adds to the delay.

Perform a rolling-action restart with max-unavailable set to 20%. is the right answer.

This option achieves the outcome in the most optimal manner. The restart action restarts instances in a managed instance group. By performing a rolling restart with max-unavailable set to 20%, the rolling update restarts instances while ensuring there is at least 80% available capacity. The rolling update carries on restarting all the remaining instances until all instances in the MIG have been restarted.

Ref: <https://cloud.google.com/sdk/gcloud/reference/alpha/compute/instance-groups/managed/rolling-action/restart>

Bottom of Form

Top of Form

Question 45: Correct

You are hosting a new application on https://www.my-new-gcp-ace-website.com. The static content of the application is served from /static path. The dynamic content is served from /dynamic path and is hosted on a fleet of compute engine instances belonging to a Managed Instance Group. How can you configure a single GCP Load Balancer to serve content from both paths?

​

1. Deploy HAProxy in a second MIG and configure it to route /app/ to the first MIG and /static/ to your Cloud Storage bucket.

2. Create a network Load Balancer in front of the HAProxy MIG

3. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer

​

1. Create a HTTPS Load Balancer

2. Create a backend service associated with the MIG and route /app/ to the backend service

3. Create a backend bucket associated with your Cloud Storage Bucket, and route /static/ to the backend bucket

4. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer.

(Correct)

​

1. Create a HTTPS Load Balancer in front of the MIG

2. In Cloud DNS in the my-new-gcp-ace-website.com zone, create a TXT record for \_app\_.\_routes\_.www.my-new-gcp-ace-website.com containing the address of the load balancer.

3. Create another TXT record for \_static\_.\_routes\_.www.my-new-gcp-ace-website.com containing the URL of your Cloud Storage bucket.

​

1. Configure www.my-new-gcp-ace-website.com as a CNAME pointing to storage.googleapis.com

2. Create a HTTPS Load Balancer in front of the MIG

3. IN the app folder of your Cloud Storage Bucket, add a file called redirect containing the address of the load balancer.

Explanation

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

Let’s look at each of the options

1. Configure www.my-new-gcp-ace-website.com as a CNAME pointing to storage.googleapis.com

2. Create a HTTPS Load Balancer in front of the MIG

3. In the app folder of your Cloud Storage Bucket, add a file called redirect containing the address of the load balancer. is not right.

We can create a CNAME www.my-new-gcp-ace-website.com pointing to storage.googleapis.com, however, the cloud storage bucket does not support routing requests to a load balancer based on routing information in a file in the app folder. So this option doesn't work.

1. Deploy HAProxy in a second MIG and configure it to route /app/ to the first MIG and /static/ to your Cloud Storage bucket.

2. Create a network Load Balancer in front of the HAProxy MIG

3. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer is not right.

This could possibly work, but we want to follow Google recommended practices and why deploy and manage HAProxy when there might be some other Google product that does exactly the same with minimal configuration (there is !!)?

1. Create a HTTPS Load Balancer in front of the MIG

2. In Cloud DNS in the example.com zone, create a TXT record for \_app\_.\_routes\_.www.my-new-gcp-ace-website.com containing the address of the load balancer.

3. Create another TXT record for \_static\_.\_routes\_.www.my-new-gcp-ace-website.com containing the URL of your Cloud Storage bucket. is not right.

TXT records are used to verify the domain and TXT records can also hold any arbitrary text but the DNS providers don’t use the text in these TXT records for routing.

Ref: https://cloud.google.com/dns/records

Ref: https://support.google.com/cloudidentity/answer/183895?hl=en

1. Create a HTTPS Load Balancer

2. Create a backend service associated with the MIG and route /app/ to the backend service

3. Create a backend bucket associated with your Cloud Storage Bucket, and route /static/ to the backend bucket

4. Configure www.my-new-gcp-ace-website.com as an A record pointing to the address of the load balancer. is the right answer.

Since we need to send requests to multiple backends, Cloud DNS can't alone help us. We need Cloud HTTPS Load Balancer - it's URL maps (a fancy name for path-based routing) helps distribute traffic to backends based on the path information. Ref https://cloud.google.com/load-balancing/docs/url-map

Traffic received by Cloud HTTPS Load Balancer can be configured to send all requests on /app path to the MIG group; and requests on /static/ path to the bucket.

Ref Adding MIG as backend service- https://cloud.google.com/load-balancing/docs/backend-service#backend\_services\_and\_autoscaled\_managed\_instance\_groups.

Ref Adding a backend bucket(s) - https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers

The Load Balancer has a public IP address. But we want to instead access on www.my-new-gcp-ace-website.com, so we configure this as an A Record in our DNS provider. So this option is the right answer.

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

Bottom of Form

Top of Form

Question 46: Correct

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

​

Cloud Datastore

​

BigQuery

​

Cloud Bigtable

(Correct)

​

Cloud Storage

Explanation

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

Cloud Bigtable is the right answer.

Cloud Bigtable is Google's flagship product for ingest and analyze large volumes of time series data from sensors in real-time, matching the high speeds of IoT data to track normal and abnormal behavior.

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

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

Bottom of Form

Top of Form

Question 47: Correct

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

​

Managed Instance Group on Compute Engine

(Correct)

​

Cloud Functions

​

Network Load Balance

​

App Engine Standard environment

​

HTTP(S) Load Balancer

(Correct)

Explanation

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

Cloud Functions. is not right.

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

App Engine Standard environment. is not right.

The App Engine Standard Environment is based on container instances running on Google's infrastructure. Containers are preconfigured with one of several available runtimes such as Python, Java, NodeJS, PHP, Ruby, GO etc. It is not possible to specify a custom Linux distribution with App Engine Standard.

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

Network Load Balance. is not right.

The external (TCP/UDP) Network Load Balancing is a regional load balancer. Since we need to cater to a global user base, this load balancer is not suitable.

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

HTTP(S) Load Balancer. is the right answer.

HTTP(S) Load Balancing is a global service (when the Premium Network Service Tier is used). We can create backend services in more than one region and have them all serviced by the same global load balancer

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

Managed Instance Group on Compute Engine. is the right answer.

Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An autohealing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.

Ref: <https://cloud.google.com/compute/docs/instance-groups>

Bottom of Form

Top of Form

Question 48: Correct

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

​

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver

3. Export logs to Google Cloud Storage

(Correct)

​

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver

3. Export logs to BigQuery

​

Grant the security team access to the logs in each Project

​

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver

Explanation

Grant the security team access to the logs in each Project. is not right.

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

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver. is not right.

In Stackdriver, application logs are retained by default for just 30 days after which they are purged.

Ref: https://cloud.google.com/logging/quotas

While it is possible to configure a custom retention period of 10 years, storing logs in Stackdriver is very expensive compared to Cloud Storage. Stackdriver charges $.01 per GB per month, whereas something like Cloud Storage Coldline Storage costs $0.007 per GB per month (30% cheaper) and Cloud Storage Archive Storage costs 0.004 per GB per month (60% cheaper than Stackdriver)

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

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

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

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver

3. Export logs to BigQuery. is not right.

While enabling Stackdriver Logging API and having the applications send logs to stack driver is a good start, exporting and storing logs in BigQuery is fairly expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.

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

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

1. Enable Stackdriver Logging API

2. Configure web applications to send logs to Stackdriver

3. Export logs to Google Cloud Storage. is the right answer.

Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.

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

Bottom of Form

Top of Form

Question 49: Incorrect

A mission-critical application running in Google Cloud Platform requires an urgent update to fix a security issue without any downtime. How should you do this in CLI using deployment manager?

​

gcloud deployment-manager deployments update --config <deployment-config-path>

(Correct)

​

gcloud deployment-manager deployments create --config <deployment-config-path>

​

gcloud deployment-manager resources create --config <deployment-config-path>

​

gcloud deployment-manager resources update --config <deployment-config-path>

(Incorrect)

Explanation

gcloud deployment-manager resources create --config <deployment-config-path>. is not right.

gcloud deployment-manager resources command does not support the action create. The supported actions are describe and list. So this option is not right.

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

gcloud deployment-manager resources update --config <deployment-config-path>. is not right.

gcloud deployment-manager resources command does not support the action update. The supported actions are describe and list. So this option is not right.

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

gcloud deployment-manager deployments create --config <deployment-config-path>. is not right.

gcloud deployment-manager deployments create - creates a deployment but we want to update a deployment. So this option is not right.

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

gcloud deployment-manager deployments update --config <deployment-config-path>. is the right answer.

gcloud deployment-manager deployments update - updates a deployment based on a provided config file and fits our requirement.

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

Bottom of Form

Top of Form

Question 50: Correct

Your company has many Citrix services deployed in the on-premises datacenter, and they all connect to the Citrix Licensing Server on 10.10.10.10 in the same data centre. Your company wants to migrate the Citrix Licensing Server and all Citrix services to Google Cloud Platform. You want to minimize changes while ensuring the services can continue to connect to the Citrix licensing server. How should you do this in Google Cloud?

​

Reserve the IP 10.10.10.10 as a static public IP address using gcloud and assign it to the licensing server.

​

Use the IP 10.10.10.10 as a custom ephemeral IP address and assign it to the licensing server.

​

Start the licensing server with an automatic ephemeral IP address, and then promote it to a static internal IP address.

​

Reserve the IP 10.10.10.10 as a static internal IP address using gcloud and assign it to the licensing server.

(Correct)

Explanation

Reserve the IP 10.10.10.10 as a static public IP address using gcloud and assign it to the licensing server. is not right.

The private network range is defined by IETF (Ref: https://tools.ietf.org/html/rfc1918) and includes 10.0.0.0/8. So all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. As the IP of interest 10.10.10.10 falls within this range, it can not be reserved as a public IP Address.

Use the IP 10.10.10.10 as a custom ephemeral IP address and assign it to the licensing server. is not right.

Ephemeral IP address is the public IP Address assigned to compute instance. An ephemeral external IP address is an IP address that doesn't persist beyond the life of the resource. When you create an instance or forwarding rule without specifying an IP address, the resource is automatically assigned an ephemeral external IP address.

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

The private network range is defined by IETF (Ref: https://tools.ietf.org/html/rfc1918) and includes 10.0.0.0/8. So all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. As the IP of interest 10.10.10.10 falls within this range, it can not be used as a public IP Address (ephemeral IP is public).

Start the licensing server with an automatic ephemeral IP address, and then promote it to a static internal IP address. is not right.

When a compute instance is started with public IP, it gets an ephemeral IP address. An ephemeral external IP address is an IP address that doesn't persist beyond the life of the resource.

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

You can promote this ephemeral address into a Static IP address but this will be an external IP address and not an internal one.

Ref: https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#promote\_ephemeral\_ip

Reserve the IP 10.10.10.10 as a static internal IP address using gcloud and assign it to the licensing server. is right.

This is the only option that lets us reserve IP 10.10.10.10 as a static internal IP address because it falls within the standard IP Address range as defined by IETF (Ref: https://tools.ietf.org/html/rfc1918). This includes the range 10.0.0.0/8 so all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. Since we can now reserve this IP Address as a static internal IP address, it can be assigned to the licensing server in the VPC so that the application is able to reach the licensing server.