SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Google Cloud / By SkillCertPro

Practice Set 7

Your results are here!! for" Google Certified Associate Cloud Engineer Practice Test 7 "

0 of 65 questions answered correctly

Your time: 00:00:15

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0

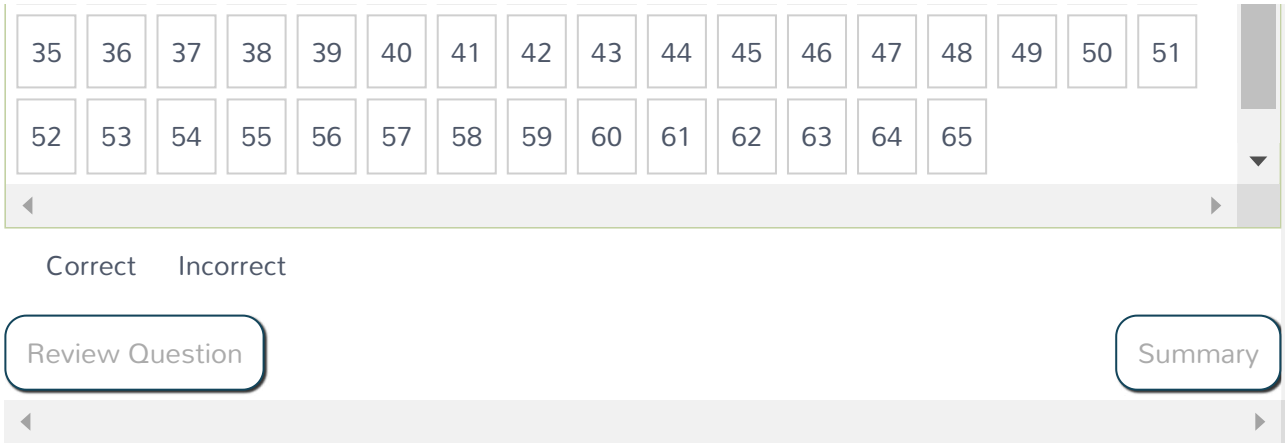
Average score	54.65%
Your score	0.00%

You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test | View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34



1. Question

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

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

Unattempted

1. Go to the GKE console, and delete existing clusters.
2. Recreate a new cluster.
3. Clear the option to enable legacy Stackdriver Logging. is not right.

Our requirement is to disable the logs ingested from the GKE container. We don t need to delete the existing cluster and create a new one.

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

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

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

2. Question

Your team is working towards using the desired state configuration for your application deployed on the GKE cluster. You have YAML files for the Kubernetes Deployment and Service objects. Your application is

designed to have 2 pods, which is defined by the replicas parameter in app-deployment.yaml. Your service uses GKE Load Balancer which is defined in app-service.yaml

You created the Kubernetes resources by running

kubectl apply -f app-deployment.yaml

kubectl apply -f app-service.yaml

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

- Disregard the YAML file. Use the kubectl scale command to scale the replicas to 5. kubectl scale --replicas=5 -f app-deployment.yaml
- Disregard the YAML file. Enable autoscaling on the deployment to trigger on CPU usage and set max pods to 5. kubectl autoscale myapp --max=5 --cpu-percent=80
- Modify the current configuration of the deployment by using kubectl edit to open the YAML file of the current configuration, modify and save the configuration. kubectl edit deployment/app-deployment -o yaml --save-config
- **Edit the number of replicas in the YAML file and rerun the kubectl apply. kubectl apply -f app-deployment.yaml**

Unattempted

Disregard the YAML file. Use the kubectl scale command to scale the replicas to 5. kubectl scale replicas=5 -f app-deployment.yaml. is not right.
While the outcome is the same, this approach doesn t update the change in the desired state configuration (YAML file). If you were to make some changes in your app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.
Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#scaling-a-deployment

Disregard the YAML file. Enable autoscaling on the deployment to trigger on CPU usage and set minimum pods as well as maximum pods to 5. kubectl autoscale myapp min=5 max=5 cpu-percent=80. is not right.
While the outcome is the same, this approach doesn t update the change in the desired state configuration (YAML file). If you were to make some changes in your app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.
Ref: https://kubernetes.io/blog/2016/07/autoscaling-in-kubernetes/

Modify the current configuration of the deployment by using kubectl edit to open the YAML file of the current configuration, modify and save the configuration. kubectl edit deployment/app-deployment -o yaml save-config. is not right.
Like the above, the outcome is the same. This is equivalent to first getting the resource, editing it in a text editor, and then applying the resource with the updated version. This approach doesn t update the replicas change in our local YAML file. If you were to make some changes in your local app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.
Ref: https://kubernetes.io/docs/concepts/cluster-administration/manage-deployment/#in-place-updates-of-resources

Edit the number of replicas in the YAML file and rerun the kubectl apply. kubectl apply -f app-deployment.yaml. is the right answer.
This is the only approach that guarantees that you use desired state configuration. By updating the YAML file to have 5 replicas and applying it using kubectl apply, you are preserving the intended state of Kubernetes cluster in the YAML file.
Ref: https://kubernetes.io/docs/concepts/cluster-administration/manage-deployment/#in-place-updates-of-resources

3. Question

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?

- Include the forwarder agent in a DaemonSet deployment.
- Use Deployment Manager to orchestrate the deployment of forwarder agents on all nodes.
- Include the forwarder agent in a StatefulSet deployment.
- SSH to each node and run a script to install the forwarder agent.

Unattempted

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

4. Question

Your VMs are running in a subnet that has a subnet mask of 255.255.255.240. The current subnet has no more free IP addresses and you require an additional 10 IP addresses for new VMs. The existing and new VMs should all be able to reach each other without additional routes. What should you do?

- Use gcloud to expand the IP range of the current subnet.
- Delete the subnet, and recreate it using a wider range of IP addresses.
- Create a new project. Use Shared VPC to share the current network with the new project.
- Create a new subnet with the same starting IP but a wider range to overwrite the current subnet.

Unattempted

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

Subnet mask of the existing subnet is 255.255.255.240 which means the max possible address in are 16. So the net prefix is /28 i.e. 4 bits free so 2 to the power of 4 is 16 IP Addresses.

As per IETF (Ref: https://tools.ietf.org/html/rfc1918), the supported internal IP Address ranges are
1. 24-bit block 10.0.0.0/8 (16777216 IP Addresses)
2. 20-bit block 172.16.0.0/12 (1048576 IP Addresses)
3. 16-bit block 192.168.0.0/16 (65536 IP Addresses)

A prefix of 28 is a very small subnet and could be in any of the ranges above; and all ranges have scope to accommodate a higher prefix.
A prefix of 27 gives you 32 IP Addresses i.e. 16 IP address more and we just need 10 more. So expanding the subnet to a prefix of 27 should give us the required capacity. And GCP lets you do exactly that running a gcloud command
https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range
gcloud compute networks subnets expand-ip-range region= prefix-length=27

5. Question

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

- gcloud container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20
- **gcloud container clusters resize my-gcp-ace-proj-1 –node-pool my-gcp-ace-primary-node-pool –num-nodes 20**
- kubectl container clusters update my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --num-nodes 20
- gcloud container clusters resize my-gcp-ace-proj-1 --node-pool my-gcp-ace-primary-node-pool --new-size 20

Unattempted
kubectl container clusters update my-gcp-ace-proj-1 node-pool my-gcp-ace-primary-node-pool num-nodes 20. is not right.
kubectl does not accept container as an operation.
Ref: https://kubernetes.io/docs/reference/kubectl/overview/#operations

gcloud container clusters update my-gcp-ace-proj-1 node-pool my-gcp-ace-primary-node-pool num-nodes 20. is not right.
gcloud container clusters update can not be used to specify the number of nodes. It can be used to specify the node locations, but not the number of nodes.
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/update

gcloud container clusters resize my-gcp-ace-proj-1 node-pool my-gcp-ace-primary-node-pool new-size 20. is not right.
gcloud container clusters resize command does not support the parameter new-size. While size can be used to resize the cluster node pool, use of size is discouraged as this is a deprecated parameter. The

size flag is now deprecated. Please use num-nodes instead.
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/resize

gcloud container clusters resize my-gcp-ace-proj-1 node-pool my-gcp-ace-primary-node-pool num-nodes 20. is the right answer
gcloud container clusters resize can be used to specify the number of nodes using the num-nodes parameter which is the target number of nodes in the cluster.
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/resize

6. Question

You are designing a large distributed application with 30 microservices. Each of your distributed microservices needs to connect to a database back-end. You want to store the credentials securely. Where should you store the credentials?

- A. In the source code
- B. In an environment variable
- C. In a secret management system
- D. In a config file that has restricted access through ACLs

Unattempted

Correct answer is C as it is a recommended practice to store the credentials in a secret management system such as KMS. Applications often require access to small pieces of sensitive data at build or run time. These pieces of data are often referred to as secrets. Secrets are similar in concept to configuration files, but are generally more sensitive, as they may grant access to additional data, such as user data.

Refer GCP documentation Authentication Managing Credentials

Best practices for managing credentials

Credentials provide access to sensitive data. The following practices help protect access to these resources.

Do not embed secrets related to authentication in source code, such as API keys, OAuth tokens, and service account credentials. You can use an environment variable pointing to credentials outside of the application s source code, such as Cloud Key Management Service.

Do use different credentials in different contexts, such as in testing and production environments.

Do transfer credentials only over HTTPS to prevent a third party from intercepting your credentials. Never transfer in clear text or as part of the URL.

Never embed long-lived credentials into your client-side app. For example, do not embed service account credentials into a mobile app. Client-side apps can be examined and credentials can easily be found and used by a third party.

Do revoke a token if you no longer need it.

Options A, B & D are wrong as they are not recommended and does not provide security.

7. Question

Your company s test suite is a custom C++ application that runs tests throughout each day on Linux virtual machines. The full test suite takes several hours to complete, running on a limited number of on-premises servers reserved for testing. Your company wants to move the testing infrastructure to the cloud, to reduce the amount of time it takes to fully test a change to the system, while changing the tests as little as possible. Which cloud infrastructure should you recommend?

- A. Google Compute Engine unmanaged instance groups and Network Load Balancer.
- **B. Google Compute Engine managed instance groups with auto-scaling.**
- C. Google Cloud Dataproc to run Apache Hadoop jobs to process each test.
- D. Google App Engine with Google Stackdriver for logging.

Unattempted

Correct answer is B as Google Compute Engine managed instance group can help the testing application to scale to reduce the amount of time to run tests.

Refer GCP documentation Instance groups

A managed instance group uses an instance template to create a group of identical instances. You control a managed instance group as a single entity. If you wanted to make changes to instances that are part of a managed instance group, you would make the change to the whole instance group. Because managed instance groups contain identical instances, they offer the following features.

When your applications require additional compute resources, managed instance groups can automatically scale the number of instances in the group.

Managed instance groups work with load balancing services to distribute traffic to all of the instances in the group.

If an instance in the group stops, crashes, or is deleted by an action other than the instance groups commands, the managed instance group automatically recreates the instance so it can resume its processing tasks. The recreated instance uses the same name and the same instance template as the previous instance, even if the group references a different instance template.

Managed instance groups can automatically identify and recreate unhealthy instances in a group to ensure that all of the instances are running optimally.

The managed instance group updater allows you to easily deploy new versions of software to instances in your managed instance groups, while controlling the speed and scope of deployment as well as the level of disruption to your service.

Option A is wrong as unmanaged group does not scale.

Option C is wrong as Dataproc is for big data batch jobs.

Option D is wrong as App Engine standard does not support C++ application and the testing application needs to be dockerized to be used with flexible engine.

8. Question

Your company collects and stores security camera footage in Google Cloud Storage. Within the first 30 days, footage is processed regularly for threat detection, object detection, trend analysis, and suspicious behavior detection. You want to minimize the cost of storing all the data. How should you store the videos?

- A. Use Google Cloud Regional Storage for the first 30 days, and then move to Coldline Storage.
- B. Use Google Cloud Nearline Storage for the first 30 days, and then move to Coldline Storage.
- C. Use Google Cloud Regional Storage for the first 30 days, and then move to Nearline Storage.
- D. Use Google Cloud Regional Storage for the first 30 days, and then move to Google Persistent Disk.

Unattempted

Correct answer is A as the data is accessed frequently within the first 30 days, using Google Cloud Regional Storage will enable the most cost-effective solution for storing and accessing the data. For videos older than 30 days, Google Cloud Coldline Storage offers the most cost-effective solution since it won t be accessed.

Refer GCP documentation Cloud Storage Storage Classes

Option B is wrong as while Google Cloud Coldline storage is cost-effective for long-term video storage, Google Cloud Nearline Storage would not be an effective solution for the first 30 days as the data is expected to be accessed frequently.

Option C is wrong as while Google Cloud Regional Storage is the most cost-effective solution for the first 30 days, Google Cloud Nearline Storage is not cost effective for long-term storage.

Option D is wrong as while Google Cloud Regional Storage is the most cost-effective solution for the first 30 days, storing the data on Google Cloud Persistent Disk would not be cost-effective for long term storage.

9. Question

Your company processes high volumes of IoT data that are time-stamped. The total data 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?

- A. Cloud Datastore
- B. Cloud Storage
- C. Cloud Bigtable
- D. BigQuery

Unattempted

Correct answer is C as Cloud Bigtable is the most performant storage option to work with IoT and time series data. Google Cloud Bigtable is a fast, fully managed, highly-scalable NoSQL database service. It is designed for the collection and retention of data from 1TB to hundreds of PB.

Refer GCP documentation Bigtable Time series data

Option A is wrong as Cloud Datastore is not the most performant product for frequent writes or timestamp-based queries.

Option B is wrong as Cloud Storage is designed for object storage not for this type of data ingestion and collection.

Option D is wrong as BigQuery is more of an a scalable, fully managed enterprise data warehousing solution and not ideal fast changing data.

10. Question

Your company is planning the infrastructure for a new large-scale application that will need to store over 100 TB or a petabyte of data in NoSQL format for Low-latency read/write and High-throughput analytics. Which storage option should you use?

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

Unattempted

Correct answer is A as Bigtable is an ideal solution to provide low latency, high throughput data processing storage option with analytics

Refer GCP documentation Storage Options

Cloud Bigtable logoCloud Bigtable

A scalable, fully managed NoSQL wide-column database that is suitable for both low-latency single-point lookups and precalculated analytics.

Low-latency read/write access IoT, finance, adtech High-throughput data processing Personalization, recommendations Time series support Monitoring Geospatial datasets Graphs

Options B & C are wrong as they are relational databases

Option D is wrong as Cloud Datastore is not ideal for analytics.

11. Question

A company wants building an application stores images in a Cloud Storage bucket and want to generate thumbnails as well resize the images. They want to use managed service which will help them scale automatically from zero to scale and back to zero. Which GCP service satisfies the requirement?

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

Unattempted

Correct answer is D as Cloud Functions can help automatically scale as per the demand, with no invocations if no demand.

Refer GCP documentation Cloud Functions

Google Cloud Functions is a serverless execution environment for building and connecting cloud services. With Cloud Functions you write simple, single-purpose functions that are attached to events emitted from your cloud infrastructure and services. Your function is triggered when an event being watched is fired. Your code executes in a fully managed environment. There is no need to provision any infrastructure or worry about managing any servers.

Cloud Functions removes the work of managing servers, configuring software, updating frameworks, and patching operating systems. The software and infrastructure are fully managed by Google so that you just add code. Furthermore, provisioning of resources happens automatically in response to events. This means that a function can scale from a few invocations a day to many millions of invocations without any work from you.

Options A, B & C are wrong as they need to be configured to scale down and would need warm up time to scale back again as compared to Cloud Functions.

12. Question

Your company is planning on deploying a web application to Google Cloud hosted on a custom Linux distribution. Your website will be accessible globally and needs to scale to meet demand. Choose all of the components that will be necessary to achieve this goal. (Select TWO)

- [ ] A. App Engine Standard environment
- [ ] B. HTTP Load Balancer
- [ ] C. Managed Instance Group on Compute Engine
- [ ] D. Network Load Balancer

Unattempted

Correct answers are B & C

Option B as only HTTP load balancer support global access.

Option C as the requirement is to support custom Linux distribution, only Compute Engine supports the same.

Refer GCP documentation Load Balancing

HTTP(S) load balancing can balance HTTP and HTTPS traffic across multiple backend instances, across multiple regions. Your entire app is available via a single global IP address, resulting in a simplified DNS setup. HTTP(S) load balancing is scalable, fault-tolerant, requires no pre-warming, and enables content-based load balancing. For HTTPS traffic, it provides SSL termination and load balancing.

Option A is wrong as App Engine does not support custom linux distribution.

Option D is wrong as Network load balancer does not support global access.

13. Question

Your customer is moving their corporate applications to Google Cloud Platform. The security team wants detailed visibility of all projects in the organization. You provision the Google Cloud Resource Manager and set up yourself as the org admin. What Google Cloud Identity and Access Management (Cloud IAM) roles should you give to the security team?

- A. Org viewer, project owner
- B. Org viewer, project viewer
- C. Org admin, project browser
- D. Project owner, network admin

Unattempted

Correct answer is B as the security team only needs visibility to the projects, project viewer provides the same with the best practice of least privilege.

Refer GCP documentation Organization & Project access control

Option A is wrong as project owner will provide access however it does not align with the best practice of least privilege.

Option C is wrong as org admin does not align with the best practice of least privilege.

Option D is wrong as the user needs to be provided organization viewer access to see the organization.

14. Question

Auditors visit your teams every 12 months and ask to review all the Google Cloud Identity and Access Management (Cloud IAM) policy changes in the previous 12 months. You want to streamline and expedite the analysis and audit process. What should you do?

A. Create custom Google Stackdriver alerts and send them to the auditor

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

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

D. Enable Google Cloud Storage (GCS) log export to audit logs into a GCS bucket and delegate access to the bucket

Unattempted

Correct answer is B as BigQuery is a good storage option with analysis capability. Also, the access to the data can be controlled using ACLs and Views.

BigQuery uses access control lists (ACLs) to manage permissions on projects and datasets.

BigQuery is a petabyte-scale analytics data warehouse that you can use to run SQL queries over vast amounts of data in near realtime.

Giving a view access to a dataset is also known as creating an authorized view in BigQuery. An authorized view allows you to share query results with particular users and groups without giving them access to the underlying tables. You can also use the view s SQL query to restrict the columns (fields) the users are able to query. In this tutorial, you create an authorized view.

Option A is wrong as alerts are real time and auditor do not need them.

Option C is wrong as Cloud SQL is not ideal for storage of log files and cannot be controlled through ACLs.

Option D is wrong as Cloud Storage is a good storage option but does not provide direct analytics capabilities.

15. Question

Your App Engine application needs to store stateful data in a proper storage service. Your data is non-relational database 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?

A. Cloud Bigtable

B. Cloud Dataproc

C. Cloud SQL

D. Cloud Datastore

Unattempted

Correct answer is D as Cloud Datastore provides a scalable, fully managed NoSQL document database for your web and mobile applications.

Cloud Datastore A scalable, fully managed NoSQL document database for your web and mobile applications. Semistructured application data User profiles Hierarchical data Product catalogs Durable key-value data Game state

Option A is wrong as Bigtable is not an ideal storage option for state management. Cloud Bigtable A scalable, fully managed NoSQL wide-column database that is suitable for both low-latency single-point lookups and precalculated analytics.Low-latency read/write access IoT, finance, adtech High-throughput data processing Personalization, recommendations Time series support Monitoring Geospatial datasets Graphs

Option B is wrong as Dataproc is not a storage solution. Cloud Dataproc is a fast, easy-to-use, fully-managed cloud service for running Apache Spark and Apache Hadoop clusters in a simpler, more cost-efficient way.

Option C is wrong as you need to define a capacity while provisioning a database.

Cloud SQL A fully managed MySQL and PostgreSQL database service that is built on the strength and reliability of Google s infrastructure. Web frameworks Websites, blogs, and content management systems (CMS) Structured data Business intelligence (BI) applications

OLTP workloads ERP, CRM, and ecommerce applications Geospatial application

16. Question

You have a collection of media files over 50GB each that you need to migrate to Google Cloud Storage. The files are in your on-premises data center. What migration method can you use to help speed up the transfer process?

A. Use multi-threaded uploads using the -m option.

B. Use parallel uploads to break the file into smaller chunks then transfer it simultaneously.

C. Use the Cloud Transfer Service to transfer.

D. Start a recursive upload.

Unattempted

Correct answer is B as gsutil provide object composition or parallel upload to handle upload of larger files.

Refer GCP documentation Optimizing for Cloud Storage Performance

More efficient large file uploads

The gsutil utility can also automatically use object composition to perform uploads in parallel for large, local files that you want to upload to Cloud Storage. It splits a large file into component pieces, uploads them in parallel and then recomposes them once they re in the cloud (and deletes the temporary components it created locally).

You can enable this by setting the `parallel_composite_upload_threshold` option on gsutil (or, updating your .boto file, like the console output suggests).

gsutil -o GSUtil:parallel_composite_upload_threshold=150M cp ./localbigfile gs://your-bucket

Where localbigfile is a file larger than 150MB. This divides up your data into chunks ˜150MB and uploads them in parallel, increasing upload performance.

Option A is wrong as multi-threaded options is best suited for uploading multiple files to better utilize the bandwidth.

Option C is wrong as Cloud Transfer service cannot handle uploads from on-premises data center.

Option D is wrong as recursive upload helps handle folders and subfolders.

17. Question

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

- A. Setup the application using App Engine Standard environment with Cloud VPN to connect to database
- **B. Setup the application using App Engine Flexible environment with Cloud VPN to connect to database**
- C. Setup the application using App Engine Standard environment with Cloud Router to connect to database
- D. Setup the application using App Engine Flexible environment with Cloud Router to connect to database

Unattempted

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

Refer GCP documentation App Engine Flexible Network Settings

Advanced network configuration

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

To enable subnetworks for your App Engine application:

Create a custom subnet network.

Add the network name and subnetwork name to your app.yaml file, as specified above.

To establish a simple VPN based on static routing, create a gateway and a tunnel for a custom subnet network. Otherwise, see how to create other types of VPNs.

Option A is wrong as Google App Engine Standard cannot use Cloud VPN.

Options C & D are wrong as you need a Cloud VPN to connect to on-premises data center. Cloud Route support dynamic routing.

18. Question

A lead software engineer tells you that his new application design uses websockets and HTTP sessions that are not distributed across the web servers. You want to help him ensure his application will run properly on Google Cloud Platform. What should you do?

- A. Help the engineer to convert his websocket code to use HTTP streaming.
- B. Review the encryption requirements for websocket connections with the security team.
- **C. Meet with the cloud operations team and the engineer to discuss load balancer options.**
- D. Help the engineer redesign the application to use a distributed user session service that does not rely on websockets and HTTP sessions.

Unattempted

Correct answer is C as the HTTP(S) load balancer in GCP handles websocket traffic natively. Backends that use WebSocket to communicate with clients can use the HTTP(S) load balancer as a front end, for scale and availability.

Refer GCP documentation HTTP Load Balancer

HTTP(S) Load Balancing has native support for the WebSocket protocol. Backends that use WebSocket to communicate with clients can use the HTTP(S) load balancer as a front end, for scale and availability. The load balancer does not need any additional configuration to proxy WebSocket connections.

The WebSocket protocol, which is defined in RFC 6455, provides a full-duplex communication channel between clients and servers. The channel is initiated from an HTTP(S) request

Option A is wrong as there is no compelling reason to move away from websockets as part of a move to GCP.

Option B is wrong as is this may be a good exercise anyway, but it doesn t really have any bearing on the GCP migration.

Option D is wrong as there is no compelling reason to move away from websockets as part of a move to GCP.

19. Question

Your customer is moving their storage product to Google Cloud Storage (GCS). The data contains personally identifiable information (PII) and sensitive customer information. What security strategy should you use for GCS?

- A. Use signed URLs to generate time bound access to objects.
- B. Grant IAM read-only access to users, and use default ACLs on the bucket.
- **C. Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.**
- D. Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.

Unattempted

Correct answer is C as this grants the least privilege required to access the data and minimizes the risk of accidentally granting access to the wrong people.

Refer GCP documentation Cloud Storage Access Control

Option A is wrong as Signed URLs could potentially be leaked as anyone who gets access to the URL can access the data.

Option B is wrong as this is needlessly permissive, users only require one permission in order to get access.

Option D is wrong as this is security through obscurity, also known as no security at all.

20. Question

You ve created a Kubernetes engine cluster named project-1 , which has a cluster pool named primary-node-pool . You ve realized that you need more total nodes within your cluster pool to meet capacity demands from 10 to 20. What is the command to change the number of nodes in your pool?

- A. gcloud container clusters update project-1 --node pool 'primary-node-pool' --num-nodes 20
- B. gcloud container clusters resize project-1 --node pool 'primary-node-pool' --size 20
- C. gcloud container clusters resize project-1 --node pool 'primary-node-pool' --num-nodes 20
- D. kubectl container clusters update project-1 --node pool 'primary-node-pool' --num-nodes 20

Unattempted

Correct answer is B as the resize command with gcloud can be used to increase the nodes.

NOTE The size flag has been renamed to num-nodes flag from 242.0.0 (2019-04-16)

Kubernetes Engine

Renamed size flag of gcloud container clusters resize to num-nodes. size retained as an alias.

Disabled node auto-repair and node auto-upgrade by default when enable-kubernetes-alpha flag is used to create clusters with Kubernetes alpha features enabled. Users may now create alpha clusters without specifying no-enable-autorepair or no-enable-autoupgrade flags. However, for creating new node pools in an existing alpha cluster, these two flags may still be required.

Refer GCP documentation Resizing Kubernetes Cluster

gcloud container clusters resize [CLUSTER_NAME] node-pool [POOL_NAME] size [SIZE];

Option A is wrong as update command takes in the max-nodes & min-nodes flags which are defining the autoscaling. num-nodes flag is not applicable.

Option C is wrong as num-nodes is a wrong flag for cluster resize command.

Option D is wrong as kubectl command cannot be used for resizing the cluster.

21. Question

A Company is using Cloud SQL to host critical data. They want to enable high availability in case a complete zone goes down. How should you configure the same?

- A. Create a Read replica in the same region different zone
- B. Create a Read replica in the different region different zone
- C. Create a Failover replica in the same region different zone
- D. Create a Failover replica in the different region different zone

Unattempted

Correct answer is C as a failover replica helps provides High Availability for Cloud SQL. The failover replica must be in the same region as the primary instance.

Refer GCP documentation Cloud SQL High Availability

The HA configuration, sometimes called a cluster, provides data redundancy. The configuration is made up of a primary instance (master) in the primary zone and a failover replica in the secondary zone. Through semisynchronous replication, all changes made to the primary instance s data and user tables are copied onto the failover replica. In the event of an instance or zone failure, this configuration reduces downtime, and your data continues to be available to client applications.

The failover replica must be in the same region as the primary instance, but in a different zone.

Diagram overview of MySQL HA configuration. Described in text below.

Option A & B are wrong as Read replicas do not provide failover capability and just additional read capacity.

Option D is wrong as failover replica must be in the same region as the primary instance.

22. Question

Your application is hosted across multiple regions and consists of both relational database data and static images. Your database has over 10 TB of data. You want to use a single storage repository for each data type across all regions. Which two products would you choose for this task? (Choose two)

- A. Cloud Bigtable
- B. Cloud Spanner
- C. Cloud SQL
- D. Cloud Storage

Unattempted

Correct answers are B & D

Option B to store the relational data. As the data is over 10TB and need across region, Cloud Spanner is preferred over Cloud SQL.

Option D to store unstructured static images.

Refer GCP documentation Storage Options

Option A is wrong as Bigtable is a NoSQL data storage and not suitable to store unstructured data as images and files.

Option C is wrong as Cloud SQL is regional and not a preferred option for data over 10TB.

23. Question

Your project has all its Compute Engine resources in the europe-west1 region. You want to set europe-west1 as the default region for gcloud commands. What should you do?

A. Use Cloud Shell instead of the command line interface of your device. Launch Cloud Shell after you navigate to a resource in the europe-west1 region. The europe-west1 region will automatically become the default region.

B. Use gcloud config set compute/region europe-west1 to set the default region for future gcloud commands.

C. Use gcloud config set compute/zone europe-west1 to set the default region for future gcloud commands.

D. Create a VPN from on-premises to a subnet in europe-west1, and use that connection when executing gcloud commands.

Unattempted

Correct answer is B as this will ensure that the relevant region is used when not overwritten by a command parameter.

Refer GCP documentation Change default zone and region

You can manually choose a different zone or region without updating the metadata server by setting these properties locally on your gcloud client.

gcloud config compute/region REGION

Option A is wrong as Cloud Shell will not default to the location that it s launched from.

Option C is wrong as this command should be used to set a zone, not a region.

Option D is wrong as a VPN to a specific subnet does not have any effect on the gcloud command region.

24. Question

You have an application server running on Compute Engine in the europe-west1-d zone. You need to ensure high availability and replicate the server to the europe-west2-c zone using the fewest steps possible. What should you do?

- A. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west2-c zone. Create a new VM with that disk.
- B. Create a snapshot from the disk. Create a disk from the snapshot in the europe-west1-d zone and then move the disk to europe-west2-c. Create a new VM with that disk.
- C. Use gcloud to copy the disk to the europe-west2-c zone. Create a new VM with that disk.
- D. Use gcloud compute instances move with parameter --destination-zone europe-west2-c to move the instance to the new zone.

Unattempted

Correct answer is A as the best way to create a replica of disk is to create a snapshot and create a disk from the snapshot in the zone.

Refer GCP documentation Disks

Disks are zonal resources, so they reside in a particular zone for their entire lifetime. The contents of a disk can be moved to a different zone by snapshotting the disk (using gcloud compute disks snapshot) and creating a new disk using source-snapshot in the desired zone. The contents of a disk can also be moved across project or zone by creating an image (using gcloud compute images create) and creating a new disk using image in the desired project and/or zone.

Option B is wrong as the approach is possible, but not with the fewest steps.

Option C is wrong as gcloud cannot be used to copy the disk to different zone.

Option D is wrong as it would move and not create a copy. gcloud compute disks move facilitates moving a Google Compute Engine disk volume from one zone to another. You cannot move a disk if it is attached to a running or stopped instance; use the gcloud compute instances move command instead.

25. Question

You need to estimate the annual cost of running a BigQuery query that is scheduled to run nightly. What should you do?

A. Use gcloud query --dry_run to determine the number of bytes read by the query. Use this number in the Pricing Calculator.

B. Use bq query --dry_run to determine the number of bytes read by the query. Use this number in the Pricing Calculator.

C. Use gcloud estimate to determine the amount billed for a single query. Multiply this amount by 365.

D. Use bq estimate to determine the amount billed for a single query. Multiply this amount by 365.

Unattempted

Correct answer is B as this is the correct way to estimate the yearly BigQuery querying costs.

Refer GCP documentation BigQuery Best Practices Price your Query

Best practice: Before running queries, preview them to estimate costs.

Queries are billed according to the number of bytes read. To estimate costs before running a query use:

The query validator in the GCP Console or the classic web UI

The dry_run flag in the CLI

The dryRun parameter when submitting a query job using the API

The Google Cloud Platform Pricing Calculator

Option A is wrong as you should use bq , not gcloud , to estimate the amount of bytes read.

Option C is wrong as you should use bq , not gcloud , to work with BigQuery.

Option D is wrong as this will not give the amount billed for a query.

26. Question

You work in a small company where everyone should be able to view all resources of a specific project. You want to grant them access following Google s recommended practices. What should you do?

A. Create a script that uses gcloud projects add-iam-policy-binding for all users email addresses and the Project Viewer role.

B. Create a script that uses gcloud iam roles create for all users email addresses and the Project Viewer role.

C. Create a new Google Group and add all users to the group. Use gcloud projects add-iam-policy-binding with the Project Viewer role and Group email address.

D. Create a new Google Group and add all members to the group. Use gcloud iam roles create with the Project Viewer role and Group email address.

Unattempted

Correct answer is C as Google recommends to use groups where possible.

Refer GCP documentation gcloud IAM

Option A is wrong as groups are recommended over individual assignments.

Option B is wrong as this command is to create roles, not to assign them.

Option D is wrong as this command is to create roles, not to assign them.

27. Question

Your developers are trying to select the best compute service to run a static website. They have a dozen HTML pages, a few JavaScript files, and some CSS. They need the site to be highly available for the few weeks it is running. They also have a limited budget. What is the best service to use to run the site?

A. Kubernetes Engine

B. Compute Engine

C. Cloud Storage

D. App Engine

Unattempted

Correct answer is C as the website is static and needs to be hosted with high availability and limited budget, Cloud Storage would be an ideal choice.

Refer GCP documentation Cloud Storage Static Website

To host a static site in Cloud Storage, you need to create a Cloud Storage bucket, upload the content, and test your new site. You can serve your data directly from storage.googleapis.com, or you can verify

that you own your domain and use your domain name. Either way, you ll get consistent, fast delivery from global edge caches.

You can create your static web pages however you choose. For example, you could hand-author pages by using HTML and CSS. You can use a static-site generator, such as Jekyll, Ghost, or Hugo, to create the content. Static-site generators make it easier for you to create a static website by letting you author in markdown, and providing templates and tools. Site generators generally provide a local web server that you can use to preview your content.

After your static site is working, you can update the static pages by using any process you like. That process could be as straightforward as hand-copying an updated page to the bucket. You might choose to use a more automated approach, such as storing your content on GitHub and then using a webhook to run a script that updates the bucket. An even more advanced system might use a continuous-integration /continuous-delivery (CI/CD) tool, such as Jenkins, to update the content in the bucket. Jenkins has a Cloud Storage plugin that provides a Google Cloud Storage Uploader post-build step to publish build artifacts to Cloud Storage.

If you have a web application that needs to serve static content or user-uploaded static media, using Cloud Storage can be a cost-effective and efficient way to host and serve this content, while reducing the amount of dynamic requests to your web application.

Options A, B & D are wrong as they would be an expensive option as compared to Cloud Storage hosting.

28. Question

You have an autoscaled managed instance group that is set to scale based on CPU utilization of 60%. There are currently 3 instances in the instance group. You re connected to one of the instances and notice that the CPU usage is a 70%. However, the instance group isn t starting up another instance. What s the most likely reason?

- A. The autoscaler is disabled.
- B. The autoscaler takes 60 seconds before creating a new instance.
- C. The load balancer doesn't recognize the instance as healthy.
- **D. The average CPU for the entire instance group is below 60%.**

Unattempted

Correct answer is D as the Auto Scaler checks for the average CPU utilization across the instances and is not done on the basis of a single instance.

Refer GCP documentation Auto Scaler CPU based Scaling

You can autoscale based on the average CPU utilization of a managed instance group. Using this policy tells the autoscaler to collect the CPU utilization of the instances in the group and determine whether it needs to scale. You set the target CPU utilization the autoscaler should maintain and the autoscaler will work to maintain that level.

The autoscaler treats the target CPU utilization level as a fraction of the average use of all vCPUs over time in the instance group. If the average usage of your total vCPUs exceeds the target utilization, the autoscaler will add more virtual machines. For example, setting a 0.75 target utilization tells the autoscaler to maintain an average usage of 75% among all vCPUs in the instance group.

Option A is wrong as the group is set to CPU utilization already, it is not disabled.

Option B is wrong as Auto Scaler takes action immediately if the target is hit.

Option C is wrong as if the instance is marked unhealthy it would not serve any traffic and might be replaced.

29. Question

You are required to fire a query on large amount of data stored in BigQuery. You know the query is expected to return a large amount of data. How would you estimate the cost for the query?

- A. Using Command line, use the --dry_run option on BigQuery to determine the amount of bytes read, and then use the price calculator to determine the cost.
- B. Using Command line, use the --dry_run option on BigQuery to determine the amount of bytes returned, and then use the price calculator to determine the cost.
- C. Using Command line, use the --dry_run option on BigQuery to determine the amount of time taken, and then use the price calculator to determine the cost.
- D. Using Command line, use the --dry_run option on BigQuery to determine the total amount of table data in bytes, as it would be a full scan, and then use the price calculator to determine the cost.

Unattempted

Correct answer is A as the dry-run option can be used to price your queries before they are actually fired. The Query returns the bytes read, which can then be used with the Pricing Calculator to estimate the query cost.

Refer GCP documentation BigQuery Best Practices

Price your queries before running them

Best practice: Before running queries, preview them to estimate costs.

Queries are billed according to the number of bytes read. To estimate costs before running a query use:

The query validator in the GCP Console or the classic web UI

The dry_run flag in the CLI

The dryRun parameter when submitting a query job using the API

The Google Cloud Platform Pricing Calculator

Options B, C are wrong as the estimation needs to be done on the bytes read by the query and not returned or time taken.

Option D is wrong as it the bytes read would depend on the query and would not always a full table scan.

30. Question

Your company wants to host confidential documents in Cloud Storage. Due to compliance requirements, there is a need for the data to be highly available and resilient even in case of a regional outage. Which storage classes help meet the requirement?

- A. Nearline
- B. Standard
- C. Multi-Regional
- D. Dual-Regional
- E. Regional

Unattempted

Correct answers are A & C as Multi-Regional and Nearline storage classes provide multi-region geo-redundant deployment, which can sustain regional failure.

Refer GCP documentation Cloud Storage Classes

Multi-Regional Storage is geo-redundant.

The geo-redundancy of Nearline Storage data is determined by the type of location in which it is stored: Nearline Storage data stored in multi-regional locations is redundant across multiple regions, providing

higher availability than Nearline Storage data stored in regional locations.

Data that is geo-redundant is stored redundantly in at least two separate geographic places separated by at least 100 miles. Objects stored in multi-regional locations are geo-redundant, regardless of their storage class.

Geo-redundancy occurs asynchronously, but all Cloud Storage data is redundant within at least one geographic place as soon as you upload it.

Geo-redundancy ensures maximum availability of your data, even in the event of large-scale disruptions, such as natural disasters. For a dual-regional location, geo-redundancy is achieved using two specific regional locations. For other multi-regional locations, geo-redundancy is achieved using any combination of data centers within the specified multi-region, which may include data centers that are not explicitly available as regional locations.

Options B & D are wrong as they do not exist

Option E is wrong as Regional storage class is not geo-redundant. Data stored in a narrow geographic region and Redundancy is across availability zones

31. Question

Your company needs to backup data for disaster recovery scenarios store all the backup data. This data would be required only in the event of a disaster and won t be accessed otherwise. What is the best default storage class?

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

Unattempted

Correct answer is B as Coldline storage is an ideal solution for disaster recovery data given its rarity of access.

Refer GCP documentation Cloud Storage Classes

Google Cloud Storage Coldline is a very-low-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Unlike other cold storage services, your data is available within milliseconds, not hours or days.

Coldline Storage is the best choice for data that you plan to access at most once a year, due to its slightly lower availability, 90-day minimum storage duration, costs for data access, and higher per-operation costs. For example:

Cold Data Storage Infrequently accessed data, such as data stored for legal or regulatory reasons, can be stored at low cost as Coldline Storage, and be available when you need it.

Disaster recovery In the event of a disaster recovery event, recovery time is key. Cloud Storage provides low latency access to data stored as Coldline Storage.

The geo-redundancy of Coldline Storage data is determined by the type of location in which it is stored: Coldline Storage data stored in multi-regional locations is redundant across multiple regions, providing higher availability than Coldline Storage data stored in regional locations.

Options A, C & D are wrong as they are not suited for infrequently accessed data, as disaster does not happen periodically but rarely.

32. Question

Your company needs to backup data for disaster recovery scenarios store all the backup data. You are required to perform monthly disaster recovery drills, as a part of compliance. What is the best default storage class?

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

Unattempted

Correct answer is D as the data needs to be access monthly only, Nearline is the ideal solution for data storage.

Refer GCP documentation Cloud Storage Classes

Google Cloud Storage Nearline is a low-cost, highly durable storage service for storing infrequently accessed data. Nearline Storage is a better choice than Multi-Regional Storage or Regional Storage in scenarios where slightly lower availability, a 30-day minimum storage duration, and costs for data access are acceptable trade-offs for lowered storage costs.

Nearline Storage is ideal for data you plan to read or modify on average once a month or less. For example, if you want to continuously add files to Cloud Storage and plan to access those files once a month for analysis, Nearline Storage is a great choice.

Nearline Storage is also appropriate for data backup, disaster recovery, and archival storage. Note, however, that for data accessed less frequently than once a year, Coldline Storage is the most cost-effective choice, as it offers the lowest storage costs.

The geo-redundancy of Nearline Storage data is determined by the type of location in which it is stored: Nearline Storage data stored in multi-regional locations is redundant across multiple regions, providing higher availability than Nearline Storage data stored in regional locations.

Options A, B & C are wrong as they are not ideal for data that is only access onced monthly.

33. Question

Your developers are trying to connect to an Ubuntu server over SSH to diagnose some errors. However, the connection times out. Which command should help solve the problem?

- A. gcloud compute firewall-rules create open-ssh --network $NETWORK --allow tcp:22
- B. gcloud compute firewall-rules create open-ssh
- C. gcloud compute firewall-rules create open-ssh --network $NETWORK --deny tcp:22
- D. gcloud compute firewall-rules create open-ssh --network $NETWORK --allow tcp:3389

Unattempted

Correct answer is A as gcloud compute firewall-rules create is used to create firewall rules to allow/deny incoming/outgoing traffic.

Refer GCP documentation Cloud SDK Firewall Rules Create

allow=PROTOCOL[:PORT[-PORT]],[ ]

A list of protocols and ports whose traffic will be allowed.

The protocols allowed over this connection. This can be the (case-sensitive) string values tcp, udp, icmp,esp, ah, sctp, or any IP protocol number. An IP-based protocol must be specified for each rule. The rule applies only to specified protocol.

For port-based protocols tcp, udp, and sctp a list of destination ports or port ranges to which the rule applies may optionally be specified. If no port or port range is specified, the rule applies to all destination ports.

The ICMP protocol is supported, but there is no support for configuring ICMP packet filtering by ICMP code.

For example, to create a rule that allows TCP traffic through port 80 and ICMP traffic:

gcloud compute firewall-rules create MY-RULE allow tcp:80,icmp

To create a rule that allows TCP traffic from port 20000 to 25000:

gcloud compute firewall-rules create MY-RULE allow tcp:20000-25000

To create a rule that allows all TCP traffic:

gcloud compute firewall-rules create MY-RULE allow tcp

Option B is wrong as the command would result in error.

ERROR: (gcloud.compute.firewall-rules.create) Exactly one of (action | allow) must be specified.

Option C is wrong as deny rule would prevent SSH login.

Option D is wrong as the port 3389 is for RDP and not for SSH.

34. Question

You re working on creating a script that can extract the IP address of a Kubernetes Service. Your coworker sent you a code snippet that they had saved. Which one is the best starting point for your code?

- A. kubectl get svc -o filtered-json='{.items[*].status.loadBalancer.ingress[0].ip}'
- **B. kubectl get svc -o jsonpath='{.items[*].status.loadBalancer.ingress[0].ip}'**
- C. kubectl get svc -o html
- D. kubectl get svc

Unattempted

Correct answer is B as kubectl get svc can be used to the data, and jsonpath can be used to the parse the data.

Refer Kubernetes documentation Kubenetes IO & Tutorials

$ kubectl get services NAME CLUSTER-IP EXTERNAL-IP PORT(S) kubernetes 10.0.0.1 443/TCP bootcamp 10.3.245.61 104.155.111.170 8080/TCP

To access the services, use the external IP and the application port e.g. like this:

$ export EXTERNAL_IP=$(kubectl get service bootcamp output=jsonpath='{.status.loadBalancer.ingress[0].ip}) $ export PORT=$(kubectl get services output=jsonpath='{.items[0].spec.ports[0].port}) $ curl $EXTERNAL_IP:$PORT Hello Kubernetes bootcamp! | Running on: bootcamp-390780338-2fhnk | v=1

35. Question

Your team needs to set up a new Jenkins instance as quickly as possible. What s the best way to get it up-and-running?

- A. Use Google's Managed Jenkins Service.
- B. Deploy the jar file to a Compute Engine instance.
- C. Install with Cloud Launcher
- D. Create a Deployment Manager template and deploy it.

Unattempted

Correct answer is C as Cloud Launcher provides

Refer GCP documentation Marketplace (Formerly Cloud Launcher)

GCP Marketplace offers ready-to-go development stacks, solutions, and services to accelerate development. So you spend less time installing and more time developing.

Deploy production-grade solutions in a few clicks

Single bill for all your GCP and 3rd party services

Manage solutions using Deployment Manager

Notifications when a security update is available

Direct access to partner support

Option A is wrong as there is no Google s Managed Jenkins Service.

Option B is wrong as hosting on the compute engine is still a manual step.

Option D is wrong as Deployment Manager would take time to build and deploy.

36. Question

You have a Cloud Storage bucket that needs to host static web assets with a dozen HTML pages, a few JavaScript files, and some CSS. How do you make the bucket public?

- A. Set allAuthenticatedUsers to have the Storage Object Viewer role.
- B. Check the make public box on the GCP Console for the bucket
- C. Set allUsers to have the Storage Object Viewer role.
- D. gsutil make-public gs://bucket-name

Unattempted

Correct answer is C as the bucket can be shared by providing the Storage Object Viewer access to allUsers.

Refer GCP documentation Cloud Storage Sharing files

You can either make all files in your bucket publicly accessible, or you can set individual objects to be accessible through your website. Generally, making all files in your bucket accessible is easier and faster.

To make all files accessible, follow the Cloud Storage guide for making groups of objects publicly readable.

To make individual files accessible, follow the Cloud Storage guide for making individual objects publicly readable.

If you choose to control the accessibility of individual files, you can set the default object ACL for your bucket so that subsequent files uploaded to your bucket are shared by default.

1. Open the Cloud Storage browser in the Google Cloud Platform Console.

2. In the list of buckets, click on the name of the bucket that contains the object you want to make public, and navigate to the object if it s in a subdirectory.

3. Click the drop-down menu associated with the object that you want to make public.The drop-down menu appears as three vertical dots to the far right of the object s row.

4. Select Edit permissions from the drop-down menu.

5. In the overlay that appears, click the + Add item button.

6. Add a permission for allUsers.

Select User for the Entity.

Enter allUsers for the Name.

Select Reader for the Access.

7. Click Save.

Option A is wrong as access needs to be provided to allUsers to make it public and there is no allAuthenticatedUsers option.

Option B is wrong as there is no make public option with GCP Console.

Option D is wrong as there is no make public option with gsutil command.

37. Question

Your company has been running their marketing application on App Engine app for a few weeks with Autoscaling, and it s been performing well. However, the marketing team is planning on a massive campaign, and they expect a lot of burst traffic. How would you go about ensuring there are always 3 idle instances?

- A. Set the min_instances property in the app.yaml
- B. Switch to manual scaling and use the burst_traffic_protection property to True in the app.yaml.
- **C. Set the min_idle_instances property in the app.yaml.**
- D. Switch to manual scaling and use the idle_instance_count property in the app.yaml.

Unattempted

Correct answer is C as min_idle_instances property can be set to have minimum idle instances which would be always running.

Refer GCP documentation App Engine Scaling & app.yaml Reference

Auto scaling services use dynamic instances that get created based on request rate, response latencies, and other application metrics. However, if you specify a number of minimum idle instances, that specified number of instances run as resident instances while any additional instances are dynamic.

min_idle_instances

The number of instances to be kept running and ready to serve traffic. Note that you are charged for the number of instances specified whether they are receiving traffic or not. This setting only applies to the

version that receives most of the traffic. Keep the following in mind:

A low minimum helps keep your running costs down during idle periods, but means that fewer instances might be immediately available to respond to a sudden load spike.

A high minimum allows you to prime the application for rapid spikes in request load. App Engine keeps the minimum number of instances running to serve incoming requests. You are charged for the number of instances specified, whether or not they are handling requests. For this feature to function properly, you must make sure that warmup requests are enabled and that your application handles warmup requests.

If you set a minimum number of idle instances, pending latency will have less effect on your application s performance. Because App Engine keeps idle instances in reserve, it is unlikely that requests will enter the pending queue except in exceptionally high load spikes. You will need to test your application and expected traffic volume to determine the ideal number of instances to keep in reserve.

Option A is wrong as min_instances applies to dynamic scaling. Also, number of instances

Options B & D are wrong as manual scaling would not provide the minimal running instances.

38. Question

Your team has some new functionality that they want to roll out slowly so they can monitor for errors. The change contains some significant changes to the user interface. You ve chosen to use traffic splitting to perform a canary deployment. You re going to start by rolling out the code to 15% of your users. How should you go about setting up traffic splitting with the user getting the same experience?

- A. Deploy the new version. Split the traffic using an IP or cookie based distribution.
- B. Use the gcloud app deploy command with the distribution flag to deploy and split the traffic in one command.
- C. Deploy the new version using the no-promote flag. Split the traffic using a random distribution.
- **D. Deploy the new version using the no-promote flag. Split the traffic using Cookie.**

Unattempted

Correct answer is D as the application needs to be promoted using the no-promote parameter to avoid the new version getting all the 100% traffic. Once the application is deployed and tested, the traffic can be split using the Cookie approach to maintain User experience.

Refer GCP documentation Splitting Traffic

When you have specified two or more versions for splitting, you must choose whether to split traffic by using either an IP address or HTTP cookie. It s easier to set up an IP address split, but a cookie split is more precise.

Options A & B are wrong as deploying the new version would configure it to receive all the traffic.

Option C is wrong as random distribution would not help maintain user experience.

39. Question

Your company has decided to store data files in Cloud Storage. The data would be hosted in a regional bucket to start with. You need to configure Cloud Storage lifecycle rule to move the data for archival after 30 days and delete the data after a year. Which two actions should you take?

A. Create a Cloud Storage lifecycle rule with Age: 30, Storage Class: Standard, and Action: Set to Coldline, and create a second GCS life-cycle rule with Age: 365, Storage Class: Coldline, and Action: Delete.

B. Create a Cloud Storage lifecycle rule with Age: 30, Storage Class: Standard, and Action: Set to Coldline, and create a second GCS life-cycle rule with Age: 275, Storage Class: Coldline, and Action: Delete.

C. Create a Cloud Storage lifecycle rule with Age: 30, Storage Class: Standard, and Action: Set to Nearline, and create a second GCS life-cycle rule with Age: 365, Storage Class: Nearline, and Action: Delete.

D. Create a Cloud Storage lifecycle rule with Age: 30, Storage Class: Standard, and Action: Set to Nearline, and create a second GCS life-cycle rule with Age: 275, Storage Class: Nearline, and Action: Delete.

Unattempted

Correct answer is A as there are 2 actions needed. First archival after 30 days, which can be done by SetStorageClass action to Coldline. Second delete the data after an year, which can be done by delete action with Age 365 days. The Age condition is measured from the object s creation time.

Refer GCP documentation Cloud Storage Lifecycle Management

Age: This condition is satisfied when an object reaches the specified age (in days). Age is measured from the object s creation time. For example, if an object s creation time is 2019/01/10 10:00 UTC and the Age condition is 10 days, then the condition is satisfied for the object on and after 2019/01/20 10:00 UTC. This is true even if the object becomes archived through object versioning sometime after its creation.

Option B is wrong as the Age needs to be set to 365 as its relative to the object creation date and not changed date.

Options C & D are wrong Nearline storage class is not an ideal storage class for archival

40. Question

You ve been tasked with getting all of your team s public SSH keys onto all of the instances of a particular project. You ve collected them all. With the fewest steps possible, what is the simplest way to get the keys deployed?

- A. Add all of the keys into a file that's formatted according to the requirements. Use the gcloud compute instances add-metadata command to upload the keys to each instance
- **B. Add all of the keys into a file that's formatted according to the requirements. Use the gcloud compute project-info add-metadata command to upload the keys.**
- C. Use the gcloud compute ssh command to upload all the keys
- D. Format all of the keys as needed and then, using the user interface, upload each key one at a time.

Unattempted

Correct answer is B as project wide SSH keys can help provide users access to all the instances. The keys can be added or removed using the instance metadata.

Refer GCP documentation Project wide SSH keys

Use project-wide public SSH keys to give users general access to a Linux instance. Project-wide public SSH keys give users access to all of the Linux instances in a project that allow project-wide public SSH keys. If an instance blocks project-wide public SSH keys, a user cannot use their project-wide public SSH key to connect to the instance unless the same public SSH key is also added to instance metadata.

gcloud compute project-info add-metadata metadata-from-file ssh-keys=[LIST_PATH]

Option A is wrong as the gcloud compute instances provides only specific instance level access.

Option C is wrong as gcloud compute ssh is a thin wrapper around the ssh(1)command that takes care of authentication and the translation of the instance name into an IP address. It can be used to ssh to the instance.

Option D is wrong as there is no user interface to upload the keys.

41. Question

Your developers have been thoroughly logging everything that happens in the API. The API allows end users to request the data as JSON, XML, CSV, and XLS. Supporting all of these formats is taking a lot of developer effort. Management would like to start tracking which options are used over the next month. Without modifying the code, what s the fastest way to be able to report on this data at the end of the month?

- A. Create a custom counter logging metric that uses a regex to extract the data format into a label. At the end of the month, use the metric viewer to see the group by the label.
- B. Create a log sink that filters for rows that mention the data format. Export that to BigQuery, and run a query at the end of the month.
- C. Create a custom monitoring metric in code and edit the API code to set the metric each time the API is called.
- D. Export the logs to excel, and search for the different fields.

Unattempted

Correct answer is A as custom user defined log based metrics can be created on the logs already logged. These metrics can be used at the end of the month to check the stats for API call per format to gain insights.

Refer GCP documentation Stackdriver logging Log based metrics

User-defined (logs-based) metrics are created by a user on a project. They count the number of log entries that match a given filter, or keep track of particular values within the matching log entries.

Option B is wrong as the solution is possible but not the fastest as compared to log based metric.

Option C is wrong as it required a code change.

Option D is wrong as its more manual effort and not scalable.

42. Question

You ve created a new firewall rule to allow incoming traffic on port 22, using a target tag of dev-ssh . You tried to connect to one of your instances, and you re still unable to connect. What steps do you need to take to resolve the problem?

- A. Run the gcloud firewall-rules refresh command, as they need to reloaded
- B. Use source tags in place of the target tags.
- C. Reboot the instances for the firewall rule to take effect.

D. Apply a network tag of dev-ssh to the instance you're trying to connect into and test again.

Unattempted

Correct answer is D as the firewall needs to be associated with the instance for the instance to follow the firewall rules. The association can be performed by applying the network tag dev-ssh to the instance.

Refer GCP documentation VPC Network Tags

Network tags are text attributes you can add to Compute Engine virtual machine (VM) instances. Tags allow you to make firewall rules and routes applicable to specific VM instances.

You can only add network tags to VM instances or instance templates. You cannot tag other GCP resources. You can assign network tags to new instances at creation time, or you can edit the set of assigned tags at any time later. Network tags can be edited without stopping an instance.

Option A is wrong as firewalls if associated through network tags reflect immediately and do not require any refresh.

Option B is wrong as Firewall needs to associated with target tags, which dictate the instances.

Option C is wrong as instance do not need to be rebooted and its at the network level with no changes in the instances.

43. Question

You re migrating an on-premises application to Google Cloud. The application uses a component that requires a licensing server. The license server has the IP address 10.28.0.10. You want to deploy the application without making any changes to the code or configuration. How should you go about deploying the application?

A. Create a subnet with a CIDR range of 10.28.0.0/29. Reserve a static internal IP address of 10.28.0.10. Assign the static address to the license server instance.

B. Create a subnet with a CIDR range of 10.28.0.0/28. Reserve a static external IP address of 10.28.0.10. Assign the static address to the license server instance.

C. Create a subnet with a CIDR range of 10.28.0.0/10. Reserve a static external IP address of 10.28.0.10. Assign the static address to the license server instance.

D. Create a subnet with a CIDR range of 10.28.0.0/28. Reserve a static internal IP address of 10.28.0.10. Assign the static address to the license server instance.

Unattempted

Correct answer is D as the IP is internal it can be reserved using the static internal IP address, which blocks it and prevents it from getting allocated to other resource.

Refer GCP documentation Compute Network Addresses

In Compute Engine, each VM instance can have multiple network interfaces. Each interface can have one external IP address, one primary internal IP address, and one or more secondary internal IP addresses. Forwarding rules can have external IP addresses for external load balancing or internal addresses for internal load balancing.

Static internal IPs provide the ability to reserve internal IP addresses from the private RFC 1918 IP range configured in the subnet, then assign those reserved internal addresses to resources as needed. Reserving an internal IP address takes that address out of the dynamic allocation pool and prevents it from being used for automatic allocations. Reserving static internal IP addresses requires specific IAM permissions so that only authorized users can reserve a static internal IP address.

Option A is wrong as the 10.28.0.0/29 CIDR provides only 8 IP addresses and would not include 10.28.0.10.

Options B & C are wrong as the IP address is RFC 1918 address and needs to be an internal static IP address.

44. Question

You ve been running App Engine applications in a Standard Environment for a few weeks. With several successful deployments, you ve just deployed a broken version, and the developers have gone home for the day. What is the fastest way to get the site back into a functioning state?

- A. Use the gcloud app deployments revert command.
- B. Use the gcloud app deployments rollback command.
- **C. In GCP console, click Traffic Splitting and direct 100% of the traffic to the previous version.**
- D. In GCP console, click the Rollback button on the versions page.

Unattempted

Correct answer is C as the best approach is the revert by the traffic to a previous deployed version.

Refer GCP documentation Migrating & Splitting Traffic

Traffic splitting distributes a percentage of traffic to versions of your application. You can split traffic to move 100% of traffic to a single version or to route percentages of traffic to multiple versions. Splitting traffic to two or more versions allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.

Options A & B are as gcloud app command does not provide rollback and revert feature

Option D is wrong as GCP console does not provide the ability to rollback.

45. Question

You have a 20 GB file that you need to securely share with some contractors. They need it as fast as possible. Which steps would get them the file quickly and securely?

- A. Set up a VPC with a custom subnet. Create a subnet tunnel. Upload the file to a network share. Grant the contractors temporary access.
- **B. Using composite objects and parallel uploads to upload the file to Cloud Storage quickly. Then generate a signed URL and securely share it with the contractors.**
- C. Upload the file to Bigtable using the bulk data import tool. Then provide the contractors with read access to the database.
- D. Upload the file to Cloud Storage. Grant the allAuthenticated users token view permissions.

Unattempted

Correct answer is B as the composite parallel upload can help upload the file quickly to Cloud Storage. Signed urls can be used to quickly and securely share the files with third party.

Refer GCP documentation Cloud Storage Signed URLs

Signed URLs provide a way to give time-limited read or write access to anyone in possession of the URL, regardless of whether they have a Google account

In some scenarios, you might not want to require your users to have a Google account in order to access Cloud Storage, but you still want to control access using your application-specific logic. The typical way to address this use case is to provide a signed URL to a user, which gives the user read, write, or delete access to that resource for a limited time. Anyone who knows the URL can access the resource until the URL expires. You specify the expiration time in the query string to be signed.

Option A is wrong as it is not a quick solution, but a cumbersome solution.

Option C is wrong as Bigtable is not an ideal storage for files.

Option D is wrong as All Authenticated access would provide access to anyone who is authenticated with a Google account. The special scope identifier for all Google account holders is allAuthenticatedUser

46. Question

You re using a self-serve Billing Account to pay for your 2 projects. Your billing threshold is set to $1000.00 and between the two projects you re spending roughly 50 dollars per day. It has been 18 days since you were last charged. Given the above data, when will you likely be charged next?

- A. On the first day of the next month.
- **B. In 2 days when you'll hit your billing threshold.**
- C. On the thirtieth day of the month.
- D. In 12 days, making it 30 days since the previous payment.

Unattempted

Correct answer is B as the billing is either monthly or the threshold, whichever comes first. As with average $50 per day and 18 days passed the $1000 threshold would hit in 2 days and so would be the billing.

Refer GCP documentation Cloud Storage Billing

Your costs are charged automatically in one of two ways, whichever comes first:

A regular monthly cycle (monthly billing)

When your account has accrued a certain amount of charges (threshold billing)

Options A & D are wrong as the billing would not be triggered in 12 days as the threshold would be hit first.

Option C is wrong as there is no such fixed date.

47. Question

Your company has created a new billing account and needs to move the projects to the billing account. What roles are needed to change the billing account? (Select two)

- A. Project Billing manager
- **B. Project Owner**

C. Billing Account Billing administrator

D. Billing Account Manager

E. Project Editor

Unattempted

Correct answers are B & C as To change the billing account for an existing project, you must be an owner on the project and a billing administrator on the destination billing account.

Refer GCP documentation Project Change Billing Account

48. Question

You have deployed an application using Deployment manager. You want to update the deployment with minimal downtime. How can you achieve the same?

A. gcloud deployment-manager deployments create

B. gcloud deployment-manager deployments update

C. gcloud deployment-manager resources create

D. gcloud deployment-manager resources update

Unattempted

Correct answer is B as gcloud deployment-manager deployments update can be used to update the existing deployment.

Refer GCP documentation Deployment Manager Update Deployment

After you have created a deployment, you can update it as your application or service changes. You can use Deployment Manager to update a deployment by:

Adding or removing resources from a deployment.

Updating the properties of existing resources in a deployment.

A single update can contain any combination of these changes. For example, you can make changes to the properties of existing resources and add new resources in the same request. You update your deployment by following these steps:

1. Make changes to or create a configuration file with the changes you want.

2. Optionally, pick the policies to use for your updates or use the default policies.

3. Make the update request to Deployment Manager.

gcloud deployment-manager deployments update example-deployment

Option A is wrong as gcloud deployment-manager deployments create is used to create deployment.

Options C & D are wrong as resources is not a valid parameter.

49. Question

You did a deployment for App Engine using gcloud app deploy. However, checking the intended project you do not find the deployment and seems the application was deployed in the wrong project. How do you find out which project the application was deployed to?

- A. Check app.yaml for the project
- B. Check application web.xml for the project
- C. Run gcloud config list to check for the project
- D. Check index.yaml for the project

Unattempted

Correct answer is C as By default, the deploycommand generates a unique ID for the version that you deploy, deploys the version to the GCP project you configured the gcloud tool to use, and routes all traffic to the new version.The project can be checked using the gcloud config list command.

Refer GCP documentation App Engine Deploying Application

gcloud app deploy app.yaml index.yaml

Optional flags:

Include the project flag to specify an alternate GCP Console project ID to what you initialized as the default in the gcloud tool. Example: project [YOUR_PROJECT_ID]

Include the -v flag to specify a version ID, otherwise one is generated for you. Example: -v [YOUR_VERSION_ID]

Options A, B & D are wrong as they do provide the ability to set the project.

50. Question

Your company has appointed external auditors for auditing the security of your setup. They want to check all the users and roles configured. What would be the best way to check the users and roles?

- A. Ask auditors to check using gcloud iam roles list command
- B. Ask auditors to check using gclould iam service-accounts listcommand
- C. Ask Auditors to navigate to the IAM page and check member and roles section
- D. Ask Auditors to navigate to the IAM page section and check roles and status section

Unattempted

Correct answer is C as the auditor can check all the members and roles created for the project from the IAM page listing the members and roles.

Option A is wrong as the gcloud iam roles list command would only list roles.

Option B is wrong as the gclould iam service-accounts list command would only list services accounts.

Option D is wrong as the roles menu only displays the predefined or custom roles and their status.

51. Question

Your project manager wants to delegate the responsibility to manage files and buckets for Cloud Storage to his team members. Considering the principle of least privilege, which role should you assign to the team members?

- A. roles/storage.objectAdmin
- B. roles/storage.admin
- C. roles/storage.objectCreator
- D. roles/owner

Unattempted

Correct answer is B as roles/storage.admin would provide the team members full control of buckets and objects. When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket.

Refer GCP documentation Cloud Storage IAM Roles

Options A & C are wrong as they do not provide sufficient privileges to manage buckets.

Option D is wrong as it provides more privileges than required.

52. Question

Your company is designing an application, which would interact with Cloud Spanner. The application should have the ability to view and edit Cloud Spanner tables. Considering the principle of least privilege, which role should you assign to the team members?

- A. roles/spanner.viewer
- **B. roles/spanner.databaseUser**
- C. roles/spanner.databaseReader
- D. roles/spanner.databaseAdmin

Unattempted

Correct answer is B as roles/spanner.databaseUser is a machine only roles and provides the ability to read and write to database.

Recommended to grant at the databaselevel. A principal with this role can:

Read from and write to the Cloud Spanner database.

Execute SQL queries on the database, including DML and Partitioned DML.

View and update schema for the database.

Refer GCP documentation Spanner IAM Roles

Options A & D are wrong as they are person role and either provide more or less privileges than required.

Option C is wrong as it provides only read permissions.

53. Question

A Company is using Cloud SQL to host critical data. They want to enable Point In Time recovery (PIT) to be able to recover the instance to a specific point in. How should you configure the same?

- A. Create a Read replica for the instance
- B. Switch to Spanner 3 node cluster
- C. Create a Failover replica for the instance
- **D. Enable Binary logging and backups for the instance**

Unattempted

Correct answer is D as for performing Point In Time recovery for the Cloud SQL, you should enabled backups and binary logging.

Refer GCP documentation Cloud SQL Point In Time Recovery

Point-in-time recovery enables you to recover an instance to a specific point in time. A point-in-time recovery always creates a new instance; you cannot perform a point-in-time recovery to an existing instance.

Before completing this task, you must have:

Binary logging and backups enabled for the instance, with continuous binary logs since the last backup before the event you want to recover from.For more information, see Enabling binary logging.

A binary log file name and the position of the event you want to recover from (that event and all events that came after it will not be reflected in the new instance).

Options A & C are wrong Read and Failover replicas do not aid in Point In Recovery.

Option B is wrong as it is not required to switch to Cloud Spanner.

54. Question

Your organization requires that log from all applications be archived for 10 years as a part of compliance. Which approach should you use?

- A. Configure Stackdriver Monitoring for all Projects, and export to BigQuery
- B. Configure Stackdriver Monitoring for all Projects with the default retention policies
- C. Configure Stackdriver Monitoring for all Projects, and export to Google Cloud Storage
- D. Grant the security team access to the logs in each Project

Unattempted

Correct answer is C as Stackdriver monitoring metrics can be exported to BigQuery or Google Cloud Storage. As the logs need to be archived, GCS is a better option.

Refer GCP documentation Stackdriver

Stackdriver Logging provides you with the ability to filter, search, and view logs from your cloud and open source application services. Allows you to define metrics based on log contents that are incorporated into

dashboards and alerts. Enables you to export logs to BigQuery, Google Cloud Storage, and Pub/Sub.

Option A is wrong as BigQuery would be a better storage option for analytics capability.

Option B is wrong as Stackdriver cannot retain data for 5 year. Refer Stackdriver data retention

Option D is wrong as project logs are maintained in Stackdriver and it has limited data retention capability.

55. Question

You are running an application in Google App Engine that is serving production traffic. You want to deploy a risky but necessary change to the application. It could take down your service if not properly coded. During development of the application, you realized that it can only be properly tested by live user traffic. How should you test the feature?

- A. Deploy the new application version temporarily, and then roll it back.
- B. Create a second project with the new app in isolation, and onboard users.
- C. Set up a second Google App Engine service, and then update a subset of clients to hit the new service.
- **D. Deploy a new version of the application, and use traffic splitting to send a small percentage of traffic to it.**

Unattempted

Correct answer is D as deploying a new version without assigning it as the default version will not create downtime for the application. Using traffic splitting allows for easily redirecting a small amount of traffic to the new version and can also be quickly reverted without application downtime.

Refer GCP documentation App Engine Splitting Traffic

Traffic migration smoothly switches request routing, gradually moving traffic from the versions currently receiving traffic to one or more versions that you specify.

Traffic splitting distributes a percentage of traffic to versions of your application. You can split traffic to move 100% of traffic to a single version or to route percentages of traffic to multiple versions. Splitting traffic to two or more versions allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.

Option A is wrong as deploying the application version as default requires moving all traffic to the new version. This could impact all users and disable the service.

Option B is wrong as deploying a second project requires data synchronization and having an external traffic splitting solution to direct traffic to the new application. While this is possible, with Google App Engine, these manual steps are not required.

Option C is wrong as App Engine services are intended for hosting different service logic. Using different services would require manual configuration of the consumers of services to be aware of the deployment process and manage from the consumer side who is accessing which service.

56. Question

Using principal of least privilege and allowing for maximum automation, what steps can you take to store audit logs for long-term access and to allow access for external auditors to view? (Choose two)

- [ ] A. Generate a signed URL to the Stackdriver export destination for auditors to access.
- [ ] B. Create an account for auditors to have view access to Stackdriver Logging.
- [ ] C. Export audit logs to Cloud Storage via an export sink.
- [ ] D. Export audit logs to BigQuery via an export sink.

Unattempted

Correct answers are A & C as Stackdriver logging allows export to Cloud Storage which can be used for long term access and exposed to external auditors using signed urls.

Refer GCP documentation Stackdriver logging export

Stackdriver Logging provides an operational datastore for logs and provides rich export capabilities. You might export your logs for several reasons, such as retaining logs for long-term storage (months or years) to meet compliance requirements or for running data analytics against the metrics extracted from the logs. Stackdriver Logging can export to Cloud Storage, BigQuery, and Cloud Pub/Sub.

Option B is wrong as Stackdriver logging does not support long term retention of logs

Option D is wrong as BigQuery can be used to export logs and retain for long term, however the access can be provided to only GCP users and not external auditors.

57. Question

You created an update for your application on App Engine. You want to deploy the update without impacting your users. You want to be able to roll back as quickly as possible if it fails. What should you do?

A. Delete the current version of your application. Deploy the update using the same version identifier as the deleted version.

B. Notify your users of an upcoming maintenance window. Deploy the update in that maintenance window.

C. Deploy the update as the same version that is currently running.

D. Deploy the update as a new version. Migrate traffic from the current version to the new version.

Unattempted

Correct answer is D as the deployment can be done seamlessly by deploying a new version and migrating the traffic gradually from the old version to the new version. If any issue is encountered, the traffic can be migrated 100% to the old version.

Refer GCP documentation App Engine Migrating Traffic

Manage how much traffic is received by a version of your application by migrating or splitting traffic.

Traffic migration smoothly switches request routing, gradually moving traffic from the versions currently receiving traffic to one or more versions that you specify.

Traffic splitting distributes a percentage of traffic to versions of your application. You can split traffic to move 100% of traffic to a single version or to route percentages of traffic to multiple versions. Splitting traffic to two or more versions allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.

Options A & B are wrong as there is a downtime involved.

Option C is wrong as it would not allow an easier rollback in case of any issues.

58. Question

Using the principle of least privilege, your colleague Bob needs to be able to create new instances on Compute Engine in project Project A . How should you give him access without giving more permissions than is necessary?

A. Give Bob Compute Engine Instance Admin Role for Project A.

B. Give Bob Compute Engine Admin Role for Project A.

C. Create a shared VPC that Bob can access Compute resources from.

D. Give Bob Project Editor IAM role for Project A.

Unattempted

Correct answer is A as the access needs to be given only to create instances, the user should be given compute instance admin role, which provides the least privilege.

Refer GCP documentation Compute IAM

roles/compute.instanceAdmin.v1

roles/compute.admin

Options B & D are wrong as it gives more permission than required

Option C is wrong as shared VPC does not give permissions to create instances to the use.

59. Question

You need to create a new Kubernetes Cluster on Google Cloud Platform that can autoscale the number of worker nodes. What should you do?

- A. Create a cluster on Kubernetes Engine and enable autoscaling on Kubernetes Engine.
- B. Create a cluster on Kubernetes Engine and enable autoscaling on the instance group of the cluster.
- C. Configure a Compute Engine instance as a worker and add it to an unmanaged instance group. Add a load balancer to the instance group and rely on the load balancer to create additional Compute Engine instances when needed.
- D. Create Compute Engine instances for the workers and the master and install Kubernetes. Rely on Kubernetes to create additional Compute Engine instances when needed.

Unattempted

Correct answer is A as Kubernetes cluster provides auto scaling feature which can be enabled on the cluster engine.

Refer GCP documentation Kubernetes Cluster Autoscaler

GKE s cluster autoscaler automatically resizes clusters based on the demands of the workloads you want to run. With autoscaling enabled, GKE automatically adds a new node to your cluster if you ve created new Pods that don t have enough capacity to run; conversely, if a node in your cluster is underutilized and its Pods can be run on other nodes, GKE can delete the node.

Cluster autoscaling allows you to pay only for resources that are needed at any given moment, and to automatically get additional resources when demand increases.

Option B is wrong as auto scaling is not configured on instance group.

Option C is wrong as unmanaged group cannot be scaled.

Option D is wrong as you don t manage kubernetes using compute engine.

60. Question

You are creating a solution to remove backup files older than 90 days from your backup Cloud Storage bucket. You want to optimize ongoing Cloud Storage spend. What should you do?

- A. Write a lifecycle management rule in XML and push it to the bucket with gsutil`
- **B. Write a lifecycle management rule in JSON and push it to the bucket with gsutil**
- C. Schedule a cron script using gsutil ls lr gs://backups/** to find and remove items older than 90 days
- D. Schedule a cron script using gsutil ls l gs://backups/** to find and remove items older than 90 days and schedule it with cron

Unattempted

Correct answer is B as the object lifecycle in Cloud Storage can be automatically controlled using a JSON document defining the rules.

Refer GCP documentation gsutil lifecycle

Sets the lifecycle configuration on one or more buckets. The config-json-file specified on the command line should be a path to a local file containing the lifecycle configuration JSON document.

Option A is wrong as XML is not supported by the gsutil command. It works with direct REST APIs only.

Options C & D are wrong as it is quite cumbersome to list the objects, calculate the age and then delete the objects.

61. Question

You want to create a Google Cloud Storage regional bucket logs-archive in the Los Angeles region (us-west2). You want to use Coldline storage class to minimize costs and you want to retain files for 10 years. Which of the following commands should you run to create this bucket?

- gsutil mb -l us-west2 -s nearline --retention 10y gs://logs-archive
- gsutil mb -l los-angeles -s coldline --retention 10m gs://logs-archive

gsutil mb -l us-west2 -s coldline --retention 10m gs://logs-archive

gsutil mb -l us-west2 -s coldline --retention 10y gs://logs-archive

Unattempted

gsutil mb -l us-west2 -s nearline retention 10y gs://logs-archive. is not right.
This command creates a bucket that uses nearline storage class whereas we want to use Coldline storage class.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

gsutil mb -l los-angeles -s coldline retention 10m gs://logs-archive. is not right.
This command uses los-angeles as the location but los-angeles is not a supported region name. The region name for Los Angeles is us-west-2.
Ref: https://cloud.google.com/storage/docs/locations

gsutil mb -l us-west2 -s coldline retention 10m gs://logs-archive. is not right.
This command creates a bucket with retention set to 10 months whereas we want to retain the objects for 10 years.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

gsutil mb -l us-west2 -s coldline retention 10y gs://logs-archive. is the right answer.
This command correctly creates a bucket in Los Angeles, uses Coldline storage class and retains objects for 10 years.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

62. Question

You want to create a new role and grant it to the SME team. The new role should provide your SME team BigQuery Job User and Cloud Bigtable User roles on all projects in the organization. You want to minimize operational overhead. You want to follow Google recommended practices. How should you create the new role?

Execute command gcloud iam combineroles --global to combine the 2 roles into a new custom role and grant them globally to SME team group.

In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at the organization level.

In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Use gcloud iam promote-role to promote the role to all other projects and grant the role in each project to the SME team group.

In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Repeat this step for each project.

Unattempted

We want to create a new role and grant it to a team. Since you want to minimize operational overhead, we need to grant it to a group so that new users who join the team just need to be added to the group and they inherit all the permissions. Also, this team needs to have the role for all projects in the organization. And since we want to minimize the operational overhead, we need to grant it at the organization level so that all current projects, as well as future projects, have the role granted to them. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Repeat this step for each project. is not right. ?Repeating the step for all projects is a manual, error-prone and time-consuming task. Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Use gcloud iam promote-role to promote the role to all other projects and grant the role in each project to the SME team group. is not right.

?Repeating the step for all projects is a manual, error-prone and time-consuming task. Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead. Execute command gcloud iam combine-roles global to combine the 2 roles into a new custom role and grant them globally to all. is not right.

?There are several issues with this. gcloud iam command doesn t support the action combine-roles. Secondly, we don t want to grant the roles globally. We want to grant them to the SME team and no one else. In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at the organization level. is the right answer.

?This correctly creates the role and assigns the role to the group at the organization. When any new users join the team, the only additional task is to add them to the group. Also, when a new project is created under the organization, no additional human intervention is needed. Since the role is granted at the organization level, it automatically is granted to all the current and future projects belonging to the organization.

63. Question

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?

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

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 --metadata-from-file 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 --startup-script=/scripts/install_app.sh

Unattempted

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

64. Question

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

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

Unattempted

1. Create a Cloud Function that uses a Cloud Pub/Sub trigger on that topic.
2. Call your application on Cloud Run from the Cloud Function for every message. is not right.
Both Cloud functions and Cloud Run are serverless offerings from GCP and they are both capable of integrating with Cloud Pub/Sub. It is pointless to invoking Cloud Function from Cloud Run.

1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run.
2. Create a Cloud Pub/Sub subscription for that topic.
3. Make your application pull messages from that subscription. is not right.
You need to provide Cloud Run Invoker role to that service account for your Cloud Run application.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub

1. Deploy your application on Cloud Run on GKE with the connectivity set to Internal.
2. Create a Cloud Pub/Sub subscription for that topic.
3. In the same Google Kubernetes Engine cluster as your application, deploy a container that takes the messages and sends them to your application. is not right.
Like above, you need cloud Run Invoker role on the service account.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub
Also, our question states the application on Cloud Run processes messages from a Cloud Pub/Sub topic; whereas in this option, we are utilizing a separate container to process messages from the topic. So this doesn t satisfy our requirements.

1. Create a service account.

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

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

This exact process is described in

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

You create a service account.

```
gcloud iam service-accounts create cloud-run-pubsub-invoker \
 display-name  Cloud Run Pub/Sub Invoker
```

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

```
gcloud run services add-iam-policy-binding pubsub-tutorial \
 member=serviceAccount:cloud-run-pubsub-invoker@PROJECT_ID.iam.gserviceaccount.com \
 role=roles/run.invoker
```

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

```
gcloud pubsub subscriptions create myRunSubscription  topic myRunTopic \
 push-endpoint=SERVICE-URL/ \
 push-auth-service-account=cloud-run-pubsub-invoker@PROJECT_ID.iam.gserviceaccount
```

65. Question

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

- gcloud compute instances create [INSTANCE_NAME] --preemptible --no-boot-disk-auto-delete
- gcloud compute instances create [INSTANCE_NAME] --preemptible --boot-disk-auto-delete=no
- gcloud compute instances create [INSTANCE_NAME] --no-auto-delete
- gcloud compute instances create [INSTANCE_NAME] --preemptible. The flag --boot-disk-auto-delete is disabled by default.

Unattempted

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

gcloud compute instances create doesn t provide a parameter called boot-disk-auto-delete. It does have a flag by the same name. boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use no-boot-disk-auto-delete to disable.

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

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

boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the

instances are deleted. Use no-boot-disk-auto-delete to disable.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

gcloud compute instances create [INSTANCE_NAME] no-auto-delete. is not right.
gcloud compute instances create doesn t provide a flag called no-auto-delete
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

gcloud compute instances create [INSTANCE_NAME] preemptible no-boot-disk-auto-delete. is the right answer.
Use no-boot-disk-auto-delete to disable automatic deletion of boot disks when the instances are deleted. boot-disk-auto-delete flag is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. In order to prevent automatic deletion, we have to specify no-boot-disk-auto-delete flag.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

Use Page numbers below to navigate to other practice tests

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13

← Previous Post Next Post →

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy