SKILLCERTPRO

IT CERTIFICATION TRAININGS

0

Google Cloud / By SkillCertPro

Practice Set 6

Your results are here!! for" Google Certified Associate Cloud Engineer Practice Test 6 "

0 of 69 questions answered correctly

Your time: 00:00:44

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	53.73%
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

35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51
52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68
69

Correct Incorrect

Review Question Summary

1. Question

You've been asked to add a new IAM member and grant her access to run some queries on BigQuery. Considering the principle of least privilege, which role should you assign?

- A. roles/bigquery.dataEditor and roles/bigquery.jobUser
- B. roles/bigquery.dataViewer and roles/bigquery.user
- C. roles/bigquery.dataViewer and roles/bigquery.jobUser
- D. roles/bigquery.dataOwner and roles/bigquery.jobUser

Unattempted

Correct answer is C as the user needs to only query the data, they should have access to view the dataset and query the dataset which would provided
by roles/bigquery.dataViewer and roles/bigquery.jobUser inline with the least privilege principle
Refer GCP documentation – BigQuery Access Control
Option A is wrong as roles/bigquery.dataEditor provides more than required privileges
Option B is wrong as roles/bigquery.user provides more than required privileges
Option D is wrong as roles/bigquery.dataOwner provides more than required privileges

2. Question

You have a managed instance group comprised of preemptible VM's. All of the VM's keep deleting and recreating themselves every minute. What is a possible cause of this behavior?

- A. Your zonal capacity is limited, causing all preemptible VM's to be shutdown to recover capacity. Try deploying your group to another zone.
- B. You have hit your instance quota for the region.
- C. Your managed instance group's VM's are toggled to only last 1 minute in preemptible settings.

D. Your managed instance group's health check is repeatedly failing, either to a misconfigured health check or misconfigured firewall rules not allowing the health check to access the instances.

Unattempted

Correct answer is D as the instances (normal or preemptible) would be terminated and relaunched if the health check fails either due to application not configured properly or the instances firewall do not allow health check to happen.

Refer GCP documentation – Health Check concepts

GCP provides health check systems that connect to virtual machine (VM) instances on a configurable, periodic basis. Each connection attempt is called a probe. GCP records the success or failure of each probe.

Health checks and load balancers work together. Based on a configurable number of sequential successful or failed probes, GCP computes an overall health state for each VM in the load balancer. VMs that respond successfully for the configured number of times are considered healthy. VMs that fail to respond successfully for a separate number of times are unhealthy.

GCP uses the overall health state of each VM to determine its eligibility for receiving new requests. In addition to being able to configure probe frequency and health state thresholds, you can configure the criteria that define a successful probe.

3. Question

You write a Python script to connect to Google BigQuery from a Google Compute Engine virtual machine. The script is printing errors that it cannot connect to BigQuery. What should you do to fix the script?

A. Install the latest BigQuery API client library for Python

B. Run your script on a new virtual machine with the BigQuery access scope enabled

C. Create a new service account with BigQuery access and execute your script with that user

D. Install the bq component for gcloud with the command gcloud components install bq.

Unattempted

Correct answer is B as by default an instance is associated with default service account and default access scope, neither of which provides an access to BigQuery. While Service account is the recommended approach and Access scope are legacy, access scope still need to granted to the instance for applications to access the services. So enabling only the Service Account with role would not enable the script to access BigQuery.

Refer GCP documentation – Service Account

When you set up an instance to run as a service account, you determine the level of access the service account has by the IAM roles you grant to the service account. If the service account has no IAM roles, then no API methods can be run by the service account on that instance.

Furthermore, an instance's access scopes determine the default OAuth scopes for requests made through the gcloudtool and client libraries on the instance. As a result, access scopes potentially further limit access to API methods when authenticating through OAuth. However, they do not extend to other authentication protocols like gRPC.

The best practice is to set the full cloud-platform access scope on the instance, then securely limit the service account's access using IAM roles.

Essentially:

IAM restricts access to APIs based on the IAM roles that are granted to the service account.

Access scopes potentially further limit access to API methods when authenticating through OAuth.

You must set access scopes on the instance to authorize access.

While a service account's access level is determined by the IAM roles granted to the service account, an instance's access scopes determine the default OAuth scopes for requests made through the gcloud tool and client libraries on the instance. As a result, access scopes potentially further limit access to API methods when authenticating through OAuth.

Option A is wrong as it is an issue with connectivity to BigQuery and not a client version mismatch issue.

Option C is wrong as adding a service account would not work without having the access granted through access scope.

Option D is wrong as bq command is installed by default and not needed with the python client. It is for direct command line interaction with BigQuery.

4. Question

You have created a Kubernetes engine cluster named 'project-1'. You've realized that you need to change the machine type for the cluster from n1-standard-1 to n1-standard-4. What is the command to make this change?

- A. Create a new node pool in the same cluster, and migrate the workload to the new pool.
- B. gcloud container clusters resize project-1 --machine-type n1-standard-4
- C. gcloud container clusters update project-1 --machine-type n1-standard-4
- D. gcloud container clusters migrate project-1 --machine-type n1-standard-4

Unattempted

Correct answer is A as the machine type for the cluster cannot be changed through commands. A new node pool with the updated machine type needs to be created and workload migrated to the new node pool.

Refer GCP documentation – Kubernetes Engine – Migrating Node Pools

A node pool is a subset of machines that all have the same configuration, including machine type (CPU and memory) authorization scopes. Node pools represent a subset of nodes within a cluster; a container cluster can contain one or more node pools.

When you need to change the machine profile of your Compute Engine cluster, you can create a new node pool and then migrate your workloads over to the new node pool.

To migrate your workloads without incurring downtime, you need to:

Mark the existing node pool as unschedulable.

Drain the workloads running on the existing node pool.

Delete the existing node pool.

5. Question

You need to have a backup/rollback plan in place for your application that is distributed across a large managed instance group. What is the preferred method for doing so?

- A. Use the Rolling Update feature to deploy/roll back versions with different managed instance group templates.
- B. Use the managed instance group snapshot function that is included in Compute Engine.
- C. Have each instance write critical application data to a Cloud Storage bucket.
- D. Schedule a cron job to take snapshots of each instance in the group.

Unattempted

Correct answer is A as rolling update helps to apply the update on a controlled number of instances to maintain high availability and ability to rollback in case of any issues.

Refer GCP documentation – Updating Managed Instance Groups

A managed instance group contains one or more virtual machine instances that are controlled using an instance template. To update instances in a managed instance group, you can make update requests to the group as a whole, using the Managed Instance Group Updater feature.

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 of deployment, the level of disruption to your service, and the scope of the update. The Updater offers two primary advantages:

The rollout of an update happens automatically to your specifications, without the need for additional user input after the initial request.

You can perform partial rollouts which allows for canary testing.

By allowing new software to be deployed inside an existing managed instance group, there is no need for you to reconfigure the instance group or reconnect load balancing, autoscaling, or autohealing each time new version of software is rolled out. Without the Updater, new software versions must be deployed either by creating a new managed instance group with a new software version, requiring additional set up each time, or through a manual, user-initiated, instance-by-instance recreate. Both of these approaches require significant manual steps throughout the process.

A rolling update is an update that is gradually applied to all instances in an instance group until all instances have been updated. You can control various aspects of a rolling update, such as how many

instances can be taken offline for the update, how long to wait between updating instances, whether the update affects all or just a portion of instances, and so on.
Options B, C & D are wrong as the key for scaling is to create stateless, disposable VMs to be able scale and have seamless deployment.

6. Question

You have a project using BigQuery. You want to list all BigQuery jobs for that project. You want to set this project as the default for the bq command-line tool. What should you do?

- A. Use gcloud config set project to set the default project
- B. Use bq config set project to set the default project.
- C. Use gcloud generate config-url to generate a URL to the Google Cloud Platform Console to set the default project.
- D. Use bq generate config-url to generate a URL to the Google Cloud Platform Console to set the default project.

Unattempted
Correct answer is A as you need to use gcloud to manage the config/defaults.
Refer GCP documentation – Cloud SDK Config Set
–project=PROJECT_ID
The Google Cloud Platform project name to use for this invocation. If omitted, then the current project is assumed; the current project can be listed using gcloud config list –format='text(core.project)' and can be set using gcloud config set project PROJECTID. Overrides the default core/project property value for this command invocation.
Option B is wrong as the bq command-line tool assumes the gcloud configuration settings and can't be set through BigQuery.
Option C is wrong as entering this command will not achieve the desired result and will generate an error.
Option D is wrong as entering this command will not achieve the desired result and will generate an error.

7. Question

You're deploying an application to a Compute Engine instance, and it's going to need to make calls to read from Cloud Storage and Bigtable. You want to make sure you're following the principle of least privilege. What's the easiest way to ensure the code can authenticate to the required Google Cloud APIs?

- A. Create a new user account with the required roles. Store the credentials in Cloud Key Management Service and download them to the instance in code.

B. Use the default Compute Engine service account and set its scopes. Let the code find the default service account using Application Default Credentials.

C. Create a new service account and key with the required limited permissions. Set the instance to use the new service account. Edit the code to use the service account key.

D. Register the application with the Binary Registration Service and apply the required roles.

Unattempted

Correct answer is C as the best practice is to use a Service Account to grant the application the required access.

Refer GCP documentation – Service Accounts

A service account is a special type of Google account that belongs to your application or a virtual machine (VM), instead of to an individual end user. Your application assumes the identity of the service account to call Google APIs, so that the users aren't directly involved.

A service account is a special type of Google account that represents a Google Cloud service identity or app rather than an individual user. Like users and groups, service accounts can be assigned IAM roles to grant access to specific resources. Service accounts authenticate with a key rather than a password. Google manages and rotates the service account keys for code running on GCP. We recommend that you use service accounts for server-to-server interactions.

Option A is wrong as it is not the recommended approach

Option B is wrong as the default Service Account does not have the required permissions.

Option D is wrong as there is Binary Registration service.

8. Question

You've been trying to deploy a container to Kubernetes; however, kubectl doesn't seem to be able to connect to the cluster. Of the following, what is the most likely cause and how can you fix it?

A. The firewall rules are preventing the connection. Open up the firewall rules to allow traffic to port 1337.

B. The kubeconfig is missing the credentials. Run the gcloud container clusters get-credentials command.

C. The kubeconfig is missing the credentials. Run the gcloud container clusters auth login command.

D. The firewall rules are preventing the connection. Open up the firewall rules to allow traffic to port 3682.

Unattempted

Correct answer is B as the connection is refused, the context needs to be set using the gcloud container clusters get-credentials command

Refer GCP documentation – Kubernetes Engine Troubleshooting

kubectl commands return "connection refused" error

Set the cluster context with the following command:

gcloud container clusters get-credentials [CLUSTER_NAME]

If you are unsure of what to enter for CLUSTER_NAME, use the following command to list your clusters:

gcloud container clusters list

Options A & D are wrong as only SSH access is required and it is automatically added.

Option C is wrong as auth login would be needed if the Resource was not found.

9. Question

Your engineers have hardcoded the database credentials to be used by application on Kubernetes Engine.

The YAML they're using looks similar to the following:

apiVersion: "extensions/v1beta1"

kind: "Deployment"

metadata:

name: "products-service"

namespace: "default"

labels:

app: "products-service"

spec:

replicas: 3

selector:

matchLabels:

app: "products-service"

template:

metadata:

labels:

app: "products-service"

spec:

containers:

– name: "products"

image: "gcr.io/find-seller-app-dev/products:latest"

env:

– name: "database_user"

value: "admin"

– name: "database_password"

value: "TheB3stP@ssW0rd"

What is Google's recommended best practice for working with sensitive information inside of Kubernetes?

- A. Store the credentials in a ConfigMap.

B. Mount the credentials in a volume.

C. Use an environment variable.

D. Store the credentials in a Secret.

Unattempted

Correct answer is D as the Kubernetes allows credentials to be stored in Secret, which can be used by the containers.

Refer GCP documentation – Kubernetes Secrets

Kubernetes offers the Secret resource type to store credentials inside the container cluster and use them in the applications deployed on GKE directly.

Kubernetes secret objects let you store and manage sensitive information, such as passwords, OAuth tokens, and ssh keys. Putting this information in a secret is safer and more flexible than putting it verbatim in a Pod Lifecycle definition or in a container image.

Option A is wrong as ConfigMaps bind configuration files, command-line arguments, environment variables, port numbers, and other configuration artifacts to your Pods' containers and system components at runtime. ConfigMaps allow you to separate your configurations from your Pods and components, which helps keep your workloads portable, makes their configurations easier to change and manage, and prevents hardcoding configuration data to Pod specifications.

Option B is wrong as credentials cannot be mounted in the volume.

Option C is wrong as environment variable does not secure the credentials.

10. Question

A SysOps admin has configured a lifecycle rule on an object versioning disabled multi-regional bucket.

Which of the following statement effect reflects the following lifecycle config?

```
{
“rule”:
[
{
“action”: {“type”: “Delete”},
“condition”: {“age”: 30, “isLive”: false}
},
{
“action”: {“type”: “SetStorageClass”, “storageClass”: “COLDLINE”},
“condition”: {“age”: 365, “matchesStorageClass”: “MULTI_REGIONAL”}
}
]
}
```

A. Archive objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional

B. Delete objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.

C. Delete archived objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.

D. Move objects to Coldline Storage after 365 days if the storage class in Multi-regional First rule has no effect on the bucket.

Unattempted

Correct answer is D.

First rule will delete any object if it has a age over 30 days and is not live (not the latest version). However as the bucket is not versioning enabled it does not have any effect. Second rule will change the storage class of the live object from multi-regional to Coldline for objects with age over 365 days.

Refer GCP documentation – Object Lifecycle

The following conditions are supported for a lifecycle rule:

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.

CreatedBefore: This condition is satisfied when an object is created before midnight of the specified date in UTC.

IsLive: If the value is true, this lifecycle condition matches only live objects; if the value is false, it matches only archived objects. For the purposes of this condition, objects in non-versioned buckets are considered live.

MatchesStorageClass: This condition is satisfied when an object in the bucket is stored as the specified storage class. Generally, if you intend to use this condition on Multi-Regional Storage or Regional Storage objects, you should also include STANDARD and DURABLE_REDUCED_AVAILABILITY in the condition to ensure all objects of similar storage class are covered.

Option A is wrong as the first rule does not archive but deletes the archived objects, but does not have any impact on a versioning disabled bucket.

Option B is wrong as the first rule does not delete live objects but only archives objects.

Option C is wrong as first rule does not have any impact on a versioning disabled bucket.

11. Question

A SysOps admin has configured a lifecycle rule on an object versioning enabled multi-regional bucket.

Which of the following statement effect reflects the following lifecycle config?

```
{
“rule”:
[
{
“action”: {“type”: “Delete”},
“condition”: {“age”: 30, “isLive”: false}
},
{
“action”: {“type”: “SetStorageClass”, “storageClass”: “COLDLINE”},
“condition”: {“age”: 365, “matchesStorageClass”: “MULTI_REGIONAL”}
}
]
}
```

- A. Archive objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional
- B. Delete objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.
- **C. Delete archived objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.**
- D. Move objects to Coldline Storage after 365 days if the storage class in Multi-regional First rule has no effect on the bucket.

Unattempted

Correct answer is C.

First rule will delete any object if it has a age over 30 days and is not live (not the latest version). Second rule will change the storage class of the live object from multi-regional to Coldline for objects with age over 365 days.

Refer GCP documentation – Object Lifecycle

The following conditions are supported for a lifecycle rule:

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.

CreatedBefore: This condition is satisfied when an object is created before midnight of the specified date in UTC.

IsLive: If the value is true, this lifecycle condition matches only live objects; if the value is false, it matches only archived objects. For the purposes of this condition, objects in non-versioned buckets are

considered live.

MatchesStorageClass: This condition is satisfied when an object in the bucket is stored as the specified storage class. Generally, if you intend to use this condition on Multi-Regional Storage or Regional Storage objects, you should also include STANDARD and DURABLE_REDUCED_AVAILABILITY in the condition to ensure all objects of similar storage class are covered.

Option A is wrong as the first rule does not archive but deletes the archived objects.

Option B is wrong as the first rule does not delete live objects but only archives objects.

Option D is wrong as first rule applies to archived or not live objects.

12. Question

A SysOps admin has configured a lifecycle rule on an object versioning enabled multi-regional bucket.

Which of the following statement effect reflects the following lifecycle config?

```
{
“rule”:
[
{
“action”: {“type”: “Delete”},
“condition”: {“age”: 30, “isLive”: false}
},
{
“action”: {“type”: “SetStorageClass”, “storageClass”: “COLDLINE”},
“condition”: {“age”: 365, “matchesStorageClass”: “MULTI_REGIONAL”}
}
]
}
```

- A. Archive objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional
- B. Delete objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.
- **C. Delete archived objects older than 30 days and move objects to Coldline Storage after 365 days if the storage class in Multi-regional.**
- D. Move objects to Coldline Storage after 365 days if the storage class in Multi-regional First rule has no effect on the bucket.

Unattempted

Correct answer is C.

First rule will delete any object if it has a age over 30 days and is not live (not the latest version). Second

rule will change the storage class of the live object from multi-regional to Coldline for objects with age over 365 days.

Refer GCP documentation – Object Lifecycle

The following conditions are supported for a lifecycle rule:

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.

CreatedBefore: This condition is satisfied when an object is created before midnight of the specified date in UTC.

IsLive: If the value is true, this lifecycle condition matches only live objects; if the value is false, it matches only archived objects. For the purposes of this condition, objects in non-versioned buckets are considered live.

MatchesStorageClass: This condition is satisfied when an object in the bucket is stored as the specified storage class. Generally, if you intend to use this condition on Multi-Regional Storage or Regional Storage objects, you should also include STANDARD and DURABLE_REDUCED_AVAILABILITY in the condition to ensure all objects of similar storage class are covered.

Option A is wrong as the first rule does not archive but deletes the archived objects.

Option B is wrong as the first rule does not delete live objects but only archives objects.

Option D is wrong as first rule applies to archived or not live objects.

13. Question

You want to enable your running Google Container Engine cluster to scale as demand for your application changes. What should you do?

- A. Add additional nodes to your Container Engine cluster using the following command: gcloud container clusters resize CLUSTER_Name –-size 10
- B. Add a tag to the instances in the cluster with the following command: gcloud compute instances add-tags INSTANCE --tags --enable-autoscaling max-nodes-10
- **C. Update the existing Container Engine cluster with the following command: gcloud alpha container clusters update mycluster –-enable-autoscaling –-min-nodes=1 –-max-nodes=10**
- D. Create a new Container Engine cluster with the following command: gcloud alpha container clusters create mycluster --enable-autoscaling --min-nodes=1 --max-nodes=10 and redeploy your application

Unattempted

Correct answer is C as you need to update the cluster to enable auto scaling with min and max nodes to scale as per the demand.

Refer GCP documentation – Cluster Autoscaling

Option A is wrong as it would only increase the nodes.

Option B is wrong as the cluster needs to updated and not the instances.

Option D is wrong as you do not need to create a new cluster and the existing cluster can be updated to enable auto scaling.

14. Question

You've set up an instance inside your new network and subnet. Your firewall rules are set to target all instances in your network with the following firewall rules.

NAME:deny-all | NETWORK:devnet | DIRECTION:INGRESS | PRIORITY:1000 | DENY:tcp:0-65535,udp:0-6553

NAME:open-ssh | NETWORK:devnet | DIRECTION:INGRESS | PRIORITY:5000 | ALLOW:tcp:22

However, when you attempt to connect to your instance via SSH, your connection is timing out. What is the most likely cause?

- A. SSH would be denied and would need instance reboot for the allow rule to take effect
- B. SSH key hasn't been uploaded to the instance.
- C. Firewall rule needs to be applied to the instance specifically.
- **D. SSH would be denied as the deny rule overrides the allow**

Unattempted

Correct answer is D as the firewall rules are applied as per the priority and as the deny rule has the higher priority as compared to the allow rule, the SSH access is denied.

Refer GCP documentation – VPC Firewall Rules – Priority

The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. If you do not specify a priority when creating a rule, it is assigned a priority of 1000.

The relative priority of a firewall rule determines if it is applicable when evaluated against others. The evaluation logic works as follows:

The highest priority rule applicable to a target for a given type of traffic takes precedence. Target specificity does not matter. For example, a higher priority ingress rule for certain ports and protocols intended for all targets overrides a similarly defined rule for the same ports and protocols intended for specific targets.

The highest priority rule applicable for a given protocol and port definition takes precedence, even when the protocol and port definition is more general. For example, a higher priority ingress rule allowing traffic for all protocols and ports intended for given targets overrides a lower priority ingress rule denying TCP 22 for the same targets.

A rule with a deny action overrides another with an allow action only if the two rules have the same priority. Using relative priorities, it is possible to build allowrules that override deny rules, and vice versa. Rules with the same priority and the same action have the same result. However, the rule that is used during the evaluation is indeterminate. Normally, it doesn't matter which rule is used except when you enable firewall rule logging. If you want your logs to show firewall rules being evaluated in a consistent and well-defined order, assign them unique priorities.
Option A is wrong as firewall rules are applied directly and do not require an instance restart.
Option B is wrong as SSH are autogenerated and transferred to the instance.
Option C is wrong as firewall are not applied to instance directly but through network tags.

15. Question

You've set up an instance inside your new network and subnet. You create firewall rules to target all instances in your network with the following firewall rules.
NAME:open-ssh | NETWORK:devnet | DIRECTION:INGRESS | PRIORITY:1000 | ALLOW:tcp:22
NAME:deny-all | NETWORK:devnet | DIRECTION:INGRESS | PRIORITY:5000 | DENY:tcp:0-65535,udp:0-6553
If you try to SSH to the instance, what would be the result?

- A. SSH would be denied and would need gcloud firewall refreshcommand for the allow rule to take effect.
- **B. SSH would be allowed as the allow rule overrides the deny**
- C. SSH would be denied as the deny rule overrides the allow
- D. SSH would be denied and would need instance reboot for the allow rule to take effect

Unattempted
Correct answer is B as the firewall rules are applied as per the priority and as the allow rule has the higher priority as compared to the deny rule, the SSH access is allowed.
Refer GCP documentation – VPC Firewall Rules – Priority
The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. If you do not specify a priority when creating a rule, it is assigned a priority of 1000.
The relative priority of a firewall rule determines if it is applicable when evaluated against others. The evaluation logic works as follows:
The highest priority rule applicable to a target for a given type of traffic takes precedence. Target specificity does not matter. For example, a higher priority ingress rule for certain ports and protocols intended for all targets overrides a similarly defined rule for the same ports and protocols intended for specific targets.
The highest priority rule applicable for a given protocol and port definition takes precedence, even when the protocol and port definition is more general. For example, a higher priority ingress rule allowing traffic

for all protocols and ports intended for given targets overrides a lower priority ingress rule denying TCP 22 for the same targets.

A rule with a deny action overrides another with an allow action only if the two rules have the same priority. Using relative priorities, it is possible to build allowrules that override deny rules, and vice versa. Rules with the same priority and the same action have the same result. However, the rule that is used during the evaluation is indeterminate. Normally, it doesn't matter which rule is used except when you enable firewall rule logging. If you want your logs to show firewall rules being evaluated in a consistent and well-defined order, assign them unique priorities.

Options A, C & D are wrong the SSH access would be allowed.

16. Question

Your company has a number of internal backends that they do not want to be exposed to the public Internet. How can they reduce their external exposure while still allowing maintenance access to resources when working remotely?

- A. Remove the external IP address and use Cloud Shell to access internal-only resources
- **B. Remove the external IP address and use a bastion host to access internal-only resources.**
- C. Remove the external IP address and have remote employees dial into the company VPN connection for maintenance work.
- D. Hide the external IP address behind a load balancer and restrict load balancer access to the internal company network.

Unattempted

Correct answer is B as it is a best practice to remove external ip address from the instances so that they are not reachable from the internet and have a Bastion host of Jump server to be able to login into the servers.

Refer GCP documentation – Bastion Hosts

Bastion hosts provide an external facing point of entry into a network containing private network instances. This host can provide a single point of fortification or audit and can be started and stopped to enable or disable inbound SSH communication from the Internet.

By using a bastion host, you can connect to an instance that does not have an external IP address. This approach allows you to connect to a development environment or manage the database instance for your external application, for example, without configuring additional firewall rules.

A complete hardening of a bastion host is outside the scope of this article, but some initial steps taken can include:

Limit the CIDR range of source IPs that can communicate with the bastion.

Configure firewall rules to allow SSH traffic to private instances from only the bastion host.

By default, SSH on instances is configured to use private keys for authentication. When using a bastion

host, you log into the bastion host first, and then into your target private instance. Because of this two-step login, which is why bastion hosts are sometimes called "jump servers," you should use ssh-agent forwarding instead of storing the target machine's private key on the bastion host as a way of reaching the target machine. You need to do this even if using the same key-pair for both bastion and target instances, as the bastion has direct access to only the public half of the key-pair.

17. Question

The development team has provided you with a Kubernetes Deployment file. You have no infrastructure yet and need to deploy the application. What should you do?

- A. Use gcloud to create a Kubernetes cluster. Use Deployment Manager to create the deployment.
- **B. Use gcloud to create a Kubernetes cluster. Use kubectl to create the deployment.**
- C. Use kubectl to create a Kubernetes cluster. Use Deployment Manager to create the deployment.
- D. Use kubectl to create a Kubernetes cluster. Use kubectl to create the deployment.

Unattempted

Correct answer is B as you would need gcloud to create a kubernetes cluster. Once the cluster is created you can use kubectl to manage the deployments.

Refer GCP documentation – Kubernetes Cluster Tutorial

To create a cluster with the gcloud command-line tool, use the gcloud container clusters command:

gcloud container clusters create hello-cluster –num-nodes=3

To deploy and manage applications on a GKE cluster, you must communicate with the Kubernetes cluster management system. You typically do this by using the kubectl command-line tool.

Kubernetes represents applications as Pods, which are units that represent a container (or group of tightly-coupled containers). The Pod is the smallest deployable unit in Kubernetes. In this tutorial, each Pod contains only your hello-app container.

The kubectl run command below causes Kubernetes to create a Deployment named hello-web on your cluster. The Deployment manages multiple copies of your application, called replicas, and schedules them to run on the individual nodes in your cluster. In this case, the Deployment will be running only one Pod of your application.

kubectl run hello-web –image=gcr.io/${PROJECT_ID}/hello-app:v1 –port 8080

Options A & C are wrong as you need kubectl to do a kubernetes deployment.

Options C & D are wrong as you need gcloud to create the kubernetes cluster.

18. Question

One of the microservices in your application has an intermittent performance problem. You have not observed the problem when it occurs but when it does, it triggers a particular burst of log lines. You want to debug a machine while the problem is occurring. What should you do?

A. Log into one of the machines running the microservice and wait for the log storm.

B. In the Stackdriver Error Reporting dashboard, look for a pattern in the times the problem occurs.

C. Configure your microservice to send traces to Stackdriver Trace so you can find what is taking so long.

D. Set up a log metric in Stackdriver Logging, and then set up an alert to notify you when the number of log lines increases past a threshold.

Unattempted

Correct answer is D as there is a burst of log lines you can set up a metric that identifies those lines. Stackdriver will also allow you to set up a text, email or messaging alert that can notify promptly when the error is detected so you can hop onto the system to debug.

Option A is wrong as logging into an individual machine may not see the specific performance problem as multiple machines may be in the configuration and reducing the chances of interacting with an intermittent performance problem.

Option B is wrong as error reporting won't necessarily catch the log lines unless they are stack traces in the proper format. Additionally just because there is a pattern doesn't mean you will know exactly when and where to log in to debug.

Option C is wrong as trace may tell you where time is being spent but wont let you hone in on the exact host that the problem is occurring on because you generally only send samples of traces. There is also no alerting on traces to notify exactly when the problem is happening.

19. Question

You're writing a Java application with lot a threading and concurrency. You want your application to run in a sandboxed managed environment with the ability to perform SSH debugging to check on any thread dump for troubleshooting. Which service should you host your application on?

A. Compute Engine

B. App Engine Flexible Environment

C. Cloud Functions

D. App Engine Standard Environment

Unattempted

Correct answer is B as App Engine provides the managed service and Flexible environment supports the ability to perform SSH debugging.

Refer GCP documentation – App Engine Environments

Feature – SSH-debugging

Standard environment – No

Flexible environment – Yes
Flexible environment instances are permitted to have higher CPU and memory limits than is possible with standard environment instances. This allows flexible instances to run applications that are more memory and CPU intensive. However, it may increase the likelihood of concurrency bugs due to the increase in threads within a single instance.
Developers can SSH to an flexible environment instance and obtain a thread dump to troubleshoot this type of problem.
Option A is wrong as Compute Engine does not provide managed service
Option C is wrong as Cloud Functions provides serverless event driven compute platform.
Option D is wrong as App Engine Standard environment does not provide SSH debugging

20. Question

Several employees at your company have been creating projects with Cloud Platform and paying for it with their personal credit cards, which the company reimburses. The company wants to centralize all these projects under a single, new billing account. What should you do?

- A. Contact cloud-billing@google.com with your bank account details and request a corporate billing account for your company.
- B. Create a ticket with Google Support and wait for their call to share your credit card details over the phone.
- **C. In the Google Platform Console, go to the Resource Manager and move all projects to the root Organization.**
- D. ?In the Google Cloud Platform Console, create a new billing account and set up a payment method.

Unattempted
Correct answer is C as Google Cloud Resource Manager can help group the existing accounts under an Organization for centralized billing.
Refer GCP documentation – Resource Manager
Google Cloud Platform (GCP) customers need an easy way to centrally manage and control GCP resources, projects and billing accounts that belong to their organization. As companies grow, it becomes progressively difficult to keep track of an ever-increasing number of projects, created by multiple users, with different access control policies and linked to a variety of billing instruments. Google Cloud Resource Manager allows you to group resource containers under the Organization resource, providing full visibility, centralized ownership and unified management of your company's assets on GCP.
Options A & B are wrong as billing consolidation is User responsibility and GCP does not support it.
Option D is wrong as it would not centralize the billing under a single account.

21. Question

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

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

Unattempted

Correct answer is A as the image can be directly updated using the kubectl command and Kubernetes Engine performs a rolling update.

Refer GCP documentation – Kubernetes Engine Rolling updates

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

You can use kubectl set to make changes to an object's image, resources (compute resource such as CPU and memory), or selector fields.

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

kubectl set image deployment nginx nginx=nginx:1.9.1

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

Option B is wrong as creating a new deployment would result in downtime.

Option C is wrong as service does not have a mapping of image.

Option D is wrong as Kubernetes Engine does not work with instance template and managed instance groups

22. Question

A member of the finance team informed you that one of the projects is using the old billing account. What steps should you take to resolve the problem?

- A. Go to the Project page; expand the Billing tile; select the Billing Account option; select the correct billing account and save.
- B. Go to the Billing page; view the list of projects; find the project in question and select Change billing account; select the correct billing account and save.

C. Delete the project and recreate it with the correct billing account.

D. Submit a support ticket requesting the change.

Unattempted

Correct answer is B as the billing account for the project can be modified from the Billing page.

Refer GCP documentation – Billing Modify Project

If you are a billing administrator on only one billing account, new projects you create are automatically linked to your existing billing account. If you create and have access to multiple billing accounts, you can change the billing account a project is billed to. This article describes how to change the billing account for your project, as well as how to enable and disable billing for a project.

To change the billing account:

Sign in to the Google Cloud Platform Console.

Open the console navigation menu (menu) and select Billing.

If you have more than one billing account, you'll be prompted to select Go to linked billing account to manage the current project's billing.

From the Billing navigation menu, click Account management.

Under Projects linked to this billing account, locate the name of the project that you want to change billing for, and then click the menu (more_vert) next to it.

Select Change billing, then choose the desired destination billing account.

23. Question

A company uses Cloud Storage for storing their critical data. As a part of compliance, the objects need to be encrypted using customer-supplied encryption keys. How should the object be handled to support customer-supplied encryption?

A. Use gsutil with ——encryption-key to pass the encryption key

B. Use gsutil with GSUtil:encryption_key=[YOUR_ENCRYPTION_KEY] to pass the encryption key

C. Use gcloud config to define the encryption

D. Create bucket with ——encryption-key and use gsutil to upload files

Unattempted

Correct answer is B as the customer supplied encryption key can be passed using the encryption_key parameter.

Refer GCP documentation – Cloud Storage Encryption

Add the following option to the [GSUtil] section of your boto configuration file:

encryption_key = [YOUR_ENCRYPTION_KEY]

where [YOUR_ENCRYPTION_KEY] is the key for encrypting the uploaded file.

Note: You can alternatively include this information in each gsutil command by using the -o top level

flag: -o “GSUtil:encryption_key=[YOUR_ENCRYPTION_KEY]”.

Option A is wrong as the parameter is wrong. Parameter -o “GSUtil:encryption_key=[YOUR_ENCRYPTION_KEY]” can be used.

Option C is wrong as encryption key cannot be defined using gcloud config.

Option D is wrong as encryption is not set on bucket and needs to applied when the object is uploaded.

24. Question

The development team needs a regional MySQL database with point-in-time recovery for a new proof-of-concept application. What’s the most inexpensive way to enable point-in-time recovery?

- A. Replicate to a Cloud Spanner database.
- B. Create a read replica in the same region.
- C. Enable binary logging.
- D. Create hourly back-ups.

Unattempted

Correct answer is C as binary logging helps Point-in-time recovery.

Refer GCP documentation – Cloud SQL MySQL 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.

Options A & B are wrong as Read Replica and Cloud Spanner are not cost-effective options.

Option D is wrong as hourly back-ups does not meet the point-in-time requirement.

25. Question

Your application deployed on a Google Compute Engine virtual machine instance needs to connect to Google Cloud Pub/Sub. What is the best way to provision the access to the application?

- A. Whitelist Google Compute Engine virtual machine instance IP on the Cloud Pub/Sub firewall
- B. Build or leverage an OAuth-compatible access control system
- C. Create a new service account with no access and enable access scope to allow Cloud Pub/Sub access for the instance
- D. ?Create a new service account with Cloud Pub/Sub access and associate with the instance

Unattempted

Correct answer is D as the VM needs to be granted permissions using the service account to be able to communicate with Cloud Pub/Sub.

Refer GCP documentation – Service Account Permissions

When you set up an instance to run as a service account, the level of access the service account has is determined by the combination of access scopes granted to the instance and IAM roles granted to the service account. You need to configure both access scopes and IAM roles to successfully set up an instance to run as a service account. Essentially:

Access scopes authorize the potential access that an instance has to API methods.

IAM restricts that access to the roles granted to the service account.

Option A is wrong as there is feature to whitelist IPs as firewalls only apply to Compute Engines.

Option B is wrong as service accounts handle the OAuth authentication and it is best suited for service to service communication.

Google OAuth 2.0 system supports server-to-server interactions such as those between a web application and a Google service. For this scenario you need a service account, which is an account that belongs to your application instead of to an individual end user. Your application calls Google APIs on behalf of the service account, so users aren't directly involved. This scenario is sometimes called "two-legged OAuth," or "2LO." (The related term "three-legged OAuth" refers to scenarios in which your application calls Google APIs on behalf of end users, and in which user consent is sometimes required.) Typically, an application uses a service account when the application uses Google APIs to work with its own data rather than a user's data. For example, an application that uses Google Cloud Datastore for data persistence would use a service account to authenticate its calls to the Google Cloud Datastore API.

Option C is wrong as access scope and service account IAM role permissions are applied together with the more restrictive taking effect. With no permissions to the Service Account, the instance would not be able to communicate with the VM instance.

26. Question

Your company pushes batches of sensitive transaction data from its application server VMs to Cloud Pub/Sub for processing and storage. What is the Google-recommended way for your application to authenticate to the required Google Cloud services?

- A. Ensure that VM service accounts are granted the appropriate Cloud Pub/Sub IAM roles.
- B. Ensure that VM service accounts do not have access to Cloud Pub/Sub, and use VM access scopes to grant the appropriate Cloud Pub/Sub IAM roles.
- C. Generate an OAuth2 access token for accessing Cloud Pub/Sub, encrypt it, and store it in Cloud Storage for access from each VM.
- D. Create a gateway to Cloud Pub/Sub using a Cloud Function, and grant the Cloud Function service account the appropriate Cloud Pub/Sub IAM roles.

Unattempted

Correct answer is A as the VM needs to be granted permissions using the service account to be able to communicate with Cloud Pub/Sub.

Refer GCP documentation – Service Account Permissions

When you set up an instance to run as a service account, the level of access the service account has is determined by the combination of access scopes granted to the instance and IAM roles granted to the service account. You need to configure both access scopes and IAM roles to successfully set up an instance to run as a service account. Essentially:

Access scopes authorize the potential access that an instance has to API methods.

IAM restricts that access to the roles granted to the service account.

Google OAuth 2.0 system supports server-to-server interactions such as those between a web application and a Google service. For this scenario you need a service account, which is an account that belongs to your application instead of to an individual end user. Your application calls Google APIs on behalf of the service account, so users aren't directly involved. This scenario is sometimes called "two-legged OAuth," or "2LO." (The related term "three-legged OAuth" refers to scenarios in which your application calls Google APIs on behalf of end users, and in which user consent is sometimes required.) Typically, an application uses a service account when the application uses Google APIs to work with its own data rather than a user's data. For example, an application that uses Google Cloud Datastore for data persistence would use a service account to authenticate its calls to the Google Cloud Datastore API.

Option B is wrong as access scope and service account IAM role permissions are applied together with the more restrictive taking effect. With no permissions to the Service Account, the instance would not be able to communicate with the VM instance.

Option C is wrong as service accounts handle the OAuth authentication and it is best suited for service to service communication.

Option D is wrong as there is no need for the gateway. Also, the VM and Cloud Function access needs to be handled.

27. Question

You can SSH into an instance from another instance in the same VPC by its internal IP address, but not its external IP address. What is one possible reason why this is so?

- A. The outgoing instance does not have correct permission granted to its service account.
- B. The external IP address is disabled.
- C. The firewall rule to allow SSH is restricted to the internal VPC.
- D. The receiving instance has an ephemeral address instead of a reserved address.

Unattempted

Correct answer is C as firewall rules need to be enabled for within the network and external network to be allowed to ssh into the instances.

Refer GCP documentation – VPC Firewalls

Google Cloud Platform (GCP) firewall rules let you allow or deny traffic to and from your virtual machine (VM) instances based on a configuration you specify. GCP firewall rules are applied at the virtual networking level, so they provide effective protection and traffic control regardless of the operating system your instances use.

Every VPC network functions as a distributed firewall. While firewall rules are defined at the network level, connections are allowed or denied on a per-instance basis. You can think of the GCP firewall rules as existing not only between your instances and other networks, but between individual instances within the same network

Source IP ranges: You can specify ranges of IP addresses as sources for packets. The ranges can include addresses inside your VPC network and those outside of it. Source IP ranges can be used to define sources both inside and outside of GCP.

28. Question

You have an application deployed on Kubernetes Engine using a Deployment named echo-deployment. The deployment is exposed using a Service called echo-service. You need to perform an update to the application with minimal downtime to the application. What should you do?

- A. Use the rolling update functionality of the Instance Group behind the Kubernetes cluster
- B. Update the deployment yaml file with the new container image. Use kubectl delete deployment/echo-deployment and kubectl create –f
- C. Use kubectl set image deployment/echo-deployment
- D. Update the service yaml file which the new container image. Use kubectl delete service/echoservice and kubectl create –f

Unattempted

Correct answer is C as the image can be directly updated using the kubectl command and Kubernetes Engine performs a rolling update.

Refer GCP documentation – Kubernetes Engine Rolling updates

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

You can use kubectl set to make changes to an object's image, resources (compute resource such as CPU and memory), or selector fields.

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

kubectl set image deployment nginx nginx=nginx:1.9.1

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

Option A is wrong as you do not work with underlying managed instance groups. It is managed by Kubernetes.

Option B is wrong as creating a new deployment would result in downtime.

Option D is wrong as service does not have a mapping of image.

29. Question

You have created an App engine application in the us-central region. However, you found out the network team has configured all the VPN connections in the asia-east2 region, which are not possible to move. How can you change the location efficiently?

- A. Change the region in app.yaml and redeploy
- B. From App Engine console, change the region of the application
- C. Change the region in application.xml within the application and redeploy
- D. ?Create a new project in the asia-east2 region and create app engine in the project

Unattempted

Correct answer is D as app engine is a regional resource, it needs to be redeployed to the different region.

Refer GCP documentation – App Engine locations

App Engine is regional, which means the infrastructure that runs your apps is located in a specific region and is managed by Google to be redundantly available across all the zones within that region.

Meeting your latency, availability, or durability requirements are primary factors for selecting the region where your apps are run. You can generally select the region nearest to your app's users but you should consider the location of the other GCP products and services that are used by your app. Using services across multiple locations can affect your app's latency as well as pricing

You cannot change an app's region after you set it.

Options A, B & C are wrong as once the region it set for the app engine it cannot be modified.

30. Question

You want to verify the IAM users and roles assigned within a GCP project named my-project. What should you do?

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

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

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

Unattempted

Correct answer is C as IAM section provides the list of both Members and Roles.

Option A is wrong as it would provide information about the roles only.

Option B is wrong as it would provide only the service accounts.

Option D is wrong as it would provide information about the roles only.

31. Question

You have a Linux VM that must connect to Cloud SQL. You created a service account with the appropriate access rights. You want to make sure that the VM uses this service account instead of the default Compute Engine service account. What should you do?

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

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

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

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

Unattempted

Correct answer is A as the service account can be specified to replace the default service account when the VM is created.

Refer GCP documentation – Compute Enable Service Accounts for Instances

After creating a new service account, you can create new virtual machine instances to run as the service account.

You can enable multiple virtual machine instances to use the same service account, but a virtual machine instance can only have one service account identity. If you assign the same service account to multiple virtual machine instances, any subsequent changes you make to the service account will affect instances using the service account. This includes any changes you make to the IAM roles granted to the service account. For example, if you remove a role, all instances using the service account will lose permissions granted by that role.

You can set up a new instance to run as a service account through the Google Cloud Platform Console,

the gcloud command-line tool, or directly through the API.

In the GCP Console, go to the VM Instances page.GO TO THE VM INSTANCES PAGE

Click Create instance.

On the Create a new instance page, fill in the properties for your instance.

In the Identity and API Access section, choose the service account you want to use from the dropdown list.

Click Create to create the instance.

Options B, C & D are wrong as the approaches would not work and replace the default service account.

32. Question

You have an instance group that you want to load balance. You want the load balancer to terminate the client SSL session. The instance group is used to serve a public web application over HTTPS. You want to follow Google-recommended practices. What should you do?

- A. Configure an HTTP(S) load balancer.
- B. Configure an internal TCP load balancer.
- C. Configure an external SSL proxy load balancer.
- D. Configure an external TCP proxy load balancer.

Unattempted

Correct answer is A as HTTPS load balancer supports the HTTPS traffic with the SSL termination ability.

Refer GCP documentation – Choosing Load Balancer

An HTTPS load balancer has the same basic structure as an HTTP load balancer (described above), but differs in the following ways:

An HTTPS load balancer uses a target HTTPS proxy instead of a target HTTP proxy.

An HTTPS load balancer requires at least one signed SSL certificate installed on the target HTTPS proxy for the load balancer. You can use Google-managed or self-managed SSL certificates.

The client SSL session terminates at the load balancer.

HTTPS load balancers support the QUIC transport layer protocol.

Option B is wrong as internal TCP load balancer does not serve external public traffic.

Option C is wrong as SSL proxy is not recommended for HTTPS traffic.

Google Cloud SSL Proxy Load Balancing terminates user SSL (TLS) connections at the load balancing layer, then balances the connections across your instances using the SSL or TCP protocols. Cloud SSL proxy is intended for non-HTTP(S) traffic. For HTTP(S) traffic, HTTP(S) load balancing is recommended instead.

SSL Proxy Load Balancing supports both IPv4 and IPv6 addresses for client traffic. Client IPv6 requests are terminated at the load balancing layer, then proxied over IPv4 to your backends.

Option D is wrong as TCP proxy does not support SSL offload and not recommended for HTTP/S traffic.

33. Question

You need to set up a policy so that videos stored in a specific Cloud Storage Regional bucket are moved to Coldline after 90 days, and then deleted after one year from their creation. How should you set up the policy?

- A. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 275 days (365 – 90)
- **B. Use Cloud Storage Object Lifecycle Management using Age conditions with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days.**
- C. Use gsutil rewrite and set the Delete action to 275 days (365-90).
- D. Use gsutil rewrite and set the Delete action to 365 days.

Unattempted

Correct answer is B as there are 2 actions needed. First archival after 90 days, which can be done by SetStorageClass action to Coldline. Second delete the data after a 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 A 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 as gsutil rewrite can be used to change the storage class. However, it needs to be triggered and the solution does not handle archival of data.

34. Question

You have 32 GB of data in a single file that you need to upload to a Nearline Storage bucket. The WAN connection you are using is rated at 1 Gbps, and you are the only one on the connection. You want to use as match of the rated 1 Gbps as possible to transfer the file rapidly. How should you upload the file?

- A. Use the GCP Console to transfer the file instead of gsutil.
- **B. Enable parallel composite uploads using gsutil on the file transfer.**
- C. Decrease the TCP window size on the machine initiating the transfer.
- D. ?Change the storage class of the bucket from Nearline to Multi-Regional.

Unattempted

Correct answer is B as the bandwidth is good and its a single file, gsutil parallel composite uploads can be used to split the large file and upload in parallel.

Refer GCP documentation – Transferring Data to GCP & Storage Composite Objects

To support parallel uploads and limited append/edit functionality, Cloud Storage allows users to compose up to 32 existing objects into a new object without transferring additional object data.

Object composition can be used for uploading an object in parallel: simply divide your data into multiple chunks, upload each chunk to a distinct object in parallel, compose your final object, and delete any temporary objects.

gsutil tool is an open-source command-line utility available for Windows, Linux, and Mac.

Multi-threaded/processed: Useful when transferring large number of files.

Parallel composite uploads: Splits large files, transfers chunks in parallel, and composes at destination.

Retry: Applies to transient network failures and HTTP/429 and 5xx error codes.

Resumability: Resumes the transfer after an error.

Option A is wrong as it is not recommended for large files and it would do a sequential upload of a single file.

Options C & D are wrong as they would not help in improving the performance.

35. Question

You need to monitor resources that are distributed over different projects in Google Cloud Platform. You want to consolidate reporting under the same Stackdriver Monitoring dashboard. What should you do?

- A. Use Shared VPC to connect all projects, and link Stackdriver to one of the projects.
- B. For each project, create a Stackdriver account. In each project, create a service account for that project and grant it the role of Stackdriver Account Editor in all other projects.
- **C. Configure a single Stackdriver account, and link all projects to the same account.**
- D. ?Configure a single Stackdriver account for one of the projects. In Stackdriver, create a Group and add the other project names as criteria for that Group.

Unattempted

Correct answer is C as you can create a single Stackdriver account and add multiple projects to the same account.

Refer GCP documentation – Stackdriver Monitoring

A single Workspace can monitor any number of GCP projects or AWS accounts. The best-practice recommendation to create a multi-project Workspace is as follows:

Create a new GCP project. For instructions on creating a a new GCP project, go to Before you begin.

Create a new Workspace for that project. For detailed steps, go to Creating a single-project Workspace.

Add GCP projects or AWS accounts to the Workspace. For details, go to Adding monitored projects.

Option A is wrong as Shared VPC would not allow consolidation of multiple project monitoring. Shared VPC allows an organization to connect resources from multiple projects to a common VPC network, so that they can communicate with each other securely and efficiently using internal IPs from that network.
Option B is wrong as you do not need to create stackdriver account for each project.
Option D is wrong as it is recommended to create a separate stackdriver account instead of an account for one of the project.

36. Question

You are deploying an application to a Compute Engine VM in a managed instance group. The application must be running at all times, but only a single instance of the VM should run per GCP project. How should you configure the instance group?

- A. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
- B. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 1.
- C. Set autoscaling to On, set the minimum number of instances to 1, and then set the maximum number of instances to 2.
- D. Set autoscaling to Off, set the minimum number of instances to 1, and then set the maximum number of instances to 2.

Unattempted

Correct answer is A as you can configure Auto Scaling with minimum and maximum 1, to ensure only 1 instance is running. Auto Scaling needs be configured with an Auto Scaling policy to detect the failure and create a new instance. Ideally, you can enabled Auto Healing to recover the instance, however that is not covered in any answer option.
Refer GCP documentation – Compute Engine Auto Scaler
Managed instance groups offer autoscaling capabilities that allow you to automatically add or delete instances from a managed instance group based on increases or decreases in load. Autoscaling helps your applications gracefully handle increases in traffic and reduce costs when the need for resources is lower. You define the autoscaling policy and the autoscaler performs automatic scaling based on the measured load.
Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).
Option C is wrong as you need only 1 instance at a time, the maximum needs to be set to 1.
Options B & D are wrong as you need to enable autoscaling.

37. Question

You need to allow traffic from specific virtual machines in 'subnet-a' network access to machines in 'subnet-b' without giving the entirety of subnet-a access. How can you accomplish this?

- A. Create a firewall rule to allow traffic from resources with specific network tags, then assign the machines in subnet-a the same tags.
- B. Relocate the subnet-a machines to a different subnet and give the new subnet the needed access.
- C. Create a rule to deny all traffic to the entire subnet, then create a second rule with higher priority giving access to tagged VM's in subnet-a.
- D. You can only grant firewall access to an entire subnet and not individual VM's inside.

Unattempted

Correct answer is A as Network tags allow more granular access based on individually tagged instances.

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.

Network tags allow you to apply firewall rules and routes to a specific instance or set of instances:

You make a firewall rule applicable to specific instances by using target tags and source tags.

You make a route applicable to specific instances by using a tag.

Option B is wrong as this would give the entire subnet access which is against the requirements: allow traffic from specific virtual machines in 'subnet-a' network access to machines in 'subnet-b' without giving the entirety of subnet-a access.

Option C is wrong as an explicit deny is not needed as implicitly all traffic is allowed.

Option D is wrong as firewall access can be granted to individual instances.

38. Question

You want to send and consume Cloud Pub/Sub messages from your App Engine application. The Cloud Pub/Sub API is currently disabled. You will use a service account to authenticate your application to the API. You want to make sure your application can use Cloud Pub/Sub. What should you do?

- A. Enable the Cloud Pub/Sub API in the API Library on the GCP Console.
- B. Rely on the automatic enablement of the Cloud Pub/Sub API when the Service Account accesses it.
- C. Use Deployment Manager to deploy your application. Rely on the automatic enablement of all APIs used by the application being deployed.

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

Unattempted

Correct answer is A as the standard method is to enable services in the Google Cloud Console. You can also enable services with the Cloud SDK CLI gcloud services enable pubsub.googleapis.com

Refer GCP documentation – Cloud Pub/Sub Quick Setup

Option B is wrong as Google Cloud Services are not automatically enabled when the service account accesses it. First, service accounts do not access APIs. Service accounts are used to obtain an OAuth Access Token (or Identity Token). These tokens are used to authorize APIs. Services are not automatically enabled with an API makes first access.

Option C is wrong as Deployment Manager does not automatically enable services. You can use Deployment Manager Resource Types to enable services. You must create a virtual resource for each API that you want enabled.

Option D is wrong as Cloud Pub/Sub Admin does not have permissions to enable services. To enable services the service account (or User Account) will need roles/serviceusage.serviceUsageAdmin or another role with the permission serviceusage.services.enable.

39. Question

You are using Cloud Shell and need to install a custom utility for use in a few weeks. Where can you store the file so it is in the default execution path and persists across sessions?

A. Cloud Storage

B. /google/scripts

C. ~/bin

D. ?/usr/local/bin

Unattempted

Correct answer is C as only HOME directory is persisted across sessions.

Refer GCP documentation – Cloud Shell

Cloud Shell provisions 5 GB of free persistent disk storage mounted as your $HOME directory on the virtual machine instance. This storage is on a per-user basis and is available across projects. Unlike the instance itself, this storage does not time out on inactivity. All files you store in your home directory, including installed software, scripts and user configuration files like .bashrc and .vimrc, persist between sessions. Your $HOME directory is private to you and cannot be accessed by other users.

Options A, B & D are wrong as they are not persistent across sessions.

40. Question

You have a single binary application that you want to run on Google Cloud Platform. You decided to automatically scale the application based on underlying infrastructure CPU usage. Your organizational policies require you to use virtual machines directly. You need to ensure that the application scaling is operationally efficient and completed as quickly as possible. What should you do?

- A. Create a Google Kubernetes Engine cluster, and use horizontal pod autoscaling to scale the application.
- **B. Create an instance template, and use the template in a managed instance group with autoscaling configured.**
- C. Create an instance template, and use the template in a managed instance group that scales up and down based on the time of day.
- D. ?Use a set of third-party tools to build automation around scaling the application up and down, based on Stackdriver CPU usage monitoring.

Unattempted

Correct answer is B as a managed instance group can help use virtual machines directly and with autoscaling can scaling as per the demand.

Refer GCP documentation – Managed Instance Groups AutoScaling

Managed instance groups offer autoscaling capabilities that allow you to automatically add or delete instances from a managed instance group based on increases or decreases in load. Autoscaling helps your applications gracefully handle increases in traffic and reduce costs when the need for resources is lower. You define the autoscaling policy and the autoscaler performs automatic scaling based on the measured load.

Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).

Option A is wrong as Google Kubernetes Engine cluster can support scaling, however it would not meet the requirement of using virtual machines directly.

Option C is wrong as scaling based on time does not effectively utilize the scaling as per the demand.

Option D is wrong as using external tools is the least preferred option.

41. Question

You have a project for your App Engine application that serves a development environment. The required testing has succeeded and you want to create a new project to serve as your production environment. What should you do?

- **A. Use gcloud to create the new project, and then deploy your application to the new project.**
- B. Use gcloud to create the new project and to copy the deployed application to the new project.

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

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

Unattempted

Correct answer is A as gcloud can be used to create a new project and the gcloud app deploy can point to the new project.

Refer GCP documentation – GCloud App Deploy

–project=PROJECT_ID

The Google Cloud Platform project name to use for this invocation. If omitted, then the current project is assumed; the current project can be listed using gcloud config list –format='text(core.project)' and can be set using gcloud config set project PROJECTID.

–project and its fallback core/project property play two roles in the invocation. It specifies the project of the resource to operate on. It also specifies the project for API enablement check, quota, and billing. To specify a different project for quota and billing, use –billing-project or billing/quota_project property.

Option B is wrong as the option to use gcloud app cp does not exist.

Option C is wrong as Deployment Manager does not copy the application, but allows you to specify all the resources needed for your application in a declarative format using yaml

Option D is wrong as gcloud app deploy would not create a new project. The project should be created before usage.

42. Question

Your company uses Cloud Storage to store application backup files for disaster recovery purposes. You want to follow Google's recommended practices. Which storage option should you use?

A. Multi-Regional Storage

B. Regional Storage

C. Nearline Storage

D. ?Coldline Storage

Unattempted

Correct answer is D 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, B & C are wrong as they are not suited for infrequently accessed data, as disaster does not happen periodically but rarely.

43. Question

You've deployed a microservice called myapp1 to a Google Kubernetes Engine cluster using the YAML file specified below:

apiVersion: apps/vl

kind: Deployment

metadata:

name: myappl-deployment

spec:

selector:

matchLabels:

app: myappl

replicas: 2

template:

metadata:

labels:

app: myappl

spec:

containers:

name: main-container

image: gcr.io/my-company-repo/myapp1:1.4

env:

name: DS _PASSWORD

value: "tOugh2guess!"

ports: – containerPort: 8080

You need to refactor this configuration so that the database password is not stored in plain text. You want to follow Google-recommended practices. What should you do?

A. Store the database password inside the Docker image of the container, not in the YAML file.

B. Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.

C. Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.

D. ?Store the database password in a file inside a Kubernetes persistent volume, and use a persistent volume claim to mount the volume to the container.

Unattempted

Correct answer is B as Google Kubernetes Engine supports secret to store sensitive data such as database passwords and is a google recommended practice.

Refer GCP documentation – Kubernetes Engine Secret

Secrets are secure objects which store sensitive data, such as passwords, OAuth tokens, and SSH keys, in your clusters. Storing sensitive data in Secrets is more secure than plaintext ConfigMaps or in Pod specifications. Using Secrets gives you control over how sensitive data is used, and reduces the risk of exposing the data to unauthorized users.

Options A, C & D are wrong as others options are not secured and not recommended as best practice.

44. Question

You created an instance of SQL Server 2017 on Compute Engine to test features in the new version. You want to connect to this instance using the fewest number of steps. What should you do?

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

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

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

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

Unattempted

Correct answer is A as it mentions fewest number of steps to connect to the instance. You can download the RDP Client and verify 3389 firewall is open. If the RDP asks for username and password, the instance is working.

Option B is wrong as it fails to mention the key requirement of port 3389 be opened.

Option C is wrong as RDP requires port 3389 to be opened.

Option D is wrong as you need an RDP client.

45. Question

You are building a pipeline to process time-series data. Which Google Cloud Platform services should you put in boxes 1,2,3, and 4?

- A. Cloud Pub/Sub, Cloud Dataflow, Cloud Datastore, BigQuery
- B. Firebase Messages, Cloud Pub/Sub, Cloud Spanner, BigQuery
- C. Cloud Pub/Sub, Cloud Storage, BigQuery, Cloud Bigtable
- **D. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery**

Unattempted

Correct answer is D as Cloud Pub/Sub for data ingestion, Dataflow for data handling and transformation, Bigtable for storage to provide low latency data access and BigQuery for analytics.

Refer GCP documentation – Time Series Dataflow

Cloud Pub/Sub. As well as performing ingestion, Cloud Pub/Sub can also act as the glue between the loosely coupled systems. You can send the processed data to other systems to consume; for example, you might send all correlations with more than the value of ABS(0.2) to other systems.

BigQuery. Place any data that you want to process or access later using a SQL interface into BigQuery.

Cloud Bigtable. Place any data that you want to use for low-latency storage, or where you might want to get at a very small subset of a larger dataset quickly (key lookups as well as range scans), in Cloud Bigtable.

Option A is wrong as Datastore is not an ideal solution to store large time series data.

Option B is wrong as Cloud Spanner is not an ideal solution for storage.

Option C is wrong as Cloud Storage is for storage and doesn't help handle and source data to storage and analytics.

46. Question

You are deploying an application to App Engine. You want the number of instances to scale based on request rate. You need at least 3 unoccupied instances at all times. Which scaling type should you use?

- A. Manual Scaling with 3 instances.
- B. Basic Scaling with min_instances set to 3.
- C. Basic Scaling with max_instances set to 3.
- **D. Automatic Scaling with min_idle_instances set to 3.**

Unattempted

Correct answer is D 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 manual scaling would not provide the scaling based on the request rate and would need manual intervention.

Options B & C are wrong as basic scaling will not allow the scaling based on the request rate.

47. Question

You significantly changed a complex Deployment Manager template and want to confirm that the dependencies of all defined resources are properly met before committing it to the project. You want the most rapid feedback on your changes. What should you do?

- A. Use granular logging statements within a Deployment Manager template authored in Python.
- B. Monitor activity of the Deployment Manager execution on the Stackdriver Logging page of the GCP Console.
- C. Execute the Deployment Manager template against a separate project with the same configuration, and monitor for failures.
- **D. ?Execute the Deployment Manager template using the –-preview option in the same project, and observe the state of interdependent resources.**

Unattempted

Correct answer is D as Deployment Manager provides the preview feature to check on what resources would be created.

Refer GCP documentation – Deployment Manager Preview

After you have written a configuration file, you can preview the configuration before you create a deployment. Previewing a configuration lets you see the resources that Deployment Manager would create but does not actually instantiate any actual resources. The Deployment Manager service previews the configuration by:

Expanding the full configuration, including any templates.

Creating a deployment and "shell" resources.

You can preview your configuration by using the preview query parameter when making an insert() request.

gcloud deployment-manager deployments create example-deployment \

–config configuration-file.yaml –preview

48. Question

You have a development project with appropriate IAM roles defined. You are creating a production project and want to have the same IAM roles on the new project, using the fewest possible steps. What should you do?

- A. Use gcloud iam roles copy and specify the production project as the destination project.
- B. Use gcloud iam roles copy and specify your organization as the destination organization.
- C. In the Google Cloud Platform Console, use the 'create role from role' functionality.
- D. ?In the Google Cloud Platform Console, use the 'create role' functionality and select all applicable permissions.

Unattempted

Correct answer is A as Cloud SDK gcloud iam roles copy can be used to copy the roles to different organization or project.

Refer GCP documentation – Cloud SDK IAM Copy Role

gcloud iam roles copy – create a role from an existing role

–dest-organization=DEST_ORGANIZATION (The organization of the destination role)

–dest-project=DEST_PROJECT (The project of the destination role)

Option B is wrong as the destination new project needs to be specified instead of the organization.

Option C is wrong as creating roles through GCP Console is cumbersome, time consuming and error prone.

Option D is wrong as it does not replicate the IAM roles permission.

49. Question

You have one GCP account running in your default region and zone and another account running in a non-default region and zone. You want to start a new Compute Engine instance in these two Google Cloud Platform accounts using the command line interface. What should you do?

- **A. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.**
- B. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations list to start the Compute Engine instances.
- C. Activate two configurations using gcloud config configurations activate [NAME] . Run gcloud config configurations list to start the Compute Engine instances.
- D. Activate two configurations using gcloud config configurations activate [NAME] . Run gcloud config configurations list to start the Compute Engine instances.

Unattempted

Correct answer is A as you can create different configurations for each account and create compute instances in each account by activating the respective account.

Refer GCP documentation – Configurations Create & Activate

Options B, C & D are wrong as gcloud config configurations list does not help create instances. It would only lists existing named configurations.

50. Question

You recently deployed a new version of an application to App Engine and then discovered a bug in the release. You need to immediately revert to the prior version of the application. What should you do?

- A. Run gcloud app restore.
- B. On the App Engine page of the GCP Console, select the application that needs to be reverted and click Revert.
- **C. On the App Engine Versions page of the GCP Console, route 100% of the traffic to the previous version.**
- D. ?Deploy the original version as a separate application. Then go to App Engine settings and split traffic between applications so that the original version serves 100% of the requests.

Unattempted

Correct answer is C as you can migrate all the traffic back to the previous version.

Refer GCP documentation – App Engine Overview

Having multiple versions of your app within each service allows you to quickly switch between different versions of that app for rollbacks, testing, or other temporary events. You can route traffic to one or more specific versions of your app by migrating or splitting traffic.
Option A is wrong as gcloud app restore was used for backup and restore and has been deprecated.
Option B is wrong as there is no application revert functionality available.
Option D is wrong as App Engine maintains version and need not be redeployed.

51. Question

You need to select and configure compute resources for a set of batch processing jobs. These jobs take around 2 hours to complete and are run nightly. You want to minimize service costs. What should you do?

- A. Select Google Kubernetes Engine. Use a single-node cluster with a small instance type.
- B. Select Google Kubernetes Engine. Use a three-node cluster with micro instance type.
- C. Select Compute Engine. Use preemptible VM instances of the appropriate standard machine type.
- D. ?Select Compute Engine. Use VM instance types that support micro bursting.

Unattempted
Correct answer is C as Compute Engine preemptible VMs are ideal for batch processing jobs and are able run at a much lower prices than standard instances.
Refer GCP documentation – Compute Engine Preemptible
A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage.
If your apps are fault-tolerant and can withstand possible instance preemptions, then preemptible instances can reduce your Compute Engine costs significantly. For example, batch processing jobs can run on preemptible instances. If some of those instances terminate during processing, the job slows but does not completely stop. Preemptible instances complete your batch processing tasks without placing additional workload on your existing instances and without requiring you to pay full price for additional normal instances.
Options A, B & D are wrong as they would Compute Engine instances running, which is not a cost effective option for batch processing jobs.

52. Question

You are analyzing Google Cloud Platform service costs from three separate projects. You want to use this information to create service cost estimates by service type, daily and monthly, for the next six months using standard query syntax. What should you do?

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

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

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

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

Unattempted

Correct answer is D as BigQuery provides an ideal storage option to store and query in standard SQL dialect.

BigQuery, Google's serverless, highly scalable enterprise data warehouse, is designed to make data analysts more productive with unmatched price-performance. Because there is no infrastructure to manage, you can focus on uncovering meaningful insights using familiar SQL without the need for a database administrator.

Option A is wrong Bigtable is a NoSQL solution and does not support SQL dialect.

Cloud Bigtable is Google's sparsely populated NoSQL database which can scale to billions of rows, thousands of columns, and petabytes of data. Cloud Bigtable has a data model similar to Apache HBase and provides an HBase-compatible client library.

Options B & C are wrong as Google Sheets and local file does not provide standard query syntax querying.

53. Question

You need a dynamic way of provisioning VMs on Compute Engine. The exact specifications will be in a dedicated configuration file. You want to follow Google's recommended practices. Which method should you use?

A. Deployment Manager

B. Cloud Composer

C. Managed Instance Group

D. Unmanaged Instance Group

Unattempted

Correct answer is A as Deployment Manager provide Infrastructure as a Code capability.

Refer GCP documentation – Deployment Manager

Google Cloud Deployment Manager allows you to specify all the resources needed for your application in a declarative format using yaml. You can also use Python or Jinja2 templates to parameterize the configuration and allow reuse of common deployment paradigms such as a load balanced, auto-scaled instance group. Treat your configuration as code and perform repeatable deployments.

Option B is wrong as Cloud Composer is a fully managed workflow orchestration service that empowers you to author, schedule, and monitor pipelines that span across clouds and on-premises data centers.
Options C & D are wrong as An instance group is a collection of VM instances that you can manage as a single entity.
Managed instance groups (MIGs) allow you to operate applications on multiple identical VMs. You can make your workloads scalable and highly available by taking advantage of automated MIG services, including: autoscaling, autohealing, regional (multi-zone) deployment, and auto-updating.
Unmanaged instance groups allow you to load balance across a fleet of VMs that you manage yourself.

54. Question

Your team is developing a product catalog that allows end users to search and filter. The full catalog of products consists of about 500 products. The team doesn't have any experience with SQL, or schema migrations, so they're considering a NoSQL option. Which database service would work best?

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

Unattempted
Correct answer is D as Cloud Datastore would provide the NoSQL option for storing the product catalog. As the data is limited, it would be a good fit.
Option A is wrong as Cloud SQL is a relational SQL solution.
Option B is wrong as Cloud Memorystore for Redis provides a fully managed in-memory data store service built on scalable, secure, and highly available infrastructure managed by Google. Use Cloud Memorystore to build application caches that provides sub-millisecond data access. Cloud Memorystore is compatible with the Redis protocol, allowing easy migration with zero code changes.
Option C is wrong as although Bigtable provides a NoSQL solution, it is a petabyte-scale, fully managed NoSQL database service ideal for large analytical and operational workloads.

55. Question

You're trying to provide temporary access to some files in a Cloud Storage bucket. You want to limit the time that the files are available to 10 minutes. With the fewest steps possible, what is the best way to generate a signed URL?

- A. Create a service account and JSON key. Use the gsutil signurl -t 10m command and pass in the JSON key and bucket.

B. Create a service account and JSON key. Use the gsutil signurl -d 10m command and pass in the JSON key and bucket.

C. Create a service account and JSON key. Use the gsutil signurl -p 10m command and pass in the JSON key and bucket.

D. ?Create a service account and JSON key. Use the gsutil signurl -m 10m command and pass in the JSON key and bucket.

Unattempted

Correct answer is B as signurl command will generate a signed URL that embeds authentication data so the URL can be used by someone who does not have a Google account. -d can help provide the time duration.

Refer GCP documentation – Cloud Storage gsutil signurl

gsutil signurl [-c] [-d] [-m] \

[-p] [-r] keystore-file url...

-m Specifies the HTTP method to be authorized for use with the signed url, default is GET. You may also specify RESUMABLE to create a signed resumable upload start URL. When using a signed URL to start a resumable upload session, you will need to specify the 'x-goog-resumable:start' header in the request or else signature validation will fail.

-d Specifies the duration that the signed url should be valid for, default duration is 1 hour. Times may be specified with no suffix (default hours), or with s = seconds, m = minutes, h = hours, d = days. This option may be specified multiple times, in which case the duration the link remains valid is the sum of all the duration options. The max duration allowed is 7d.

-c Specifies the content type for which the signed url is valid for.-p Specify the keystore password instead of prompting.

-r Specifies the region in which the resources for which you are creating signed URLs are stored. Default value is 'auto' which will cause gsutil to fetch the region for the resource. When auto-detecting the region, the current gsutil user's credentials, not the credentials from the private-key-file, are used to fetch the bucket's metadata. This option must be specified and not 'auto' when generating a signed URL to create a bucket.

56. Question

You're about to deploy your team's App Engine application. They're using the Go runtime with a Standard Environment. Which command should you use to deploy the application?

A. gcloud app deploy app.yaml

B. gcloud app-engine apply app.yaml

C. gcloud app apply app.yaml

D. ?gcloud app-engine deploy app.yaml

Unattempted

Correct answer is A as gcloud app deploy provides an ability to deploy the local code and/or configuration of your app to App Engine.

Refer GCP documentation – gcloud app deploy

This command is used to deploy both code and configuration to the App Engine server. As an input it takes one or more `DEPLOYABLES that should be uploaded. A DEPLOYABLE can be a service's .yaml file or a configuration's .yaml file.`

`Option C is wrong as gcloud app apply is not a valid command.`

`Options B & D are wrong as gcloud app-engine is not a valid command.`

57. Question

You have a Windows server running on a custom network. There's an allow firewall rule with an IP filter of 0.0.0.0/0 with a protocol/port of tcp:3389. The logs on the instance show a constant stream of attempts from different IP addresses, trying to connect via RDP. You suspect this is a brute force attack. How might you change the firewall rule to stop this from happening and still enable access for legit users?

A. Stop the instance.

B. Deny all traffic to port 3389.

C. Change the port that RDP is running on in the instance and change the port number in the firewall rule.

D. Change the IP address range in the filter to only allow known IP addresses.

Unattempted

Correct answer is D as by using 0.0.0.0/0, you're opening the port to the internet. By whitelisting known IP addresses, it will block anyone not on the list.

Option A is wrong as it is not a viable solution for protect the instances.

Option B is wrong denying all traffic would block all.

Option C is wrong as it is not possible to change the default RDP port.

58. Question

You've found that your Linux server keeps running low on memory. It's currently using 8GB of memory, and it needs to be increased to 16. What is the simplest way to do that?

A. Use the gcloud compute add-memory command to increase the memory.

B. Use the Linux memincr command to increase the memory.

C. Stop the instance and change the machine type.

D. Create a new instance with the correct amount of memory.

Unattempted

Correct answer is C as you can increase the memory by changing the instance machine type.

Refer GCP documentation – Changing Machine Type

You can change the machine type of a stopped instance if it is not part of a managed instance group. If you need to change the machine type of instances within a managed instance group, read Updating managed instance groups.

Change the machine types of your instances if your existing machine type is not a good fit for the workloads you run on that instance. You can change the machine type of an instance to adjust the number of vCPUs and memory as your workload changes. For example, you can start an instance with a smaller machine during setup, development, and testing and change the instance to use a larger machine type when you are ready for production workloads.

Options A & B are wrong as the options are invalid.

Option D is wrong as the solution is valid, but it is not the simplest.

59. Question

You're working on setting up a cluster of virtual machines with GPUs to perform some 3D rendering for a customer. They're on a limited budget and are looking for ways to save money. What is the best solution for implementing this?

A. Use an autoscaled managed instance group containing some preemptible instances.

B. Use an unmanaged instance group with preemptible instances.

C. Use App Engine with Flexible Environments.

D. Use App Engine with Standard Environments.

Unattempted

Correct answer is A as Preemptible with managed instance groups would help add GPUs at a lower cost.

Refer GCP documentation – Compute Engine Preemptible

A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage.

If your apps are fault-tolerant and can withstand possible instance preemptions, then preemptible instances can reduce your Compute Engine costs significantly. For example, batch processing jobs can run on preemptible instances. If some of those instances terminate during processing, the job slows but does not completely stop. Preemptible instances complete your batch processing tasks without placing

additional workload on your existing instances and without requiring you to pay full price for additional normal instances.

You can add GPUs to your preemptible VM instances at lower preemptible prices for the GPUs. GPUs attached to preemptible instances work like normal GPUs but persist only for the life of the instance. Preemptible instances with GPUs follow the same preemption process as all preemptible instances.

Option B is wrong as unmanaged instance group does not provide scaling.

Options C & D are wrong as GCP currently does not support GPUs for App Engine.

60. Question

Your coworker has helped you set up several configurations for gcloud. You've noticed that you're running commands against the wrong project. Being new to the company, you haven't yet memorized any of the projects. With the fewest steps possible, what's the fastest way to switch to the correct configuration?

- A. Run gcloud configurations list followed by gcloud configurations activate.
- B. Run gcloud config list followed by gcloud config activate.
- **C. Run gcloud config configurations list followed by gcloud config configurations activate.**
- D. Re-authenticate with the gcloud auth login command and select the correct configurations on login.

Unattempted

Correct answer is C as gcloud config configurations list can help check for the existing configurations and activate can help switch to the configuration.

Refer GCP documentation – Cloud SDK gcloud config

gcloud config configurations list – lists existing named configurations

gcloud config configurations activate – activates an existing named configuration

Options A & B are wrong as they are invalid commands.

Option D is wrong as does not help to identify and activate configurations.

gcloud auth login – authorize gcloud to access the Cloud Platform with Google user credentials

Obtains access credentials for your user account via a web-based authorization flow. When this command completes successfully, it sets the active account in the current configuration to the account specified. If no configuration exists, it creates a configuration named default.

61. Question

You have an App Engine application running in us-east1. You've noticed 90% of your traffic comes from the West Coast. You'd like to change the region. What's the best way to change the App Engine region?

- A. Use the gcloud app region set command and supply the name of the new region.

B. Contact Google Cloud Support and request the change.

C. From the console, under the App Engine page, click edit, and change the region drop-down.

D. ?Create a new project and create an App Engine instance in us-west2.

Unattempted

Correct answer is D as app engine is a regional resource, it needs to be redeployed to the different region.

Refer GCP documentation – App Engine locations

App Engine is regional, which means the infrastructure that runs your apps is located in a specific region and is managed by Google to be redundantly available across all the zones within that region.

Meeting your latency, availability, or durability requirements are primary factors for selecting the region where your apps are run. You can generally select the region nearest to your app's users but you should consider the location of the other GCP products and services that are used by your app. Using services across multiple locations can affect your app's latency as well as pricing

You cannot change an app's region after you set it.

Options A, B & C are wrong as once the region it set for the app engine it cannot be modified.

62. Question

You're using Deployment Manager to deploy your application to an autoscaled, managed instance group on Compute Engine. The application is a single binary. What is the fastest way to get the binary onto the instance, without introducing undue complexity?

A. When creating the instance template use the startup-script metadata key to bootstrap the application.

B. When creating the instance template use the initialize-script metadata key to bootstrap the application.

C. When creating the instance template, use the startup script metadata key to install Ansible. Have the instance run the play-book at startup to install the application.

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

Unattempted

Correct answer is A as Instance Template can be specified startup-script to install/download the binary artifact.

Refer GCP documentation – Deployment Manager Startup Scripts

When you are deploying more complex configurations, you might have tens, hundreds, or even thousands of virtual machine instances. If you're familiar with Compute Engine, it's likely that you want to use startup scripts to help install or configure your instances automatically.

Using Deployment Manager, you can run the same startup scripts or add metadata to virtual machine instances in your deployment by specifying the metadata in your template or configuration.
To add metadata or startup scripts to your template, add the metadata property and the relevant metadata keys and values. For example, for specifying a startup script, the metadata key must be startup-script and the value would be the contents of your startup script.
Option B is wrong as initialize-script is not a valid option.
Option C is wrong as although the solution is valid, it introduces complexity.
Option D is wrong as it is cumbersome to do it for a autoscaled managed instance group.

63. Question

You've created a Pod using the kubectl run command. Now you're attempting to remove the Pod, and it keeps being recreated. Which command might help you as you attempt to remove the pod?

- A. gcloud container describe pods
- B. kubectl get pods
- C. kubectl get secrets
- **D. kubectl get deployments**

Unattempted
Correct answer is D as Pods would be recreated and you need to remove the deployment to remove the associated pods. kubectl get deployments would help get the list of deployments
Refer GCP documentation – Kubernetes Deployment
Deployments represent a set of multiple, identical Pods with no unique identities. A Deployment runs multiple replicas of your application and automatically replaces any instances that fail or become unresponsive. In this way, Deployments help ensure that one or more instances of your application are available to serve user requests. Deployments are managed by the Kubernetes Deployment controller.
Option A is wrong as it is not a valid command.
Option B is wrong as it would only provide the information for the pods.
Option C is wrong as it would provide information about the secrets.

64. Question

You're attempting to remove the zone property from the Compute Engine service, that was set with the incorrect value. Which command would accomplish your task?

- **A. gcloud config unset compute/zone**
- B. gcloud config unset zone
- C. gcloud config configurations unset compute/zone

D. ?gcloud unset compute/zone

Unattempted

Correct answer is A as Zone can be corrected using the gcloud config unset compute/zone

Refer GCP documentation – gcloud config unset

To unset the zone property in the compute section, run:

gcloud config unset compute/zone

65. Question

You've seen some errors in the logs for a specific Deployment. You've narrowed the issue down to the Pod named "ad-generator" that is throwing the errors. Your engineers aren't able to reproduce the error in any other environment. They've told you that if they could just "connect into the container" for 5 minutes, they could figure out the root cause. What steps would allow them to run commands against the container?

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

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

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

D. Use the kubectl run ad-generator /bin/ bash command to run a shell on that container.

Unattempted

Correct answer is A as kubectl exec can help open a shell on the pod in an interactive mode.

Refer GCP documentation – Kubernetes Engine Troubleshooting

Connect to a running container

Open a shell to the Pod:

kubectl exec -it [POD_NAME] —– /bin/ bash

If there is more than one container in your Pod, add -c [CONTAINER_NAME].

Now, you can run bash commands from the container: you can test the network or check if you have access to files or databases used by your application.

66. Question

Your team has been working towards using desired state configuration for your entire infrastructure, which is why they're excited to store the Kubernetes Deployments in YAML. You created a Kubernetes Deployment with the kubectl apply command and passed on a YAML file. You need to edit the number of replicas. What steps should you take to update the Deployment?

A. Edit the number of replicas in the YAML file and rerun the kubectl apply.

B. Edit the YAML and push it to Github so that the git triggers deploy the change.

C. Disregard the YAML file. Use the kubectl scale command.

D. Edit the number of replicas in the YAML file and run the kubectl set image command

Unattempted

Correct answer is A as to set the desired state, the replicas of needs to be updated in the configuration file and changes applied.

Refer GCP documentation – Kubernetes Scaling Apps

Kubernetes uses the Deployment controller to deploy stateless applications as uniform, non-unique Pods. Deployments manage the desired state of your application: how many Pods should run your application, what version of the container image should run, what the Pods should be labelled, and so on. The desired state can be changed dynamically through updates to the Deployment's Pod specification.

You can use kubectl apply to apply a new configuration file to an existing controller object. kubectl apply is useful for making multiple changes to a resource, and may be useful for users who prefer to manage their resources in configuration files.

To scale using kubectl apply, the configuration file you supply should include a new number of replicas in the replicas field of the object's specification.

Options B & D are wrong they are not valid options to update the desired state.

Option C is wrong as kubectl scale disregards the configuration files, which is the key requirement. kubectl scale lets your instantaneously change the number of replicas you want to run your application.

67. Question

Your developers have some application metrics that they're tracking. They'd like to be able to create alerts based on these metrics. What steps need to happen in order to alert based on these metrics?

A. In the UI create a new logging metric with the required filters, edit the application code to set the metric value when needed, and create an alert in Stackdriver based on the new metric.

B. Create a custom monitoring metric in code, edit the application code to set the metric value when needed, create an alert in Stackdriver based on the new metric.

C. Add the Stackdriver monitoring and logging agent to the instances running the code.

D. Create a custom monitoring metric in code, in the UI create a matching logging metric, and create an alert in Stackdriver based on the new metric.

Unattempted

Correct answer is B as Stackdriver allows custom metrics, which can be used to create alerts.

Refer GCP documentation – Stackdriver Monitoring Custom Metrics

Custom metrics are metrics defined by users. Custom metrics use the same elements that the built-in

Stackdriver Monitoring metrics use:

A set of data points.

Metric-type information, which tells you what the data points represent.

Monitored-resource information, which tells you where the data points originated.

To use a custom metric, you must have a metric descriptor for your new metric type. Stackdriver Monitoring can create the metric descriptor for you automatically, or you can use the metricDescriptors.create API method to create it yourself.

To have Stackdriver Monitoring create the metric descriptor for you, you simply write time series data for your metric, and Stackdriver Monitoring creates a descriptor based on the data you are writing. There are limits to auto-creation, so it's helpful to know what information goes into a metric definition.

After you have a new custom metric descriptor, whether you or Monitoring created it, you can use the metric descriptor with the metric descriptor API methods and the time series API methods.

You can also create charts and alerts for your custom metric data.

Options A & D are wrong as you need to create monitoring metric and not logging metric

Option C is wrong as Stackdriver agent, by default, would not track custom metrics.

68. Question

Your developers have created an application that needs to be able to make calls to Cloud Storage and BigQuery. The code is going to run inside a container and will run on Kubernetes Engine and on-premises. What's the best way for them to authenticate to the Google Cloud services?

- A. Create a service account, grant it the least viable privileges to the required services, generate and download a key. Use the key to authenticate inside the application.
- B. Use the default service account for App Engine, which already has the required permissions.
- C. Use the default service account for Compute Engine, which already has the required permissions.
- D. Create a service account, with editor permissions, generate and download a key. Use the key to authenticate inside the application.

Unattempted

Correct answer is A as Service accounts can be used by the application to authenticate and call the service apis securely.

Refer GCP documentation – IAM Service Account

To use a service account outside of GCP, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal.

When you create a key, your new public/private key pair is generated and downloaded to your machine; it serves as the only copy of the private key. You are responsible for storing the private key securely. Take note of its location and ensure the key is accessible to your application; it needs the key to make

authenticated API calls.
Options B & C are wrong as default service account does not provide the requirement permissions and would not be available for application deployed on on-premises.
Option D is wrong as although the solution would work, however, it violates the principle of least privilege. Also, it would still require a service account key for the on-premises code.

69. Question

You need to connect to one of your Compute Engine instances using SSH. You've already authenticated gcloud, however, you don't have an SSH key deployed yet. In the fewest steps possible, what's the easiest way to connect to the app?

- A. Create a key with the ssh-keygen command. Upload the key to the instance. Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.
- B. Use the gcloud compute ssh command.
- C. Create a key with the ssh-keygen command. Then use the gcloud compute ssh command.
- D. ?Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.

Unattempted
Correct answer is B as using gcloud compute ssh is the easiest and quickest way to use SSH. It would generate the keys and add to the project metadata to enable login.
Refer GCP documentation – gcloud compute ssh
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.
gcloud compute ssh ensures that the user's public SSH key is present in the project's metadata. If the user does not have a public SSH key, one is generated using ssh-keygen(1) (if the –quiet flag is given, the generated key will have an empty passphrase).

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 →

Skillcertpro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy