Question 1:

Skipped

Your finance department wants you to create a new billing account and link all development and test Google Cloud Projects to the new billing account. What should you do?

- ○

  Ask your security administrator to grant you the Billing Account Administrator role on the existing Billing Account. Create new development and test projects and link them to the existing Billing Account.

- ○

  Ask your security administrator to grant you the Billing Account Creator role on the GCP organization and Project Billing Manager role on all the development and test projects. Link all the development and test projects to an existing Billing Account.

- ○

  Ask your security administrator to grant you the Billing Account Creator role on the GCP organization and Project Billing Manager role on all the development and test projects. Create a new Billing Account and link all the development and test projects to the new Billing Account.

  (Correct)

- ○

  Ask your security administrator to grant you the Billing Account Administrator role on the existing Billing Account. Link all development and test projects to the existing Billing Account.

Explanation

We are required to link an existing google cloud project with a new billing account.

`Ask your security administrator to grant you the Billing Account Administrator role on the existing Billing Account. Create new development and test projects and link them to the existing Billing Account.` **is not right.**

We do not need to create new projects.

`Ask your security administrator to grant you the Billing Account Creator role on the GCP organization and Project Billing Manager role on all the development and test projects. Link all the development and test projects`

`to an existing Billing Account.` **is not right.**
We want to link the projects with a new billing account, so this option is not right.

`Ask your security administrator to grant you the Billing Account Administrator role on the existing Billing Account. Link all development and test projects to the existing Billing Account.` **is not right.**
We want to link the projects with a new billing account, so this option is not right.

`Ask your security administrator to grant you the Billing Account Creator role on the GCP organization and Project Billing Manager role on all the development and test projects. Create a new Billing Account and link all the development and test projects to the new Billing Account.` **is the right answer.**
The purpose of the Project Billing Manager is to Link/unlink the project to/from a billing account. It is granted at the organization or project level. Project Billing Manager role allows a user to attach the project to the billing account, but does not grant any rights over resources. Project Owners can use this role to allow someone else to manage the billing for the project without granting them resource access.

Billing Account Creator - Use this role for initial billing setup or to allow the creation of additional billing accounts.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Question 2:
Skipped
Your manager asked you to write a script to upload objects to a Cloud Storage bucket. How should you set up the IAM access to enable the script running in a Google Compute VM upload objects to Cloud Storage?

- ○

  Create a new IAM service account with the access scope cloud-platform and configure the script to use this service account.

- ○

  Create a new IAM service account with the access scope devstorage.write_only and configure the script to use this service account.

- ○

  Grant roles/storage.objectCreator IAM role to the service account used by the VM.

  (Correct)

- ○

  Grant roles/storage.objectAdmin IAM role to the service account used by the VM.

Explanation
Our requirements are

Google recommended practices

Multiple compute engine instances to write data to a bucket.

`Create a new IAM service account with the access scope devstorage.write_only and configure the script to use this service account.` **is not right.**
You can't attach scope when creating a service account.
Ref: https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/create

`Create a new IAM service account with the access scope cloud-platform and configure the script to use this service account.` **is not right.**
You can't attach scope when creating a service account.
Ref: https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/create

`Grant roles/storage.objectAdmin IAM role to the service account used by the VM.` **is not right.**
You need to provide Compute Engine instances permissions to write data into a particular Cloud Storage bucket. Storage Object Admin (roles/storage.objectAdmin) grants full control over objects, including listing, creating, viewing, and deleting objects. Granting this role goes against the principle of least privilege.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles

`Grant roles/storage.objectCreator IAM role to the service account used by the VM.` **is the right answer.**
You need to provide Compute Engine instances permissions to write data into a particular Cloud Storage bucket. Storage Object Creator (roles/storage.objectCreator) allows users to create objects. Does not permit to view, delete, or overwrite objects. This permission is what the script needs to write data to the bucket. So we create a service account, add this IAM role and let the compute engine instances use this service account to write objects to the bucket.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles

Question 3:
Skipped
You deployed a Java application on four Google Cloud Compute Engine VMs in two zones behind a network load balancer. During peak usage, the application has stuck threads. This issue ultimately takes down the whole system and requires a reboot

of all VMs. Your operations team have recently heard about self-healing mechanisms in Google Cloud and have asked you to identify if it is possible to automatically recreate the VMs if they remain unresponsive for 3 attempts 10 seconds apart. What should you do?

- ○

  Use a global HTTP(s) Load Balancer instead and set the load balancer health check to healthy (HTTP).

- ○

  Enable autohealing and set the autohealing health check to healthy (HTTP).

  (Correct)

- ○

  Enable autoscaling on the Managed Instance Group (MIG).

- ○

  Use a global HTTP(s) Load Balancer instead and limit Requests Per Second (RPS) to 10.

Explanation

`Enable autoscaling on the Managed Instance Group (MIG).` **is not right.**
Auto-scaling capabilities of Managed instance groups let you automatically add or delete instances from a managed instance group based on increases or decreases in load. They don't help you with re-creation should the VMs go unresponsive (unless you also enable the autohealing health checks).
Ref: https://cloud.google.com/compute/docs/autoscaler

`Use a global HTTP(s) Load Balancer instead and limit Requests Per Second (RPS) to 10.` **is not right.**
You set RPS (Requests per Second) on load balancer when using RATE balancing mode. RPS does not affect auto-healing.
Ref: https://cloud.google.com/load-balancing/docs/https/

`Use a global HTTP(s) Load Balancer instead and set the load balancer health check to healthy (HTTP).` **is not right.**
The health checks defined on the load balancer determine whether VM instances respond correctly to traffic. The Load balancer health checks have no impact on auto-healing. It is important to note that the health checks defined on the load balancer are different to the health checks defined on the auto-healing for managed instances group - see the explanation in the right answer for more information.

Ref: https://cloud.google.com/load-balancing/docs/health-checks#create_a_health_check

`Enable autohealing and set the autohealing health check to healthy (HTTP).` **is the right answer.**

To enable auto-healing, you need to group the instances into a managed instance group. Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An auto-healing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.

It is essential to use separate health checks for load balancing and auto-healing. Health checks for load balancing can and should be more aggressive because these health checks determine whether an instance receives user traffic. You want to catch non-responsive instances quickly, so you can redirect traffic if necessary. In contrast, health checking for auto-healing causes Compute Engine to replace failing instances proactively, so this health check should be more conservative than a load balancing health check.

Question 4:

Skipped

Your company retains all its audit logs in BigQuery for 10 years. At the annual audit every year, you need to provide the auditors' access to the audit logs. You want to follow Google recommended practices. What should you do?

- ○

  Grant the auditors' group roles/logging.viewer and roles/bigquery.dataViewer IAM roles.

  (Correct)

- ○

  Grant the auditors' group custom IAM roles with specific permissions.

- ○

  Grant the auditors' user accounts custom IAM roles with specific permissions.

- ○

  Grant the auditors' user accounts roles/logging.viewer and roles/bigquery.dataViewer IAM roles.

Explanation

`Grant the auditors’ user accounts roles/logging.viewer and roles/bigquery.dataViewer IAM roles.` **is not right.**

Since auditing happens several times a year, we don't want to repeat the process of granting multiple roles to multiple users every time. Instead, we want to define a group with the required grants (a one time task) and assign this group to the auditor users during the time of the audit.

`Grant the auditors’ user accounts custom IAM roles with specific permissions.` **is not right.**

Google already provides roles that fit the external auditing requirements, so we don't need to create custom roles. Nothing stops us from creating custom IAM roles to achieve the same purpose, but this doesn't follow "Google-recommended practices."

`Grant the auditors’ group custom IAM roles with specific permissions.` **is not right.**

Google already provides roles that fit the external auditing requirements, so we don't need to create custom roles. Nothing stops us from creating custom IAM roles to achieve the same purpose, but this doesn't follow "Google-recommended practices."

`Grant the auditors’ group roles/logging.viewer and roles/bigquery.dataViewer IAM roles.` **is the right answer.**

For external auditors, Google recommends we grant logging.viewer and bigquery.dataViewer roles. Since auditing happens several times a year to review the organization's audit logs, it is recommended we create a group with these grants and assign the group to auditor user accounts during the time of the audit.
Ref: https://cloud.google.com/iam/docs/roles-audit-logging#scenario_external_auditors

Question 5:

Skipped

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

- ○

  Grant the data custodian team Storage Admin IAM role.

  (Correct)

- ○

  Grant the data custodian team Storage Object Creator IAM role.

- ○

  Grant the data custodian team Project Editor IAM role.

- ○

  Grant the data custodian team Storage Object Admin IAM role.

Explanation

`Grant the data custodian team Project Editor IAM role.` **is not right.**
The project editor is a primitive role that grants a lot more than what we need here. Google doesn't recommend using Primitive roles.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_role_definitions
The project editor role provides all viewer permissions, plus permissions for actions that modify state, such as changing existing resources.

`Grant the data custodian team Storage Object Admin IAM role.` **is not right.**
While this role grants full access to the objects, it does not grant access to the buckets so users of this role can not "manage buckets". This role grants full control over objects, including listing, creating, viewing, and deleting objects.
Ref: https://cloud.google.com/iam/docs/understanding-roles#storage-roles

`Grant the data custodian team Storage Object Creator IAM role.` **is not right.**
This role allows users to create objects. It does not permit to view, delete, or overwrite objects.
Ref: https://cloud.google.com/iam/docs/understanding-roles#storage-roles

`Grant the data custodian team Storage Admin IAM role.` **is the right answer.**
This role grants full control of buckets and objects. When applied to an individual bucket, control applies only to the specified bucket and objects within the bucket.
Ref: https://cloud.google.com/iam/docs/understanding-roles#storage-roles

Question 6:

Skipped

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

- ○

  Store the data in a 2-node Cloud Spanner instance.

- ○

Store the data in Highly Available Cloud SQL for MySQL instance.

- ○

Store the data in a multi-regional Cloud Spanner instance.

- ○

Store the data in Cloud SQL for MySQL instance. Ensure Binary Logging on the Cloud SQL instance.

(Correct)

Explanation

`Store the data in a 2-node Cloud Spanner instance.` **is not right.**
Cloud spanner is a massively scalable, fully managed, relational database service for regional and global application data. Cloud spanner is expensive compared to Cloud SQL. We have a small set of data, and we want to be cost-effective, so Cloud Spanner doesn't fit these requirements. Furthermore, Cloud Spanner does not offer a "Point in time" recovery feature.
Ref: https://cloud.google.com/spanner

`Store the data in a multi-regional Cloud Spanner instance.` **is not right.**
Cloud spanner is a massively scalable, fully managed, relational database service for regional and global application data. Cloud spanner is expensive compared to Cloud SQL. We don't require more than "one geographic location", and we want to be cost-effective, so Cloud Spanner doesn't fit these requirements. Furthermore, Cloud Spanner does not offer a "Point in time" recovery feature.
Ref: https://cloud.google.com/spanner

`Store the data in Highly Available Cloud SQL for MySQL instance.` **is not right.**
Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. But This option does not enable point in time recovery, so our requirement to support point-in-time recovery is not met.
Ref: https://cloud.google.com/sql/docs/mysql

`Store the data in Cloud SQL for MySQL instance. Ensure Binary Logging on the Cloud SQL instance.` **is the right answer.**
Cloud SQL can easily handle small sets of relational data and is cost-effective compared to Cloud Spanner. And by enabling binary logging, we can enable point-in-time recovery, which fits our requirement.

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

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

Question 7:
Skipped
You are in the process of migrating a mission-critical application from your on-premises data centre to Google Kubernetes Engine (GKE). Your operations team do not want to take on the overhead for upgrading the GKE cluster and have asked you to ensure the Kubernetes version is always stable and supported. What should you do?

- ○

  When provisioning the GKE cluster, use Container Optimized OS node images.

- ○

  When provisioning the GKE cluster, ensure you use the latest stable and supported version.

- ○

  Update your GKE cluster to turn on GKE’s node auto-repair feature.

- ○

  Update your GKE cluster to turn on GKE’s node auto-upgrade feature.

  (Correct)

Explanation
`Update your GKE cluster to turn on GKE’s node auto-repair feature.` **is not right.**
GKE's node auto-repair feature helps you keep the nodes in your cluster in a healthy, running state. When enabled, GKE makes periodic checks on the health state of each node in your cluster. If a node fails consecutive health checks over an extended period, GKE initiates a repair process for that node.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-repair

`When provisioning the GKE cluster, ensure you use the latest stable and supported version.` **is not right.**
We can select the latest available cluster version at the time of GKE cluster provisioning; however, this does not automatically upgrade the cluster if new versions become available.

`When provisioning the GKE cluster, use Container Optimized OS node images.` **is not right.**
Container-Optimized OS comes with the Docker container runtime and all Kubernetes components pre-installed for out of the box deployment, management, and orchestration of your containers. But these do not help with automatically upgrading GKE cluster versions.
Ref: https://cloud.google.com/container-optimized-os

`Update your GKE cluster to turn on GKE’s node auto-upgrade feature.` **is the right answer.**
Node auto-upgrades help you keep the nodes in your cluster up to date with the cluster master version when your master is updated on your behalf. When you create a new cluster or node pool with Google Cloud Console or the gcloud command, node auto-upgrade is enabled by default.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-upgrades

Question 8:
Skipped
Your company owns a mobile game that is popular with users all over the world. The mobile game backend uses Cloud Spanner to store user state. An overnight job exports user state to a Cloud Storage bucket. Your operations team needs access to monitor the spanner instance but not have the permissions to view or edit user data. What IAM role should you grant the operations team?

- ○

  Grant the operations team roles/monitoring.viewer IAM role.

  (Correct)

- ○

  Grant the operations team roles/spanner.database.user IAM role.

- ○

  Grant the operations team roles/stackdriver.accounts.viewer IAM role.

- ○

  Grant the operations team roles/spanner.database.reader IAM role.

Explanation
Requirements -

Monitoring access but no data access

Streamlined solution

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

`Grant the operations team roles/spanner.database.reader IAM role.` **is not right.**
roles/spanner.databaseReader provides permission to read from the Spanner database, execute SQL queries on the database, and view the schema. This role provides read access to data.

`Grant the operations team roles/spanner.database.user IAM role.` **is not right.**
roles/spanner.databaseUser provides permission to read from and write to the Spanner database, execute SQL queries on the database, and view and update the schema. This role provides both read and write access to data.

`Grant the operations team roles/stackdriver.accounts.viewer IAM role.` **is not right.**
roles/stackdriver.accounts.viewer read-only access to get and list information about Stackdriver account structure. Thie role does not provide monitor access to Cloud Spanner.

`Grant the operations team roles/monitoring.viewer IAM role.` **is the right answer.**
roles/monitoring.viewer provides read-only access to get and list information about all monitoring data and configurations. This role provides monitoring access and fits our requirements.
Ref: https://cloud.google.com/iam/docs/understanding-roles#cloud-spanner-roles

Question 9:
Skipped
Your team is responsible for the migration of all legacy on-premises applications to Google Cloud. Your team is a big admirer of serverless and has chosen App Engine Standard as the preferred choice for compute workloads. Your manager asked you to migrate a legacy accounting application built in C++, but you realized App Engine Standard doesn’t support C++. What GCP compute services should you use instead to maintain the serverless aspect? (Choose two answers)

- □

  Deploy the containerized version of the application in Cloud Run.

  (Correct)

- □

  Deploy the containerized version of the application in Cloud Run on GKE.

(Correct)

- □

  Deploy the containerized version of the application in App Engine Flex.

- □

  Deploy the containerized version of the application in Google Kubernetes Engine (GKE).

- □

  Convert the application into a set of functions and deploy them in Google Cloud Functions.

Explanation
App engine standard currently supports Python, Java, Node.js, PHP, Ruby and Go.
Ref: https://cloud.google.com/appengine/docs/standard/
The question already states App Engine doesn't support C#. We are required to ensure we maintain the serverless aspect of our application.

`Convert the application into a set of functions and deploy them in Google Cloud Functions.` **is not right.**
Cloud Functions is a serverless platform where you can run the code in the cloud without having to provision servers. You split your application functionality into multiple functions, and each of these is defined as a cloud function. Cloud Functions don't support C#. Supported runtimes are Python, Node.js and Go.
Ref: https://cloud.google.com/functions

`Deploy the containerized version of the application in App Engine Flex.` **is not right.**
While App Engine flexible lets us customize runtimes or provide our runtime by supplying a custom Docker image or Dockerfile from the open-source community, it uses compute engine virtual machines, so it is not serverless.
Ref: https://cloud.google.com/appengine/docs/flexible/

`Deploy the containerized version of the application in Google Kubernetes Engine (GKE).` **is not right.**
GKE, i.e. Google Kubernetes Clusters uses compute engine virtual machines, so it is not serverless.
Ref: https://cloud.google.com/kubernetes-engine

`Deploy the containerized version of the application in Cloud Run.` **is the right answer.**
Cloud Run is a fully managed compute platform that automatically scales your

stateless containers. Cloud Run is serverless: it abstracts away all infrastructure management, so you can focus on what matters most—building great applications. Run your containers in fully managed Cloud Run or on Anthos, which supports both Google Cloud and on-premises environments. Cloud Run is built upon an open standard, Knative, enabling the portability of your applications.
Ref: https://cloud.google.com/run

`Deploy the containerized version of the application in Cloud Run on GKE.` **is the right answer.**
Cloud Run implements the Knative serving API, an open-source project to run serverless workloads on top of Kubernetes. That means you can deploy Cloud Run services anywhere Kubernetes runs. And suppose you need more control over your services (like access to GPU or more memory). In that case, you can also deploy these serverless containers in your GKE cluster instead of using the fully managed environment. When using the fully managed environment, Cloud Run on GKE is serverless.
Ref: https://github.com/knative/serving/blob/master/docs/spec/spec.md
Ref: https://cloud.google.com/blog/products/serverless/cloud-run-bringing-serverless-to-containers

Question 10:
Skipped
You have a Cloud Function that is triggered every night by Cloud Scheduler. The Cloud Function creates a snapshot of VMs running in all projects in the department. Your team created a new project ptech-vm, and you now need to provide IAM access to the service account used by the Cloud Function to let it create snapshots of VMs in the new ptech-vm project. You want to follow Google recommended practices. What should you do?

- ○

  Use gcloud to generate a JSON key for the existing service account used by the Cloud Function. Register the JSON key as SSH key on all VM instances in the ptech-vm project.

- ○

  Grant Compute Storage Admin IAM role on the ptech-vm project to the service account used by the Cloud Function.

  (Correct)

- ○

  Use gcloud to generate a JSON key for the existing service account used by the Cloud Function. Add a metadata tag to all compute engine instances in

the ptech-vm project with key: service-account and value: <JSON file contents>.

- ○

Set the scope of the service account to Read/Write when provisioning compute engine instances in the ptech-vm project.

Explanation

`Use gcloud to generate a JSON key for the existing service account used by the Cloud Function. Add a metadata tag to all compute engine instances in the ptech-vm project with key: service-account and value: {JSON file contents}.` **is not right.**

Adding service accounts private key (JSON file) to VMs custom metadata does not affect the permissions granted to the Cloud Function's service account. Metadata entries are key-value pairs and do not influence any other behaviour.
Ref: https://cloud.google.com/compute/docs/storing-retrieving-metadata

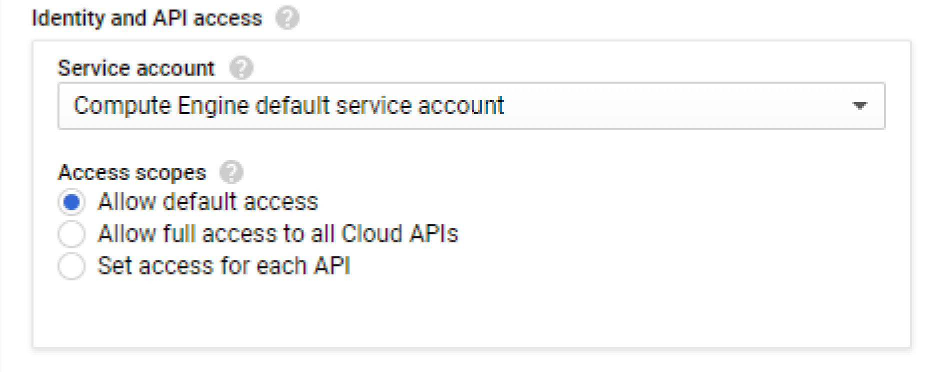
`Use gcloud to generate a JSON key for the existing service account used by the Cloud Function. Register the JSON key as SSH key on all VM instances in the ptech-vm project.` **is not right.**

Adding service accounts private key to the VMs SSH keys does not influence any other behaviour. SSH keys are used for SSHing to the instance.
Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys

`Set the scope of the service account to Read/Write when provisioning compute engine instances in the ptech-vm project.` **is not right.**

The scopes can be modified when using compute engine default service account only.
Ref: https://cloud.google.com/compute/docs/access/service-accounts#default_service_account

See the screenshot below.



Identity and API access

Service account

Compute Engine default service account

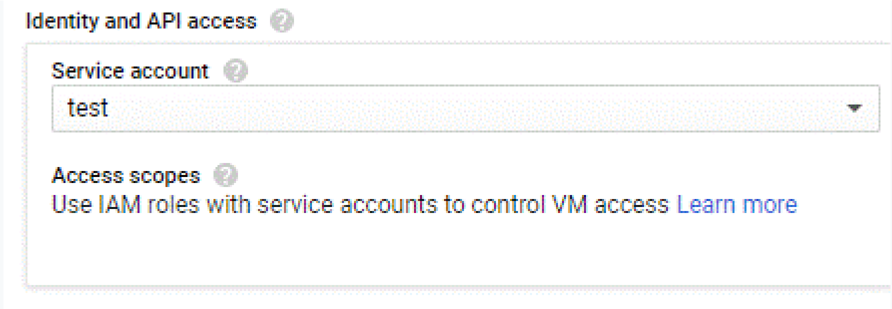
Access scopes

● Allow default access

○ Allow full access to all Cloud APIs

○ Set access for each API

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


Identity and API access

Service account: test

Access scopes
Use IAM roles with service accounts to control VM access Learn more

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

`Grant Compute Storage Admin IAM role on the ptech-vm project to the service account used by the Cloud Function.` **is the right answer.**

Compute Storage Admin role provides permissions to create, modify, and delete disks, images, and snapshots. If the service account in ptech-sa is granted the IAM Role of Compute Storage Admin in the project called ptech-vm, it can take snapshots and carry out other activities as defined by the role.
Ref: https://cloud.google.com/compute/docs/access/iam#compute.storageAdmin

Question 11:

Skipped

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

- ○

  Add a firewall rule to allow TCP traffic on port 22. In the GCP console, add a password for the Windows VM instance. Install Chrome RDP for Google Cloud Platform extension and click the RDP button in the console to connect to the instance with the credentials.

- ○

  Add a firewall rule to allow TCP traffic on port 3389. In the GCP console, add a username and password for the Windows VM instance. Install Chrome RDP for Google Cloud Platform extension and click the RDP button in the console to connect to the instance with the credentials.

  (Correct)

- ○

In the GCP console, add a username and password for the Windows VM instance. Install an RDP client and connect to the instance with username and password.

- ○

  Add a firewall rule to allow TCP traffic on port 3389. Install an RDP client and connect to the instance.

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

`Add a firewall rule to allow TCP traffic on port 3389. Install an RDP client and connect to the instance.` **is not right.**
Although opening port 3389 is essential for serving RDP traffic, we do not have the credentials to RDP, so this isn't going to work.

`Add a firewall rule to allow TCP traffic on port 22. In the GCP console, add a password for the Windows VM instance. Install Chrome RDP for Google Cloud Platform extension and click the RDP button in the console to connect to the instance with the credentials.` **is not right.**
RDP uses port 3389 and not 22.
Ref: https://cloud.google.com/compute/docs/troubleshooting/troubleshooting-rdp

`In the GCP console, add a username and password for the Windows VM instance. Install an RDP client and connect to the instance with username and password.` **is not right.**
This option correctly sets the username/password, which is essential. However, the port on 3389 has not been opened to allow RDP. Therefore, RDP connection from an external client fails.

`Add a firewall rule to allow TCP traffic on port 3389. In the GCP console, add a username and password for the Windows VM instance. Install Chrome RDP for Google Cloud Platform extension and click the RDP button in the console to connect to the instance with the credentials.` **is the right answer.**
This option correctly sets the username and password on the console and verifies a firewall rule is set on port 3389 to allow RDP traffic. You also install Chrome RDP for Google Cloud Platform extension to RDP from the console. (See Chrome Desktop for GCP tab in https://cloud.google.com/compute/docs/instances/connecting-to-

instance#windows) which lets you click on the RDP button to launch an RDP session where you will be prompted for a username and password.

Question 12:

Skipped

You migrated an internal HR system from an on-premises database to Google Cloud Compute Engine Managed Instance Group (MIG). The networks team at your company has asked you to associate the internal DNS records of the VMs with a custom DNS zone. You want to follow Google recommended practices. What should you do?

- ○

  1. Install a new BIND DNS server on Google Compute Engine, using the BIND name server software (BIND9). 2. Configure a Cloud DNS forwarding zone to direct all requests to the Internal BIND DNS server. 3. When provisioning the VMs, associate the DNS records with the Internal BIND DNS server.

- ○

  1. Provision the VMs with custom hostnames.

- ○

  1. Create a new Cloud DNS zone and set its visibility to private. 2. When provisioning the VMs, associate the DNS records with the new DNS zone.

  (Correct)

- ○

  1. Create a new Cloud DNS zone and a new VPC and associate the DNS zone with the VPC. 2. When provisioning the VMs, associate the DNS records with the new DNS zone. 3. Configure firewall rules to block all external (public) traffic. 4. Finally, configure the DNS zone associated with the default VPC to direct all requests to the new DNS zone.

Explanation

Our requirements here are

Internal, and

Custom Zone

`1. Provision the VMs with custom hostnames.` **is not right.**

This option doesn't create the DNS records in a custom DNS zone.

`1. Install a new BIND DNS server on Google Compute Engine, using the BIND` `name server software (BIND9).`
`2. Configure a Cloud DNS forwarding zone to direct all requests to the` `Internal BIND DNS server.`
`3. When provisioning the VMs, associate the DNS records with the Internal` `BIND DNS server.` **is not right.**
This option might be possible but not something Google recommends. The Cloud DNS service offering from Google already offers these features, so it is pointless installing a custom DNS server to do that.

`1. Create a new Cloud DNS zone and a new VPC and associate the DNS zone` `with the VPC.`
`2. When provisioning the VMs, associate the DNS records with the new DNS` `zone.`
`3. Configure firewall rules to block all external (public) traffic.`
`4. Finally, configure the DNS zone associated with the default VPC to` `direct all requests to the new DNS zone.` **is not right.**
This doesn't make any sense. Moreover, the two VPCs can't communicate without VPC peering.
Ref: https://cloud.google.com/dns/docs/overview#concepts

`1. Create a new Cloud DNS zone and set its visibility to private.`
`2. When provisioning the VMs, associate the DNS records with the new DNS` `zone.` **is the right answer.**
You should do when you want internal DNS records in a custom zone. Cloud DNS gives you the option of private zones and internal DNS names.
Ref: https://cloud.google.com/dns/docs/overview#concepts

Question 13:
Skipped
Your company owns a mobile game that is popular with users all over the world. The mobile game backend uses Cloud Spanner to store user state. An overnight job exports user state to a Cloud Storage bucket. The app pushes all time-series events during the game to a streaming Dataflow service that saves them to Cloud Bigtable. You are debugging an in-game issue raised by a gamer, and you want to join the user state information with data stored in Bigtable to debug. How can you do this one-off join efficiently?

- ○

  Create two external tables in BigQuery and link them to the Cloud BigTable and Cloud Storage data sources, respectively. Execute a query in BigQuery console to join up data between the two external tables for the specific gamer.

(Correct)

- ○

  Set up a Cloud Dataflow job to read data from Cloud Spanner and Cloud BigTable for the specific gamer.

- ○

  Set up a Cloud Dataflow job to read data from Cloud Storage and Cloud BigTable for the specific gamer.

- ○

  Set up a Cloud Dataproc Cluster to run a Hadoop job to join up data from Cloud BigTable and Cloud Storage for the specific gamer.

Explanation
We are required to join user sessions with user events efficiently. We need to look for an option that is primarily a Google service and provides this feature out of the box or with minimal configuration.

`Set up a Cloud Dataflow job to read data from Cloud Spanner and Cloud BigTable for the specific gamer.` **is not right.**
You can make use of the Cloud Dataflow connector for Cloud Spanner (https://cloud.google.com/spanner/docs/dataflow-connector) and Dataflow Connector for Cloud Bigtable (https://cloud.google.com/bigtable/docs/hbase-dataflow-java) to retrieve data from these sources, but you can't use Dataflow SQL to restrict this to specific users. Dataflow SQL natively only works when reading data from Pub/Sub topics, Cloud Storage file sets, and BigQuery tables.
Ref: https://cloud.google.com/dataflow/docs/guides/sql/data-sources-destinations

`Set up a Cloud Dataproc Cluster to run a Hadoop job to join up data from Cloud BigTable and Cloud Storage for the specific gamer.` **is not right.**
While it is certainly possible to do this using a Hadoop job, it is complicated as we would have to come up with the code/logic to extract the data and certainly not straightforward.

`Set up a Cloud Dataflow job to read data from Cloud Storage and Cloud BigTable for the specific gamer.` **is not right.**
This option is possible, but it is not as efficient as using Big Query.
Ref: https://cloud.google.com/dataflow/docs/guides/sql/dataflow-sql-intro

Here is some more documentation around this option, some of the issues are

Dataflow SQL expects CSV files in Cloud Storage filesets. CSV files must not contain a header row with column names; the first row in each CSV file is interpreted as a data record. - but our question doesn't say how the exported data is stored in cloud storage.

You can only run jobs in regions that have a Dataflow regional endpoint. Our question doesn't say which region.
Ref: https://cloud.google.com/dataflow/docs/concepts/regional-endpoints.

Creating a Dataflow job can take several minutes - unlike Big Query external tables which can be created very quickly. Too many unknowns. Otherwise, this option is a good option. Here is some more information if you'd like to get a better understanding of how to use Cloud Dataflow to achieve this result. Cloud Dataflow SQL lets you use SQL queries to develop and run Dataflow jobs from the BigQuery web UI. You can join streams (such as Pub/Sub) and snapshotted datasets (such as BigQuery tables and Cloud Storage filesets); query your streams or static datasets with SQL by associating schemas with objects, such as tables, Cloud Storage filesets and Pub/Sub topics; and write your results into a BigQuery table for analysis and dashboarding.

Cloud Dataflow SQL supports multiple data sources including Cloud Storage and Big Query tables which are of interest for this scenario.
Ref: https://cloud.google.com/dataflow/docs/guides/sql/data-sources-destinations

`Create two external tables in BigQuery and link them to the Cloud BigTable and Cloud Storage data sources, respectively. Execute a query in BigQuery console to join up data between the two external tables for the specific gamer.` **is the right answer.**
Big query lets you create tables that reference external data sources such as Bigtable and Cloud Storage. You can then join up these two tables through user fields and apply appropriate filters. You can achieve the result with minimal configuration using this option.
Ref: https://cloud.google.com/bigquery/external-data-sources

Question 14:
Skipped
Your team created two networks (VPC) with non-overlapping ranges in Google Cloud in the same region. The first VPC hosts an encryption service on a GKE cluster with cluster autoscaling enabled. The encryption service provides TCP endpoints to encrypt and decrypt data. The second VPC pt-network hosts a user management system on a single Google Cloud Compute Engine VM. The user management system deals with PII data and needs to invoke the encryption endpoints running on the GKE cluster to encrypt and decrypt data. What should you do to enable the compute engine VM invoke the TCP encryption endpoints while minimizing effort?

- ○

Create a Kubernetes Service with type: NodePort to expose the encryption endpoints running in the pods. Set up a custom proxy in another compute engine VM in pt-network and configure it to forward the traffic to the Kubernetes Service in the other VPC. Have the GCE VM invoke the TCP encryption endpoints on the proxy DNS address.

- ○

Create a Kubernetes Service with type: Loadbalancer to expose the encryption endpoints running in the pods. Configure a Cloud Armour security policy to allow traffic from GCE VM to the Kubernetes Service. Have the GCE VM invoke the TCP encryption endpoints on the Kubernetes Service DNS address.

- ○

Create a Kubernetes Service with type: Loadbalancer and the cloud.google.com/load-balancer-type: Internal annotation to expose the encryption endpoints running in the pods. Peer the two VPCs and have the GCE VM invoke the TCP encryption endpoints on the (Internal) Kubernetes Service DNS address.

(Correct)

- ○

Create a Kubernetes Service with type: Loadbalancer to expose the encryption endpoints running in the pods. Disable propagating Client IP Addresses to the pods by setting Services' .spec.externalTrafficPolicy to Cluster. Have the GCE VM invoke the TCP encryption endpoints on the Kubernetes Service DNS address.

Explanation
While it may be possible to set up the networking to let the compute engine instance in pt-network communicate with pods in the GKE cluster in multiple ways, we need to look for an option that minimizes effort. Generally speaking, this means using Google Cloud Platform services directly over setting up the service ourselves.

`Create a Kubernetes Service with type: Loadbalancer to expose the encryption endpoints running in the pods. Disable propagating Client IP Addresses to the pods by setting Services' .spec.externalTrafficPolicy to Cluster. Have the GCE VM invoke the TCP encryption endpoints on the Kubernetes Service DNS address.` **is not right.**
In GKE, services are used to expose pods to the outside world. There are multiple types of services. The three common types are - NodePort, ClusterIP, and LoadBalancer (there are two more service types - ExternalName and Headless, which are not relevant in this context). We do not want to create a Cluster IP as this is not

accessible outside the cluster. And we do not want to create NodePort as this results in exposing a port on each node in the cluster; and as we have multiple replicas, this will result in them trying to open the same port on the nodes which fail. The compute engine instance in pt-network needs a single point of communication to reach GKE, and you can do this by creating a service of type LoadBalancer. The LoadBalancer service is given a public IP that is externally accessible.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/exposing-apps

externalTrafficPolicy denotes how the service should route external traffic - including public access. Rather than trying to explain, I'll point you to an excellent blog that does a great job of answering how this works. https://www.asykim.com/blog/deep-dive-into-kubernetes-external-traffic-policies

Since we have cluster autoscaling enabled, we can have more than 1 node and possibly multiple replicas running on each node. So externalTrafficPolicy set to Cluster plays well with our requirement. Finally, we configure the compute engine to use the (externally accessible) address of the load balancer.

So this certainly looks like an option, but is it the best option that minimizes effort? One of the disadvantages of this option is that it exposes the pods publicly by using a service of type LoadBalancer. We want our compute engine to talk to the pods, but do we want to expose our pods to the whole world? Maybe not!! Let's look at the other options to find out if there is something more relevant and secure.

`Create a Kubernetes Service with type: NodePort to expose the encryption endpoints running in the pods. Set up a custom proxy in another compute engine VM in pt-network and configure it to forward the traffic to the Kubernetes Service in the other VPC. Have the GCE VM invoke the TCP encryption endpoints on the proxy DNS address.` **is not right.**
For reasons explained in the above option, we don't want to create a service of type NodePort. This service opens up a port on each node for each replica (pod). If we choose to do this, the compute engine doesn't have a single point to contact. Instead, it would need to contact the GKE cluster nodes individually - and that is bound to have issues because we have autoscaling enabled and the nodes may scale up and scale down as per the scaling requirements. New nodes may have different IP addresses to the previous nodes, so unless the Compute engine is continuously supplied with the IP addresses of the nodes, it can't reach them. Moreover, we have multiple replicas, and we might have multiple replicas of the pod on the same node in which case they all can't open the same node port - once a node port is opened by one replica (pod), it can't be used by other replicas on the same node. So this option can be ruled out without going into the rest of the answer.

`Create a Kubernetes Service with type: Loadbalancer to expose the encryption endpoints running in the pods. Configure a Cloud Armour security policy to allow traffic from GCE VM to the Kubernetes Service. Have the GCE VM invoke the TCP encryption endpoints on the Kubernetes`

`Service DNS address.` **is not right.**
Creating a service of type LoadBalancer and getting a Compute Engine instance to use the address of the load balancer is fine, but Cloud Armor is not required. You could use Cloud Armor to set up a whitelist policy to only let traffic through from the compute engine instance, but hang on - this option says “MIG instances”. We don’t have a managed instance group. The question mentions a single instance but not MIG. If we were to assume the single instance is part of a MIG, i.e. a MIG with a single instance, this option works too. It is more secure than the first option discussed in the explanation but at the same time more expensive. Let’s look at the other option to see if it provides a secure yet cost-effective way of achieving the same.

`Create a Kubernetes Service with type: Loadbalancer and the cloud.google.com/load-balancer-type: Internal annotation to expose the encryption endpoints running in the pods. Peer the two VPCs and have the GCE VM invoke the TCP encryption endpoints on the (Internal) Kubernetes Service DNS address.` **is the right answer.**
Creating a service of type LoadBalancer and getting a Compute Engine instance to use the address of the load balancer is fine. We covered this previously in the first option in the explanations section. Adding the annotation cloud.google.com/load-balancer-type: Internal makes your cluster's services accessible to applications outside of your cluster that use the same VPC network and are located in the same Google Cloud region. So this improves security by not allowing public access; however, the compute engine is located in a different VPC so it can’t access.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/internal-load-balancing
But peering the VPCs together enables the compute engine to access the load balancer IP. And peering is possible because they do not use overlapping IP ranges. Peering links up the two VPCs and resources inside the VPCs can communicate with each other as if they were all in a single VPC. More info about VPC peering: https://cloud.google.com/vpc/docs/vpc-peering

So this option is the right answer. It provides a secure and cost-effective way of achieving our requirements. There are several valid answers, but this option is better than the others.

Question 15:
Skipped
You are hosting a new application on https://www.my-new-gcp-ace-website.com. The static content of the application is served from /static path and is hosted in a Cloud Storage bucket. The dynamic content is served from /dynamic path and is hosted on a fleet of compute engine instances belonging to a Managed Instance Group. How can you configure a single GCP Load Balancer to serve content from both paths?

- ○

Configure an HTTP(s) Load Balancer and configure it to route requests on /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket. Create a DNS A record on www.my-new-gcp-ace-website.com to point to the address of LoadBalancer.

(Correct)

- ○

  Configure an HTTP(s) Load Balancer for the Managed Instance Group (MIG). Configure the necessary TXT DNS records on www.my-new-gcp-ace-website.com to route requests on /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket.

- ○

  Create a CNAME DNS record on www.my-new-gcp-ace-website.com to point to storage.googleapis.com. Configure an HTTP(s) Load Balancer for the Managed Instance Group (MIG). Set up redirection rules in Cloud Storage bucket to forward requests for non-static content to the Load Balancer address.

- ○

  Use HAProxy Alpine Docker images to deploy to GKE cluster. Configure HAProxy to route /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket. Create a service of type LoadBalancer. Create a DNS A record on www.my-new-gcp-ace-website.com to point to the address of LoadBalancer.

Explanation

As a rule of thumb, Google recommended practices mean you need to select Google Services that offer out of the box features with minimal configuration. Our requirement here is to serve content from two backends while following Google recommended practices.

`Create a CNAME DNS record on www.my-new-gcp-ace-website.com to point to storage.googleapis.com. Configure an HTTP(s) Load Balancer for the Managed Instance Group (MIG). Set up redirection rules in Cloud Storage bucket to forward requests for non-static content to the Load Balancer address.` **is not right.**

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

`Use HAProxy Alpine Docker images to deploy to GKE cluster. Configure HAProxy to route /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket. Create a service of type LoadBalancer. Create a DNS A record on www.my-new-gcp-ace-website.com to point to the address of LoadBalancer.` **is not right.**

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

`Configure an HTTP(s) Load Balancer for the Managed Instance Group (MIG). Configure the necessary TXT DNS records on www.my-new-gcp-ace-website.com to route requests on /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket.` **is not right.**

TXT records are used to verify the domain and TXT records can also hold any arbitrary text, but the DNS providers don't use the text in these TXT records for routing.
Ref: https://cloud.google.com/dns/records
Ref: https://support.google.com/cloudidentity/answer/183895?hl=en

`Configure an HTTP(s) Load Balancer and configure it to route requests on /dynamic/ to the Managed Instance Group (MIG) and /static/ to GCS bucket. Create a DNS A record on www.my-new-gcp-ace-website.com to point to the address of LoadBalancer.` **is the right answer.**

Since we need to send requests to multiple backends, Cloud DNS can't alone help us. We need Cloud HTTPS Load Balancer - it's URL maps (a fancy name for path-based routing) helps distribute traffic to backends based on the path information.
Ref https://cloud.google.com/load-balancing/docs/url-map
Traffic received by Cloud HTTPS Load Balancer can be configured to send all requests on /dynamic path to the MIG group; and requests on /static/ path to the bucket.
Ref Adding MIG as backend service - https://cloud.google.com/load-balancing/docs/backend-service#backend_services_and_autoscaled_managed_instance_groups.
Ref Adding a backend bucket(s) - https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers
The Load Balancer has a public IP address. But we want to instead access on www.my-new-gcp-ace-website.com, so we configure this as an A Record in our DNS provider.
Ref: https://cloud.google.com/dns/records.

Question 16:
Skipped

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

- ○

  Create a single Stackdriver account and link all production GCP projects to it. Configure a monitoring dashboard in the Stackdriver account.

  (Correct)

- ○

  Create a Stackdriver account in each project and configure all accounts to use the same service account. Create a monitoring dashboard in one of the projects.

- ○

  Create a Stackdriver account and a Stackdriver group in one of the production GCP projects. Add all other projects as members of the group. Configure a monitoring dashboard in the Stackdriver account.

- ○

  Set up a shared VPC across all production GCP projects and configure Cloud Monitoring dashboard on one of the projects.

Explanation

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

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

`Create a Stackdriver account and a Stackdriver group in one of the production GCP projects. Add all other projects as members of the group. Configure a monitoring dashboard in the Stackdriver account.` **is not right.**
As the other projects are not linked to the stack driver, they can't be monitored. Moreover, you can not add projects to Stackdriver groups. Groups provide a mechanism for alerting on the behaviour of a set of resources, rather than on individual resources. For example, you can create an alerting policy that is triggered if some number of resources in the group violates a particular condition (for example, CPU load), rather than having each resource inform you of violations individually.
Ref: https://cloud.google.com/monitoring/groups

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

Question 17:
Skipped
You want to deploy a cost-sensitive application to Google Cloud Compute Engine. You want the application to be up at all times, but because of the cost-sensitive nature of the application, you only want to run the application in a single VM instance. How should you configure the managed instance group?

- ○

  Enable autoscaling on the Managed Instance Group (MIG) and set minimum instances to 1 and maximum instances to 1.

  (Correct)

- ○

  Disable autoscaling on the Managed Instance Group (MIG) and set mininum instances to 1 and maximum instances to 1.

- ○

  Enable autoscaling on the Managed Instance Group (MIG) and set minimum instances to 1 and maximum instances to 2.

- ○

  Disable autoscaling on the Managed Instance Group (MIG) and set mininum instances to 1 and maximum instances to 2.

Explanation
Requirements

1. Since we need the application running at all times, we need a minimum 1 instance.

2. Only a single instance of the VM should run, we need a maximum 1 instance.

We want the application running at all times. If the VM crashes due to any underlying hardware failure, we want another instance to be added to MIG so that application can continue to serve requests. We can achieve this by enabling autoscaling.

The only option that satisfies these three is `Enable autoscaling on the Managed Instance Group (MIG) and set minimum instances to 1 and maximum instances to 1.`
Ref: https://cloud.google.com/compute/docs/autoscaler

Question 18:
Skipped
You are the Cloud Security Manager at your company, and you want to review IAM users and their assigned roles in the production GCP project. You want to follow Google recommended practices. What should you do?

- ○

  Check the output of gcloud iam roles list command.

- ○

  Review the information in the Roles section for the production GCP project in Google Cloud Console.

- ○

  Check the output of gcloud iam service-accounts list command.

- ○

  Review the information in the IAM section for the production GCP project in Google Cloud Console.

  (Correct)

Explanation

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

`Check the output of gcloud iam roles list command.` **is not right.**

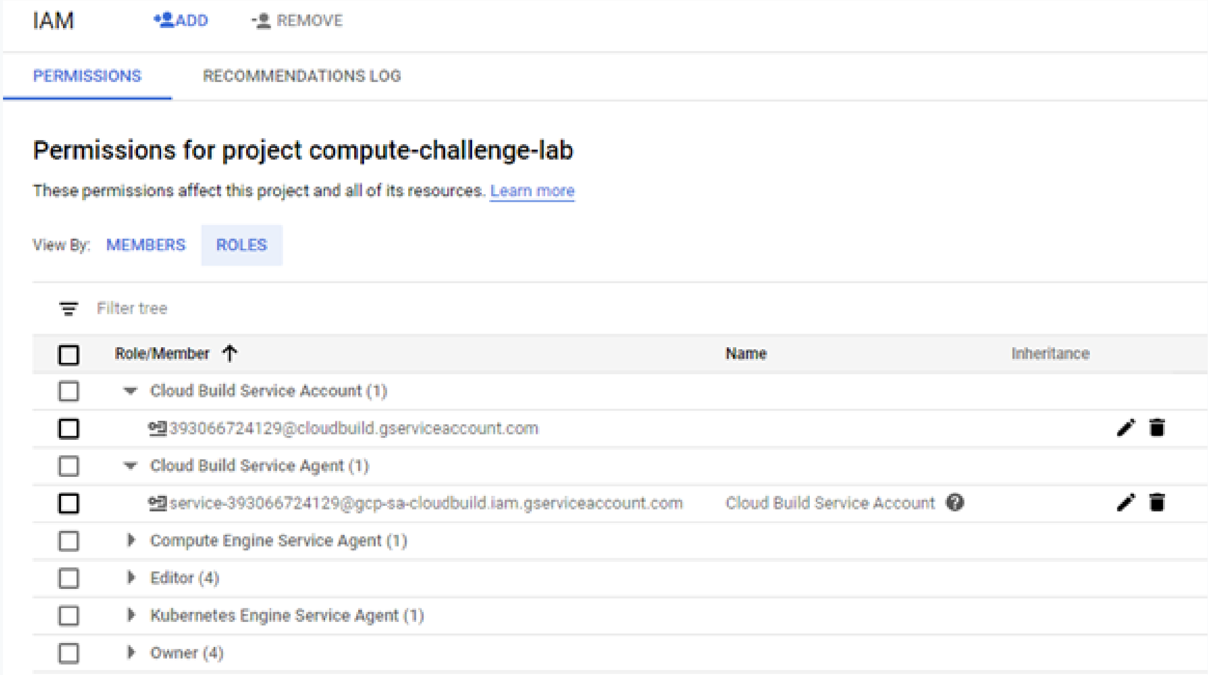
gcloud iam roles list lists the roles but does not list the users (i.e. IAM members)

`Check the output of gcloud iam service-accounts list command.` **is not right.**

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

`Review the information in the Roles section for the production GCP project in Google Cloud Console.` **is not right.**

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



Permissions for project compute-challenge-lab

These permissions affect this project and all of its resources. Learn more

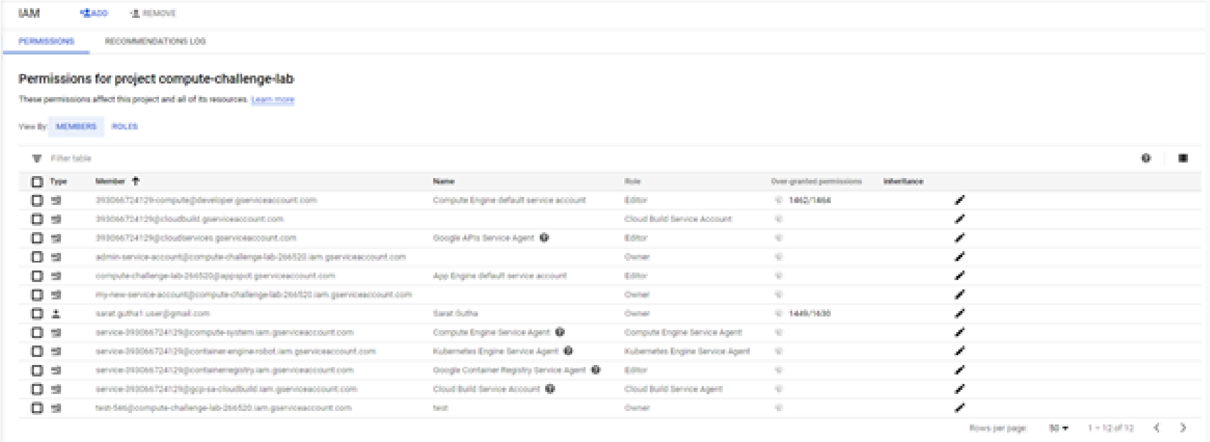
☐	Role/Member ↑	Name	Inheritance
☐	Cloud Build Service Account (1)		
☐	393066724129@cloudbuild.gserviceaccount.com		
☐	Cloud Build Service Agent (1)		
☐	service-393066724129@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Account	
☐	Compute Engine Service Agent (1)		
☐	Editor (4)		
☐	Kubernetes Engine Service Agent (1)		
☐	Owner (4)		

`Review the information in the IAM section for the production GCP project in Google Cloud Console.` **is the right answer.**

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

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

See the screenshot below.



IAM ADD REMOVE

PERMISSIONS RECOMMENDATIONS LOG

Permissions for project compute-challenge-lab

These permissions affect this project and all of its resources. Learn more

View By: MEMBERS ROLES

Filter table

□	Type	Member ↑	Name	Role	Over-granted permissions	Inheritance
□		393066724129-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	1462/1464	
□		393066724129@cloudbuild.gserviceaccount.com		Cloud Build Service Account		
□		393066724129@cloudservices.gserviceaccount.com	Google APIs Service Agent	Editor		
□		admin-service-account@compute-challenge-lab-266520.iam.gserviceaccount.com		Owner		
□		compute-challenge-lab-266520@appspot.gserviceaccount.com	App Engine default service account	Editor		
□		my-new-service-account@compute-challenge-lab-266520.iam.gserviceaccount.com		Owner		
□		sarat.gutha1.user@gmail.com	Sarat Gutha	Owner	1449/1630	
□		service-393066724129@compute-system.iam.gserviceaccount.com	Compute Engine Service Agent	Compute Engine Service Agent		
□		service-393066724129@container-engine-robot.iam.gserviceaccount.com	Kubernetes Engine Service Agent	Kubernetes Engine Service Agent		
□		service-393066724129@containerregistry.iam.gserviceaccount.com	Google Container Registry Service Agent	Editor		
□		service-393066724129@gcp-sa-cloudbuild.iam.gserviceaccount.com	Cloud Build Service Account	Cloud Build Service Agent		
□		test-546@compute-challenge-lab-266520.iam.gserviceaccount.com	test	Owner		

Rows per page: 50 ▾ 1 – 12 of 12 < >

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

Question 19:

Skipped

A production application serving live traffic needs an important update deployed gradually. The application is deployed in a Managed Instance Group (MIG) in the US-Central region. The application receives millions of requests each minute, and you want to patch the application while ensuring the number of instances (capacity) in the Managed Instance Group (MIG) does not decrease. What should you do?

- ○

  Update the existing Managed Instance Group (MIG) to point to a new instance template containing the updated version. Terminate all existing instances in the MIG and wait until they are all replaced by new instances created from the new template.

- ○

  Carry out a rolling update by executing gcloud compute instance-groups {managed group name} rolling-action start-update --max-surge 0 --max-unavailable 1.

- ○

  Deploy the update in a new MIG and add it as a backend service to the existing production Load Balancer. Once all instances in the new group have warmed up, remove the old MIG from the Load Balancer backend and delete the group.

- ○

Carry out a rolling update by executing gcloud compute instance-groups {managed group name} rolling-action start-update --max-surge 1 --max-unavailable 0.

(Correct)

Explanation
Our requirements are

Deploy a new version gradually and

Ensure available capacity does not decrease during deployment.

`Update the existing instance template with the required changes and deploy the changes to a new MIG. Update the existing production Load Balancer configuration to add the newly created MIG as a backend service. Once all instances in the new group have warmed up, remove the old MIG from the Load Balancer backend. When all instances belonging to the old MIG have been drained, delete the OLD mig.` **is not right.**
First of all instance, instance templates can not be updated. So the phrase *Update the existing instance template* rules out this option.
Ref: https://cloud.google.com/compute/docs/instance-templates/

`Update the existing Managed Instance Group (MIG) to point to a new instance template containing the updated version. Terminate all existing instances in the MIG and wait until they are all replaced by new instances created from the new instance template.` **is not right.**
If we follow these steps, we end up with a full fleet of instances belonging to the new managed instances group (i.e. based on the new template) behind the load balancer. Our requirement to gradually deploy the new version is not met. Also, deleting the existing instances of the managed instance group would almost certainly result in an outage to our application which is not desirable when we are serving live web traffic.

`Carry out a rolling update by executing gcloud compute instance-groups {managed group name} rolling-action start-update --max-surge 0 --max-unavailable 1.` **is not right.**
maxSurge specifies the maximum number of instances that can be created over the desired number of instances. If maxSurge is set to 0, the rolling update can not create additional instances and is forced to update existing instances resulting in a reduction in capacity. Therefore, it does not satisfy our requirement to ensure that the available capacity does not decrease during the deployment. maxUnavailable - specifies the maximum number of instances that can be unavailable during the update process. When maxUnavailable is set to 1, the rolling update updates 1 instance at a time. i.e. it takes 1 instance out of service, updates it, and puts it back into service. This option results in a reduction in capacity while the instance is out of

service. Example - if we have 10 instances in service, this combination of setting results in 1 instance at a time taken out of service for an upgrade while the remaining 9 continue to serve live traffic. That's a reduction of 10% in available capacity and does not satisfy our requirement to ensure that the available capacity does not decrease during the deployment.

`Carry out a rolling update by executing gcloud compute instance-groups {managed group name} rolling-action start-update --max-surge 1 --max-unavailable 0.` **is the right answer.**

This option is the only one that satisfies our two requirements - deploying gradually and ensuring the available capacity does not decrease. When maxUnavailable is set to 0, the rolling update can not take existing instances out of service. And when maxSurge is set to 1, we let the rolling update spin a single additional instance. The rolling update then puts the additional instance into service and takes one of the existing instances out of service for the upgrade. There is no reduction in capacity at any point in time. And the rolling upgrade upgrades 1 instance at a time, so we gradually deploy the new version. As an example - if we have 10 instances in service, this combination of setting results in 1 additional instance put into service (resulting in 11 instances serving traffic), then an older instance taken out of service (resulting in 10 instances serving traffic) and the upgraded instance put back into service (resulting in 11 instances serving traffic). The rolling upgrade continues updating the remaining 9 instances one at a time. Finally, when all 10 instances have been upgraded, the additional instance that is spun up is deleted. We still have 10 instances serving live traffic but now on the new version of code.
Ref: https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

Question 20:

Skipped

Your colleague updated a deployment manager template of a production application serving live traffic. You want to deploy the update to the live environment later during the night when user traffic is at its lowest. The git diff on the pull request shows the changes are substantial and you would like to review the intended changes without applying the changes in the live environment. You want to do this as efficiently and quickly as possible. What should you do?

- ○

  Preview the changes by applying the deployment manager template with the --preview flag.

  (Correct)

- ○

  Add logging statements in the deployment manager template YAML file.

- ○

  Apply the deployment manager template and review the actions in Cloud Logging.

- ○

  Clone the GCP project and apply the deployment manager template in the new project. Review the actions in Cloud Logging and monitor for failures before applying the template in the production GCP project.

Explanation

Requirements - confirm dependencies, rapid feedback.

`Add logging statements in the deployment manager template YAML file.` **is not right.**

Deployment Manager doesn't provide the ability to set granular logging statements. Moreover, if that were possible, the logging statements wouldn't be written to a log file until the template is applied and it is already too late as the template is applied. We haven't had a chance to confirm that the dependencies of all defined resources are adequately met.

`Apply the deployment manager template and review the actions in Cloud Logging.` **is not right.**

This option doesn't give us a chance to confirm that the dependencies of all defined resources are adequately met before executing it.

`Clone the GCP project and apply the deployment manager template in the new project. Review the actions in Cloud Logging and monitor for failures before applying the template in the production GCP project.` **is not right.**

While we can identify whether dependencies are met by monitoring the failures, it is not rapid. We need rapid feedback on changes, and we want that before changes are committed (i.e. applied) to the project.

`Preview the changes by applying the deployment manager template with the --preview flag.` **is the right answer.**

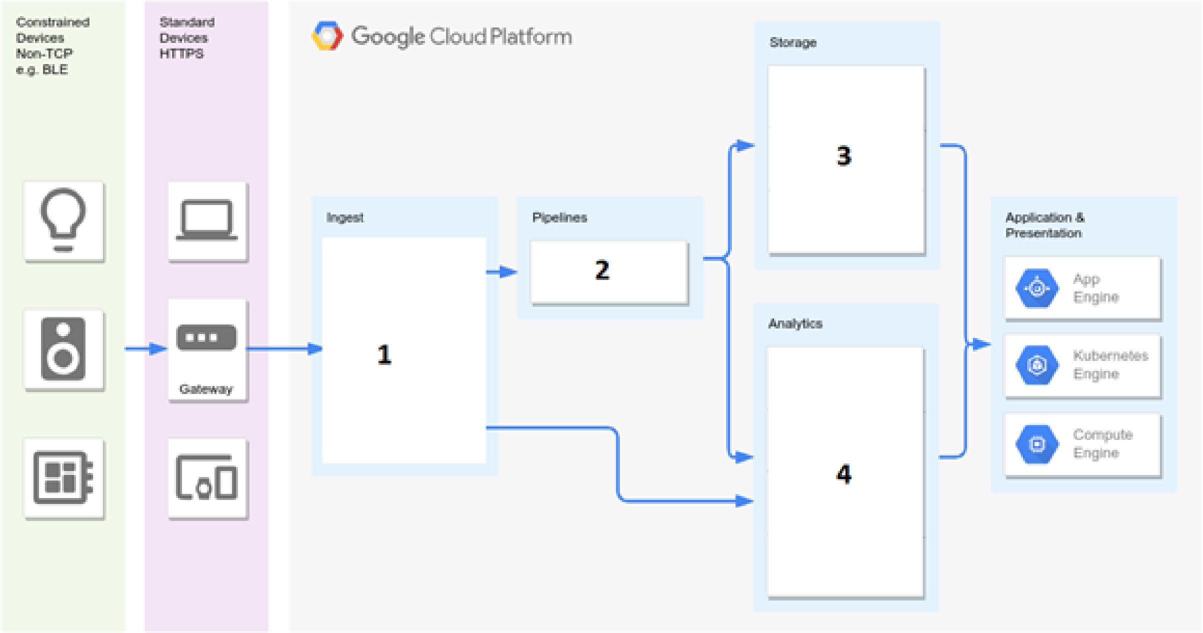
After we have written a configuration file, we can preview the configuration before you create a deployment. Previewing a configuration lets you see the resources that Deployment Manager would create but does not instantiate any resources. In gcloud command-line, you use the create sub-command with the --preview flag to preview configuration changes.

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

Question 21:

Skipped

Your company installs and manages several types of IoT devices all over the world. Events range from 50,000 to 500,000 messages a second. You want to identify the best solution for ingesting, transforming, storing and analyzing this data in GCP platform. What GCP services should you use?



- ○

  Cloud Pub/Sub for ingesting, Cloud Dataflow for transforming, Cloud Datastore for storing and BigQuery for analyzing the time-series data.

- ○

  Cloud Pub/Sub for ingesting, Cloud Storage for transforming, BigQuery for storing and Cloud Bigtable for analyzing the time-series data.

- ○

  Cloud Pub/Sub for ingesting, Cloud Dataflow for transforming, Cloud Bigtable for storing and BigQuery for analyzing the time-series data.

  (Correct)

- ○

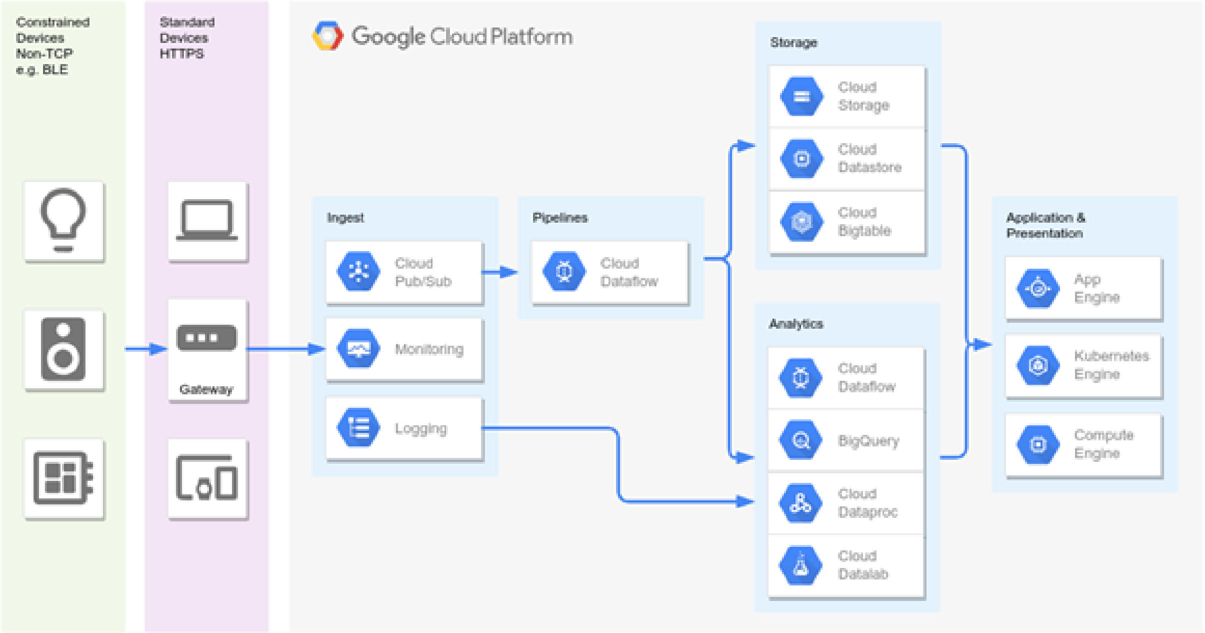
  Firebase Messages for ingesting, Cloud Pub/Sub for transforming, Cloud Spanner for storing and BigQuery for analyzing the time-series data.

Explanation

`Cloud Pub/Sub for ingesting, Cloud Dataflow for transforming, Cloud Bigtable for storing and BigQuery for analyzing the time-series data.` **is the right answer.**

For ingesting time series data, your best bet is Cloud Pub/Sub. For processing the data in pipelines, your best bet is Cloud Dataflow.

That leaves us with two remaining options; both have BigQuery for analyzing the data. For storage, it is a choice between Bigtable and Datastore. Bigtable provides out of the box support for time series data. So using Bigtable for Storage is the right answer.
Ref: https://cloud.google.com/bigtable/docs/schema-design-time-series



Question 22:

Skipped

You've deployed a microservice that uses sha1 algorithm with a salt value to has usernames. You deployed this to GKE cluster using deployment file:

```
apiVersion: apps/v1
kind: Deployment
metadata:
name: sha1_hash_app-deployment
spec:
selector:
    matchLabels:
    app: sha1_hash_app
    replicas: 3
    template:
    metadata:
        labels:
        app: sha1_hash_app
    spec:
        containers:
        - name: hash-me
        image: gcr.io/hash-repo/sha1_hash_app:2.17
        env:
        - name: SALT_VALUE
            value: "z0rtkty12$!"
        ports:
        - containerPort: 8080
```

You need to make changes to prevent the salt value from being stored in plain text. You want to follow Google-recommended practices. What should you do?

- ○

  Bake the salt value into the container image.

- ○

  Save the salt value in a Kubernetes ConfigMap object. Modify the YAML configuration file to reference the ConfigMap object.

- ○

  Save the salt value in a Kubernetes Persistent Volume. Modify the YAML configuration file to include a Persistent Volume Claim to mount the volume and reference the password from the file.

- ○

  Save the salt value in a Kubernetes secret object. Modify the YAML configuration file to reference the secret object.

  (Correct)

Explanation

`Bake the salt value into the container image.` **is not right.**
Baking passwords into Docker images is a terrible idea. Anyone who spins up a container from this image has access to the password.

`Save the salt value in a Kubernetes ConfigMap object. Modify the YAML configuration file to reference the ConfigMap object.` **is not right.**
ConfigMaps are useful for storing and sharing non-sensitive, unencrypted configuration information. To use sensitive information in your clusters, you must use Secrets.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/configmap

`Save the salt value in a Kubernetes Persistent Volume. Modify the YAML configuration file to include a Persistent Volume Claim to mount the volume and reference the password from the file.` **is not right.**
Persistent volumes should not be used for storing sensitive information. PersistentVolume resources are used to manage durable storage in a cluster, and PersistentVolumeClaim is a request for and claim to a PersistentVolume resource.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/persistent-volumes

`Save the salt value in a Kubernetes secret object. Modify the YAML configuration file to reference the secret object.` **is the right answer.**
In GKE, you can create a secret to hold the password; and then use the secret as an environment variable in the YAML file.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/secret
You can create a secret using

```
kubectl create secret generic passwords --from-literal sha1_hash_app_SALT_VALUE= z0rtkty12$!
```

And you can then modify the YAML file to reference this secret as shown below.

```
apiVersion: apps/v1
kind: Deployment
metadata:
name: sha1_hash_app-deployment
spec:
selector:
    matchLabels:
    app: sha1_hash_app
    replicas: 3
    template:
    metadata:
        labels:
        app: sha1_hash_app
    spec:
        containers:
        - name: hash-me
        image: gcr.io/hash-repo/sha1_hash_app:2.17
        env:
        - name: SALT_VALUE
            valueFrom:
                    secretKeyRef:
                        name: passwords
                        key: sha1_hash_app_SALT_VALUE
        ports:
        - containerPort: 8080
```

Question 23:

Skipped

Your company runs several internal applications on bare metal Kubernetes servers in your on-premises data centre. One of the applications deployed in the Kubernetes cluster uses a NAS share to save files. In preparation for the upcoming migration to Google Cloud, you want to update the application to use Google Cloud Storage instead; however, security policies prevent virtual machines from having public IP addresses. What should you do?

- ○

  Migrate all VMs from the data centre to Google Compute Engine. Set up a Load Balancer on the GCP bucket and have the servers access Cloud Storage through the load balancer.

- ○

  Configure a VPN tunnel between the on-premises data centre and the GCP VPC. Create a custom route in the VPC for Google Restricted APIs IP range (199.36.153.4/30) and propagate the route over VPN. Resolve *.googleapis.com as a CNAME record to restricted.googleapis.com in your on-premises DNS server.

  (Correct)

- ○

  Create a new VPC in GCP and deploy a proxy server like HAProxy/Squid to forward requests to Cloud Storage. Configure a VPN tunnel between the on-premises data centre and the GCP VPC. Have the servers access Cloud Storage through the proxy.

- ○

  Make an exception and assign public IP addresses to the servers. Configure firewall rules to allow traffic from the VM public IP addresses to the IP range of Cloud Storage.

Explanation

We need to follow Google recommended practices to achieve the result. Configuring Private Google Access for On-Premises Hosts is best achieved by VPN/Interconnect + Advertise Routes + Use restricted Google IP Range.

`Configure a VPN tunnel between the on-premises data centre and the GCP VPC. Create a custom route in the VPC for Google Restricted APIs IP range (199.36.153.4/30) and propagate the route over VPN. Resolve *.googleapis.com as a CNAME record to restricted.googleapis.com in your on-premises DNS server.` **is the right answer**, and it is what Google recommends.

Ref: https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid
“You must configure routes so that Google API traffic is forwarded through your Cloud VPN or Cloud Interconnect connection, firewall rules on your on-premises firewall to allow the outgoing traffic, and DNS so that traffic to Google APIs resolves to the IP range you've added to your routes.” “You can use Cloud Router Custom Route Advertisement to announce the Restricted Google APIs IP addresses through Cloud Router to your on-premises network. The Restricted Google APIs IP range is 199.36.153.4/30. While this is technically a public IP range, Google does not announce it publicly. This IP range is only accessible to hosts that can reach your Google Cloud projects through internal IP ranges, such as through a Cloud VPN or Cloud Interconnect connection.”

Question 24:

Skipped

Your company’s new mobile game has gone live, and you have transitioned the backend application to the operations team. The mobile game uses Cloud Spanner to persist game state, leaderboard and player profile. All operations engineers require access to view and edit table data to support runtime issues. What should you do?

- ○

  Grant roles/spanner.databaseUser IAM role to all operations engineers user accounts.

- ○

  Grant roles/spanner.viewer IAM role to all operations engineers user accounts.

- ○

  Grant roles/spanner.viewer IAM role to all operations engineers group.

- ○

  Grant roles/spanner.databaseUser IAM role to all operations engineers group.

  (Correct)

Explanation

Our requirements

View and Edit table data

Multiple users

Multiple users indicate that we do not want to assign roles/permissions at the user level. Instead, we should do it based on groups so that we can create one group with all the required permissions and all such users who need this access can be assigned to the group.
Ref: https://cloud.google.com/iam/docs/reference/rest/v1/Policy#Binding
Ref: https://cloud.google.com/iam/docs/granting-changing-revoking-access#granting-gcloud-manual

`Grant roles/spanner.databaseUser IAM role to all operations engineers user accounts.` **is not right.**
We are looking for an option that assigns users to a group (to maximise reuse and minimize maintenance overhead). This option assigns users to the role so is not the right answer.

`Grant roles/spanner.viewer IAM role to all operations engineers user accounts.` **is not right.**
We are looking for an option that assigns users to a group (to maximise reuse and minimize maintenance overhead). This option assigns users to the role so is not the right answer.

`Grant roles/spanner.viewer IAM role to all operations engineers group.` **is not right.**
Adding users to a group and granting the role to the group is the right way forward. But the role used in this option is spanner.viewer which allows viewing all Cloud Spanner instances (but cannot modify instances). It allows viewing all Cloud Spanner databases (but cannot modify databases and cannot read from databases). Since we required edit access as well, this option is not right.
Ref: https://cloud.google.com/spanner/docs/iam

`Grant roles/spanner.databaseUser IAM role to all operations engineers group.` **is the right answer.**
Adding users to a group and granting the role to the group is the right way forward. Also, we assign the role spanner.databaseUser which allows Read from and write to the Cloud Spanner database; execute SQL queries on the database, including DML and Partitioned DML; and View and update schema for the database. This option grants the right role to a group and assigns users to the group.

Question 25:
Skipped
You are migrating your on-premises workloads to GCP VPC, and you want to use Compute Engine virtual machines. You want to separate the Finance team VMs and the Procurement team VMs into separate subnets. You need all VMs to communicate with each other over their internal IP addresses without adding routes. What should you do?

- ○

Use Deployment Manager to create two VPCs, each with a subnet in a different region. Ensure the subnets use non-overlapping IP range.

- ○

  Use Deployment Manager to create a new VPC with 2 subnets in the same region. Ensure the subnets use the same IP range.

- ○

  Use Deployment Manager to create two VPCs, each with a subnet in the same region. Ensure the subnets use overlapping IP range.

- ○

  Use Deployment Manager to create a new VPC with 2 subnets in 2 different regions. Ensure the subnets use non-overlapping IP range.

  (Correct)

Explanation

`Use Deployment Manager to create two VPCs, each with a subnet in a different region. Ensure the subnets use non-overlapping IP range.` **is not right.**
We need to get our requirements working with 1 VPC, not 2 !!

`Use Deployment Manager to create two VPCs, each with a subnet in the same region. Ensure the subnets use overlapping IP range.` **is not right.**
We need to get our requirements working with 1 VPC, not 2 !!

`Use Deployment Manager to create a new VPC with 2 subnets in the same region. Ensure the subnets use the same IP range.` **is not right.**
We can not create two subnets in one VPC with the same CIDR range. "Primary and secondary ranges for subnets cannot overlap with any allocated range, any primary or secondary range of another subnet in the same network, or any IP ranges of subnets in peered networks."
Ref: https://cloud.google.com/vpc/docs/using-vpc#subnet-rules

`Use Deployment Manager to create a new VPC with 2 subnets in 2 different regions. Ensure the subnets use non-overlapping IP range.` **is the right answer.**
When we create subnets in the same VPC with different CIDR ranges, they can communicate automatically within VPC. "Resources within a VPC network can communicate with one another by using internal (private) IPv4 addresses, subject to applicable network firewall rules."
Ref: https://cloud.google.com/vpc/docs/vpc

Question 26:

Skipped

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

- ○

  Add the logging pod in the Deployment YAML file.

- ○

  Initialize the logging pod during the GKE Cluster creation.

- ○

  Deploy the logging pod in a DaemonSet Kubernetes object.

  (Correct)

- ○

  Deploy the logging pod in a StatefulSet Kubernetes object.

Explanation

`Add the logging pod in the Deployment YAML file.` **is not right.**

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

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

`Initialize the logging pod during the GKE Cluster creation.` **is not right.**

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

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

Sets up a new or existing configuration.

Sets properties in that configuration, including the current project and optionally, the default Google Compute Engine region and zone you'd like to use.
Ref: https://cloud.google.com/sdk/gcloud/reference/init

`Deploy the logging pod in a StatefulSet Kubernetes object.` **is not right.**
In GKE, StatefulSets represents a set of Pods with unique, persistent identities and stable hostnames that GKE maintains regardless of where they are scheduled. The state information and other resilient data for any given StatefulSet Pod are maintained in persistent disk storage associated with the StatefulSet. The primary purpose of StatefulSets is to set up persistent storage for pods that are deployed across multiple zones.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset
Although persistent volumes can be used, they are limited to two zones, and you'd have to get into node affinity if you want to use a persistent volume with a pod on a zone that is not covered by the persistent volumes zones.
Ref: https://kubernetes.io/docs/setup/best-practices/multiple-zones/

`Deploy the logging pod in a DaemonSet Kubernetes object.` **is the right answer.**
In GKE, DaemonSets manage groups of replicated Pods and adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed. So, this is a perfect fit for our monitoring pod.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset
DaemonSets are useful for deploying ongoing background tasks that you need to run on all or certain nodes, and which do not require user intervention. Examples of such tasks include storage daemons like ceph, log collection daemons like fluentd, and node monitoring daemons like collectd. For example, you could have DaemonSets for each type of daemon run on all of your nodes. Alternatively, you could run multiple DaemonSets for a single type of daemon, but have them use different configurations for different hardware types and resource needs.

Question 27:

Skipped

You deployed a Python application to GCP App Engine Standard service in the us-central region. Most of your customers are based in Japan and are experiencing slowness due to the latency. You want to transfer the application from us-central region to asia-northeast1 region to minimize latency. What should you do?

- ○

  Deploy a new app engine application in the same GCP project and set the region to asia-northeast1. Delete the old App Engine application.

- ○

  Update the default region property to asia-northeast1 on the App Engine Service.

- ○

  Update the region property to asia-northeast1 on the App Engine application.

- ○

  Create a new GCP project. Create a new App Engine Application in the new GCP project and set its region to asia-northeast-1. Delete the old App Engine application.

  (Correct)

Explanation

`Update the default region property to asia-northeast1 on the App Engine Service.` **is not right.**
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. You cannot change an app's region after you set it.
Ref: https://cloud.google.com/appengine/docs/locations

`Update the region property to asia-northeast1 on the App Engine application.` **is not right.**
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. You cannot change an app's region after you set it.
Ref: https://cloud.google.com/appengine/docs/locations

`Deploy a new app engine application in the same GCP project and set the region to asia-northeast1. Delete the old App Engine application.` **is not right.**
App Engine is regional, and you cannot change an app's region after you set it. You can deploy additional services in the App Engine, but they will all be targeted to the same region.
Ref: https://cloud.google.com/appengine/docs/locations

`Create a new GCP project. Create a new App Engine Application in the new GCP project and set its region to asia-northeast-1. Delete the old App Engine application.` **is the right answer.**
App Engine is regional, and you cannot change an app's region after you set it. Therefore, the only way to have an app run in another region is by creating a new project and targeting the app engine to run in the required region (asia-northeast1 in our case).
Ref: https://cloud.google.com/appengine/docs/locations

Question 28:

Skipped

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

- ○

  Set the service account in the Identity and API access section when provisioning the compute engine VM.

  (Correct)

- ○

  Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Add a metadata tag to the compute instance with key: service-account and value: <contents of JSON key file>.

- ○

  Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Add a metadata tag on the GCP project with key: service-account and value: <contents of JSON key file>.

- ○

  Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Copy the contents of JSON key to ~/.identity/default-service-account.json overwrite the default service account.

Explanation

`Set the service account in the Identity and API access section when provisioning the compute engine VM.` **is the right answer.**

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

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

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

`Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Add a metadata tag on the GCP project with key: service-account and value: {contents of JSON key file}.` **is not right.**
While updating the service account for a compute instance can be done through the console, gcloud or the REST API, they don't do it based on the JSON Private Key.

`Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Add a metadata tag to the compute instance with key: service-account and value: {contents of JSON key file}.` **is not right.**
Setting the metadata tag does not force the compute engine instance to use the specific service account.

`Execute gcloud iam service-accounts keys create to generate a JSON key for the service account. Copy the contents of JSON key to ~/.identity/default-service-account.json overwrite the default service account.` **is not right.**
You can configure a VM to use a specific service account by providing the relevant JSON credentials file, but the procedure is different. Copying the JSON file to a specific path alone is not sufficient. Moreover, the path mentioned is wrong. See below for a use case where a VM which is unable to list cloud storage buckets is updated to use a service account, and it can then list the buckets. Before using a specific service account, execute gsutil ls to list buckets, and it fails.

```
$ gsutil ls

ServiceException: 401 Anonymous caller does not have storage.buckets.list acce
ss to project 393066724129.
```

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

```
gcloud auth activate-service-account admin-service-account@gcloud-gcp-ace-2665
20.iam.gserviceaccount.com --key-file=~/compute-engine-service-account.json

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

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

```
/home/gcloud_gcp_ace_user/.config/gcloud/legacy_credentials/admin-service-acco
unt@gcloud-gcp-ace-266520.iam.gserviceaccount.com/adc.json
```

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

```
$ gsutil ls

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

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

Question 29:

Skipped

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

- ○

  Use a Cloud Function to rewrite the storage class to Coldline for objects older than 90 days. Use another Cloud Function to delete objects older than 365 days from Coldline Storage Class.

- ○

  Use a Cloud Function to rewrite the storage class to Coldline for objects older than 90 days. Use another Cloud Function to delete objects older than 275 days from Coldline Storage Class.

- ○

  Configure a lifecycle rule to transition objects older than 90 days to Coldline Storage Class. Configure another lifecycle rule to delete objects older than 365 days from Coldline Storage Class.

  (Correct)

- ○

  Configure a lifecycle rule to transition objects older than 90 days to Coldline Storage Class. Configure another lifecycle rule to delete objects older than 275 days from Coldline Storage Class.

Explanation

`Use a Cloud Function to rewrite the storage class to Coldline for objects older than 90 days. Use another Cloud Function to delete objects older than 365 days from Coldline Storage Class.` **is not right.**

gsutil rewrite is used to change the storage class of objects within a bucket through overwriting the object. Upon overwriting, the age on the objects is reset. Deleting them after 365 days would result in the original objects being deleted in 90+365 days.

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

`Use a Cloud Function to rewrite the storage class to Coldline for objects older than 90 days. Use another Cloud Function to delete objects older than 275 days from Coldline Storage Class.` **is not right.**

gsutil rewrite is used to change the storage class of objects within a bucket through

overwriting the object. Upon overwriting, the age on the objects is reset. Deleting them after 275 days would result in the original objects being deleted in 90+275 days. Although this is the expected outcome, you should avoid doing this as the Cloud Storage lifecycle management rules provide a better way to achieve this without relying on other GCP services.
Ref: https://cloud.google.com/storage/docs/changing-storage-classes

`Configure a lifecycle rule to transition objects older than 90 days to Coldline Storage Class. Configure another lifecycle rule to delete objects older than 275 days from Coldline Storage Class.` **is not right.**
Object Lifecycle Management does not rewrite an object when changing its storage class. When an object is transitioned to Nearline Storage, Coldline Storage, or Archive Storage using the SetStorageClass feature, any subsequent early deletion and associated charges are based on the original creation time of the object, regardless of when the storage class changed.

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

`Configure a lifecycle rule to transition objects older than 90 days to Coldline Storage Class. Configure another lifecycle rule to delete objects older than 365 days from Coldline Storage Class.` **is the right answer.**
Object Lifecycle Management does not rewrite an object when changing its storage class. When an object is transitioned to Nearline Storage, Coldline Storage, or Archive Storage using the SetStorageClass feature, any subsequent early deletion and associated charges are based on the original creation time of the object, regardless of when the storage class changed.
Ref: https://cloud.google.com/storage/docs/lifecycle

Question 30:

Skipped

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

- ○

  Deploy the application on a Managed Instance Group (MIG) that disables the creation retry mode by setting the --nocreation-retries flag.

- ○

Create an instance template with availability policy that turns off the automatic restart behaviour and sets on-host maintenance to terminate instances during maintenance events. Deploy the application on a Managed Instance Group (MIG) based on this template.

- ○

Deploy the application on a Managed Instance Group (MIG) with autohealing health check set to healthy (HTTP).

- ○

Create an instance template with availability policy that turns on the automatic restart behaviour and sets on-host maintenance to live migrate instances during maintenance events. Deploy the application on a Managed Instance Group (MIG) based on this template.

(Correct)

Explanation
Requirements

12 instances - indicates we need to look for MIG (Managed Instances Group) where we can configure healing/scaling settings.

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

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

`Create an instance template with availability policy that turns off the automatic restart behaviour and sets on-host maintenance to terminate instances during maintenance events. Deploy the application on a Managed Instance Group (MIG) based on this template.` **is not right.**
If Automatic Restart is off, then the compute engine instances are not automatically restarted and results in loss of capacity. If GCP decides to start system maintenance on all instances at the same time, all instances are down, and this does not meet our requirement "Highly available during system maintenance" so this option is not right.

`Deploy the application on a Managed Instance Group (MIG) with autohealing health check set to healthy (HTTP).` **is not right.**
While auto-healing helps with the recreation of VM instances when needed, it doesn't Live-migrate the instances so our requirement of "highly available including during system maintenance" is not met. More info about Autohealing - Auto-healing allows the recreation of VM instances when needed. You can use a health check to recreate

a VM instance if the health check finds it unresponsive. If you don't select a health check, Compute Engine will recreate VM instances only when they're not running.
Ref: https://cloud.google.com/compute/docs/instance-groups/?hl=en_GB#managed_instance_groups_and_autohealing

`Deploy the application on a Managed Instance Group (MIG) that disables the creation retry mode by setting the --nocreation-retries flag.` **is not right.**
Like above - this option doesn't Live-migrate the instances so our requirement of "highly available including during system maintenance" is not met.

`Create an instance template with availability policy that turns on the automatic restart behaviour and sets on-host maintenance to live migrate instances during maintenance events. Deploy the application on a Managed Instance Group (MIG) based on this template.` **is the right option.**
Enabling automatic restart ensures that compute engine instances are automatically restarted when they crash. And Enabling "Migrate VM Instance" enables live migrates, i.e. compute instances are migrated during system maintenance and remain running during the migration. Automatic Restart - If your instance is set to terminate when there is a maintenance event, or if your instance crashes because of an underlying hardware issue, you can set up Compute Engine to automatically restart the instance by setting the automaticRestart field to true. This setting does not apply if the instance is taken offline through a user action, such as calling sudo shutdown, or during a zone outage.
Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#autorestart
Enabling the Migrate VM Instance option migrates your instance away from an infrastructure maintenance event, and your instance remains running during the migration. Your instance might experience a short period of decreased performance, although generally, most instances should not notice any difference. Live migration is ideal for instances that require constant uptime and can tolerate a short period of decreased performance.
Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options#live_migrate

Question 31:

Skipped

You are working for a cryptocurrency startup, and you have enabled a link to the company’s Initial Coin Offering (ICO) whitepaper on the company website – which runs off Google Cloud Storage. Your CTO clicked on this link and got prompted to save the file to their desktop. The CTO thinks this is a poor user experience and has asked you to identify if it is possible to render the file directly in the browser for all users. What should you do?

- ○

Modify the bucket ACLs to make all PDF files public.

- ○

  Add a metadata tag on all the PDF file objects with key: Content-Type and value: application/pdf.

  (Correct)

- ○

  Use Cloud CDN to front the static bucket and set the HTTP header displayInBrowser to 1.

- ○

  Add a label on the Cloud Storage bucket with key: Content-Type and value: application/pdf.

Explanation

`Use Cloud CDN to front the static bucket and set the HTTP header displayInBrowser to 1.` **is not right.**
CDN helps with caching content at the edge but doesn't help the browser in displaying pdf files.

`Modify the bucket ACLs to make all PDF files public.` **is not right.**
The fact that the browser lets users download the file suggests the browser can reach out and download the file. Sharing the PDF files publicly wouldn't make any difference.

`Add a label on the Cloud Storage bucket with key: Content-Type and value: application/pdf.` **is not right.**
Bucket labels are key: value metadata pairs that allow you to group your buckets along with other Google Cloud resources such as virtual machine instances and persistent disks. They don't determine the file's content type.

`Add a metadata tag on all the PDF file objects with key: Content-Type and value: application/pdf.` **is the right answer.**
Content-Type allows browsers to render the object correctly. If the browser prompts users to save files to their machine, it means the browser does not see the Content-Type as application/pdf. Setting this would ensure the browser displays PDF files within the browser instead of popping up a download dialogue.
Ref: https://cloud.google.com/storage/docs/gsutil/addlhelp/WorkingWithObjectMetadata#content-type_1

Question 32:

Skipped

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

- ○

  Switch to BigQuery flat-rate pricing. Coordinate with the analyst to run the query while on flat-rate pricing and switch back to on-demand pricing.

- ○

  Run the query using bq with the --dry_run flag to estimate the number of bytes returned by the query. Make use of the pricing calculator to estimate the query cost.

- ○

  Execute the query using bq to estimate the number of rows returned by the query. Make use of the pricing calculator to estimate the query cost.

- ○

  Run the query using bq with the --dry_run flag to estimate the number of bytes read by the query. Make use of the pricing calculator to estimate the query cost.

  (Correct)

Explanation

`Switch to BigQuery flat-rate pricing. Coordinate with the analyst to run the query while on flat-rate pricing and switch back to on-demand pricing.` **is not right.**

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

`Run the query using bq with the --dry_run flag to estimate the number of bytes returned by the query. Make use of the pricing calculator to estimate the query cost.` **is not right.**

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

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

`Execute the query using bq to estimate the number of rows returned by the query. Make use of the pricing calculator to estimate the query cost.` **is not right.**

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

`Run the query using bq with the --dry_run flag to estimate the number of bytes read by the query. Make use of the pricing calculator to estimate the query cost.` **is the right answer.**

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

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

Question 33:

Skipped

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

- ○

  Increase the transfer speed by decreasing the TCP window size.

- ○

  Use parallel composite uploads to speed up the transfer.

  (Correct)

- ○

  Restart the transfer from GCP console.

- ○

  Upload the file Multi-Regional instead and move the file to Nearline Storage Class.

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

`Restart the transfer from GCP console.` **is not right.**
GCP Console does not offer any specific features that help in improving the upload speed.

`Increase the transfer speed by decreasing the TCP window size.` **is not right.**
By decreasing the TCP window size, you are reducing the chunks of data sent in the TCP window, and this has the effect of underutilizing your bandwidth and can slow down the upload.

`Upload the file Multi-Regional instead and move the file to Nearline Storage Class.` **is not right.**
Multi-Regional is not a storage class. It is a bucket location. You can transition between storage classes, but that does not improve the upload speed.
Ref: https://cloud.google.com/storage/docs/locations
Ref: https://cloud.google.com/storage/docs/storage-classes

`Use parallel composite uploads to speed up the transfer.` **is the right answer.**
With cloud storage, Object composition can be used for uploading an object in parallel: you can divide your data into multiple chunks, upload each chunk to a distinct object in parallel, compose your final object, and delete any temporary source objects. This option helps maximize your bandwidth usage and ensures the file is uploaded as fast as possible.
Ref: https://cloud.google.com/storage/docs/composite-objects#uploads

Question 34:
Skipped
You are migrating a Python application from your on-premises data centre to Google Cloud. You want to deploy the application Google App Engine, and you modified the python application to use Cloud Pub/Sub instead of RabbitMQ. The

application uses a specific service account which has the necessary permissions to publish and subscribe on Cloud Pub/Sub; however, the operations team have not enabled the Cloud Pub/Sub API yet. What should you do?

- ○

  Use deployment manager to configure the App Engine Application to use the specific Service Account with the necessary IAM permissions and rely on the automatic enablement of the Cloud Pub/Sub API on the first request to publish or subscribe.

- ○

  Navigate to the APIs & Services section in GCP console and enable Cloud Pub/Sub API.

  (Correct)

- ○

  Grant roles/pubsub.admin IAM role to the service account and modify the application code to enable the API before publishing or subscribing.

- ○

  Configure the App Engine Application in GCP Console to use the specific Service Account with the necessary IAM permissions and rely on the automatic enablement of the Cloud Pub/Sub API on the first request to publish or subscribe.

Explanation
Requirements

We need to enable Cloud Pub/Sub API

Get our application to use the service account.

`Grant roles/pubsub.admin IAM role to the service account and modify the application code to enable the API before publishing or subscribing.` **is not right.**
APIs are not automatically enabled on the first connection to the service (Cloud Pub/Sub in this scenario). APIs can be enabled through Google Cloud Console, gcloud command-line and REST API.
Ref: https://cloud.google.com/service-usage/docs/enable-disable

`Configure the App Engine Application in GCP Console to use the specific Service Account with the necessary IAM permissions and rely on the `automatic enablement of the Cloud Pub/Sub API on the first request to publish or subscribe.` **is not right.**

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

`Use deployment manager to configure the App Engine Application to use the specific Service Account with the necessary IAM permissions and rely on the automatic enablement of the Cloud Pub/Sub API on the first request to publish or subscribe.` **is not right.**

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

`Navigate to the APIs & Services section in GCP console and enable Cloud Pub/Sub API.` **is the right answer.**

For most operational use cases, the simplest way to enable and disable services is to use the Google Cloud Console. You can create scripts; you can also use the gcloud command-line interface. If you need to program against the Service Usage API, we recommend that you use one of our provided client libraries.
Ref: https://cloud.google.com/service-usage/docs/enable-disable
Secondly, after you create an App Engine application, the App Engine default service account is created and used as the identity of the App Engine service. The App Engine default service account is associated with your Cloud project and executes tasks on behalf of your apps running in App Engine. By default, the App Engine default service account has the Editor role in the project, so this already has the permissions to push/pull/receive messages from Cloud Pub/Sub.

Question 35:

Skipped

You are developing a mobile game that uses Cloud Datastore for gaming leaderboards and player profiles. You want to test an aspect of this solution locally on your Ubuntu workstation which already has Cloud SDK installed. What should you do?

- ○

  Add a new index to Cloud Datastore instance in the development project by running gcloud datastore indexes create and modify your application on your workstation to retrieve the data from Cloud Datastore using the index.

- ○

Install Datastore emulator to provide local emulation of the production datastore environment in your local workstation by running gcloud components install.

(Correct)

- ○

  Install Datastore emulator to provide local emulation of the production datastore environment in your local workstation by running apt get install.

- ○

  Initiate an export of Cloud Datastore instance from development GCP project by executing gcloud datastore export. Modify your applications to point to the export.

Explanation
Requirements - test your application locally.

`Initiate an export of Cloud Datastore instance from development GCP project by executing gcloud datastore export. Modify your applications to point to the export.` **is not right.**
By all means, you can export a copy of all or a subset of entities from Google Cloud Datastore to another storage system such as Google Cloud Storage. But, the application is configured to connect to a Cloud Datastore instance, not another system that stores a raw dump of exported data. So this option is not right.

`Add a new index to Cloud Datastore instance in the development project by running gcloud datastore indexes create and modify your application on your workstation to retrieve the data from Cloud Datastore using the index.` **is not right.**
You could create an index, but this doesn't help your application emulate connections to Cloud Datastore on your laptop. So this option is not right.

`Install Datastore emulator to provide local emulation of the production datastore environment in your local workstation by running apt get install.` **is not right.**
Datastore emulator is a gcloud component, and you can't install gcloud components using apt get. So this option is not right.

`Install Datastore emulator to provide local emulation of the production datastore environment in your local workstation by running gcloud components install.` **is the right answer.**

The Datastore emulator provides local emulation of the production Datastore environment. You can use the emulator to develop and test your application locally.
Ref: https://cloud.google.com/datastore/docs/tools/datastore-emulator

Question 36:
Skipped
You deployed a java application in a single Google Cloud Compute Engine VM. During peak usage, the application CPU is maxed out and results in stuck threads which ultimately make the system unresponsive, and requires a reboot. Your operations team want to receive an email alert when the CPU utilization is greater than 95% for more than 10 minutes so they can manually change the instance type to another instance that offers more CPU. What should you do?

- ○

  In Cloud Logging, create logs based metric for CPU usage and store it as a custom metric in Cloud Monitoring. Create an Alerting policy based on CPU utilization in Cloud Monitoring and trigger an email notification when the utilization exceeds the threshold.

- ○

  Link the GCP project to a Cloud Monitoring workspace. Configure an Alerting policy based on CPU utilization in Cloud Monitoring and trigger an email notification when the utilization exceeds the threshold.

  (Correct)

- ○

  Write a custom script to monitor CPU usage and send an email notification when the usage exceeds the threshold.

- ○

  Link the project to a Cloud Monitoring workspace. Write a custom script that captures CPU utilization every minute and sends to Cloud Monitoring as a custom metric. Add an uptime check based on the CPU utilization.

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

Cloud logging does not log CPU usage. (Cloud monitoring does that) So that rules out the other option.
Ref: https://cloud.google.com/logging/

`Link the GCP project to a Cloud Monitoring workspace. Configure an Alerting policy based on CPU utilization in Cloud Monitoring and trigger an email notification when the utilization exceeds the threshold.` **is the right answer.**

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

Cloud monitoring captures the CPU usage. By default, the Monitoring agent collects disk, CPU, network, and process metrics. You can also have the agent send custom metrics to Cloud monitoring.
Ref: https://cloud.google.com/monitoring/

You can then set up an alerting policy to alert with CPU utilization exceeds 90% for 15 minutes.
Ref: https://cloud.google.com/monitoring/alerts/.

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

Cloud monitoring supports multiple notification options for triggering alerts; email is one of them.
Ref: https://cloud.google.com/monitoring/support/notification-options

Question 37:

Skipped

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

- ○

  Deploy the application to GKE cluster with Horizontal Pod Autoscaling (HPA) enabled based on CPU utilization.

- ○

  Deploy the application to Google Compute Engine Managed Instance Group (MIG) with autoscaling enabled based on CPU utilization.

(Correct)

- ○

  Deploy the application to Google Compute Engine Managed Instance Group (MIG) with time-based autoscaling based on last months' traffic patterns.

- ○

  Deploy the application to Google Compute Engine Managed Instance Group (MIG). Deploy a Cloud Function to look up CPU utilization in Cloud Monitoring every minute and scale up or scale down the MIG group as needed.

Explanation

Our requirements are

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

Scale Automatically

Scaling is automatic, efficient & quick

`Deploy the application to GKE cluster with Horizontal Pod Autoscaling (HPA) enabled based on CPU utilization.` **is not right.**

We want to use virtual machines directly. A "lift and shift" from the on-premise VMs to GKE cluster is not possible. Although GKE uses virtual machines under the hood for its cluster, the autoscaling is different. It uses scaling at VMs (cluster auto-scaling) as well as at pod level (horizontal and vertical pod autoscaling). In this option, although horizontal pod autoscaling is enabled, Cluster Autoscaling isn't, and this limits the ability to scale up.

`Deploy the application to Google Compute Engine Managed Instance Group (MIG) with time-based autoscaling based on last months' traffic patterns.` **is not right.**

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

`Deploy the application to Google Compute Engine Managed Instance Group (MIG). Deploy a Cloud Function to look up CPU utilization in Cloud Monitoring every minute and scale up or scale down the MIG group as needed.` **is not right.**

While this can be done, it is not the most efficient solution when the same can be achieved more efficiently using a MIG with autoscaling based on CPU utilization.

`Deploy the application to Google Compute Engine Managed Instance Group (MIG) with autoscaling enabled based on CPU utilization.` **is the right answer.** Managed instance groups offer autoscaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load (CPU Utilization in this case). Autoscaling helps your apps gracefully handle traffic increases and reduce costs when the need for resources is lower. You define the autoscaling policy, and the autoscaler performs automatic scaling based on the measured load (CPU Utilization in this case). Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).
Ref: https://cloud.google.com/compute/docs/autoscaler

Question 38:
Skipped
Your compliance department has asked you to share a compressed zip of sensitive audit logs with an external auditor. The external auditor does not have a Google account, and you want to remove the access after 4 hours. How can you do this securely with the least number of steps?

- ○

  Configure Static Website hosting on the Cloud Storage bucket, make the zip file public and ask the auditor to download the file from the website. Delete the zip file after 4 hours.

- ○

  Use gcloud to generate a signed URL on the object with a four-hour expiry. Securely share the URL with the external auditor.

  (Correct)

- ○

  Make the zip file public and securely share the URL with the external auditor. Set up a lifecycle policy to delete the object after 4 hours.

- ○

  Copy the zip file to a new Cloud Storage bucket, make the bucket public and share the URL securely with the external auditor. Delete the new bucket after 4 hours.

Explanation

`Make the zip file public and securely share the URL with the external auditor. Set up a lifecycle policy to delete the object after 4 hours.` **is not right.**

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

`Configure Static Website hosting on the Cloud Storage bucket, make the zip file public and ask the auditor to download the file from the website. Delete the zip file after 4 hours.` **is not right.**

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

`Copy the zip file to a new Cloud Storage bucket, make the bucket public and share the URL securely with the external auditor. Delete the new bucket after 4 hours.` **is not right.**

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

`Use gcloud to generate a signed URL on the object with a four-hour expiry. Securely share the URL with the external auditor.` **is the right answer.**

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

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

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

Question 39:

Skipped

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

- ○

Run a script to generate SSH key pairs for all developers. Send an email to each developer with their private key attached. Add public keys to project-wide public SSH keys in your GCP project and configure all VM instances in the project to allow project-wide SSH keys.

- ○

  Run a script to generate SSH key pairs for all developers. Send an email to each developer with their private key attached. Update all VM instances in the development to add all the public keys. Have the developers present their private key to SSH to the instances.

- ○

  Share a script with the developers and ask them to run it to generate a new SSH key pair. Have them email their pubic key to you and run a script to add all the public keys to all instances in the project.

- ○

  Share a script with the developers and ask them to run it to generate a new SSH key pair. Have the developers add their public key to their Google Account. Ask the security administrator to grant compute.osAdminLogin role to the developers' Google group.

  (Correct)

Explanation

`Run a script to generate SSH key pairs for all developers. Send an email to each developer with their private key attached. Update all VM instances in the development to add all the public keys. Have the developers present their private key to SSH to the instances.` **is not right.** Sending the private keys in an email is a bad practice. Updating all VM instances to add public keys is not operationally efficient as it needs to be carried out on a per-user per-VM basis. You also need to take into consideration new user onboarding and user de-provisioning scenarios which add to the operational overhead.

`Run a script to generate SSH key pairs for all developers. Send an email to each developer with their private key attached. Add public keys to project-wide public SSH keys in your GCP project and configure all VM instances in the project to allow project-wide SSH keys.` **is not right.** Sending the private keys in an email is a bad practice. Adding public keys is not operationally efficient as it needs to be carried out on a per-user. You also need to take into consideration new user onboarding and user de-provisioning scenarios which add to the operational overhead.

`Share a script with the developers and ask them to run it to generate a new SSH key pair. Have them email their pubic key to you and run a script to add all the public keys to all instances in the project.` **is not right.**
Sending the private keys in an email is a bad practice. Updating all VM instances to add public keys is not operationally efficient as it needs to be carried out on a per-user per-VM basis. You also need to take into consideration new user onboarding and user de-provisioning scenarios which add to the operational overhead.

`Share a script with the developers and ask them to run it to generate a new SSH key pair. Have the developers add their public key to their Google Account. Ask the security administrator to grant compute.osAdminLogin role to the developers' Google group.` **is the right answer.**
By letting users manage their SSH key pair (and it's rotation, etc.), you delete the operational burden of managing SSH keys to individual users. Secondly, granting compute.osAdminLogin role grants the group administrator permissions (as opposed to granting compute.osLogin, which does not grant administrator permissions). Finally, managing provisioning and de-provisioning is as simple as adding or removing the user from the group.

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

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

roles/compute.osAdminLogin, which grants administrator permissions

At any point, to revoke user access to instances that are enabled to use OS Login, remove the user roles from that user account
Ref: https://cloud.google.com/compute/docs/instances/managing-instance-access#enable_oslogin

Question 40:

Skipped

You want to migrate a public NodeJS application, which serves requests over HTTPS, from your on-premises data centre to Google Cloud Platform. You plan to host it on a fleet of instances behind Managed Instances Group (MIG) in Google Compute Engine. You need to configure a GCP load balancer to terminate SSL session before passing traffic to the VMs. Which GCP Load balancer should you use?

- ○

  Use HTTP(S) load balancer.

  (Correct)

- ○

  Use External TCP proxy load balancer.

- ○

  Use Internal TCP load balancer.

- ○

  Use External SSL proxy load balancer.

Explanation

`Use Internal TCP load balancer.` **is not right.**
Internal TCP Load Balancing is a regional load balancer that enables you to run and scale your services behind an internal load balancing IP address that is accessible only to your internal virtual machine (VM) instances. Since we need to serve public traffic, this load balancer is not suitable for us.
Ref: https://cloud.google.com/load-balancing/docs/internal

`Use External SSL proxy load balancer.` **is not right.**
Google says "SSL Proxy Load Balancing is intended for non-HTTP(S) traffic. For HTTP(S) traffic, we recommend that you use HTTP(S) Load Balancing." So this option can be ruled out.
Ref: https://cloud.google.com/load-balancing/docs/ssl

`Use External TCP proxy load balancer.` **is not right.**
Google says "TCP Proxy Load Balancing is intended for non-HTTP traffic. For HTTP traffic, use HTTP Load Balancing instead. For proxied SSL traffic, use SSL Proxy Load Balancing." So this option can be ruled out.
Ref: https://cloud.google.com/load-balancing/docs/tcp

`Use HTTP(S) load balancer.` **is the right answer.**
This option fits all requirements. It can serve public traffic, can terminate SSL at the load balancer and follows google recommended practices.

"The backends of a backend service can be either instance groups or network endpoint groups (NEGs), but not a combination of both."

"An external HTTP(S) load balancer distributes traffic from the internet."

"The client SSL session terminates at the load balancer."

"For HTTP traffic, use HTTP Load Balancing instead."

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

Question 41:

Skipped

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

- ○

  Create a new GCP project for the performance testing environment using gcloud and copy the application from the development GCP project into the performance testing GCP project.

- ○

  Create a new GCP project for the performance testing environment using gcloud and deploy your App Engine application to the new GCP project.

  (Correct)

- ○

  Use gcloud to deploy the application to a new performance testing GCP project by specifying the --project parameter. Select Yes when prompted for confirmation on creating a new project.

- ○

  Configure a Deployment Manager YAML template to copy the application from the development GCP project into the performance testing GCP project.

Explanation

`Create a new GCP project for the performance testing environment using gcloud and copy the application from the development GCP project into the performance testing GCP project.` **is not right.**

You can use gcloud to create a new project, but you can not copy a deployed application from one project to another. Google App Engine doesn't offer this feature.

`Configure a Deployment Manager YAML template to copy the application from the development GCP project into the performance testing GCP project.` **is**

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

`Use gcloud to deploy the application to a new performance testing GCP project by specifying the --project parameter. Select Yes when prompted for confirmation on creating a new project.` **is not right.**
You can deploy using gcloud app deploy and target it to a different project using --project flag. However, you can only deploy to an existing project as the gcloud app deploy command is unable to create a new project if it doesn't already exist.

`Create a new GCP project for the performance testing environment using gcloud and deploy your App Engine application to the new GCP project.` **is the right answer.**
You can deploy to a different project by using --project flag. By default, the service is deployed the current project configured via:

```
$ gcloud config set core/project PROJECT
```

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

```
$ gcloud app deploy ~/my_app/app.yaml --project=PROJECT
```

Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy
Question 42:
Skipped
An application that you are migrating to Google Cloud relies on overnight batch jobs that take between 2 to 3 hours to complete. You want to do this at a minimal cost. Where should you run these batch jobs?

- ○

  Run the batch jobs in a GKE cluster on a node pool with four instances of type f1-micro.

- ○

  Run the batch jobs in a GKE cluster on a node pool with a single instance of type e2-small.

- ○

  Run the batch jobs in a non-preemptible shared core compute engine instance that supports short periods of bursting.

- ○

Run the batch jobs in a preemptible compute engine instance of appropriate machine type.

(Correct)

Explanation
Requirements - achieve end goal while minimizing service costs.

`Run the batch jobs in a GKE cluster on a node pool with a single instance of type e2-small.` **is not right.**
We do not know if a small instance is capable of handling all the batch volume. Plus this is not the most cost-effective of the options.

`Run the batch jobs in a GKE cluster on a node pool with four instances of type f1-micro.` **is not right.**
We do not know if four micro instances are capable of handling all the batch volume. Plus this is not the most cost-effective of the options.

`Run the batch jobs in a non-preemptible shared core compute engine instance that supports short periods of bursting.` **is not right.**
We can use an instance that supports micro bursting, but we have a job that runs for 2 hours. Bursting is suitable for short periods.

`Run the batch jobs in a preemptible compute engine instance of appropriate machine type.` **is the right answer.**
We minimize the cost by selecting a preemptible instance of the appropriate type. If the preemptible instance is terminated, the next nightly run picks up the unprocessed volume.

Question 43:

Skipped

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

- ○

  In the App Engine Console, identify the App Engine application versions and make the previous version the default to route all traffic to it.

  (Correct)

- ○

In the App Engine Console, identify the App Engine application and select Revert.

- ○

  Deploy the previous version as a new App Engine Application and use traffic splitting feature to send all traffic to the new application.

- ○

  Execute gcloud app restore to rollback to the previous version.

Explanation

`Execute gcloud app restore to rollback to the previous version.` **is not right.**
restore action is not supported by gcloud app command.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy

`In the App Engine Console, identify the App Engine application and select Revert.` **is not right.**
Revert option is not present on the App Engine page of the GCP Console.

`Deploy the previous version as a new App Engine Application and use traffic splitting feature to send all traffic to the new application.` **is not right.**
Each application in the app engine is different, and it is not possible to split traffic between applications in App Engine. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service but not across applications.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

`In the App Engine Console, identify the App Engine application versions and make the previous version the default to route all traffic to it.` **is the right answer**
You can roll back to a previous version in the app engine GCP console. Go back to the list of versions and check the box next to the version that you want to receive all traffic and click the MAKE DEFAULT button located above the list. Traffic immediately switches over to the selected version.
Ref: https://cloud.google.com/community/tutorials/how-to-roll-your-app-engine-managed-vms-app-back-to-a-previous-version-part-1

Question 44:

Skipped

Your company has three GCP projects – for development, test and production environments. The budgeting team in the finance department needs to know the cost estimates for the next financial year to include it in the budget. They have years of experience using SQL and need to group costs by parameters such as

duration (day/week/month/quarter), service type, region, etc. How can you enable this?

- ○

  Export billing data to a BigQuery dataset. Ask the budgeting team to run queries against BigQuery to analyze current costs and estimate future costs.

  (Correct)

- ○

  Export billing data to Google Cloud Storage bucket. Trigger a Cloud Function that reads the data and inserts into Cloud BigTable. Ask the budgeting team to run queries against BigTable to analyze current costs and estimate future costs.

- ○

  Export billing data to Google Cloud Storage bucket. Manually copy the data from Cloud Storage bucket to a Google sheet. Ask the budgeting team to apply formulas in the Google sheet to analyze current costs and estimate future costs.

- ○

  Download the costs as CSV file from the Cloud Table page. Ask the budgeting team to open this file Microsoft Excel and apply formulas to analyze current costs and estimate future costs.

Explanation

Requirements

use query syntax

need the billing data of all three projects

`Export billing data to a Google Cloud Storage bucket. Trigger a Cloud Function that reads the data and inserts into Cloud BigTable. Ask the budgeting team to run queries against BigTable to analyze current costs and estimate future costs.` **is not right.**
BigTable is a NoSQL database and doesn't offer query syntax support.

`Export billing data to a Google Cloud Storage bucket. Manually copy the data from Cloud Storage bucket to a Google sheet. Ask the budgeting team to apply formulas in the Google sheet to analyze current costs and`

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

`Download the costs as CSV file from the Cost Table page. Ask the budgeting team to open this file Microsoft Excel and apply formulas to analyze current costs and estimate future costs.` **is not right.**
Billing data can't be exported to a local file; it can only be exported to a BigQuery Dataset or Cloud Storage bucket.

`Export billing data to a BigQuery dataset. Ask the budgeting team to run queries against BigQuery to analyze current costs and estimate future costs.` **is the right answer.**
You can export billing information from multiple projects into a BigQuery dataset. Unlike the export to Cloud Storage bucket, export to BigQuery dataset includes all information making it easy and straightforward to construct queries in BigQuery to estimate the cost. BigQuery supports Standard SQL so you can join tables and group by fields (labels in this case) as needed.
Ref: https://cloud.google.com/billing/docs/how-to/export-data-bigquery.

Question 45:

Skipped

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

- ○

  Update the Managed Instances template to set the maximum instances to 5.

- ○

  Update the autoscaling health check to increase the initial delay to 200 seconds.

  (Correct)

- ○

  Update the autoscaling health check from HTTP to TCP.

- ○

  Update the Managed Instances template to set the maximum instances to 1.

Explanation
Scenario

- Autoscaling is enabled and kicks off the scale-up

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

- The initial delay is 30 seconds.

- VM startup time is 3 minutes.

- Auto-scaling creates more instances than necessary.

`Update the Managed Instances template to set the maximum instances to 1.` **is not right.**
Setting the maximum number of instances to 1 effectively limits the scale up to 1 instance, which is undesirable as in this case, we may still be struggling with the CPU usage and can't scale up. Therefore this is not the right answer.

`Update the Managed Instances template to set the maximum instances to 5.` **is not right.**
Setting the maximum number of instances to 5 effectively limits the scale up to 5 instances. In this scenario, we may still be struggling with CPU usage and can't scale up. Therefore this is not the right answer.

`Update the autoscaling health check from HTTP to TCP.` **is not right.**
A TCP health check is a legacy health check, whereas HTTP health check is more advanced and "non-legacy". A TCP health check might say the application is UP when it is not as it only listens on application servers TCP port and doesn't validate the application health through HTTP check on its health endpoint. This configuration results in the load balancer sending requests to the application server when it is still loading the application resulting in failures.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/health-checks/create/tcp
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/health-checks/create/http

`Update the autoscaling health check to increase the initial delay to 200 seconds.` **is the right answer.**

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

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

"Initial Delay Seconds" - This setting delays autohealing from potentially prematurely recreating the instance if the instance is in the process of starting up. The initial delay timer starts when the currentAction of the instance is VERIFYING.
Ref: https://cloud.google.com/compute/docs/instance-groups/autohealing-instances-in-migs

Question 46:

Skipped

Your company stores sensitive user information (PII) in three multi-regional buckets in US, Europe and Asia. All three buckets have data access logging enabled on them. The compliance team has received reports of fraudulent activity and has begun investigating a customer care representative. It believes the specific individual may have accessed some objects they are not authorized to and may have added labels to some files in the buckets to enable favourable discounts for their friends. The compliance team has asked you to provide them with a report of activities for this customer service representative on all three buckets. How can you do this efficiently?

- ○

  Apply the necessary filters in Cloud Logging Console to retrieve this information.

  (Correct)

- ○

  Retrieve this information from Activity logs in GCP Console.

- ○

Retrieve this information from the Cloud Storage bucket page in GCP Console.

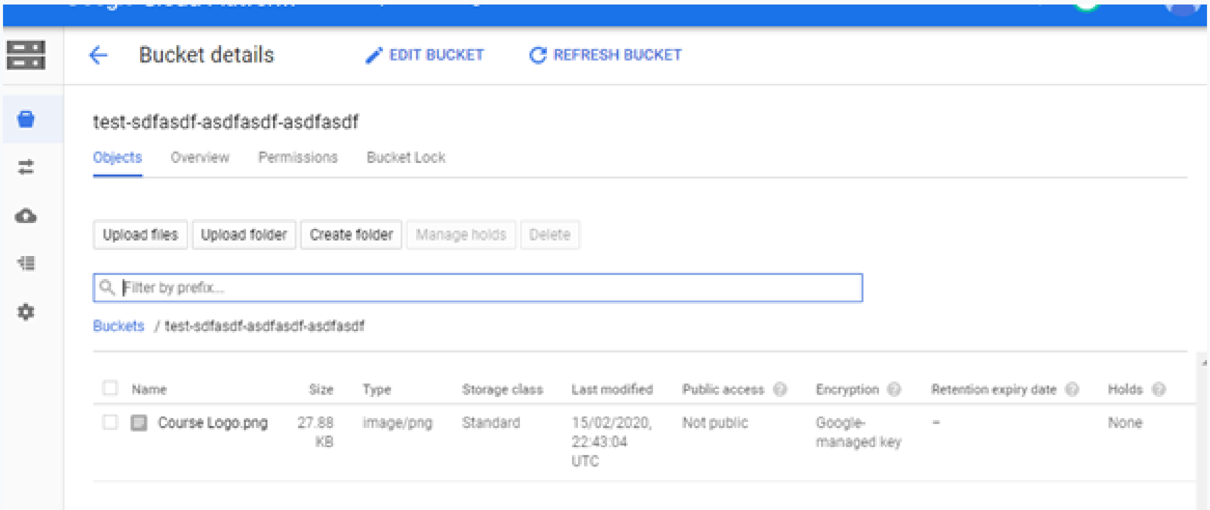
- ○

Enable a Cloud Trace on the bucket and wait for the user to access objects/set metadata to capture their activities.

Explanation
Our requirements are - sensitive data, verify access, fewest possible steps.

`Retrieve this information from Activity logs in GCP Console.` **is not right.**
Since data access logging is enabled, you can see relevant log entries in both activity Logs as well as stack driver logs. However, verifying what has been viewed/updated is not straightforward in activity logs. Activity logs display a list of all actions, and you can restrict this down to a user and further filter by specifying Data access as the Activity types and GCS Bucket as the Resource type. But that is the extent of the filter functionality in Activity logs. It is not possible to restrict the activity logs to just the three interested buckets. Secondly, it is not possible to restrict the activity logs to just the gets and updates. So we'd have to go through the full list to identify activities of interest before verifying them which is a manual process and can be time taking depending on the number of activities in the list.
Ref: https://cloud.google.com/storage/docs/audit-logs

`Retrieve this information from the Cloud Storage bucket page in GCP Console.` **is not right.**
The bucket page in the GCP console does not show the logs.



test-sdfasdf-asdfasdf-asdfasdf

Buckets / test-sdfasdf-asdfasdf-asdfasdf

Name	Size	Type	Storage class	Last modified	Public access	Encryption	Retention expiry date	Holds
Course Logo.png	27.88 KB	image/png	Standard	15/02/2020, 22:43:04 UTC	Not public	Google-managed key	-	None

`Enable a Cloud Trace on the bucket and wait for the user to access objects/set metadata to capture their activities.` **is not right.**
Cloud Trace is not supported on Google Cloud Storage. Stackdriver Trace runs on

Linux in the following environments: Compute Engine, Google Kubernetes Engine (GKE), App Engine flexible environment, App Engine standard environment.
Ref: https://cloud.google.com/trace/docs/overview

`Apply the necessary filters in Cloud Logging Console to retrieve this information.` **is the right answer.**

Data access logs are already enabled, so we already record all API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. Data Access audit logs do not record the data-access operations on resources that are publicly shared (available to All Users or All Authenticated Users), or that can be accessed without logging into Google Cloud.

Since we are dealing with sensitive data, it is safe to assume that these buckets are not publicly shared and therefore enabling Data access logging logs all data-access operations on resources. These logs are sent to Stackdriver where they can be viewed by applying a suitable filter.

Unlike activity logs, retrieving the required information to verify is quicker through Stackdriver as you can apply filters such as

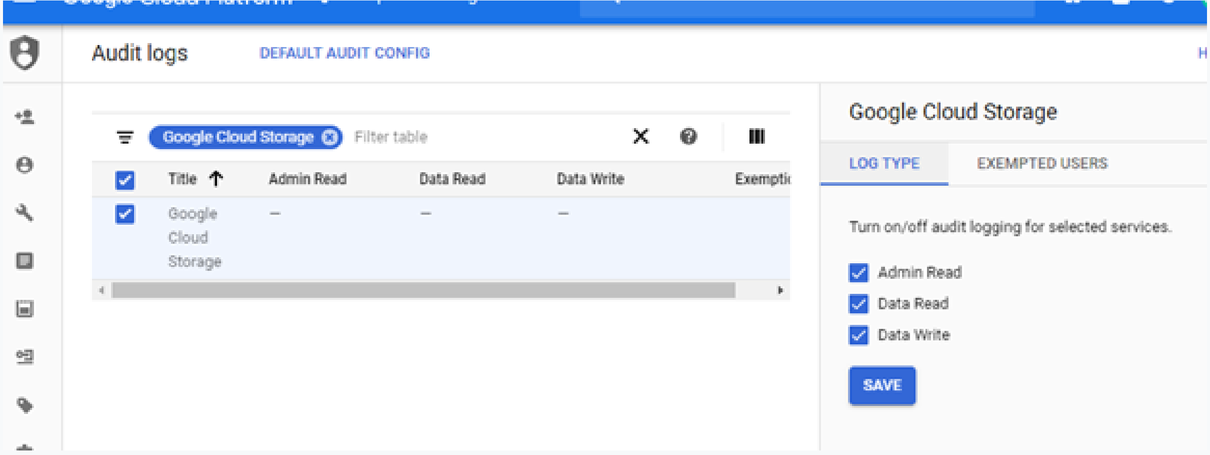
```
resource.type="gcs_bucket"

(resource.labels.bucket_name="gcp-ace-lab-255520" OR resource.labels.bucket_name="gcp-ace-lab-255521" OR resource.labels.bucket_name="gcp-ace-lab-255522")

(protoPayload.methodName="storage.objects.get" OR protoPayload.methodName="storage.objects.update")

protoPayload.authenticationInfo.principalEmail="test.gcp.labs.user@gmail.com"
```

and query just the gets and updates, for specific buckets for a specific user. This option involves fewer steps and is more efficient. Data access logging is not enabled by default and needs to be enabled explicitly. The screenshot below shows a screenshot for enabling the data access logging for Google Cloud Storage.



☑	Title ↑	Admin Read	Data Read	Data Write	Exempti
☑	Google Cloud Storage	–	–	–	

Google Cloud Storage

Turn on/off audit logging for selected services.

☑ Admin Read
☑ Data Read
☑ Data Write

Question 47:

Skipped

You deployed a Java application in a Google Compute Engine VM that has 3.75 GB Memory and 1 vCPU. At peak usage, the application experiences java.lang.OutOfMemory errors that take down the application entirely and requires a restart. The CPU usage at all times is minimal. Your operations team have asked you to increase the memory on the VM instance to 8 GB. You want to do this while minimizing the cost. What should you do?

- ○

  Make use of the live-migration feature of Google Compute Engine to migrate the application to another instance with more memory.

- ○

  Add a metadata tag to the instance with key: new-memory-size and value: 8GB.

- ○

  Stop the compute engine instance, update the memory on the instance to 8 GB and start the compute engine instance.

  (Correct)

- ○

  Stop the compute engine instance, update the machine to n1-standard-2 and start the compute engine instance.

Explanation

`Make use of the live-migration feature of Google Compute Engine to migrate the application to another instance with more memory.` **is not right.**
Live migration migrates your running instances to another host in the same zone so that Google can perform maintenance such as a software or hardware update. It can not be used for changing machine type.
Ref: https://cloud.google.com/compute/docs/instances/live-migration

`Add a metadata tag to the instance with key: new-memory-size and value: 8GB.` **is not right.**
There is no such setting as new-memory-size.

`Stop the compute engine instance, update the machine to n1-standard-2 and start the compute engine instance.` **is not right.**
n1-standard-2 instance offers less than 8 GB (7.5 GB to be precise), so this falls short of the required memory.
Ref: https://cloud.google.com/compute/docs/machine-types

`Stop the compute engine instance, update the memory on the instance to 8 GB and start the compute engine instance.` **is the right answer.**
In Google compute engine, if predefined machine types don't meet your needs, you can create an instance with custom virtualized hardware settings. Specifically, you can create an instance with a custom number of vCPUs and custom memory, effectively using a custom machine type. Custom machine types are ideal for the following scenarios:

Workloads that aren't a good fit for the predefined machine types that are available to you.

Workloads that require more processing power or more memory but don't need all of the upgrades that are provided by the next machine type level.

In our scenario, we only need a memory upgrade. Moving to a bigger instance would also bump up the CPU which we don't need so we have to use a custom machine type. It is not possible to change memory while the instance is running, so you need to stop the instance first, change the memory and then start it again.
Ref: https://cloud.google.com/compute/docs/instances/creating-instance-with-custom-machine-type

Question 48:
Skipped
You have one GCP project with default region and zone set to us-east1 and us-east1-b respectively. You have another GCP project with default region and zone set to us-west1 and us-west1-a respectively. You want to provision a VM in each of these projects efficiently using gcloud CLI. What should you do?

- ○

  Execute gcloud config configuration create [config name] to create two configurations, one for each project. Execute gcloud configurations list to create and start the VMs.

- ○

  Execute gcloud configurations activate [config name] to activate the configuration for each project and execute gcloud configurations list to create and start the VM.

- ○

  Execute gcloud config configuration create [config name] to create two configurations, one for each project. Execute gcloud config configurations activate [config name] to activate the first configuration, and gcloud compute instances create to create the VM. Repeat the steps for other configuration.

(Correct)

- ○

Execute gcloud configurations activate [config name] to activate the configuration for each project and execute gcloud config list to create and start the VM.

Explanation

`Execute gcloud config configuration create [config name] to create two configurations, one for each project. Execute gcloud configurations list to create and start the VMs.` **is not right.**

gcloud configurations list is an invalid command. To list the existing named configurations, you need to execute gcloud config configurations list, but this does not start the compute engine instances.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list

`Execute gcloud config configurations activate [config name] to activate the configuration for each project and execute gcloud configurations list to create and start the VM.` **is not right.**

gcloud configurations list is an invalid command. To list the existing named configurations, you need to execute gcloud config configurations list, but this does not start the compute engine instances.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list

`Execute gcloud config configurations activate [config name] to activate the configuration for each project and execute gcloud config list to create and start the VM.` **is not right.**

gcloud configurations activate [NAME] activates an existing named configuration. It can't be used to activate two configurations at the same time. Moreover, gcloud config list lists Cloud SDK properties for the currently active configuration. It does not start the Compute Engine instances.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate
Ref: https://cloud.google.com/sdk/gcloud/reference/config/list

`Execute gcloud config configuration create [config name] to create two configurations, one for each project. Execute gcloud config configurations activate [config name] to activate the first configuration, and gcloud compute instances create to create the VM. Repeat the steps for other configuration.` **is the right answer.**

Each gcloud configuration has a 1 to 1 relationship with the region (if a region is defined). Since we have two different regions, we would need to create two separate

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

Secondly, you can activate each configuration independently by running gcloud config configurations activate [NAME]
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate

Finally, while each configuration is active, you can run the gcloud compute instances start [NAME] command to start the instance in the configuration's region.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/start

Question 49:

Skipped

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

- ○

  Use 0.0.0.0/0 CIDR range.

- ○

  Use 192.168.0.0/16 CIDR range.

- ○

  Use 172.16.0.0/12 CIDR range.

- ○

  Use 10.0.0.0/8 CIDR range.

  (Correct)

Explanation

`Use 10.0.0.0/8 CIDR range.` **is the right answer.**

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

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

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

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

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

Question 50:

Skipped

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

- ○

  Review the project settings in the Deployment Manager console.

- ○

  Review the properties of the active gcloud configurations by executing gcloud config list.

  (Correct)

- ○

  Review the project settings in the App Engine deployment YAML file.

- ○

  Review the project settings in the App Engine application configuration files.

Explanation

`Review the project settings in the App Engine deployment YAML file.` **is not right.**

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

`Review the project settings in the App Engine application configuration files.` **is not right.**

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

`Review the project settings in the Deployment Manager console.` **is not right.**

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

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

`Review the properties of the active gcloud configurations by executing gcloud config list.` **is the right answer.**

If the deployment was successful, but it did not deploy to the intended project, the application would have been deployed to a different project. In the same gcloud

shell, you can identify the current properties of the configuration by executing gcloud config list. The output returns config properties such as project, account, etc., as well as app-specific properties such as app/promote_by_default,
app/stop_previous_version.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/list

Question 1:

Skipped

To facilitate disaster recovery, your company wants to save database backup tar files in Cloud Storage bucket. You want to minimize the cost. Which GCP Cloud Storage class should you use?

- ○

  Use Coldline Storage Class.

  (Correct)

- ○

  Use Multi-Regional Storage Class.

- ○

  Use Nearline Storage Class.

- ○

  Use Regional Storage Class.

Explanation

The ideal answer to this would have been **Archive Storage**, but that is not one of the options. **Archive Storage** is the lowest-cost, highly durable storage service for data archiving, online backup, and disaster recovery. Your data is available within milliseconds, not hours or days. https://cloud.google.com/storage/docs/storage-classes#archive

In the absence of **Archive Storage** Class, `Use Coldline Storage Class` **is the right answer.**

Coldline Storage Class is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline Storage is ideal for data you plan to read or modify at most once a quarter.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

Although Nearline, Regional and Multi-Regional can also be used to store the backups, they are expensive in comparison, and Google recommends we use Coldline for backups.
More information about Nearline: https://cloud.google.com/storage/docs/storage-classes#nearline
More information about

Standard/Regional: https://cloud.google.com/storage/docs/storage-classes#standard
More information about Standard/Multi-Regional: https://cloud.google.com/storage/docs/storage-classes#standard

Question 2:

Skipped

Your organization specializes in helping other companies detect if any pages on their website do not align to the specified standards. To do this, your company has deployed a custom C++ application in your on-premises data centre that crawls all the web pages of a customer's website, compares the headers and template to the expected standard and stores the result before moving on to another customer's website. This testing takes a lot of time and has resulted in it missing out on the SLA several times recently. The application team is aware of the slow processing time and wants to run the application on multiple virtual machines to split the load, but there is no free space in the data centre. You have been asked to identify if it is possible to migrate this application to Google cloud, ensuring it can autoscale with minimal changes and reduce the processing time. What GCP service should you recommend?

- ○

  Deploy the application on Google App Engine Standard service.

- ○

  Deploy the application as Cloud Dataproc job based on Hadoop.

- ○

  Deploy the application on a GCE Managed Instance Group (MIG) with autoscaling enabled.

  (Correct)

- ○

  Deploy the application on a GCE Unmanaged Instance Group. Front the group with a network load balancer.

Explanation

`Deploy the application on a GCE Unmanaged Instance Group. Front the group with a network load balancer.` **is not right.**

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

amount of time it takes to test a change to the system thoroughly.
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

`Deploy the application on Google App Engine Standard service.` **is not right.**
App Engine supports many popular languages like Java, PHP, Node.js, Python, C#, .Net, Ruby, and Go. However, C++ isn't supported by App Engine.
Ref: https://cloud.google.com/appengine

`Deploy the application as Cloud Dataproc job based on Hadoop.` **is not right.**
Cloud Dataproc is a fast, easy-to-use, fully managed cloud service for running Apache Spark and Apache Hadoop clusters in a simpler, more cost-efficient way. While Dataproc is very efficient at processing ETL and Big Data pipelines, it is not as suitable for running a ruby application that runs tests each day.
Ref: https://cloud.google.com/dataproc

`Deploy the application on a GCE Managed Instance Group (MIG) with autoscaling enabled.` **is the right answer.**
A managed instance group (MIG) contains identical virtual machine (VM) instances that are based on an instance template. MIGs support auto-healing, load balancing, autoscaling, and auto-updating. Managed instance groups offer auto-scaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load. Autoscaling helps your apps gracefully handle traffic increases and reduce costs when the need for resources is lower. Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).
Ref: https://cloud.google.com/compute/docs/autoscaler/

Question 3:

Skipped

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

- ○

  Grant the finance team Billing Account User (roles/billing.user) role on the billing account and Project Billing Manager (roles/billing.projectManager) on the GCP organization.

  (Correct)

- ○

Grant the development team Billing Account User (roles/billing.user) role on the billing account.

- ○

Grant the finance team Billing Account User (roles/billing.user) role on the billing account.

- ○

Grant the development team Billing Account User (roles/billing.user) role on the billing account and Project Billing Manager (roles/billing.projectManager) on the GCP organization.

Explanation

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

`Grant the development team Billing Account User (roles/billing.user) role on the billing account.` **is not right.**
To link a project to a billing account, you need the necessary roles at the project level as well as at the billing account level. In this scenario, we are granting just the Billing Account User role on the billing account to the Engineering team which allows them to link projects to the billing account and our question clearly states we do not want to do that.

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

`Grant the finance team Billing Account User (roles/billing.user) role on the billing account and Project Billing Manager`

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

Question 4:
Skipped
Your company's auditors carry out an annual audit every year and have asked you to provide them with all the IAM policy changes in Google Cloud since the last audit. You want to streamline and expedite the analysis for audit. How should you share the information requested by auditors?

- ○

  Export all audit logs to BigQuery dataset. Make use of ACLs and views to restrict the data shared with the auditors. Have the auditors query the required information quickly.

  (Correct)

- ○

  Export all audit logs to Google Cloud Storage bucket and set up the necessary IAM acces to restrict the data shared with auditors.

- ○

  Configure alerts in Cloud Monitoring and trigger notifications to the auditors.

- ○

  Export all audit logs to Cloud Pub/Sub via an export sink. Use a Cloud Function to read the messages and store them in Cloud SQL. Make use of ACLs and views to restrict the data shared with the auditors.

Explanation
`Configure alerts in Cloud Monitoring and trigger notifications to the auditors.` **is not right.**
Stackdriver Alerting gives timely awareness to problems in your cloud applications so you can resolve the problems quickly. Sending alerts to your auditor is not of much use during audits.
Ref: https://cloud.google.com/monitoring/alerts

`Export all audit logs to Cloud Pub/Sub via an export sink. Use a Cloud Function to read the messages and store them in Cloud SQL. Make use of ACLs and views to restrict the data shared with the auditors.` **is not right.** Using Cloud Functions to transfer log entries to Google Cloud SQL is expensive in comparison to audit logs export feature which exports logs to various destinations with minimal configuration.
Ref: https://cloud.google.com/logging/docs/export/
Auditors spend a lot of time reviewing log messages. And you want to expedite the audit process!! So you want to make it easier for the auditor to extract the information easily from the logs.

Between the two remaining options, the **only difference** is the log **export sink destination**.
Ref: https://cloud.google.com/logging/docs/export/

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

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

Question 5:

Skipped

You recently deployed a new application in Google App Engine to serve production traffic. After analyzing logs for various user flows, you uncovered several issues in your application code and have developed a fix to address the issues. Parts of your proposed fix could not be validated in the pre production environment by your testing team as some of the scenarios can only be validated by an end user with access to specific data in your production environment. In the company's weekly Change Approval Board meeting, concerns were raised that the fix could possibly take down the application. It was unanimously agreed that while the fix is risky, it is a necessary change to the application. You have been asked to suggest a solution that minimizes the impact of the change going wrong. You also want to minimize costs. What should you do?

- ○

Create a second Google App Engine project with the new application code, and onboard users gradually to the new application.

- ○

  Set up a second Google App Engine service, and then update a subset of clients to hit the new service.

- ○

  Deploy a new version of the application, and use traffic splitting to send a small percentage of traffic to it.

  (Correct)

- ○

  A. Deploy the new application version temporarily, capture logs and then roll it back to the previous version.

Explanation

`Deploy the new application version temporarily, capture logs and then roll it back to the previous version.` **is not right.**
Deploying a new application version and promoting it would result in your new version serving all production traffic. If the code fix doesn't work as expected, it would result in the application becoming unreachable to all users. This is a risky approach and should be avoided.

`Create a second Google App Engine project with the new application code, and onboard users gradually to the new application.` **is not right.**
You want to minimize costs. This approach effectively doubles your costs as you have to pay for two identical environments until all users are moved over to the new application. There is an additional overhead of manually onboarding users to the new application which could be expensive as well as time-consuming.

`Set up a second Google App Engine service, and then update a subset of clients to hit the new service.` **is not right.**
It is not straightforward to update a set of clients to hit the new service. When users access an App Engine service, they use an endpoint like https://SERVICE_ID-dot-PROJECT_ID.REGION_ID.r.appspot.com. Introducing a new service introduces a new URL and getting your users to use the new URL is possible but involves effort and coordination. If you want to mask these differences to the end-user, then you have to make changes in the DNS and use a weighted algorithm to split the traffic between the two services based on the weights assigned.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic
Ref: https://cloud.google.com/appengine/docs/standard/python/an-overview-of-

app-engine
This approach also has the drawback of doubling your costs until all users are moved over to the new service.

`Deploy a new version of the application, and use traffic splitting to send a small percentage of traffic to it.` **is the right answer.**
This option minimizes the risk to the application while also minimizing the complexity and cost. When you deploy a new version to App Engine, you can choose not to promote it to serve live traffic. Instead, you could set up traffic splitting to split traffic between the two versions - this can all be done within Google App Engine. Once you send a small portion of traffic to the new version, you can analyze logs to identify if the fix has worked as expected. If the fix hasn't worked, you can update your traffic splitting configuration to send all traffic back to the old version. If you are happy your fix has worked, you can send more traffic to the new version or move all user traffic to the new version and delete the old version.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic
Ref: https://cloud.google.com/appengine/docs/standard/python/an-overview-of-app-engine

Question 6:
Skipped
Your Company is planning to migrate all Java web applications to Google App Engine. However, you still want to continue using your on-premise database. How can you setup the app engine to communicate with your on-premise database while minimizing effort?

- ○

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

- ○

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

- ○

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

- ○

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

  (Correct)

Explanation

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

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

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

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

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

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

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

You need Cloud VPN to connect VPC to an on-premise network.
Ref: https://cloud.google.com/vpn/docs/concepts/overview
Unlike App Engine Standard which is serverless, App Engine Flex instances are already within the VPC, so they can use Cloud VPN to connect to the on-premise network.

Question 7:

Skipped

You have been asked to create a new Kubernetes Cluster on Google Kubernetes Engine that can autoscale the number of worker nodes as well as pods. What should you do? (Select 2)

- □

  Enable Horizontal Pod Autoscaling for the kubernetes deployment.

  (Correct)

- □

  Configure a Compute Engine instance as a worker and add it to an unmanaged instance group. Add a load balancer to the instance group and rely on the load balancer to create additional Compute Engine instances when needed.

- □

  Create a GKE cluster and enable autoscaling on Kubernetes Engine.

  (Correct)

- □

  Create Compute Engine instances for the workers and the master and install Kubernetes. Rely on Kubernetes to create additional Compute Engine instances when needed.

- □

  Create a GKE cluster and enable autoscaling on the instance group of the cluster.

Explanation

`Create a GKE cluster and enable autoscaling on the instance group of the cluster.` **is not right.**
GKE's cluster auto-scaler automatically resizes the number of nodes in a given node pool, based on the demands of your workloads. However, we should not enable Compute Engine autoscaling for managed instance groups for the cluster nodes. GKE's cluster auto-scaler is separate from Compute Engine autoscaling.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler

`Configure a Compute Engine instance as a worker and add it to an unmanaged instance group. Add a load balancer to the instance group and rely on the load balancer to create additional Compute Engine instances when needed.` **is not right.**
When using GKE to manage your Kubernetes clusters, you can not add manually created compute instances to the worker node pool. A node pool is a group of nodes within a cluster that all have the same configuration. Node pools use a NodeConfig specification.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools
Moreover, Unmanaged instance groups do not autoscale. An unmanaged instance group is simply a collection of virtual machines (VMs) that reside in a single zone, VPC network, and subnet. An unmanaged instance group is useful for grouping together VMs that require individual configuration settings or tuning.

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

`Create Compute Engine instances for the workers and the master and install Kubernetes. Rely on Kubernetes to create additional Compute Engine instances when needed.` **is not right.**
When using Google Kubernetes Engine, you can not install master node separately. The cluster master runs the Kubernetes control plane processes, including the Kubernetes API server, scheduler, and core resource controllers. The master's lifecycle is managed by GKE when you create or delete a cluster.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture
Also, you can not add manually created compute instances to the worker node pool. A node pool is a group of nodes within a cluster that all have the same configuration. Node pools use a NodeConfig specification.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools

`Create a GKE cluster and enable autoscaling on Kubernetes Engine.` **is the right answer.**
GKE's cluster autoscaler automatically resizes the number of nodes in a given node pool, based on the demands of your workloads. You don't need to manually add or remove nodes or over-provision your node pools. Instead, you specify a minimum and maximum size for the node pool, and the rest is automatic. When demand is high, cluster autoscaler adds nodes to the node pool. When demand is low, cluster autoscaler scales back down to a minimum size that you designate. This can increase the availability of your workloads when you need it while controlling costs.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler

`Enable Horizontal Pod Autoscaling for the kubernetes deployment.` **is the right answer.**
Horizontal Pod Autoscaler scales up and scales down your Kubernetes workload by automatically increasing or decreasing the number of Pods in response to the workload's CPU or memory consumption, or in response to custom metrics reported from within Kubernetes or external metrics from sources outside of your cluster. Horizontal Pod Autoscaling cannot be used for workloads that cannot be scaled, such as DaemonSets.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/horizontalpodautoscaler

Question 8:

Skipped

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

- ○

  Execute kubectl config get-contexts.

  (Correct)

- ○

  Execute gcloud config configurations activate, then gcloud config list.

- ○

  Execute gcloud config configurations describe.

- ○

  Execute kubectl config use-context, then kubectl config view.

Explanation
We want to get to the end goal with the **fewest possible** steps.

`Execute gcloud config configurations describe.` **is not right.**
gcloud config configurations describe - describes a named configuration by listing its properties. This does not return any Kubernetes cluster details.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/describe

`Execute gcloud config configurations activate, then gcloud config list.` **is not right.**
gcloud config configurations activate - activates an existing named configuration. This does not return any Kubernetes cluster details.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate

`Execute kubectl config get-contexts.` **is the right answer.**
kubectl config get-contexts displays a list of contexts as well as the clusters that use them. Here's a sample output.

```
 $ kubectl config get-contexts

 CURRENT NAME CLUSTER

 gke_kubernetes-260922_us-central1-a_standard-cluster-1 gke_kubernetes-260922_
us-central1-a_standard-cluster-1

 gke_kubernetes-260922_us-central1-a_your-first-cluster-1 gke_kubernetes-26092
2_us-central1-a_your-first-cluster-1

 * gke_kubernetes-260922_us-central1_standard-cluster-1 gke_kubernetes-260922_
us-central1_standard-cluster-1
```

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

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

Here’s a sample execution

Step 1: First get a list of contexts

```
kubectl config get-contexts -o=name

gke_kubernetes-260922_us-central1-a_standard-cluster-1

gke_kubernetes-260922_us-central1-a_your-first-cluster-1

gke_kubernetes-260922_us-central1_standard-cluster-1
```

Step 2: Use each context and view the config.

```
kubectl config use-context gke_kubernetes-260922_us-central1-a_standard-cluster-1

Switched to context "gke_kubernetes-260922_us-central1-a_standard-cluster-1".

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



kubectl config use-context gke_kubernetes-260922_us-central1-a_your-first-cluster-1

Switched to context "gke_kubernetes-260922_us-central1-a_your-first-cluster-1".

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



kubectl config use-context gke_kubernetes-260922_us-central1_standard-cluster-1

Switched to context "gke_kubernetes-260922_us-central1_standard-cluster-1".
```

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


diff 1.out 2.out

28c28

< current-context: gke_kubernetes-260922_us-central1-a_standard-cluster-1

---

> current-context: gke_kubernetes-260922_us-central1-a_your-first-cluster-1


diff 2.out 3.out

28c28

< current-context: gke_kubernetes-260922_us-central1-a_your-first-cluster-1

---

> current-context: gke_kubernetes-260922_us-central1_standard-cluster-1
```

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

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

```
$ kubectl config view

apiVersion: v1

clusters:

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://35.222.130.166

name: gke_kubernetes-260922_us-central1-a_standard-cluster-1

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://35.225.14.172

name: gke_kubernetes-260922_us-central1-a_your-first-cluster-1

- cluster:

certificate-authority-data: DATA+OMITTED

server: https://34.69.212.109

name: gke_kubernetes-260922_us-central1_standard-cluster-1

contexts:

- context:

cluster: gke_kubernetes-260922_us-central1-a_standard-cluster-1
```

```
user: gke_kubernetes-260922_us-central1-a_standard-cluster-1
name: gke_kubernetes-260922_us-central1-a_standard-cluster-1
- context:
cluster: gke_kubernetes-260922_us-central1-a_your-first-cluster-1
user: gke_kubernetes-260922_us-central1-a_your-first-cluster-1
name: gke_kubernetes-260922_us-central1-a_your-first-cluster-1
- context:
cluster: gke_kubernetes-260922_us-central1_standard-cluster-1
user: gke_kubernetes-260922_us-central1_standard-cluster-1
name: gke_kubernetes-260922_us-central1_standard-cluster-1
current-context: gke_kubernetes-260922_us-central1-a_standard-cluster-1
```

Question 9:

Skipped

Your company wants to move all documents from a secure internal NAS drive to a Google Cloud Storage (GCS) bucket. The data contains personally identifiable information (PII) and sensitive customer information. Your company tax auditors need access to some of these documents. What security strategy would you recommend on GCS?

- ○

  Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.

  (Correct)

- ○

  Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.

- ○

  Grant IAM read-only access to users, and use default ACLs on the bucket.

- ○

  Use signed URLs to generate time bound access to objects.

Explanation

`Use signed URLs to generate time-bound access to objects.` **is not right.**

When dealing with sensitive customer information such as PII, using signed URLs is

not a great idea as anyone with access to the URL has access to PII data. Signed URLs provide time-limited resource access to anyone in possession of the URL, regardless of whether they have a Google account. With PII Data, we want to be sure who has access and signed URLs don't guarantee that.
Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

`Grant IAM read-only access to users, and use default ACLs on the bucket.` **is not right.**
We do not need to grant all IAM read-only access to this sensitive data. Just the users who need access to sensitive/PII data should be provided access to this data.

`Create randomized bucket and object names. Enable public access, but only provide specific file URLs to people who do not have Google accounts and need access.` **is not right.**
Enabling public access to the buckets and objects makes them visible to everyone. There are a number of scanning tools out in the market with the sole purpose of identifying buckets/objects that can be reached publicly. Should one of these tools be used by a bad actor to find out our public bucket/objects, it would result in a security breach.

`Grant no Google Cloud Identity and Access Management (Cloud IAM) roles to users, and use granular ACLs on the bucket.` **is the right answer.**
We start with no explicit access to any of the IAM users, and the bucket ACLs can then control which users can access what objects. This is the most secure way of ensuring just the people who require access to the bucket are provided with access. We block everyone from accessing the bucket and explicitly provided access to specific users through ACLs.

Question 10:

Skipped

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

- ○

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

- ○

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

(Correct)

- ○

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

- ○

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

Explanation

`You write a lifecycle management rule in XML and push it to the bucket with gsutil lifecycle set config-xml-file.` **is not right.**
gsutil lifecycle set enables you to set the lifecycle configuration on one or more buckets based on the configuration file provided. However, XML is not a valid supported type for the configuration file.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/lifecycle

`Write a script that runs gsutil ls -lr gs://myapp-gcp-ace-logs/** to find and remove items older than 90 days. Repeat this process every morning.` **is not right.**
This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

`Write a script that runs gsutil ls -l gs://myapp-gcp-ace-logs/** to find and remove items older than 90 days. Schedule the script with cron.` **is not right.**
This manual approach is error-prone, time-consuming and expensive. GCP Cloud Storage provides lifecycle management rules that let you achieve this with minimal effort.

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

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

Question 11:

Skipped

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

- ○

  Download Jenkins binary from https://www.jenkins.io/download/ and deploy in Google App Engine Standard Service.

- ○

  Create a Kubernetes Deployment YAML file referencing the Jenkins docker image and deploy to a new GKE cluster.

- ○

  Download Jenkins binary from https://www.jenkins.io/download/ and deploy in a new Google Compute Engine instance.

- ○

  Provision Jenkins from GCP marketplace.

  (Correct)

Explanation

`Download Jenkins binary from https://www.jenkins.io/download/ and deploy in a new Google Compute Engine instance.` **is not right.**
While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

`Create a Kubernetes Deployment YAML file referencing the Jenkins docker image and deploy to a new GKE cluster.` **is not right.**
While this can be done, this involves a lot more work than installing the Jenkins server through App Engine.

`Download Jenkins binary from https://www.jenkins.io/download/ and deploy in Google App Engine Standard Service.` **is not right.**
While this is possible, we need to ensure App Engine is enabled, we then need to download the Java project/WAR, and run gcloud app deploy to set up a Jenkins

server. This option involves more steps than spinning up an instance from GCP Marketplace.
Ref: https://cloud.google.com/appengine/docs/standard/java/tools/uploadinganapp
Ref: https://cloud.google.com/solutions/using-jenkins-for-distributed-builds-on-compute-engine

`Provision Jenkins from GCP marketplace.` **is the right answer.**
The simplest way to launch a Jenkins server is from GCP Market place. GCP market place has several builds available for Jenkins: https://console.cloud.google.com/marketplace/browse?q=jenkins.

All you need to do is spin up an instance from a suitable market place build, and you have a Jenkins server in a few minutes with just a few clicks.

Question 12:
Skipped
The deployment team currently spends a lot of time creating and configuring VMs in Google Cloud Console, and feel they could be more productive and consistent if the same can be automated using Infrastructure as Code. You want to help them identify a suitable service. What should you recommend?

- ○

  Unmanaged Instance Group.

- ○

  Managed Instance Group (MIG).

- ○

  Deployment Manager.

  (Correct)

- ○

  Cloud Build.

Explanation
`Unmanaged Instance Group.` **is not right.**
Unmanaged instance groups let you load balance across a fleet of VMs that you manage yourself. But it doesn't help with dynamically provisioning VMs.
Ref: https://cloud.google.com/compute/docs/instance-groups#unmanaged_instance_groups

`Cloud Build.` **is not right.**

Cloud Build is used for building and deploying services to serverless CI/CD platform. It can’t be used to automate the creation of VMs.

Ref: https://cloud.google.com/cloud-build

`Managed Instance Group (MIG).` **is not right.**

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

Ref: https://cloud.google.com/compute/docs/instance-groups#managed_instance_groups

`Deployment Manager.` **is the right answer.**

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

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

Question 13:

Skipped

You want to reduce storage costs for infrequently accessed data. The data will still be accessed approximately once a month and data older than 2 years is no longer needed. What should you do to reduce storage costs? (Select 2)

- □

  Store infrequently accessed data in a Nearline bucket.

  (Correct)

- □

  Set an Object Lifecycle Management policy to change the storage class to Coldline for data older than 2 years.

- □

  Store infrequently accessed data in a Multi-Regional bucket.

- □

  Set an Object Lifecycle Management policy to delete data older than 2 years.

  (Correct)

- □

  Set an Object Lifecycle Management policy to change the storage class to Archive for data older than 2 years.

Explanation

`Set an Object Lifecycle Management policy to change the storage class to Coldline for data older than 2 years.` **is not right.**
Data older than 2 years is not needed so there is no point in transitioning the data to Coldline. The data needs to be deleted.

`Set an Object Lifecycle Management policy to change the storage class to Archive for data older than 2 years.` **is not right.**
Data older than 2 years is not needed so there is no point in transitioning the data to Archive. The data needs to be deleted.

`Store infrequently accessed data in a Multi-Regional bucket.` **is not right.**
While infrequently accessed data can be stored in Multi-Regional bucket, there are several other storage classes offered by Google Cloud Storage that are primarily aimed at storing infrequently accessed data and cost less. Multi-Region buckets are primarily used for achieving geo-redundancy.
Ref: https://cloud.google.com/storage/docs/locations

`Set an Object Lifecycle Management policy to delete data older than 2 years.` **is the right answer.**
Since you don't need data older than 2 years, deleting such data is the right approach. You can set a lifecycle policy to automatically delete objects older than 2 years. The policy is valid on current as well as future objects and doesn't need any human intervention.
Ref: https://cloud.google.com/storage/docs/lifecycle

`Store infrequently accessed data in a Nearline bucket.` **is the right answer.**
Nearline Storage is a low-cost, highly durable storage service for storing infrequently accessed data. Nearline Storage is ideal for data you plan to read or modify on average once per month or less.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

Question 14:

Skipped

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

- ○

  Grant Project Editor IAM role for sandbox project.

- ○

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

- ○

  Grant Compute Engine Instance Admin Role for the sandbox project.

  (Correct)

- ○

  Grant Compute Engine Admin Role for sandbox project.

Explanation

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

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

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

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

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

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

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

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

more permissions than what is needed.
Ref: https://cloud.google.com/compute/docs/access/iam#compute.storageAdmin

`Grant Compute Engine Instance Admin Role for the sandbox project.` **is the right answer.**
Compute Engine Instance Admin Role grants full control of Compute Engine instances, instance groups, disks, snapshots, and images. It also provides read access to all Compute Engine networking resources. This provides just the required permissions to the intern.
Ref: https://cloud.google.com/compute/docs/access/iam#compute.storageAdmin

Question 15:

Skipped

Your organization is planning the infrastructure for a new large-scale application that will need to store anything between 200 TB to a petabyte of data in NoSQL format for Low-latency read/write and High-throughput analytics. Which storage option should you use?

- ○

  Cloud Bigtable.

  (Correct)

- ○

  Cloud Spanner.

- ○

  Cloud SQL.

- ○

  Cloud Datastore.

Explanation

`Cloud Spanner.` **is not right.**
Cloud Spanner is not a NoSQL database. Cloud SQL is a fully-managed relational database service.
Ref: https://cloud.google.com/sql/docs

`Cloud SQL.` **is not right.**
Cloud SQL is not a NoSQL database. Cloud Spanner is a highly scalable, enterprise-grade, globally-distributed, and strongly consistent relational database service
Ref: https://cloud.google.com/spanner

`Cloud Datastore.` **is not right.**
While Cloud Datastore is a highly scalable NoSQL database, it can't handle petabyte-scale data.
https://cloud.google.com/datastore

`Cloud Bigtable.` **is the right answer.**
Cloud Bigtable is a petabyte-scale, fully managed NoSQL database service for large analytical and operational workloads.
Ref: https://cloud.google.com/bigtable/

Question 16:
Skipped
You are designing a mobile game which you hope will be used by numerous users around the world. The game backend requires a Relational DataBase Management System (RDBMS) for persisting game state and player profiles. You want to select a database that can scale to a global audience with minimal configuration updates. Which database should you choose?

- ○

  Cloud Datastore.

- ○

  Cloud Firestore.

- ○

  Cloud SQL.

- ○

  Cloud Spanner.

  (Correct)

Explanation
Our requirements are relational data, global users, scaling

`Cloud Firestore.` **is not right.**
Cloud Firestore is not a relational database. Cloud Firestore is a flexible, scalable database for mobile, web, and server development from Firebase and Google Cloud Platform.
Ref: https://firebase.google.com/docs/firestore

`Cloud Datastore.` **is not right.**
Cloud Datastore is not a relational database. Datastore is a NoSQL document

database built for automatic scaling, high performance, and ease of application development
Ref: https://cloud.google.com/datastore/docs/concepts/overview

`Cloud SQL.` **is not right.**
While Cloud SQL is a relational database, it does not offer infinite automated scaling with minimum configuration changes. Cloud SQL is a fully-managed database service that makes it easy to set up, maintain, manage, and administer your relational databases on Google Cloud Platform
Ref: https://cloud.google.com/sql/docs

`Cloud Spanner.` **is the right answer.**
Cloud Spanner is a relational database and is highly scalable. Cloud Spanner is a highly scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the benefits of relational database structure with a non-relational horizontal scale. This combination delivers high-performance transactions and strong consistency across rows, regions, and continents with an industry-leading 99.999% availability SLA, no planned downtime, and enterprise-grade security
Ref: https://cloud.google.com/spanner

Question 17:
Skipped
A company wants to build an application that stores images in a Cloud Storage bucket and want to generate thumbnails as well resize the images. They want to use a google managed service that can scale up and scale down to zero automatically with minimal effort. You have been asked to recommend a service. Which GCP service would you suggest?

- ○

  Google Kubernetes Engine

- ○

  Google App Engine

- ○

  Cloud Functions

  (Correct)

- ○

  Google Compute Engine

Explanation

`Cloud Functions.` **is the right answer.**

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

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

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

Question 18:

Skipped

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

- ○

  In the GCP Console, move all projects to the root organization in the Resource Manager.

  (Correct)

- ○

  Send an email to billing.support@cloud.google.com and request them to create a new billing account and link all the projects to the billing account.

- ○

  Ensure you have the Billing Account Creator Role. Create a new Billing account yourself and set up a payment method with company credit card details.

- ○

  Raise a support request with Google Billing Support and request them to create a new billing account and link all the projects to the billing account.

Explanation

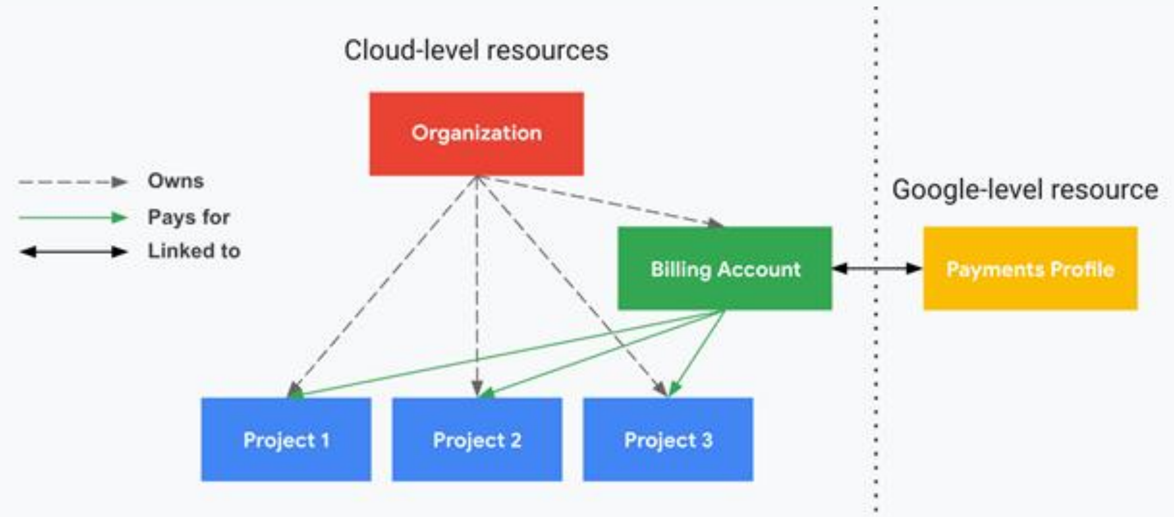
`Send an email to billing.support@cloud.google.com and request them to create a new billing account and link all the projects to the billing`

`account.` **is not right.**
That is not how we set up billing for the organization.
Ref: https://cloud.google.com/billing/docs/concepts

`Raise a support request with Google Billing Support and request them to create a new billing account and link all the projects to the billing account.` **is not right.**
That is not how we set up billing for the organization.
Ref: https://cloud.google.com/billing/docs/concepts

`Ensure you have the Billing Account Creator Role. Create a new Billing account yourself and set up a payment method with company credit card details.` **is not right.**
Unless all projects are modified to use the new billing account, this doesn't work.
Ref: https://cloud.google.com/billing/docs/concepts

`In the GCP Console, move all projects to the root organization in the Resource Manager.` **is the right answer.**
If we move all projects under the root organization hierarchy, they still need to modify to use a billing account within the organization (same as the previous option).
Ref: https://cloud.google.com/resource-manager/docs/migrating-projects-billing#top_of_page
Note: The link between projects and billing accounts is preserved, irrespective of the hierarchy. When you move your existing projects into the organization, they will continue to work and be billed as they used to before the migration, even if the corresponding billing account has not been migrated yet.
But in this option, all projects are in the organization resource hierarchy so the organization can uniformly apply organization policies to all its projects which is a Google recommended practice. So this is the better of the two options.
Ref: https://cloud.google.com/billing/docs/concepts



Question 19:

Skipped

A mission-critical application running on a Managed Instance Group (MIG) in Google Cloud has been having scaling issues. Although the scaling works, it is not quick enough, and users experience slow response times. The solution architect has recommended moving to GKE to achieve faster scaling and optimize machine resource utilization. Your colleague containerized the application and provided you with a Dockerfile. You now need to deploy this in a GKE cluster. How should you do it?

- ○

  Deploy the application using gcloud app deploy {Dockerfile}.

- ○

  Build a container image from the Dockerfile and push it to Google Cloud Storage (GCS). Create a Kubernetes Deployment YAML file and have it use the image from GCS. Use kubectl apply -f {deployment.YAML} to deploy the application to the GKE cluster.

- ○

  Deploy the application using kubectl app deploy {Dockerfile}.

- ○

  Build a container image from the Dockerfile and push it to Google Container Registry (GCR). Create a Kubernetes Deployment YAML file and have it use the image from GCR. Use kubectl apply -f {deployment.YAML} to deploy the application to the GKE cluster.

  (Correct)

Explanation

`Deploy the application using kubectl app deploy {Dockerfile}.` **is not right.**
kubectl does not accept app as a verb. Kubectl can deploy a configuration file using kubectl deploy.
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

`Deploy the application using gcloud app deploy {Dockerfile}.` **is not right.**
gcloud app deploy - Deploys the local code and/or configuration of your app to App Engine. gcloud app deploy accepts a flag --image-url which is the docker image, but it can't directly use a docker file.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy

`Build a container image from the Dockerfile and push it to Google Cloud Storage (GCS). Create a Kubernetes Deployment YAML file and have it use the image from GCS. Use kubectl apply -f {deployment.YAML} to deploy the application to the GKE cluster.` **is not right.**
You can not upload a docker image to cloud storage. They can only be pushed to a Container Registry (e.g. GCR, Dockerhub etc.)
Ref: https://cloud.google.com/container-registry/docs/pushing-and-pulling

`Build a container image from the Dockerfile and push it to Google Container Registry (GCR). Create a Kubernetes Deployment YAML file and have it use the image from GCR. Use kubectl apply -f {deployment.YAML} to deploy the application to the GKE cluster.` **is the right answer.**
Once you have a docker image, you can push it to the container register. You can then create a deployment YAML file pointing to this image and use kubectl apply -f {deployment YAML filename} to deploy this to the Kubernetes cluster. This command assumes you already have a Kubernetes cluster and you gcloud environment is set up to talk to this container by executing *gcloud container clusters get-credentials {cluster name} --zone={container_zone}*
Ref: https://cloud.google.com/container-registry/docs/pushing-and-pulling
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/get-credentials

Question 20:
Skipped
You want to migrate a mission-critical application from the on-premises data centre to Google Cloud Platform. Due to the mission-critical nature of the application, you want to have 3 idle (unoccupied) instances all the time to ensure the application always has enough resources to handle sudden bursts in traffic. How should you configure the scaling to meet this requirement?

- ○

  Enable Automatic Scaling and set minimum idle instances to 3.

  (Correct)

- ○

  Enable Basic Scaling and set maximum instances to 3.

- ○

  Start with 3 instances and manually scale as needed.

- ○

Enable Basic Scaling and set minimum instances to 3.

Explanation

`Start with 3 instances and manually scale as needed.` **is not right.**
Manual scaling uses resident instances that continuously run the specified number of instances regardless of the load level. This scaling allows tasks such as complex initializations and applications that rely on the state of the memory over time. Manual scaling does not autoscale based on the request rate, so it doesn't fit our requirements.
Ref: https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed

`Enable Basic Scaling and set minimum instances to 3.` **is not right.**
Basic scaling creates dynamic instances when your application receives requests. Each instance will be shut down when the app becomes idle. Basic scaling is ideal for work that is intermittent or driven by user activity. In the absence of any load, the App engine may shut down all instances, so it is not suitable for our requirement of "at least 3 instances at all times".
Ref: https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed

`Enable Basic Scaling and set maximum instances to 3.` **is not right.**
Basic scaling creates dynamic instances when your application receives requests. Each instance will be shut down when the app becomes idle. Basic scaling is ideal for work that is intermittent or driven by user activity. In the absence of any load, the App engine may shut down all instances, so it is not suitable for our requirement of "at least 3 instances at all times".
Ref: https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed

`Enable Automatic Scaling and set minimum idle instances to 3.` **is the right answer.**
Automatic scaling creates dynamic instances based on request rate, response latencies, and other application metrics. However, if you specify the number of minimum idle instances, that specified number of instances run as resident instances while any additional instances are dynamic.
Ref: https://cloud.google.com/appengine/docs/standard/python/how-instances-are-managed

Question 21:

Skipped

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

- □

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

  (Correct)

- □

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

- □

  Export audit logs to Cloud Storage via an export sink.

  (Correct)

- □

  Export audit logs to BigQuery via an export sink.

- □

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

Explanation

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

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

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

Storing logs in BigQuery is expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

`Export audit logs to Cloud Filestore via a Pub/Sub export sink.` **is not right.** Storing logs in Cloud Filestore is expensive. In Cloud Filestore, Standard Tier pricing costs $0.2 per GB per month and Premium Tier pricing costs $0.3 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

`Export audit logs to Cloud Storage via an export sink.` **is the right answer.** Among all the storage solutions offered by Google Cloud Platform, Cloud storage offers the best pricing for long term storage of logs. Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.
Ref: https://cloud.google.com/storage/pricing

`Generate a signed URL to the Stackdriver export destination for auditors to access.` **is the right answer.**
In Google Cloud Storage, you can generate a signed URL to provide limited permission and time to make a request. Anyone who possesses it can use the signed URL to perform specified actions, such as reading an object, within a specified period of time.

In our scenario, we do not need to create accounts for our auditors to provide access to logs in Cloud Storage. Instead, we can generate them signed URLs which are time-bound and lets them access/download log files.
Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

Question 22:
Skipped
You want to use Google Cloud Storage to host a static website on www.example.com for your staff. You created a bucket example-static-website and uploaded index.html and css files to it. You turned on static website hosting on the bucket and set up a CNAME record on www.example.com to point to c.storage.googleapis.com. You access the static website by navigating to www.example.com in the browser but your index page is not displayed. What should you do?

- ○

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

- ○

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

- ○

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

- ○

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

(Correct)

Explanation

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

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

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

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

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

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

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

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

```
NAME            TYPE   DATA
www.example.com CNAME  c.storage.googleapis.com.
```

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

Question 23:

Skipped

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

- ○

  Deploy the update as a new version. Migrate traffic from the current version to the new version. If it fails, migrate the traffic back to your older version.

  (Correct)

- ○

  Deploy the update as the same version that is currently running. If the update fails, redeploy your older version using the same version identifier.

- ○

  Deploy the update as the same version that is currently running. You are confident the update works so you don't plan for a rollback strategy.

- ○

  Notify your users of an upcoming maintenance window and ask them not to use your application during this window. Deploy the update in that maintenance window.

Explanation

`Deploy the update as the same version that is currently running. You are confident the update works so you don't plan for a rollback strategy.` **is not right.**

Irrespective of the level of confidence, you should always prepare a rollback strategy as things can go wrong for reasons out of our control.

`Deploy the update as the same version that is currently running. If the update fails, redeploy your older version using the same version identifier.` **is not right.**

While this can be done, the rollback process is not quick. Your application is unresponsive until you have redeployed the older version which can take quite a bit of time depending on how it is set up.

`Notify your users of an upcoming maintenance window and ask them not to use your application during this window. Deploy the update in that maintenance window.` **is not right.**

Our requirement is to deploy the update without impacting our users but by asking them to not use the application during the maintenance window, you are impacting all users.

`Deploy the update as a new version. Migrate traffic from the current version to the new version. If it fails, migrate the traffic back to your older version.` **is the right answer.**
This option enables you to deploy a new version and send all traffic to the new version. If you realize your updated application is not working, the rollback is as simple as marking your older version as default. This can all be done in the GCP console with a few clicks.
Ref: https://cloud.google.com/appengine/docs/admin-api/deploying-apps

Question 24:
Skipped
Your company has an App Engine application that needs to store stateful data in a proper storage service. Your data is non-relational data. You do not expect the database size to grow beyond 10 GB and you need to have the ability to scale down to zero to avoid unnecessary costs. Which storage service should you use?

- ○

  Cloud Bigtable

- ○

  Cloud Dataproc

- ○

  Cloud SQL

- ○

  Cloud Datastore

  (Correct)

Explanation
`Cloud SQL.` **is not right.**
Cloud SQL is not suitable for non-relational data. Cloud SQL is a fully-managed database service that makes it easy to set up, maintain, manage, and administer your relational databases on Google Cloud Platform
Ref: https://cloud.google.com/sql/docs

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

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

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

`Cloud Datastore.` **is the right answer.**
Cloud Datastore is a highly-scalable NoSQL database. Cloud Datastore scales seamlessly and automatically with your data, allowing applications to maintain high performance as they receive more traffic; automatically scales back when the traffic reduces.
Ref: https://cloud.google.com/datastore/

Question 25:

Skipped

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

- ○

  Nearline storage class

- ○

  Coldline storage class

- ○

  Standard storage class

- ○

  Archive storage class

  (Correct)

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

being kept entirely for backup or archiving purposes, Archive Storage is more cost-effective, as it offers the lowest storage costs."

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

So `Archive storage class` **is the right answer**

Question 26:
Skipped
You work for a big multinational financial company that has several hundreds of Google Cloud Projects for various development, test and production workloads. Financial regulations require your company to store all audit files for three years. What should you do to implement a log retention solution while minimizing storage cost?

- ○

  Write a script that exports audit logs from Cloud Logging to BigQuery. Use Cloud Scheduler to trigger the script every hour.

- ○

  Export audit logs from Cloud Logging to Coldline Storage bucket via an export sink.

  (Correct)

- ○

  Export audit logs from Cloud Logging to BigQuery via an export sink.

- ○

  Export audit logs from Cloud Logging to Cloud Pub/Sub via an export sink. Configure a Cloud Dataflow pipeline to process these messages and store them in Cloud SQL for MySQL.

Explanation
`Export audit logs from Cloud Logging to BigQuery via an export sink.` **is not right.**
You can export logs into BigQuery by creating one or more sinks that include a logs query and an export destination (big query). However, this option is costly compared to the cost of Cloud Storage.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

`Write a script that exports audit logs from Cloud Logging to BigQuery. Use Cloud Scheduler to trigger the script every hour.` **is not right.**
Stackdriver already offers sink exports that let you copy logs from Stackdriver logs to BigQuery. While BigQuery is already quite expensive compared to Cloud Storage, coming up with a custom script and maintaining it to copy the logs from Stackdriver logs to BigQuery is going to add to the cost. This option is very inefficient and expensive.

`Export audit logs from Cloud Logging to Cloud Pub/Sub via an export sink. Configure a Cloud Dataflow pipeline to process these messages and store them in Cloud SQL for MySQL.` **is not right.**
Cloud SQL is primarily used for storing relational data. Storing vast quantities of logs in Cloud SQL is very expensive compared to Cloud Storage. And add to it the fact that you also need to pay for Cloud Pub/Sub and Cloud Dataflow pipeline, and this option gets very expensive very soon.

`Export audit logs from Cloud Logging to Coldline Storage bucket via an export sink.` **is the right answer.**
Coldline Storage is the perfect service to store audit logs from all the projects and is very cost-efficient as well. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline Storage is ideal for data you plan to read or modify at most once a quarter.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

Question 27:

Skipped

You have a collection of audio/video files over 80GB each that you need to migrate to Google Cloud Storage. The files are in your on-premises data center. What migration method can you use to help speed up the transfer process?

- ○

  Start a recursive upload.

- ○

  Use the Cloud Transfer Service to transfer.

- ○

  Use multithreaded uploads using the -m option.

- ○

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

(Correct)

Explanation

`Use parallel uploads to break the file into smaller chunks then transfer it simultaneously.` **is the right answer.**

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

`Use multithreaded uploads using the -m option.` **is not right.**
Using the -m option lets you upload multiple files at the same time, but in our case, the individual files are over 80GB each. The best upload speed can be achieved by breaking the file into smaller chunks and transferring it simultaneously.

`Use the Cloud Transfer Service to transfer.` **is not right.**
Cloud Transfer Service is used for transferring massive amounts (in the range of petabytes of data) of data to the cloud. While nothing stops us from using Cloud Transfer Service to upload our files, it would be an overkill and very expensive.
Ref: https://cloud.google.com/products/data-transfer

`Start a recursive upload.` **is not right.**
In Google Cloud Storage, there is no such thing as a recursive upload.

Question 28:

Skipped

Your organization processes a very high volume of timestamped IoT data. The total volume can be several petabytes. The data needs to be written and changed at a high speed. You want to use the most performant storage option for your data. Which product should you use?

- ○

  Cloud Bigtable

  (Correct)

- ○

  Cloud Datastore

- ○

Cloud Storage

- ○

BigQuery

Explanation
Our requirement is to write/update a very high volume of data at a high speed. Performance is our primary concern, not cost.

`Cloud Bigtable` **is the right answer.**
Cloud Bigtable is Google's flagship product for ingest and analyze large volumes of time series data from sensors in real-time, matching the high speeds of IoT data to track normal and abnormal behavior.
Ref: https://cloud.google.com/bigtable/

While all other options are capable of storing high volumes of the order of petabytes, they are not as efficient as Bigtable at processing IoT time-series data.

Question 29:
Skipped
You want to ensure the boot disk of a preemptible instance is persisted for re-use. How should you provision the gcloud compute instance to ensure your requirement is met.

- ○

  gcloud compute instances create [INSTANCE_NAME] --no-auto-delete

- ○

  gcloud compute instances create [INSTANCE_NAME] --preemptible. The flag --boot-disk-auto-delete is disbaled by default.

- ○

  gcloud compute instances create [INSTANCE_NAME] --preemptible --boot-disk-auto-delete=no

- ○

  gcloud compute instances create [INSTANCE_NAME] --preemptible --no-boot-disk-auto-delete

  (Correct)

Explanation

`gcloud compute instances create [INSTANCE_NAME] --preemptible --boot-disk-auto-delete=no.` **is not right.**
gcloud compute instances create doesn't provide a parameter called boot-disk-auto-delete. It does have a flag by the same name. --boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use --no-boot-disk-auto-delete to disable.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

`gcloud compute instances create [INSTANCE_NAME] --preemptible. --boot-disk-auto-delete flag is disabled by default.` **is not right.**
--boot-disk-auto-delete is enabled by default. It enables automatic deletion of boot disks when the instances are deleted. Use --no-boot-disk-auto-delete to disable.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

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

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

Question 30:
Skipped
You've created a Kubernetes engine cluster named "my-gcp-ace-proj-1", which has a cluster pool named my-gcp-ace-primary-node-pool. You want to increase the number of nodes within your cluster pool from 10 to 20 to meet capacity demands. What is the command to change the number of nodes in your pool?

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

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

kubectl does not accept container as an operation.

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

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

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

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

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

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

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

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

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

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

Question 31:

Skipped

You are migrating a mission-critical HTTPS Web application from your on-premises data centre to Google Cloud, and you need to ensure unhealthy compute instances within the autoscaled Managed Instances Group (MIG) are recreated automatically. What should you do?

- ○

Add a metadata tag to the Instance Template with key: healthcheck value: enabled.

- ○

  Deploy Managed Instance Group (MIG) instances in multiple zones.

- ○

  When creating the instance template, add a startup script that sends server status to Cloud Monitoring as a custom metric.

- ○

  Configure a health check on port 443 when creating the Managed Instance Group (MIG).

  (Correct)

Explanation

`Deploy Managed Instance Group (MIG) instances in multiple zones.` **is not right.**

You can create two types of MIGs: A zonal MIG, which deploys instances to a single zone and a regional MIG, which deploys instances to multiple zones across the same region. However, this doesn't help with recreating unhealthy VMs.

Ref: https://cloud.google.com/compute/docs/instance-groups

`Add a metadata tag to the Instance Template with key: healthcheck value: enabled.` **is not right.**

Metadata entries are key-value pairs and do not influence any other behaviour.

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

`When creating the instance template, add a startup script that sends server status to Cloud Monitoring as a custom metric.` **is not right.**

The startup script is executed only when the instance boots up. In contrast, we need something like a liveness check that monitors the status of the server periodically to identify if the VM is unhealthy. So this is not going to work.

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

`Configure a health check on port 443 when creating the Managed Instance Group (MIG).` **is the right answer.**

To improve the availability of your application and to verify that your application is responding, you can configure an auto-healing policy for your managed instance group (MIG). An auto-healing policy relies on an application-based health check to verify that an application is responding as expected. If the auto healer determines that an application isn't responding, the managed instance group automatically

recreates that instance. Since our application is an HTTPS web application, we need to set up our health check on port 443, which is the standard port for HTTPS.
Ref: https://cloud.google.com/compute/docs/instance-groups/autohealing-instances-in-migs

Question 32:
Skipped
Your company runs all its applications in us-central1 region in a single GCP project and single VPC. The company has recently expanded its operations to Europe, but customers in the EU are complaining about slowness accessing the application. Your manager has requested you to deploy a new instance in the same project in europe-west1 region to reduce latency to the EU customers. The newly deployed VM needs to reach a central Citrix Licensing Server in us-central-1. How should you design the network and firewall rules while adhering to Google Recommended practices?

- ○

  Deploy the VM in a new subnet in europe-west1 region in the existing VPC. Have the VM contact the Citrix Licensing Server on its internal IP Address.

  (Correct)

- ○

  Deploy the VM in a new subnet in europe-west1 region in the existing VPC. Peer the two subnets using Cloud VPN. Have the VM contact the Citrix Licensing Server on its internal IP Address.

- ○

  Deploy the VM in a new subnet in europe-west1 region in a new VPC. Peer the two VPCs and have the VM contact the Citrix Licensing Server on its internal IP Address.

- ○

  Deploy the VM in a new subnet in europe-west1 region in a new VPC. Set up an HTTP(s) Load Balancer for the Citrix Licensing Server and have the VM contact the Citrix Licensing Server through the Load Balancer's public address.

Explanation
Our requirements are to **connect** the instance in europe-west1 region with the application running in us-central1 region following **Google-recommended practices**. The two instances are in the **same project**.

`Deploy the VM in a new subnet in europe-west1 region in a new VPC. Set up an HTTP(s) Load Balancer for the Citrix Licensing Server and have the VM contact the Citrix Licensing Server through the Load Balancer’s public address.` **is not right.**
We have two different VPCs. There is no mention of the CIDR range so let's assume the two subnets in two VPCs use different CIDR ranges. However, there is no communication route between the two VPCs. If we create an internal load balancer, that load balancer is not visible outside the VPC. So the new instance cannot connect to the load balancer's internal address.
Ref: https://cloud.google.com/load-balancing/docs/internal

`Deploy the VM in a new subnet in europe-west1 region in the existing VPC. Peer the two subnets using Cloud VPN. Have the VM contact the Citrix Licensing Server on its internal IP Address.` **is not right.**
Cloud VPN securely connects your on-premises network to your Google Cloud (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection. It is not meant to connect two subnets within the same VPC. Moreover, subnets within the same VPC can communicate with each other by setting up relevant firewall rules.

`Deploy the VM in a new subnet in europe-west1 region in a new VPC. Peer the two VPCs and have the VM contact the Citrix Licensing Server on its internal IP Address.` **is not right.**
Given that the new instance wants to access the application on the existing compute engine instance, these applications seem to be related so they should be within the same VPC. This option does not mention how the VPC networks are created and what the subnet range is.

You can't connect two auto mode VPC networks using VPC Network Peering because their subnets use identical primary IP ranges. We don't know how the VPCs were created.

There are several restrictions based on the subnet ranges.

https://cloud.google.com/vpc/docs/vpc-peering#restrictions
Even if we assume the above restrictions don’t apply and enable peering is possible, this is still a lot of additional work, and we can simplify this by choosing the option below (which is the answer)

`Deploy the VM in a new subnet in europe-west1 region in the existing VPC. Have the VM contact the Citrix Licensing Server on its internal IP Address.` **is the right answer.**
We can create another subnet in the same VPC, and this subnet is located in europe-west1. We can then spin up a new instance in this subnet. We also have to set up a firewall rule to allow communication between the two subnets. All instances in the

two subnets with the same VPC can communicate through the internal IP Address.
Ref: https://cloud.google.com/vpc

Question 33:

Skipped

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

- ○

  Make use of the Create Role from Role feature in GCP console to create IAM roles in the Staging project from the Development IAM roles.

- ○

  Make use of gcloud iam roles copy command to copy the IAM roles from the Development GCP project to the Staging GCP project.

  (Correct)

- ○

  Make use of Create Role feature in GCP console to create all necessary IAM roles from new in the Staging project.

- ○

  Make use of gcloud iam roles copy command to copy the IAM roles from the Development GCP organization to the Staging GCP organization.

Explanation

We are required to create the **same iam roles in a different (staging) project with the fewest possible steps.**

`Make use of the Create Role from Role feature in GCP console to create IAM roles in the Staging project from the Development IAM roles.` **is not right.**

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

`Make use of Create Role feature in GCP console to create all necessary IAM roles from new in the Staging project.` **is not right.**

This option works but is not as efficient as copying the roles from development project to the staging project.

`Make use of gcloud iam roles copy command to copy the IAM roles from the Development GCP organization to the Staging GCP organization.` **is not right.**
We can optionally specify a destination organization but since we require to copy the roles into "staging project" (i.e. project, not organization), this option does not meet our requirement to **create same iam roles in the staging project.**
Ref: https://cloud.google.com/sdk/gcloud/reference/iam/roles/copy

`Make use of gcloud iam roles copy command to copy the IAM roles from the Development GCP project to the Staging GCP project.` **is the right answer.**
This option fits all the requirements. You copy the roles into the destination project using gcloud iam roles copy and by specifying the staging project destination project.

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

Ref: https://cloud.google.com/sdk/gcloud/reference/iam/roles/copy
Question 34:
Skipped
A GKE cluster (test environment) in your test GCP project is experiencing issues with a sidecar container connecting to Cloud SQL. This issue has resulted in a massive amount of log entries in Cloud Logging and shot up your bill by 25%. Your manager has asked you to disable these logs as quickly as possible and using the least number of steps. You want to follow Google recommended practices. What should you do?

- ○

  Recreate the GKE cluster and disable Cloud Logging.

- ○

  Recreate the GKE cluster and disable Cloud Monitoring.

- ○

  In Cloud Logging, disable the log source for GKE container resource in the Logs ingestion window.

  (Correct)

- ○

In Cloud Logging, disable the log source for GKE Cluster Operations resource in the Logs ingestion window.

Explanation

`Recreate the GKE cluster and disable Cloud Logging.` **is not right.**
We require to disable the logs ingested from the GKE container. We don't need to delete the existing cluster and create a new one.

`Recreate the GKE cluster and disable Cloud Monitoring.` **is not right.**
We require to disable the logs ingested from the GKE container. We don't need to delete the existing cluster and create a new one.

`In Cloud Logging, disable the log source for GKE Cluster Operations resource in the Logs ingestion window.` **is not right.**
We require to disable the logs ingested from GKE container, not the complete GKE Cluster Operations resource.

`In Cloud Logging, disable the log source for GKE container resource in the Logs ingestion window.` **is the right answer.**
We want to disable logs from a specific GKE container, and this is the only option that does that.
More information about logs exclusions: https://cloud.google.com/logging/docs/exclusions.

Question 35:

Skipped

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

- ○

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

- ○

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

- ○

  Enable autoscaling on Kubernetes Engine.

(Correct)

- ○

  Enable Horizontal Pod Autoscaling for the kubernetes deployment.

Explanation

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

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

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

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

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

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

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

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

`Enable autoscaling on Kubernetes Engine.` **is the right answer.**

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

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

Question 36:

Skipped

You host a production application in Google Compute Engine in us-central1-a zone. Your application needs to be available 247 all through the year. The application suffered an outage recently due to a Compute Engine outage in the zone hosting your application. Your application is also susceptible to slowness during peak usage. You have been asked for a recommendation on how to modify the

infrastructure to implement a cost-effective and scalable solution that can withstand zone failures. What would you recommend?

- ○

  Use Managed instance groups across multiple zones. Enable Autoscaling on the Managed instance group.

  (Correct)

- ○

  Use Managed instance groups with instances in a single zone. Enable Autoscaling on the Managed instance group.

- ○

  Use Unmanaged instance groups across multiple zones. Enable Autoscaling on the Unmanaged instance group.

- ○

  Use Managed instance groups with preemptible instances across multiple zones. Enable Autoscaling on the Managed instance group.

Explanation

`Use Managed instance groups with preemptible instances across multiple zones. Enable Autoscaling on the Managed instance group.` **is not right.**
A preemptible VM runs at a much lower price than normal instances and is cost-effective. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are not suitable for production applications that need to be available 24*7.
Ref: https://cloud.google.com/compute/docs/instances/preemptible

`Use Unmanaged instance groups across multiple zones. Enable Autoscaling on the Unmanaged instance group.` **is not right.**
Unmanaged instance groups do not autoscale. An unmanaged instance group is simply a collection of virtual machines (VMs) that reside in a single zone, VPC network, and subnet. An unmanaged instance group is useful for grouping together VMs that require individual configuration settings or tuning.
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

`Use Managed instance groups with instances in a single zone. Enable Autoscaling on the Managed instance group.` **is not right.**
While enabling auto-scaling is a good idea, autoscaling would spin up instances in

the same zone. Should there be a zone failure, all instances of the managed instance group would be unreachable and cause the application to be unreachable. Google recommends you distribute your resources across multiple zones to tolerate outages.
Ref: https://cloud.google.com/compute/docs/regions-zones

`Use Managed instance groups across multiple zones. Enable Autoscaling on the Managed instance group.` **is the right answer.**
Distribute your resources across multiple zones and regions to tolerate outages. Google designs zones to be independent of each other: a zone usually has power, cooling, networking, and control planes that are isolated from other zones, and most single failure events will affect only a single zone. Thus, if a zone becomes unavailable, you can transfer traffic to another zone in the same region to keep your services running.
Ref: https://cloud.google.com/compute/docs/regions-zones
In addition, a managed instance group (MIG) contains offers auto-scaling capabilities that let you automatically add or delete instances from a managed instance group based on increases or decreases in load. Autoscaling helps your apps gracefully handle increases in traffic and reduce costs when the need for resources is lower. Autoscaling works by adding more instances to your instance group when there is more load (upscaling), and deleting instances when the need for instances is lowered (downscaling).
Ref: https://cloud.google.com/compute/docs/autoscaler/

Question 37:
Skipped
Your company has many Citrix services deployed in the on-premises datacenter, and they all connect to the Citrix Licensing Server on 10.10.10.10 in the same data centre. Your company wants to migrate the Citrix Licensing Server and all Citrix services to Google Cloud Platform. You want to minimize changes while ensuring the services can continue to connect to the Citrix licensing server. How should you do this in Google Cloud?

- ○

  Deploy the Citrix Licensing Server on a Google Compute Engine instance and set its ephemeral IP address to 10.10.10.10.

- ○

  Deploy the Citrix Licensing Server on a Google Compute Engine instance with an ephemeral IP address. Once the server is responding to requests, promote the ephemeral IP address to a static internal IP address.

- ○

Use gcloud compute addresses create to reserve 10.10.10.10 as a static external IP and assign it to the Citrix Licensing Server VM Instance.

- ○

  Use gcloud compute addresses create to reserve 10.10.10.10 as a static internal IP and assign it to the Citrix Licensing Server VM Instance.

  (Correct)

Explanation

`Use gcloud compute addresses create to reserve 10.10.10.10 as a static external IP and assign it to the Citrix Licensing Server VM Instance.` **is not right.**

The private network range is defined by IETF (Ref: https://tools.ietf.org/html/rfc1918) and includes 10.0.0.0/8. So all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. As the IP of interest 10.10.10.10 falls within this range, it can not be reserved as a public IP Address.

`Deploy the Citrix Licensing Server on a Google Compute Engine instance and set its ephemeral IP address to 10.10.10.10.` **is not right.**

An ephemeral IP address is the public IP Address assigned to compute instance. An ephemeral external IP address is an IP address that doesn't persist beyond the life of the resource. When you create an instance or forwarding rule without specifying an IP address, the resource is automatically assigned an ephemeral external IP address.

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

The private network range is defined by IETF (Ref: https://tools.ietf.org/html/rfc1918) and includes 10.0.0.0/8. So all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. As the IP of interest 10.10.10.10 falls within this range, it can not be used as a public IP Address (ephemeral IP is public).

`Deploy the Citrix Licensing Server on a Google Compute Engine instance with an ephemeral IP address. Once the server is responding to requests, promote the ephemeral IP address to a static internal IP address.` **is not right.**

When a compute instance is started with public IP, it gets an ephemeral IP address. An ephemeral external IP address is an IP address that doesn't persist beyond the life of the resource.

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

You can promote this ephemeral address into a Static IP address, but this will be an external IP address and not an internal one.

Ref: https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#promote_ephemeral_ip

`Use gcloud compute addresses create to reserve 10.10.10.10 as a static internal IP and assign it to the Citrix Licensing Server VM Instance.` **is right answer.**

This option lets us reserve IP 10.10.10.10 as a static internal IP address because it falls within the standard IP Address range as defined by IETF (Ref: https://tools.ietf.org/html/rfc1918). 10.0.0.0/8 is one of the allowed ranges, so all IP Addresses from 10.0.0.0 to 10.255.255.255 belong to this internal IP range. Since we can now reserve this IP Address as a static internal IP address, it can be assigned to the licensing server in the VPC so that the application can reach the licensing server.

Question 38:

Skipped

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

- ○

  Deploy the enhancement as a new App Engine Application in the existing GCP project. Configure the network load balancer to route 99% of the requests to the old (existing) App Engine Application and 1% to the new App Engine Application.

- ○

  Use gcloud app deploy to deploy the enhancement as a new version in the existing application with --migrate flag.

- ○

  Deploy the enhancement as a new App Engine Application in the existing GCP project. Make use of App Engine native routing to have the old App Engine application proxy 1% of the requests to the new App Engine application.

- ○

  Use gcloud app deploy to deploy the enhancement as a new version in the existing application and use --splits flag to split the traffic between the old version and the new version. Assign a weight of 1 to the new version and 99 to the old version.

  (Correct)

Explanation

`Use gcloud app deploy to deploy the enhancement as a new version in the existing application with --migrate flag.` **is not right.**
migrate is not a valid flag for the gcloud app deploy command.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/deploy
Also, gcloud app versions migrate, which is a valid command to migrate traffic from one version to another for a set of services, is not suitable either as we only want to send 1% traffic.
https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

`Deploy the enhancement as a new App Engine Application in the existing GCP project. Make use of App Engine native routing to have the old App Engine application proxy 1% of the requests to the new App Engine application.` **is not right.**
While this can be done, we are increasing complexity and do not meet our requirement "minimize complexity". There is an out of the box option in the app engine to split traffic seamlessly.

`Deploy the enhancement as a new App Engine Application in the existing GCP project. Configure the network load balancer to route 99% of the requests to the old (existing) App Engine Application and 1% to the new App Engine Application.` **is not right.**
Instances that participate as backend VMs for network load balancers must be running the appropriate Linux guest environment, Windows guest environment, or other processes that provide equivalent functionality. The network load balancer is not suitable for the App Engine standard environment, which is container-based and provides us with specific runtimes without any promise on the underlying guest environments.

`Use gcloud app deploy to deploy the enhancement as a new version in the existing application and use --splits flag to split the traffic between the old version and the new version. Assign a weight of 1 to the new version and 99 to the old version.` **is the right answer.**
You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features. For this scenario, we can split the traffic as shown below, sending 1% to v2 and 99% to v1 by executing the command gcloud app services set-traffic service1 --splits v2=1,v1=99
Ref: https://cloud.google.com/sdk/gcloud/reference/app/services/set-traffic

Question 39:
Skipped
Your company has deployed a wide range of application across several Google Cloud projects in the organization. You are a security engineer within the Cloud

Security team, and an apprentice has recently joined your team. To gain a better understanding of your company's Google cloud estate, the apprentice has asked you to provide them access which lets them have detailed visibility of all projects in the organization. Your manager has approved the request but has asked you to ensure the access does not let them edit/write access to any resources. Which IAM roles should you assign to the apprentice?

- ○

  Grant roles/resourcemanager.organizationAdmin and roles/browser.

- ○

  Grant roles/resourcemanager.organizationViewer and roles/owner.

- ○

  Grant roles/resourcemanager.organizationViewer and roles/viewer.

  (Correct)

- ○

  Grant roles/owner and roles/networkmanagement.admin.

Explanation
The security team needs detailed visibility of all GCP projects in the organization so they should be able to view all the projects in the organization as well as view all resources within these projects.

`Grant roles/resourcemanager.organizationViewer and roles/owner.` **is not right.**
roles/resourcemanager.organizationViewer role provides permissions to see the organization in the Cloud Console without having access to view all resources in the organization.
roles/owner provides permissions to manage roles and permissions for a project and all resources within the project and set up billing for a project.
Neither of the roles gives the security team visibility of the projects in the organization.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

`Grant roles/resourcemanager.organizationAdmin and roles/browser.` **is not right.**
roles/resourcemanager.organizationAdmin provides access to administer all resources belonging to the organization and goes against the least privilege principle. Our security team needs detailed visibility, i.e. read-only access but should

not be able to administer resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

`Grant roles/owner and roles/networkmanagement.admin.` **is not right.**
roles/owner provides permissions to manage roles and permissions for a project and all resources within the project and set up billing for a project.
roles/networkmanagement.admin provides full access to Cloud Network Management resources.
Neither of the roles gives the security team visibility of the projects in the organization.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

`Grant roles/resourcemanager.organizationViewer and roles/viewer.` **is the right answer.**
roles/viewer provides permissions to view existing resources or data.
roles/resourcemanager.organizationViewer provides access to view an organization.
With the two roles, the security team can view the organization, including all the projects and folders; as well as view all the resources within the projects.
Ref: https://cloud.google.com/resource-manager/docs/access-control-org
Ref: https://cloud.google.com/iam/docs/understanding-roles#organization-policy-roles

Question 40:
Skipped
Your company collects and stores CCTV footage videos in raw format in Google Cloud Storage. Within the first 30 days, footage is processed regularly for detecting patterns such as threat/object/face detection and suspicious behavior detection. You want to minimize the cost of storing all the data in Google Cloud. How should you store the videos?

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

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

`Use Google Cloud Regional Storage for the first 30 days, and use lifecycle rules to transition to Nearline Storage.` **is not right.**
Transitioning the data to Nearline Storage is a good idea as Nearline Storage costs less than standard storage, is highly durable for storing infrequently accessed data and a better choice than Standard Storage in scenarios where slightly lower availability is an acceptable trade-off for lower at-rest storage costs.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

However, we do not have a requirement to access the data after 30 days; and there are storage classes that are cheaper than nearline storage, so it is not a suitable option.
Ref: https://cloud.google.com/storage/pricing#storage-pricing

`Use Google Cloud Regional Storage for the first 30 days, and then move videos to Google Persistent Disk.` **is not right.**
Persistent disk pricing is almost double that of standard storage class in Google Cloud Storage service. Plus the persistent disk can only be accessed when attached to another service such as compute engine, GKE, etc making this option very expensive.
Ref: https://cloud.google.com/storage/pricing#storage-pricing
Ref: https://cloud.google.com/compute/disks-image-pricing#persistentdisk

`Use Google Cloud Nearline Storage for the first 30 days, and use lifecycle rules to transition to Coldline Storage.` **is not right.**
Nearline storage class is suitable for storing infrequently accessed data and has costs associated with retrieval. Since the footage is processed regularly within the first 30 days, data retrieval costs may far outweigh the savings made by using nearline storage over standard storage class.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline
Ref: https://cloud.google.com/storage/pricing#archival-pricing

`Use Google Cloud Regional Storage for the first 30 days, and use` `lifecycle rules to transition to Coldline Storage.` **is the right answer.**
We save the videos initially in Regional Storage (Standard) which does not have retrieval charges so we do not pay for accessing data within the first 30 days during which the videos are accessed frequently. We only pay for the standard storage costs. After 30 days, we transition the CCTV footage videos to Coldline storage which is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is a better choice than Standard Storage or Nearline Storage in scenarios where slightly lower availability, a 90-day minimum storage duration, and higher costs for data access are acceptable trade-offs for lowered at-rest storage costs. Coldline storage class is cheaper than Nearline storage class.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

Question 41:
Skipped
Your company hosts a number of applications in Google Cloud and requires that log messages from all applications be archived for 10 years to comply with local regulatory requirements. Which approach should you use?

- ○

  Grant the security team access to the logs in each Project

- ○

  1. Enable Stackdriver Logging API

  2. Configure web applications to send logs to Stackdriver

- ○

  1. Enable Stackdriver Logging API

  2. Configure web applications to send logs to Stackdriver

  3. Export logs to Google Cloud Storage

  (Correct)

- ○

  1. Enable Stackdriver Logging API

  2. Configure web applications to send logs to Stackdriver

  3. Export logs to BigQuery

Explanation

`Grant the security team access to the logs in each Project.` **is not right.**
Granting the security team access to the logs in each Project doesn't guarantee log retention. If the security team is to come up with a manual process to copy all the logs files into another archival source, the ongoing operational costs can be huge.

`1. Enable Stackdriver Logging API`
`2. Configure web applications to send logs to Stackdriver.` **is not right.**
In Stackdriver, application logs are retained by default for just 30 days after which they are purged.
Ref: https://cloud.google.com/logging/quotas
While it is possible to configure a custom retention period of 10 years, storing logs in Stackdriver is very expensive compared to Cloud Storage. Stackdriver charges $.01 per GB per month, whereas something like Cloud Storage Coldline Storage costs $0.007 per GB per month (30% cheaper) and Cloud Storage Archive Storage costs 0.004 per GB per month (60% cheaper than Stackdriver)
Ref: https://cloud.google.com/logging/docs/storage#pricing
Ref: https://cloud.google.com/storage/pricing

The difference between the remaining two options is whether we store the logs in BigQuery or Google Cloud Storage.

`1. Enable Stackdriver Logging API`
`2. Configure web applications to send logs to Stackdriver`
`3. Export logs to BigQuery.` **is not right.**
While enabling Stackdriver Logging API and having the applications send logs to stack driver is a good start, exporting and storing logs in BigQuery is fairly expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

`1. Enable Stackdriver Logging API`
`2. Configure web applications to send logs to Stackdriver`
`3. Export logs to Google Cloud Storage.` **is the right answer.**
Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.
Ref: https://cloud.google.com/storage/pricing

Question 42:

Skipped

You have annual audits every year and you need to provide external auditors access to the last 10 years of audit logs. You want to minimize the cost and operational

overhead while following Google recommended practices. What should you do? (Select Three)

- □

  Export audit logs to Cloud Storage via an audit log export sink.

  (Correct)

- □

  Grant external auditors Storage Object Viewer role on the logs storage bucket.

  (Correct)

- □

  Configure a lifecycle management policy on the logs bucket to delete objects older than 10 years.

  (Correct)

- □

  Export audit logs to BigQuery via an audit log export sink.

- □

  Set a custom retention of 10 years in Stackdriver logging and provide external auditors view access to Stackdriver Logs.

- □

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

Explanation

`Export audit logs to Cloud Filestore via a Pub/Sub export sink.` **is not right.** Storing logs in Cloud Filestore is expensive. In Cloud Filestore, Standard Tier pricing costs $0.2 per GB per month and Premium Tier pricing costs $0.3 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

`Set a custom retention of 10 years in Stackdriver logging and provide external auditors view access to Stackdriver Logs.` **is not right.**

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

`Export audit logs to BigQuery via an audit log export sink.` **is not right.**
Storing logs in BigQuery is expensive. In BigQuery, Active storage costs $0.02 per GB per month and Long-term storage costs $0.01 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/storage/pricing

`Export audit logs to Cloud Storage via an audit log export sink.` **is the right answer.**
Among all the storage solutions offered by Google Cloud Platform, Cloud storage offers the best pricing for long term storage of logs. Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than the storage options covered by the above options above.
Ref: https://cloud.google.com/storage/pricing

`Grant external auditors Storage Object Viewer role on the logs storage bucket.` **is the right answer.**
You can provide external auditors access to the logs in the bucket by granting the Storage Object Viewer role which allows them to read any object stored in any bucket.
Ref: https://cloud.google.com/storage/docs/access-control/iam

`Configure a lifecycle management policy on the logs bucket to delete objects older than 10 years.` **is the right answer.**
You need to archive log files for 10 years but you don't need log files older than 10 years. And since you also want to minimize costs, it is a good idea to set up a lifecycle management policy on the bucket to delete objects that are older than 10 years. Livecycle management configuration is a set of rules which apply to current and future objects in the bucket. When an object meets the criteria of one of the rules, Cloud Storage automatically performs a specified action (delete in this case) on the object.
Ref: https://cloud.google.com/storage/docs/lifecycle

Question 43:
Skipped

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

- ○

  1. Create an instance from the instance template.

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

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

- ○

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

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

- ○

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

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

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

- ○

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

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

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

  (Correct)

- ○

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

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

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

Explanation

`1. Create an instance from the instance template.`
`2. Create an image from the instance's disk and export it to Cloud Storage.`
`3. Create an External HTTP(s) load balancer and add the Cloud Storage bucket as its backend service.` **is not right.**

You can upload a custom image from instance's boot disk and export it to cloud storage.
https://cloud.google.com/compute/docs/images/export-image
However, this image in the Cloud Storage bucket is unable to handle traffic as it is not a running application. Cloud Storage can not serve requests of the custom image.

`1. Create an unmanaged instance group from the instance template.`
`2. Configure autoscaling on the unmanaged instance group with a scaling policy based on HTTP traffic.`
`3. Configure the unmanaged instance group as the backend service of an Internal HTTP(S) load balancer.` **is not right.**

An unmanaged instance group does not autoscale. An unmanaged instance group is a collection of virtual machines (VMs) that reside in a single zone, VPC network, and subnet. An unmanaged instance group is useful for grouping together VMs that require individual configuration settings or tuning.
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

`1. Create the necessary number of instances based on the instance template to handle peak user traffic.`
`2. Group the instances together in an unmanaged instance group.`
`3. Configure the instance group as the Backend Service of an External HTTP(S) load balancer.` **is not right.**

An unmanaged instance group does not autoscale. Although we may have enough compute power to handle peak user traffic, it does not automatically scale down when the traffic goes down so it doesn't meet our requirements.
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

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

`2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.` **is not right.**
You can not use compute engine instance templates to deploy applications to Google Cloud App Engine. Google App Engine lets you deploy applications quickly by providing run time environments for many of the popular languages like Java, PHP, Node.js, Python, C#, .Net, Ruby, and Go. You have an option of using custom runtimes but using compute engine instance templates is not an option.
Ref: https://cloud.google.com/appengine

`1. Create a managed instance group from the instance template.`
`2. Configure autoscaling on the managed instance group with a scaling policy based on HTTP traffic.`
`3. Configure the instance group as the backend service of an External HTTP(S) load balancer.` **is the right answer.**
The auto-scaling capabilities of Managed instance groups let you automatically add or delete instances from a managed instance group based on increases or decreases in load - this can be set up by configuring scaling policies. In addition, you can configure External HTTP(S) load balancer to send traffic to the managed instance group. The External HTTP(S) load balancer tries to balance requests by using a round-robin algorithm and when the load increases beyond the threshold defined in the scaling policy, autoscaling kicks in and adds more nodes.
Ref: https://cloud.google.com/load-balancing/docs/https
Ref: https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances

Question 44:

Skipped

Your company has a number of GCP projects that are managed by the respective project teams. Your expenditure of all GCP projects combined has exceeded your operational expenditure budget. At a review meeting, it has been agreed that your finance team should be able to set budgets and view the current charges for all projects in the organization but not view the project resources; and your developers should be able to see the Google Cloud Platform billing charges for only their own projects as well as view resources within the project. You want to follow Google recommended practices to set up IAM roles and permissions. What should you do?

- ○

  Add the finance team to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only.

- ○

  Add the finance team to the Viewer role for the Project. Add the developers to the Security Reviewer role for each of the billing accounts.

- ○

  Add the developers and finance managers to the Viewer role for the Project.

- ○

  Add the finance team to the Billing Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the Project.

  (Correct)

Explanation

`Add the finance team to the default IAM Owner role. Add the developers to a custom role that allows them to see their own spend only.` **is not right.**
Granting your finance team the default IAM role provides them permissions to manage roles and permissions for a project and subsequently use that to assign them the permissions to view/edit resources in all projects. This is against our requirements. Also, you can write a custom role that lets developers view their project spend but they are missing permissions to view project resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

`Add the developers and finance managers to the Viewer role for the Project.` **is not right.**
Granting your finance team the Project viewer role lets them view resources in all projects and doesn’t let them set budgets - both are against our requirements.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

`Add the finance team to the Viewer role on all projects. Add the developers to the Security Reviewer role for each of the billing accounts.` **is not right.**
Granting your finance team the Project viewer role lets them view resources in all projects which is against our requirements. Also, the security Reviewer role enables the developers to view custom roles but doesn’t let them view the project's costs or project resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

`Add the finance team to the Billing Administrator role for each of the billing accounts that they need to manage. Add the developers to the Viewer role for the Project.` **is the right answer.**
Billing Account Administrator role is an owner role for a billing account. It provides permissions to manage payment instruments, configure billing exports, view cost information, set budgets, link and unlink projects and manage other user roles on the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Project viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data; including viewing the billing charges for the project.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

Question 45:

Skipped

You transitioned an application to your operations team. The lead operations engineer has asked you to help understand what this lifecycle management rule does. What should your response be?

```
{
   "rule":[
      {
         "action":{
            "type":"Delete"
         },
         "condition":{
            "age":60,
            "isLive":false
         }
      },
      {
         "action":{
            "type":"SetStorageClass",
            "storageClass":"NEARLINE"
         },
         "condition":{
            "age":365,
            "matchesStorageClass":"MULTI_REGIONAL"
         }
      }
   ]
}
```

- ○

  The lifecycle rule transitions Multi-regional objects older than 365 days to Nearline storage class.

- ○

  The lifecycle rule deletes non-current (archived) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.

  (Correct)

- ○

  The lifecycle rule archives current (live) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.

- ○

  The lifecycle rule deletes current (live) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.

Explanation

`The lifecycle rule archives current (live) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.` **is not right.**
The action has "type":"Delete" which means we want to Delete, not archive.
Ref: https://cloud.google.com/storage/docs/managing-lifecycles

`The lifecycle rule deletes current (live) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.` **is not right.**
We want to delete objects as indicated by the action; however, we don't want to delete all objects older than 60 days. We only want to delete archived objects as indicated by "isLive":false condition.
Ref: https://cloud.google.com/storage/docs/managing-lifecycles

`The lifecycle rule transitions Multi-regional objects older than 365 days to Nearline storage class.` **is not right.**
The first rule is missing. It deletes archived objects older than 60 days.

`The lifecycle rule deletes non-current (archived) objects older than 60 days and transitions Multi-regional objects older than 365 days to Nearline storage class.` **is the right answer.**
The first part of the rule: The action has "type":"Delete" which means we want to Delete. "isLive":false condition means we are looking for objects that are not Live, i.e. objects that are archived. Together, it means we want to delete archived objects older than 60 days. Note that if an object is deleted, it cannot be undeleted. Take care in setting up your lifecycle rules so that you do not cause more data to be deleted than you intend.
Ref: https://cloud.google.com/storage/docs/managing-lifecycles
The second part of the rule: The action indicates we want to set storage class to Nearline. The condition is satisfied if the existing storage class is multi-regional, and the age of the object is 365 days or over. Together it means we want to set the storage class to Nearline if existing storage class is multi-regional and the age of the object is 365 days or over.

Question 46:

Skipped

Your company, which runs highly rated mobile games, has chosen to migrate its analytics backend to BigQuery. The analytics team of 7 analysts need access to

perform queries against the data in BigQuery. The analytics team members change frequently. How should you grant them access?

- ○

  Create a Cloud Identity account for each analyst and add them all to a group. Grant roles/bigquery.jobUser role to the group.

- ○

  Create a Cloud Identity account for each analyst and add them all to a group. Grant roles/bigquery.dataViewer role to the group.

  (Correct)

- ○

  Create a Cloud Identity account for each analyst and grant roles/bigquery.jobUser role to each account.

- ○

  Create a Cloud Identity account for each analyst and grant roles/bigquery.dataViewer role to each account.

Explanation

`Create a Cloud Identity account for each analyst and grant roles/bigquery.dataViewer role to each account.` **is not right.**
dataViewer provides permissions to Read data (i.e. query) and metadata from the table or view so this is the right role but given that our data science team changes frequently, we do not want to go through this lengthy provisioning and de-provisioning process. Instead, we should be using groups so that provisioning and de-provisioning are as simple as adding/removing the user to/from the group. Google Groups are a convenient way to apply an access policy to a collection of users.
Ref: https://cloud.google.com/bigquery/docs/access-control

`Create a Cloud Identity account for each analyst and grant roles/bigquery.jobUser role to each account.` **is not right.**
Given that our data science team changes frequently, we do not want to go through this lengthy provisioning and de-provisioning process. Instead, we should be using groups so that provisioning and de-provisioning are as simple as adding/removing the user to/from the group. Google Groups are a convenient way to apply an access policy to a collection of users.
Ref: https://cloud.google.com/bigquery/docs/access-control
Ref: https://cloud.google.com/iam/docs/overview#google_group

`Create a Cloud Identity account for each analyst and add them all to a group. Grant roles/bigquery.jobUser role to the group.` **is not right.**
Since you want users to query the datasets, you need dataViewer role. jobUser provides the ability to run jobs, including "query jobs". The query job lets you query an authorized view. An authorized view lets you share query results with particular users and groups without giving them access to the underlying tables. You can also use the view's SQL query to restrict the columns (fields) the users can query.
Ref: https://cloud.google.com/bigquery/docs/access-control-examples
Ref: https://cloud.google.com/bigquery/docs/access-control

`Create a Cloud Identity account for each analyst and add them all to a group. Grant roles/bigquery.dataViewer role to the group.` **is the right answer.**
dataViewer provides permissions to Read data (i.e. query) and metadata from the table or view, so this is the right role, and this option also rightly uses groups instead of assigning permissions at the user level.
Ref: https://cloud.google.com/bigquery/docs/access-control-examples
Ref: https://cloud.google.com/bigquery/docs/access-control

Question 47:
Skipped
Your organization is planning to deploy a Python web application to Google Cloud. The web application uses a custom linux distribution and you want to minimize rework.The web application underpins an important website that is accessible to the customers globally. You have been asked to design a solution that scales to meet demand. What would you recommend to fulfill this requirement? (Select Two)

- ☐

  Network Load Balance

- ☐

  HTTP(S) Load Balancer

  (Correct)

- ☐

  Managed Instance Group on Compute Engine

  (Correct)

- ☐

  App Engine Standard environment

- □

  Cloud Functions

Explanation
Requirements are - use custom Linux distro, global access, auto scale.

`Cloud Functions.` **is not right.**
Cloud Functions is a serverless compute platform. You can not use a custom Linux distribution with Cloud Functions.
Ref: https://cloud.google.com/functions

`App Engine Standard environment.` **is not right.**
The App Engine Standard Environment is based on container instances running on Google's infrastructure. Containers are preconfigured with one of several available runtimes such as Python, Java, NodeJS, PHP, Ruby, GO etc. It is not possible to specify a custom Linux distribution with App Engine Standard.
Ref: https://cloud.google.com/appengine/docs/standard

`Network Load Balance.` **is not right.**
The external (TCP/UDP) Network Load Balancing is a regional load balancer. Since we need to cater to a global user base, this load balancer is not suitable.
Ref: https://cloud.google.com/load-balancing/docs/network

`HTTP(S) Load Balancer.` **is the right answer.**
HTTP(S) Load Balancing is a global service (when the Premium Network Service Tier is used). We can create backend services in more than one region and have them all serviced by the same global load balancer
Ref: https://cloud.google.com/load-balancing/docs/https

`Managed Instance Group on Compute Engine.` **is the right answer.**
Managed instance groups (MIGs) maintain the high availability of your applications by proactively keeping your virtual machine (VM) instances available. An autohealing policy on the MIG relies on an application-based health check to verify that an application is responding as expected. If the auto-healer determines that an application isn't responding, the managed instance group automatically recreates that instance.
Ref: https://cloud.google.com/compute/docs/instance-groups

Question 48:
Skipped
Your company is migrating all applications from the on-premises data centre to Google Cloud, and one of the applications is dependent on Websockets protocol and session affinity. You want to ensure this application can be migrated to Google Cloud platform and continue serving requests without issues. What should you do?

- ○

Modify application code to use HTTP streaming.

- ○

Discuss load balancer options with the relevant teams.

(Correct)

- ○

Review the design with the security team.

- ○

Modify application code to not depend on session affinity.

Explanation
Google HTTP(S) Load Balancing has native support for the WebSocket protocol when you use HTTP or HTTPS, not HTTP/2, as the protocol to the backend.
Ref: https://cloud.google.com/load-balancing/docs/https#websocket_proxy_support
The load balancer also supports session affinity.
Ref: https://cloud.google.com/load-balancing/docs/backend-service#session_affinity

So the next possible step is `Discuss load balancer options with the relevant teams.` **is the right answer.**

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

Question 49:
Skipped
A mission-critical application running in Google Cloud Platform requires an urgent update to fix a security issue without any downtime. How should you do this in CLI using deployment manager?

- ○

Use gcloud deployment-manager deployments update and point to the deployment config file.

(Correct)

- ○

Use gcloud deployment-manager resources create and point to the deployment config file.

- ○

  Use gcloud deployment-manager resources update and point to the deployment config file.

- ○

  Use gcloud deployment-manager deployments create and point to the deployment config file.

Explanation

`Use gcloud deployment-manager resources create and point to the deployment config file.` **is not right.**

gcloud deployment-manager resources command does not support the action create. The supported actions are describe and list. So this option is not right.
Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/resources

`Use gcloud deployment-manager resources update and point to the deployment config file.` **is not right.**

gcloud deployment-manager resources command does not support the action update. The supported actions are describe and list. So this option is not right.
Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/resources

`Use gcloud deployment-manager deployments create and point to the deployment config file.` **is not right.**

gcloud deployment-manager deployments create - creates a deployment, but we want to update a deployment. So this option is not right.
Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/create

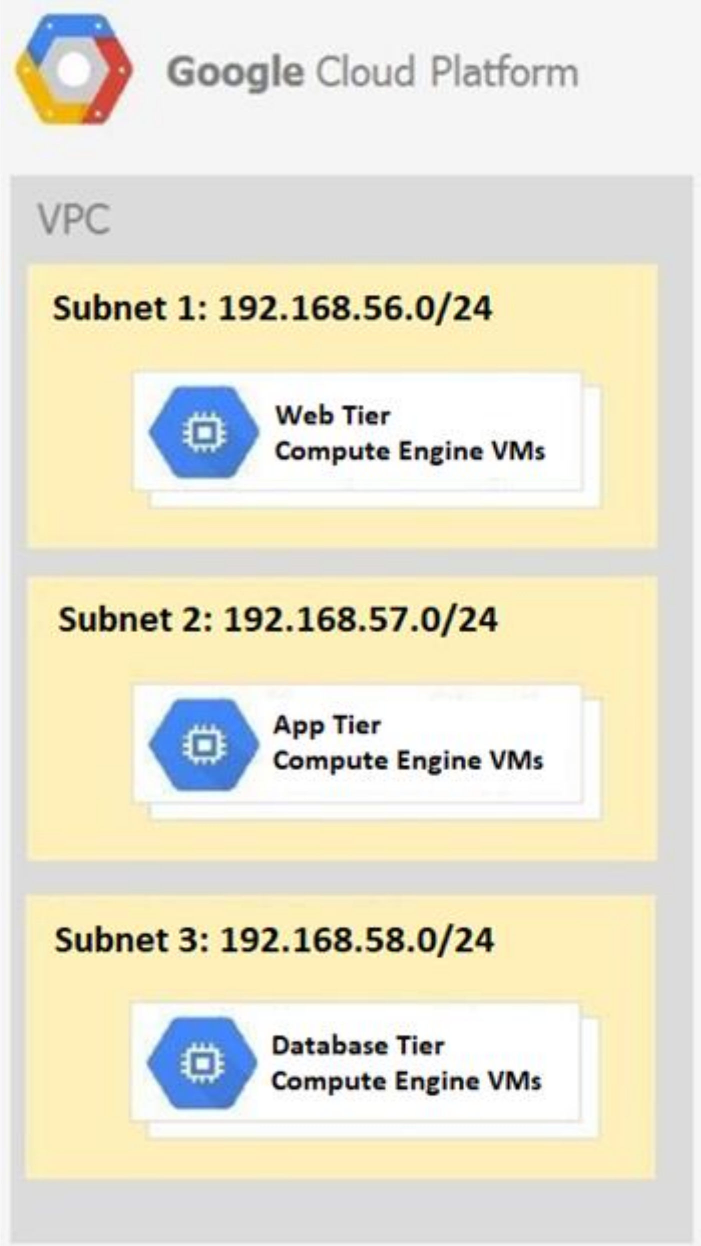
`Use gcloud deployment-manager deployments update and point to the deployment config file.` **is the right answer.**

gcloud deployment-manager deployments update - updates a deployment based on a provided config file and fits our requirement.
Ref: https://cloud.google.com/sdk/gcloud/reference/deployment-manager/deployments/update

Question 50:

Skipped

Your company is a leading multinational news media organization and runs its online news website in Google Cloud on a 3-tier architecture as described below. 1. Web tier in Subnet 1 with a CIDR range 192.168.56.0/24. All instances in this tier use serviceAccount_subnet1 2. App tier in Subnet 2 with a CIDR range 192.168.57.0/24. All instances in this tier use serviceAccount_subnet2 3. DB tier in Subnet 3 with a CIDR range 192.168.58.0/24. All instances in this tier use serviceAccount_subnet3



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

- ○

1. Create an ingress firewall rule that allows all traffic from all instances with serviceAccount_subnet1 to all instances with serviceAccount_subnet2.

2. Create an ingress firewall rule that allows all traffic from all instances with serviceAccount_subnet2 to all instances with serviceAccount_subnet3.

- ○

1. Create an ingress firewall rule that allows all traffic from Subnet 2 (range: 192.168.57.0/24) to all other instances.

2. Create another ingress firewall rule that allows all traffic from Subnet 1 (range: 192.168.56.0/24) to all other instances.

- ○

1. Create an ingress firewall rule that allows traffic on port 80 from all instances with serviceAccount_subnet1 to all instances with serviceAccount_subnet2.

2. Create an ingress firewall rule that allows traffic on port 3306 from all instances with serviceAccount_subnet2 to all instances with serviceAccount_subnet3.

(Correct)

- ○

1. Create an egress firewall rule that allows traffic on port 80 from Subnet 2 (range: 192.168.57.0/24) to all other instances.

2. Create another egress firewall rule that allows traffic on port 3306 from Subnet 1 (range: 192.168.56.0/24) to all other instances.

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

We want to ensure that **Web Tier can communicate with App Tier, and App Tier can communicate with Database Tier.**

`1. Create an egress firewall rule that allows traffic on port 80 from` `Subnet 2 (range: 192.168.57.0/24) to all other instances.` `2. Create another egress firewall rule that allows traffic on port 3306` `from Subnet 1 (range: 192.168.56.0/24) to all other instances.` **is not right.** We are creating egress rules here which allow outbound communication but not ingress rules which are for inbound traffic.

`1. Create an ingress firewall rule that allows all traffic from Subnet 2 (range: 192.168.57.0/24) to all other instances.` `2. Create another ingress firewall rule that allows all traffic from Subnet 1 (range: 192.168.56.0/24) to all other instances.` **is not right.**
If we create an ingress firewall rule with the settings

Targets: all instances

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

Protocols: allow all.

We are allowing Web Tier (192.168.56.0/24) access to all instances - including Database Tier (192.168.58.0/24) which is not desirable.

`1. Create an ingress firewall rule that allows all traffic from all instances with serviceAccount_subnet1 to all instances with serviceAccount_subnet2.` `2. Create an ingress firewall rule that allows all traffic from all instances with serviceAccount_subnet2 to all instances with serviceAccount_subnet3.` **is not right.**

The first firewall rule ensures that all instances with serviceAccount_subnet2, i.e. all instances in Subnet Tier #2 (192.168.57.0/24) can be reached from all instances with serviceAccount_subnet1, i.e. all instances in Subnet Tier #1 (192.168.56.0/24), on all ports. Similarly, the second firewall rule ensures that all instances with serviceAccount_subnet3, i.e. all instances in Subnet Tier #3 (192.168.58.0/24) can be reached from all instances with serviceAccount_subnet2, i.e. all instances in Subnet Tier #2 (192.168.57.0/24), on all ports. Though this matches our requirements, we are opening all ports instead of the specified ports, which is our requirement. While this solution works, it is not as secure as the other option (see below)

`1. Create an ingress firewall rule that allows traffic on port 80 from all instances with serviceAccount_subnet1 to all instances with serviceAccount_subnet2.` `2. Create an ingress firewall rule that allows traffic on port 3306 from all instances with serviceAccount_subnet2 to all instances with serviceAccount_subnet3.` **is the right answer.**
The first firewall rule ensures that all instances with serviceAccount_subnet2, i.e. all instances in Subnet Tier #2 (192.168.57.0/24) can be reached from all instances with serviceAccount_subnet1, i.e. all instances in Subnet Tier #1 (192.168.56.0/24), on port 80. Similarly, the second firewall rule ensures that all instances with serviceAccount_subnet3, i.e. all instances in Subnet Tier #3 (192.168.58.0/24) can

be reached from all instances with serviceAccount_subnet2, i.e. all instances in Subnet Tier #2 (192.168.57.0/24), on port 3306.

Question 1:

Skipped

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

- ○

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

  (Correct)

- ○

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

- ○

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

- ○

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

Explanation

We want to create a new role and grant it to a team. Since you want to minimize operational overhead, we need to grant it to a group - so that new users who join the team just need to be added to the group and they inherit all the permissions. Also, this team needs to have the role for all projects in the organization. And since we want to minimize the operational overhead, we need to grant it at the organization level so that all current projects, as well as future projects, have the role granted to them.

`In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Repeat this step for each project.` **is not right.**

Repeating the step for all projects is a manual, error-prone and time-consuming task.

Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead.

`In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at project. Use gcloud iam promote-role to promote the role to all other projects and grant the role in each project to the SME team group.` **is not right.** Repeating the step for all projects is a manual, error-prone and time-consuming task. Also, if any projects were to be created in the future, we have to repeat the same process again. This increases operational overhead.

`Execute command gcloud iam combine-roles --global to combine the 2 roles into a new custom role and grant them globally to all.` **is not right.** There are several issues with this. gcloud iam command doesn't support the action combine-roles. Secondly, we don't want to grant the roles globally. We want to grant them to the SME team and no one else.

`In GCP Console under IAM Roles, select both roles and combine them into a new custom role. Grant the role to the SME team group at the organization level.` **is the right answer.** This correctly creates the role and assigns the role to the group at the organization. When any new users join the team, the only additional task is to add them to the group. Also, when a new project is created under the organization, no additional human intervention is needed. Since the role is granted at the organization level, it automatically is granted to all the current and future projects belonging to the organization.

Question 2:

Skipped

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

- ○

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

- ○

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

(Correct)

- ○

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

- ○

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

Explanation

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

kubectl doesn't support the command kubectl container clusters resize. You have to use gcloud container clusters resize to resize a cluster.
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/resize

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

GKE Cluster does not use a managed instance group. Instead, the cluster master (control plan) handles the lifecycle of nodes in the node pools. The cluster master is responsible for managing the workloads' lifecycle, scaling, and upgrades. The master also manages network and storage resources for those workloads.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture

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

GKE Cluster does not use a managed instance group. Instead, the cluster master (control plan) handles the lifecycle of nodes in the node pools. The cluster master is responsible for managing the workloads' lifecycle, scaling, and upgrades. The master also manages network and storage resources for those workloads.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture

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

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

Question 3:

Skipped

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

- ○

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

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

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

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

- ○

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

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

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

- ○

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

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

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

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

(Correct)

- ○

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

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

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

Explanation

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

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

The main differences between the remaining two options are

Static route in the VPC network.

Public/Private zone.

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

So, **the right answer** is

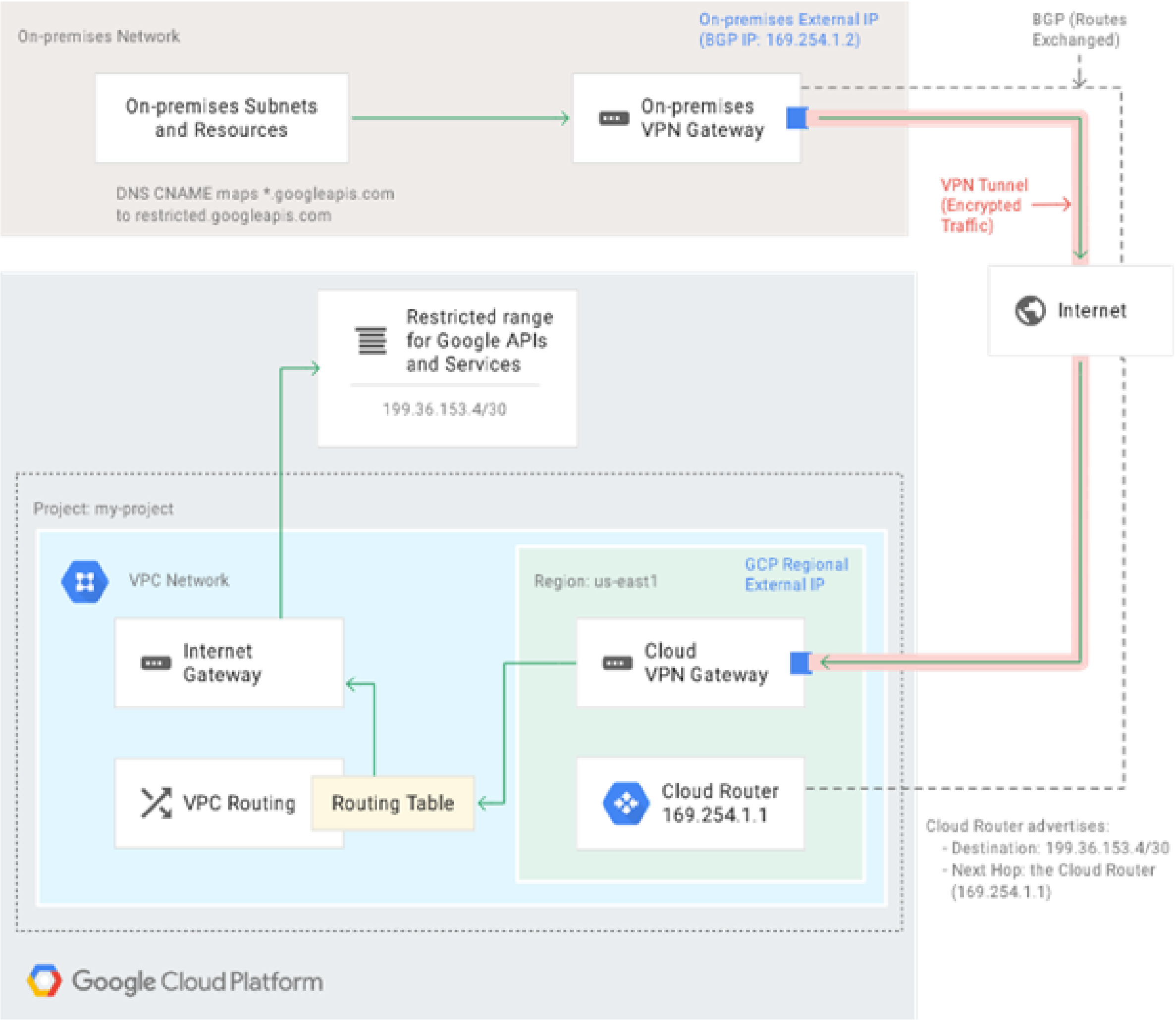
1. In on-premises DNS configuration, map *.googleapis.com to restricted.googleapis.com, which resolves to the 199.36.153.4/30.

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

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

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

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



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

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

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

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

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

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

Question 4:

Skipped

Users of your application are complaining of slowness when loading the application. You realize the slowness is because the App Engine deployment serving the application is deployed in us-central where as all users of this application are closest to europe-west3. You want to change the region of the App Engine application to europe-west3 to minimize latency. What's the best way to change the App Engine region?

- ○

  Contact Google Cloud Support and request the change.

- ○

  Create a new project and create an App Engine instance in europe-west3.

  (Correct)

- ○

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

- ○

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

Explanation

`Use the gcloud app region set command and supply the name of the new region.` **is not right.**

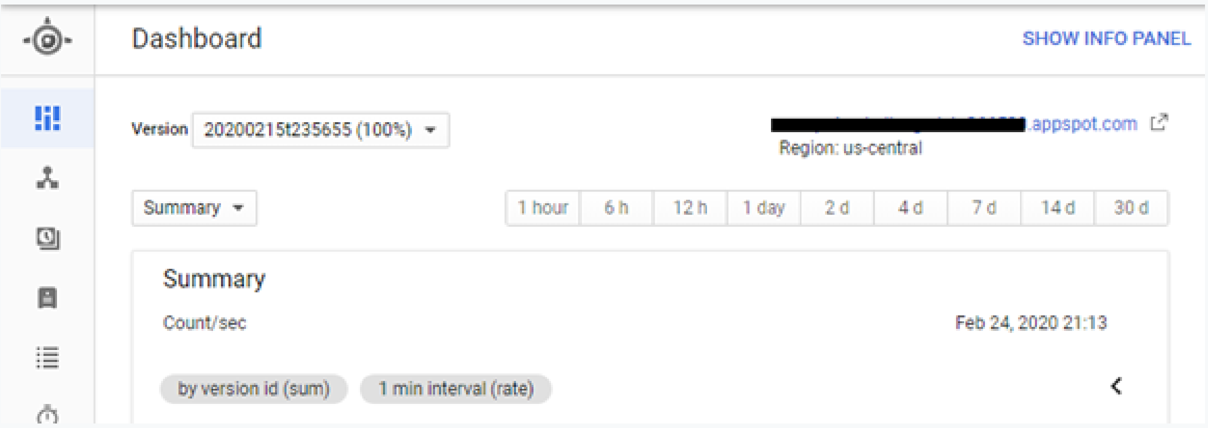
gcloud app region command does not provide a set action. The only action gcloud app region command currently supports is list which lists the availability of flex and standard environments for each region.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/regions/list

`Contact Google Cloud Support and request the change.` **is not right.**

Unfortunately, Google Cloud Support isn't of much use here as they would not be able to change the region of an App Engine Deployment. App engine is a regional service, which means the infrastructure that runs your app(s) is located in a specific region and is managed by Google to be redundantly available across all the zones within that region. Once an app engine deployment is created in a region, it can't be changed.
Ref: https://cloud.google.com/appengine/docs/locations

`From the console, Click edit in App Engine dashboard page and change the region drop-down.` **is not right.**

The settings mentioned in this option aren't available in the App Engine dashboard. App engine is a regional service. Once an app engine deployment is created in a region, it can't be changed. As shown in the screenshot below, Region is greyed out.



Dashboard

Version 20200215t235655 (100%)

[redacted].appspot.com
Region: us-central

Summary

Count/sec

Feb 24, 2020 21:13

`Create a new project and create an App Engine instance in europe-west3.` **is the right answer.**

App engine is a regional service, which means the infrastructure that runs your app(s) is located in a specific region and is managed by Google to be redundantly available across all the zones within that region. Once an app engine deployment is created in a region, it can't be changed. The only way is to create a new project and create an App Engine instance in europe-west3, send all user traffic to this instance and delete the app engine instance in us-central.

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

Question 5:

Skipped

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

- ○

  Include the forwarder agent in a StatefulSet deployment.

- ○

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

- ○

  Include the forwarder agent in a DaemonSet deployment.

  (Correct)

- ○

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

Explanation

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

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

`Include the forwarder agent in a StatefulSet deployment.` **is not right.**

In GKE, StatefulSets represents a set of Pods with unique, persistent identities and stable hostnames that GKE maintains regardless of where they are scheduled. The main purpose of StatefulSets is to set up persistent storage for pods that are deployed across multiple zones. StatefulSets are not suitable for installing the

forwarder agent nor do they provide us the ability to install forwarder agents.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset

`Use Deployment Manager to orchestrate the deployment of forwarder agents on all nodes.` **is not right.**
You can use a deployment manager to create a number of GCP resources including GKE Cluster but you can not use it to create Kubernetes deployments or apply configuration files.
Ref: https://cloud.google.com/deployment-manager/docs/fundamentals

`Include the forwarder agent in a DaemonSet deployment.` **is the right answer.**
In GKE, DaemonSets manage groups of replicated Pods and adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes. So by configuring the pod to use Splunk forwarder agent image and with some minimal configuration (e.g. identifying which logs need to be forwarded), you can automate the installation and configuration of Splunk forwarder agent on each GKE cluster node.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset

Question 6:
Skipped
You have a number of applications that have bursty workloads and are heavily dependent on topics to decouple publishing systems from consuming systems. Your company would like to go serverless to enable developers to focus on writing code without worrying about infrastructure. Your solution architect has already identified Cloud Pub/Sub as a suitable alternative for decoupling systems. You have been asked to identify a suitable GCP Serverless service that is easy to use with Cloud Pub/Sub. You want the ability to scale down to zero when there is no traffic in order to minimize costs. You want to follow Google recommended practices. What should you suggest?

- ○

  Cloud Run

- ○

  Cloud Functions

  (Correct)

- ○

  App Engine Standard

- ○

Cloud Run for Anthos

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

Lets us scale down to 0

Integrates with Cloud Pub/Sub seamlessly

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

`App Engine Standard.` **is not right.**
App Engine Standard doesn't offer an out of the box integration with Cloud Pub/Sub. We can use the Cloud Client Library to send and receive Pub/Sub messages as described in the note below but the key point to note is the absence of out of the box integration with Cloud Pub/Sub so this rules out App Engine Standard
Ref: https://cloud.google.com/appengine/docs/standard/nodejs/writing-and-responding-to-pub-sub-messages

`Cloud Run.` **is not right.**
Cloud Run is an excellent product and integrates with Cloud Pub/Sub for several use cases. For example, every time a new .csv file is created inside a Cloud Storage bucket, an event is fired and delivered via a Pub/Sub subscription to a Cloud Run service. The Cloud Run service extracts data from the file and stores it as structured data into a BigQuery table.
Ref: https://cloud.google.com/run#section-7
At the same time, we want to follow Google recommended practices. Google doesn't list integration with Cloud Pub/Sub as a key feature of Cloud Run. Contrary to this, Google says "If you're building a simple API (a small set of functions to be accessed via HTTP or Cloud Pub/Sub), we recommend using Cloud Functions."

`Cloud Functions.` **is the right answer.**
Cloud Functions is Google Cloud's event-driven serverless compute platform that lets you run your code locally or in the cloud without having to provision servers. Cloud Functions scales up or down, so you pay only for compute resources you use. Cloud Functions have excellent integration with Cloud Pub/Sub, lets you scale down to zero and is recommended by Google as the ideal serverless platform to use when dependent on Cloud Pub/Sub.
"If you're building a simple API (a small set of functions to be accessed via HTTP or Cloud Pub/Sub), we recommend using Cloud Functions."
Ref: https://cloud.google.com/serverless-options

Question 7:

Skipped

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

- ○

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

  (Correct)

- ○

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

- ○

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

- ○

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

Explanation

`gsutil mb -l us-west2 -s nearline --retention 10y gs://logs-archive.` **is not right.**

This command creates a bucket that uses nearline storage class whereas we want to use Coldline storage class.

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

`gsutil mb -l los-angeles -s coldline --retention 10m gs://logs-archive.` **is not right.**

This command uses los-angeles as the location but los-angeles is not a supported region name. The region name for Los Angeles is us-west-2.

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

`gsutil mb -l us-west2 -s coldline --retention 10m gs://logs-archive.` **is not right.**

This command creates a bucket with retention set to 10 months whereas we want to retain the objects for 10 years.

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

`gsutil mb -l us-west2 -s coldline --retention 10y gs://logs-archive.` **is the right answer.**

This command correctly creates a bucket in Los Angeles, uses Coldline storage

class and retains objects for 10 years.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/mb

Question 8:

Skipped

You developed a web application that lets users upload and share images. You deployed this application in Google Compute Engine and you have configured Stackdriver Logging. Your application sometimes times out while uploading large images, and your application generates relevant error log entries which are ingested to Stackdriver Logging. You would now like to create alerts based on these metrics. You intend to add more compute resources manually when the number of failures exceeds a threshold. What should you do in order to alert based on these metrics with minimal effort?

- ○

  In Stackdriver Logging, create a custom monitoring metric from log data and create an alert in Stackdriver based on the new metric.

  (Correct)

- ○

  In Stackdriver logging, 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.

- ○

  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.

- ○

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

Explanation

`In Stackdriver logging, 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.` **is not right.**
You don't need to edit the application code to send the metric values. The application already pushes error logs whenever the application times out. Since you already have the required entries in the Stackdriver logs, you don't need to edit the application code to send the metric values. You just need to create metrics from log

data.
Ref: https://cloud.google.com/logging

`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.` **is not right.**
You don't create a custom monitoring metric in code. Stackdriver Logging allows you to easily create metrics from log data. Since the application already pushes error logs to Stackdriver Logging, we just need to create metrics from log data in Stackdriver Logging.
Ref: https://cloud.google.com/logging

`Add the Stackdriver monitoring and logging agent to the instances running the code.` **is not right.**
The Stackdriver Monitoring agent gathers system and application metrics from your VM instances and sends them to Monitoring. In order to make use of this approach, you need application metrics but our application doesn't generate metrics. It just logs errors whenever the upload times out and these are then ingested to Stackdriver logging. We can update our application to enable custom metrics for these scenarios, but that is a lot more work than creating metrics from log data in Stackdriver Logging
Ref: https://cloud.google.com/logging

`In Stackdriver Logging, create a custom monitoring metric from log data and create an alert in Stackdriver based on the new metric.` **is the right answer.**
Our application adds entries to error logs whenever the application times out during image upload and these logs are ingested to Stackdriver Logging. Since we already have the required data in logs, we just need to create metrics from this log data in Stackdriver Logging. And we can then set up an alert based on this metric. We can trigger an alert if the number of occurrences of the relevant error message is greater than a predefined value. Based on the alert, you can manually add more compute resources.
Ref: https://cloud.google.com/logging

Question 9:

Skipped

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

- ○

  Import data into Google Cloud SQL.

- ○

  Import data into Google BigQuery.

  (Correct)

- ○

  Import flat files into Google Cloud Storage.

- ○

  Import data into Google Cloud Datastore.

Explanation

`Import data into Google Cloud SQL.` **is not right.**
Cloud SQL is a fully-managed relational database service. It supports MySQL so the migration of data from your data center to cloud can be straightforward but Google Cloud SQL cannot handle petabyte-scale data. The current second-generation instances limit the storage to approximately 30TB.
Ref: https://cloud.google.com/sql#overview
Ref: https://cloud.google.com/sql/docs/quotas

`Import flat files into Google Cloud Storage.` **is not right.**
Cloud Storage is a service for storing objects in Google Cloud. You store objects in containers called buckets. You could export the MySQL data into files and import them into Google Cloud Storage, but it doesn't offer an SQL Interface to run queries/reports.
Ref: https://cloud.google.com/storage/docs/introduction

`Import data into Google Cloud Datastore.` **is not right.**
Your business analysts are already familiar with SQL Interface so we need a service that supports SQL. However, Cloud Datastore is a NoSQL document database. Cloud Datastore doesn't support SQL (it supports GQL which is similar to SQL, but not identical).
Ref: https://cloud.google.com/datastore/docs/reference/gql_reference
Ref: https://cloud.google.com/datastore/docs/concepts/overview

`Import data into Google BigQuery.` **is the right answer.**
Bigquery is a petabyte-scale serverless, highly scalable, and cost-effective cloud data warehouse that offers blazing-fast speeds, and with zero operational overhead. BigQuery supports a standard SQL dialect that is ANSI:2011 compliant, which

reduces the impact and enables a seamless transition for your business analysts.
Ref: https://cloud.google.com/bigquery

Question 10:

Skipped

Your company wants to move 200 TB of your website clickstream logs from your on premise data center to Google Cloud Platform. These logs need to be retained in GCP for compliance requirements. Your business analysts also want to run analytics on these logs to understand user click behaviour on your website. Which of the below would enable you to meet these requirements? (Select Two)

- □

  Insert logs into Google Cloud Bigtable.

- □

  Load logs into Google BigQuery.

  (Correct)

- □

  Upload log files into Google Cloud Storage.

  (Correct)

- □

  Import logs into Google Stackdriver.

- □

  Load logs into Google Cloud SQL.

Explanation

`Load logs into Google Cloud SQL.` **is not right.**

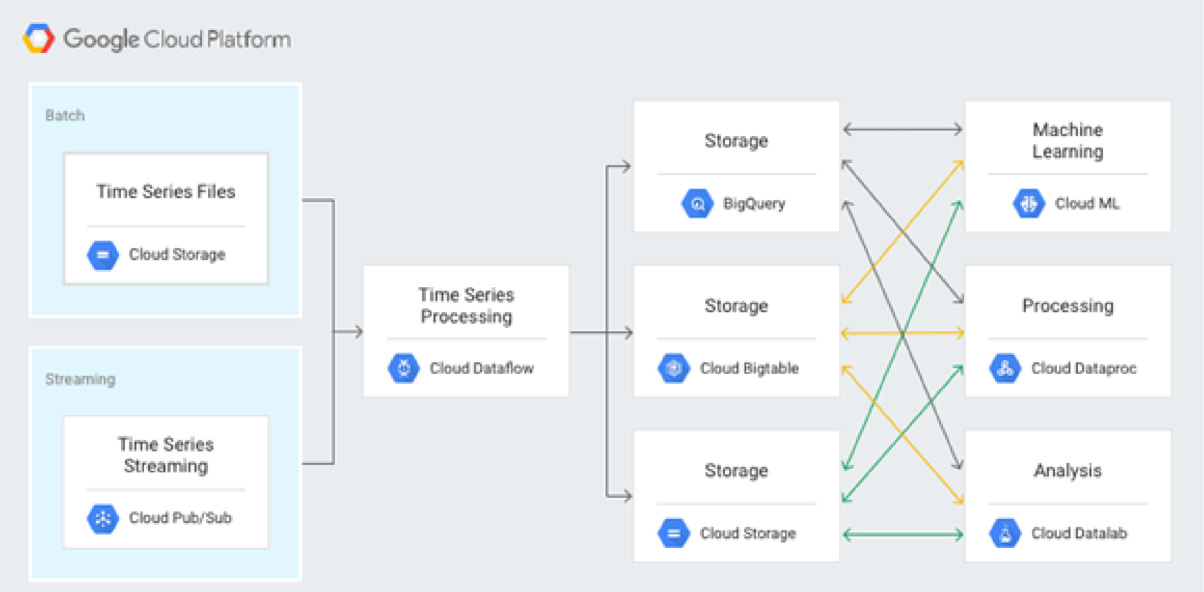
Cloud SQL is a fully-managed relational database service. Storing logs in Google Cloud SQL is very expensive. Cloud SQL doesn't help us with analytics. Moreover, Google Cloud Platform offers several storage classes in Google Cloud Storage that are more apt for storing logs at a much cheaper cost.
Ref: https://cloud.google.com/sql/docs
Ref: https://cloud.google.com/sql/pricing#sql-storage-networking-prices
Ref: https://cloud.google.com/storage/pricing

`Import logs into Google Stackdriver.` **is not right.**

You can push custom logs to Stackdriver and set custom retention periods to store

the logs for longer durations. However, Stackdriver doesn't help us with analytics. You could create a sink and export data into Cloud BigQuery for analytics but that is more work. Moreover, Google Cloud Platform offers several storage classes in Google Cloud Storage that are more apt for storing logs at a much cheaper cost.
Ref: https://cloud.google.com/logging
Ref: https://cloud.google.com/storage/pricing

`Insert logs into Google Cloud Bigtable.` **is not right.**
Cloud Bigtable is a petabyte-scale, fully managed NoSQL database service for large analytical and operational workloads. Storing data in Bigtable (approx $0.17/GB + $0.65/hr per node) is very expensive compared to storing data in Cloud Storage (approx $0.02/GB in standard storage class) - which can go down further if you transition to Nearline/Coldline after running analytics.
Ref: https://cloud.google.com/bigtable/



`Upload log files into Google Cloud Storage.` **is the right answer.**
Google Cloud Platform offers several storage classes in Google Cloud Storage that are suitable for storing/archiving logs at a reasonable cost. GCP recommends you use

Standard storage class if you need to access objects frequently

Nearline storage class if you access infrequently i.e. once a month

Coldline storage class if you access even less frequently e.g. once a quarter

Archive storage for logs archival.

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

`Load logs into Google BigQuery.` **is the right answer.**

By loading logs into Google BigQuery, you can securely run and share analytical insights in your organization with a few clicks. BigQuery's high-speed streaming insertion API provides a powerful foundation for real-time analytics, making your latest business data immediately available for analysis.

Ref: https://cloud.google.com/bigquery#marketing-analytics

Question 11:

Skipped

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

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

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

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

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

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

kubectl run creates and runs a deployment. It creates a deployment or a job to manage the created container(s). It is not possible to use kubectl run to connect to an existing container.
https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#run

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

While kubectl exec is used to execute a command in a container, the command above doesn't quite work because we haven't passed to it the identifier of the container.
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#exec

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

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

Question 12:

Skipped

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

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

`Set up a stack driver alert to detect slowness in the application. When the alert is triggered, increase nodes in the cluster by running the command gcloud container clusters resize CLUSTER_Name --size {new size}.` **is not right.**

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

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

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

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

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

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

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

Question 13:

Skipped

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

- ○

  Cloud Datastore database.

- ○

  Persistent SSD on VM instances.

- ○

  Cloud Filestore.

- ○

  Multiregional Cloud Storage bucket.

  (Correct)

Explanation

`Cloud Datastore database.` **is not right.**

Cloud Datastore is a NoSQL document database built for automatic scaling, high performance, and ease of application development. We want to store objects/files and Cloud Datastore is not a suitable storage option for such data.
Ref: https://cloud.google.com/datastore/docs/concepts/overview

`Cloud Filestore.` **is not right.**

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

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

`Persistent SSD on VM instances.` **is not right.**
Persistent SSD is a regional service and doesn't automatically scale to other regions to support a worldwide user base. Moreover, Persistent SSD disks are very expensive. A regional persistent SSD costs $0.34 per GB per month. In comparison, Google Cloud Storage offers several storage classes that are significantly cheaper.
Ref: https://cloud.google.com/persistent-disk
Ref: https://cloud.google.com/filestore/pricing

`Multiregional Cloud Storage bucket.` **is the right answer.**
Cloud Storage allows world-wide storage and retrieval of any amount of data at any time. We don't need to set up auto-scaling ourselves. Cloud Storage autoscaling is managed by GCP. Cloud Storage is an object store so it is suitable for storing photos. Cloud Storage allows world-wide storage and retrieval so cater well to our worldwide audience. Cloud storage provides us lifecycle rules that can be configured to automatically delete objects older than 30 days. This also fits our requirements. Finally, Google Cloud Storage offers several storage classes such as Nearline Storage ($0.01 per GB per Month) Coldline Storage ($0.007 per GB per Month) and Archive Storage ($0.004 per GB per month) which are significantly cheaper than any of the options above.
Ref: https://cloud.google.com/storage/docs
Ref: https://cloud.google.com/storage/pricing

Question 14:

Skipped

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

You created the kubernetes resources by running

```
kubectl apply -f app-deployment.yaml
kubectl apply -f app-service.yaml
```

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

- ○

  Modify the current configuration of the deployment by using kubectl edit to open the YAML file of the current configuration, modify and save the

configuration. kubectl edit deployment/app-deployment -o yaml --save-config

- ○

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

- ○

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

- ○

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

(Correct)

Explanation

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

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

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

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

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

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

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

Like the above, the outcome is the same. This is equivalent to first getting the

resource, editing it in a text editor, and then applying the resource with the updated version. This approach doesn't update the replicas change in our local YAML file. If you were to make some changes in your local app-deployment.yaml and apply it, the update would scale back the replicas to 2. This is undesirable.
Ref: https://kubernetes.io/docs/concepts/cluster-administration/manage-deployment/#in-place-updates-of-resources

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

Question 15:

Skipped

You created a cluster.yaml file containing

```
resources:
- name: cluster
type: container.v1.cluster
properties:
    zone: europe-west1-b
    cluster:
    description: "My GCP ACE cluster"
    initialNodeCount: 2
```

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

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

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

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

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

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

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

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

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

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

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

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

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

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

Question 16:

Skipped

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

- ○

  The external IP address is disabled.

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

`The compute instances have a static IP for their external IP.` **is not right.**
Not having a static IP is not a reason for failed SSH connections. When the firewall rules are set up correctly, SSH works fine on compute instances having ephemeral IP Address.

`The external IP address is disabled.` **is not right.**
Our question states SSH doesn't work on external IP addresses so it is safe to assume they already have an external IP. Therefore, this option is not correct.

`The compute instances are not using the right cross-region SSH IAM permissions.` **is not right.**
There is no such thing as cross region SSH IAM permissions.

`The combination of compute instance network tags and VPC firewall rules only allow SSH from the subnets IP range.` **is the right answer.**
The combination of compute instance network tags and VPC firewall rules can certainly result in SSH traffic being allowed from only subnets IP range. The firewall rule can be configured to allow SSH traffic from just the VPC range e.g. 10.0.0.0/8. In this scenario, all SSH traffic from within the VPC is accepted but external SSH traffic is blocked.
Ref: https://cloud.google.com/vpc/docs/using-firewalls

Question 17:

Skipped

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

- □

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

- □

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

  (Correct)

- □

  Use gsutil with -o "GSUtil:encryption_key=[KEY_RESOURCE]" when uploading objects to the bucket.

  (Correct)

- □

  Modify .boto configuration to include encryption_key = [KEY_RESOURCE] when uploading objects to bucket.

  (Correct)

- □

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

Explanation

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

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

`Use gsutil with --encryption-key=[ENCRYPTION_KEY] when uploading objects to the bucket.` **is not right.**

gsutil doesn't accept the flag --encryption-key. gsutil can be set up to use an encryption key by modifying boto configuration or by specifying a top-level -o flag

but neither of these is included in this option.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

`In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key.` **is the right answer.**
Our compliance department wants us to use customer-managed encryption keys. We can select Customer-Managed radio and provide a cloud KMS encryption key to encrypt objects with the customer managed key. This fit our requirements.

`Use gsutil with -o "GSUtil:encryption_key=[KEY_RESOURCE]" when uploading objects to the bucket.` **is the right answer.**
We can have gsutil use an encryption key by using the -o top-level flag: -o "GSUtil:encryption_key=[KEY_RESOURCE]".
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key

`Modify .boto configuration to include encryption_key = [KEY_RESOURCE] when uploading objects to bucket.` **is the right answer.**
As an alternative to the -o top-level flag, gsutil can also use an encryption key if .boto configuration is modified to specify the encryption key.

```
encryption_key = [KEY_RESOURCE]
```

Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-object-key
Question 18:
Skipped
You have a web application deployed as a managed instance group based on an instance template. You modified the startup script used in the instance template and would like the existing instances to pick up changes from the new startup scripts. Your web application is currently serving live web traffic. You want to propagate the startup script changes to all instances in the managed instances group while minimizing effort, minimizing cost and ensuring that the available capacity does not decrease. What would you do?

- ○

  Delete instances in the managed instance group (MIG) one at a time and rely on autohealing to provision an additional instance.

- ○

  Create a new managed instance group (MIG) based on a new template. Add the group to the backend service for the load balancer. When all instances in the new managed instance group are healthy, delete the old managed instance group

- ○

  Perform a rolling-action replace with max-unavailable set to 0 and max-surge set to 1

  (Correct)

- ○

  Perform a rolling-action start-update with max-unavailable set to 1 and max-surge set to 0

Explanation

`Perform a rolling-action start-update with max-unavailable set to 1 and max-surge set to 0.` **is not right.**

You can carry out a rolling action start update to fully replace the template by executing a command like

```
gcloud compute instance-groups managed rolling-action start-update instance-gr
oup-1 --zone=us-central1-a --version template=instance-template-1 --canary-ver
sion template=instance-template-2,target-size=100%
```

which updates the instance-group-1 to use instance-template-2 instead of instance-template-1 and have instances created out of instance-template-2 serve 100% of traffic. However, the values specified for maxSurge and maxUnavailable mean that we will lose capacity which is against our requirements.

maxSurge specifies the maximum number of instances that can be created over the desired number of instances. If maxSurge is set to 0, the rolling update can not create additional instances and is forced to update existing instances. This results in a reduction in capacity and therefore does not satisfy our requirement to ensure that the available capacity does not decrease during the deployment.

maxUnavailable - specifies the maximum number of instances that can be unavailable during the update process. When maxUnavailable is set to 1, the rolling update updates 1 instance at a time. i.e. it takes 1 instance out of service, updates it, and puts it back into service. This results in a reduction in capacity while the instance is out of service. Example - if we have 10 instances in service, this combination of setting results in 1 instance at a time taken out of service for replacement while the remaining 9 continue to serve live traffic. That's a reduction of 10% in available capacity.
Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#max-unavailable
Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#max-surge

`Create a new managed instance group (MIG) based on a new template. Add the group to the backend service for the load balancer. When all` `instances in the new managed instance group are healthy, delete the old managed instance group.` **is not right.**

While the end result is the same, we have a period of time where the traffic is served by instances from both the old managed instances group (MIG) which doubles our cost and increases effort and complexity.

`Delete instances in the managed instance group (MIG) one at a time and rely on auto-healing to provision an additional instance.` **is not right.**

While this would result in the same eventual outcome, there are two issues with this approach. First, deleting an instance one at a time would result in a reduction in capacity which is against our requirements. Secondly, deleting instances manually one at a time is error-prone and time-consuming. One of our requirements is to "minimize the effort" but deleting instances manually and relying on auto-healing health checks to provision them back is time-consuming and could take a lot of time depending on the number of instances in the MIG and the startup scripts executed during bootstrap.

`Perform a rolling-action replace with max-unavailable set to 0 and max-surge set to 1.` **is the right answer.**

This option achieves the outcome in the most optimal manner. The replace action is used to replace instances in a managed instance group. When maxUnavailable is set to 0, the rolling update can not take existing instances out of service. And when maxSurge is set to 1, we let the rolling update spin a single additional instance. The rolling update then puts the additional instance into service and takes one of the existing instances out of service for replacement. There is no reduction in capacity at any point in time.

Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#max-unavailable
Ref: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/#max-surge
Ref: https://cloud.google.com/sdk/gcloud/reference/alpha/compute/instance-groups/managed/rolling-action/replace

Question 19:

Skipped

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

```
steps:
- name: 'gcr.io/cloud-builders/docker'
args: ['build', '-t', 'gcr.io/[PROJECT_ID]/[IMAGE_NAME]', '.']
images: ['gcr.io/[PROJECT_ID]/[IMAGE_NAME]']
```

How should you execute cloud build to satisfy these requirements?

- ○

  Execute gcloud builds submit --config=[CONFIG_FILE_PATH] --gcs-log-dir=[GCS_LOG_DIR] [SOURCE]

  (Correct)

- ○

  Execute gcloud builds submit --config=[CONFIG_FILE_PATH] [SOURCE]

- ○

  Execute gcloud builds push --config=[CONFIG_FILE_PATH] [SOURCE]

- ○

  Execute gcloud builds run --config=[CONFIG_FILE_PATH] --gcs-log-dir=[GCS_LOG_DIR] [SOURCE]

Explanation

`Execute gcloud builds push --config=[CONFIG_FILE_PATH] [SOURCE].` **is not right.**
gcloud builds command does not support push operation. The correct operation to build images and push them to gcr is submit.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

`Execute gcloud builds run --config=[CONFIG_FILE_PATH] --gcs-log-dir=[GCS_LOG_DIR] [SOURCE].` **is not right.**
gcloud builds command does not support run operation. The correct operation to build images and push them to gcr is submit.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

`Execute gcloud builds submit --config=[CONFIG_FILE_PATH] [SOURCE].` **is not right.**
This command correctly builds the container image and pushes the image to GCR (Google Container Registry) but doesn't upload the build logs to a specific GCS bucket. If --gcs-log-dir is not set, gs://[PROJECT_NUMBER].cloudbuild-logs.googleusercontent.com/ will be created and used.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit
Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

`Execute gcloud builds submit --config=[CONFIG_FILE_PATH] --gcs-log-dir=[GCS_LOG_DIR] [SOURCE].` **is the right answer.**
This command correctly builds the container image, pushes the image to GCR (Google Container Registry) and uploads the build logs to Google Cloud Storage.

--config flag specifies the YAML or JSON file to use as the build configuration file.
--gcs-log-dir specifies the directory in Google Cloud Storage to hold build logs.

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

Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit
Ref: https://cloud.google.com/cloud-build/docs/building/build-containers

Question 20:

Skipped

You have two Kubernetes resource configuration files.

```
1. deployment.yaml - creates a deployment
2. service.yaml - sets up a LoadBalancer service to expose the pods.
```

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

- □

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

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

  3. kubectl apply -f deployment.yaml

  4. kubectl apply -f service.yaml

- □

  1. gcloud config set compute/zone us-central1-a

  2. gcloud container clusters create cluster-1

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

  4. kubectl apply -f deployment.yaml

  5. kubectl apply -f service.yaml

- □

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

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

  3. kubectl apply -f deployment.yaml,service.yaml

- □

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

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

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

  (Correct)

- □

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

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

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

  (Correct)

Explanation

`1. gcloud container clusters create cluster-1 --zone=us-central1-a`
`2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a`
`3. kubectl apply -f deployment.yaml`
`4. kubectl apply -f service.yaml.` **is not right (i.e. commands executes successfully)**

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

Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/create
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/get-credentials
Ref: https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands#apply

`1. gcloud container clusters create cluster-1 --zone=us-central1-a`
`2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a`
`3. kubectl apply -f deployment.yaml,service.yaml.` **is not right (i.e. commands executes successfully)**

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

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

```
1. gcloud config set compute/zone us-central1-a
2. gcloud container clusters create cluster-1
3. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
4. kubectl apply -f deployment.YAML
5. kubectl apply -f service.yaml.
```

is not right (i.e. commands executes successfully)

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

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

```
1. gcloud container clusters create cluster-1 --zone=us-central1-a
2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
3. kubectl apply -f [deployment.yaml,service.yaml].
```

is the right answer (i.e. commands fail)

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

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

```
1. gcloud container clusters create cluster-1 --zone=us-central1-a
2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
3. kubectl apply -f deployment.yaml&&service.yaml.
```

is the right answer (i.e. commands fail)

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

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

Question 21:

Skipped

Your company stores customer PII data in Cloud Storage buckets. A subset of this data is regularly imported into a BigQuery dataset to carry out analytics. You want to make sure the access to this bucket is strictly controlled. Your analytics team needs read access on the bucket so that they can import data in BigQuery. Your operations team needs read/write access to both the bucket and BigQuery dataset to add Customer PII data of new customers on an ongoing basis. Your Data Vigilance officers need Administrator access to the Storage bucket and BigQuery dataset. You want to follow Google recommended practices. What should you do?

- ○

  Use the appropriate predefined IAM roles for each of the access levels needed for Cloud Storage and BigQuery. Add your users to those roles for each of the services.

  (Correct)

- ○

  Create 3 custom IAM roles with appropriate permissions for the access levels needed for Cloud Storage and BigQuery. Add your users to the appropriate roles.

- ○

  At the Organization level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.

- ○

  At the Project level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.

Explanation

`At the Organization level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.` **is not right.**

Google recommends we apply the security principle of least privilege, where we grant only necessary permissions to access specific resources.
Ref: https://cloud.google.com/iam/docs/overview
Providing these primitive roles at the organization levels grants them permissions on all resources in all projects under the organization which violates the security

principle of least privilege.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`At the Project level, add your Data Vigilance officers user accounts to the Owner role, add your operations team user accounts to the Editor role, and add your analytics team user accounts to the Viewer role.` **is not right.**
Google recommends we apply the security principle of least privilege, where we grant only necessary permissions to access specific resources.
Ref: https://cloud.google.com/iam/docs/overview
Providing these primitive roles at the project level grants them permissions on all resources in the project which violates the security principle of least privilege.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Create 3 custom IAM roles with appropriate permissions for the access levels needed for Cloud Storage and BigQuery. Add your users to the appropriate roles.` **is not right.**
While this has the intended outcome, it is not very efficient particularly when there are predefined roles that can be used. Secondly, if Google adds/modifies permissions for these services in the future, we would have to update our roles to reflect the modifications. This results in operational overhead and increases costs.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles#primitive-roles-intrinsic
Ref: https://cloud.google.com/bigquery/docs/access-control

`Use the appropriate predefined IAM roles for each of the access levels needed for Cloud Storage and BigQuery. Add your users to those roles for each of the services.` **is the right answer.**
For Google Cloud Storage service, Google provides predefined roles roles/owner, roles/editor, roles/viewer that match the access levels we need. Similarly, Google provides the roles roles/bigquery.dataViewer, roles/bigquery.dataOwner, roles/bigquery.admin that match the access levels we need. We can assign these predefined IAM roles to the respective users. Should Google add/modify permissions for these services in the future, we don't need to modify the roles above as Google does this for us; and this helps future proof our solution.
Ref: https://cloud.google.com/storage/docs/access-control/iam-roles#primitive-roles-intrinsic
Ref: https://cloud.google.com/bigquery/docs/access-control

Question 22:
Skipped
Your company plans to store sensitive PII data in a cloud storage bucket. Your compliance department has asked you to ensure the objects in this bucket are encrypted by customer managed encryption keys. What should you do?

- ○

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

- ○

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

(Correct)

- ○

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

- ○

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

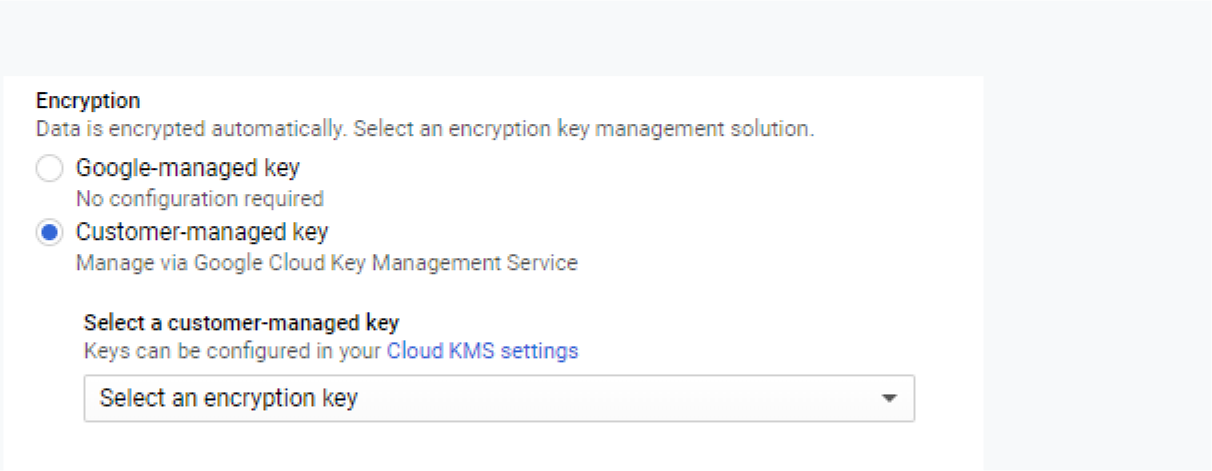
Explanation

`In the bucket advanced settings, select Customer-supplied key and then select a Cloud KMS encryption key.` **is not right.**
Customer-Supplied key is not an option when selecting the encryption method in the console. Moreover, we want to use customer managed encryption keys and not customer supplied encryption keys. This does not fit our requirements.

`In the bucket advanced settings, select Google-managed key and then select a Cloud KMS encryption key.` **is not right.**
While Google-managed key is an option when selecting the encryption method in console, we want to use customer managed encryption keys and not Google Managed encryption keys. This does not fit our requirements.

`Recreate the bucket to use a Customer-managed key. Encryption can only be specified at the time of bucket creation.` **is not right.**
Bucket encryption can be changed at any time. The bucket doesn't have to be recreated to change encryption.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

`In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key.` **is the right answer.**
This option correctly selects the Customer-managed key and then the key to use which satisfies our requirement. See the screenshot below for reference.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key



Encryption

Data is encrypted automatically. Select an encryption key management solution.

○ Google-managed key
No configuration required

● Customer-managed key
Manage via Google Cloud Key Management Service

Select a customer-managed key
Keys can be configured in your Cloud KMS settings

Select an encryption key

Question 23:

Skipped

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

- ○

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

- ○

  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.

- ○

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

- ○

  Use the gcloud compute ssh command.

  (Correct)

Explanation

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

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

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

`Run gcloud compute instances list to get the IP address of the instance, then use the ssh command.` **is not right.**
We can get the IP of the instance by executing the gcloud compute instances list but unless an SSH is generated and updated in project metadata, you would not be able to SSH to the instance. User access to a Linux instance through third-party tools is determined by which public SSH keys are available to the instance. You can control the public SSH keys that are available to a Linux instance by editing metadata, which is where your public SSH keys and related information are stored.
Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#block-project-keys

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

Question 24:

Skipped

In Cloud Shell, your active gcloud configuration is as shown below.

```
$ gcloud config list
[component_manager]
disable_update_check = True
```

```
[compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False
project = gcp-ace-lab-266520
[metrics]
environment = devshell
```

You want to create two compute instances - one in europe-west2-a and another in europe-west2-b. What should you do? (Select 2)

- □

  gcloud compute instances create instance1

  gcloud configuration set compute/zone europe-west2-b

  gcloud compute instances create instance2

- □

  gcloud compute instances create instance1

  gcloud compute instances create instance2

- □

  gcloud compute instances create instance1

  gcloud config set zone europe-west2-b

  gcloud compute instances create instance2

- □

  gcloud compute instances create instance1

  gcloud config set compute/zone europe-west2-b

  gcloud compute instances create instance2

  (Correct)

- □

  gcloud compute instances create instance1

  gcloud compute instances create instance2 --zone=europe-west2-b

(Correct)

Explanation

`1. gcloud compute instances create instance1`

`2. gcloud compute instances create instance2.` **is not right.**

The default compute/zone property is set to europe-west2-a in the current gcloud configuration. Executing the two commands above would create two compute instances in the default zone i.e. europe-west2-a which doesn't satisfy our requirement.

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

`1. gcloud compute instances create instance1`

`2. gcloud config set zone europe-west2-b`

`3. gcloud compute instances create instance2.` **is not right.**

The approach is right but the syntax is wrong. gcloud config does not have a core/zone property. The syntax for this command is gcloud config set SECTION/PROPERTY VALUE. If SECTION is missing, SECTION is defaulted to core. We are effectively trying to run gcloud config set core/zone europe-west2-b but the core section doesn't have a property called zone, so this command fails.

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

`1. gcloud compute instances create instance1`

`2. gcloud configuration set compute/zone europe-west2-b`

`3. gcloud compute instances create instance2.` **is not right.**

Like above, the approach is right but the syntax is wrong. You want to set the default compute/zone property in gcloud configuration to europe-west2-b but it needs to be done via the command gcloud config set and not gcloud configuration set.

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

`1. gcloud compute instances create instance1`

`2. gcloud config set compute/zone europe-west2-b`

`3. gcloud compute instances create instance2.` **is the right answer.**

The default compute/zone property is europe-west2-a in the current gcloud configuration so executing the first gcloud compute instances create command creates the instance in europe-west2-a zone. Next, executing the gcloud config set compute/zone europe-west2-b changes the default compute/zone property in default configuration to europe-west2-b. Executing the second gcloud compute instances create command creates a compute instance in europe-west2-b which is what we want.

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

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

`1. gcloud compute instances create instance1`

`2. gcloud compute instances create instance2 --zone=europe-west2-b.` **is the right answer.**

The default compute/zone property is europe-west2-a in the current gcloud configuration so executing the first gcloud compute instances create command creates the instance in europe-west2-a zone. Next, executing the second gcloud compute instances create command with --zone property creates a compute instance in provided zone i.e. europe-west2-b instead of using the default zone from the current active configuration.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

Question 25:

Skipped

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

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

  Google DNS, Google CDN, SSL Proxy Load Balancer

Explanation

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

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

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

Finally, we need a load balancer to front the autoscaled managed instances group. Google recommends we use HTTP(S) Load Balancer for this requirement as "SSL

Proxy Load Balancing is intended for non-HTTP(S) traffic. For HTTP(S) traffic, we recommend that you use HTTP(S) Load Balancing."
Ref: https://cloud.google.com/load-balancing/docs/ssl

So `Google Domains, Cloud DNS, HTTP(S) Load Balancer` **is the right answer.**

Question 26:

Skipped

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

- ○

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

- ○

  kubectl get deployments --output=pods

- ○

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

- ○

  kubectl get pods -l "app=prod"

  (Correct)

Explanation

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

You can not retrieve pods from the Kubernetes cluster by using gcloud. You can list pods by using Kubernetes CLI - kubectl get pods.
Ref: https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/

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

You can not retrieve pods from the Kubernetes cluster by using gcloud. You can list pods by using Kubernetes CLI - kubectl get pods.
Ref: https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/

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

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

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

`kubectl get pods -l "app=prod".` **is the right answer.**
This command correctly lists pods that have the label app=prod. When creating the deployment, we used the label app=prod so listing pods that have this label retrieve the pods belonging to nginx deployments. You can list pods by using Kubernetes CLI - kubectl get pods.
Ref: https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/
Ref: https://kubernetes.io/docs/tasks/access-application-cluster/list-all-running-container-images/#list-containers-filtering-by-pod-label

Question 27:

Skipped

You want to list all the compute instances in zones us-central1-b and europe-west1-d. Which of the commands below should you run to retrieve this information?

- ○

  gcloud compute instances get --filter="zone:(us-central1-b)" and gcloud compute instances list --filter="zone:(europe-west1-d)" and combine the results.

- ○

  gcloud compute instances list --filter="zone:(us-central1-b europe-west1-d)"

  (Correct)

- ○

  gcloud compute instances get --filter="zone:(us-central1-b europe-west1-d)"

- ○

  gcloud compute instances list --filter="zone:(us-central1-b)" and gcloud compute instances list --filter="zone:(europe-west1-d)" and combine the results.

Explanation

`gcloud compute instances get --filter="zone:( us-central1-b europe-west1-d )".` **is not right.**

gcloud compute instances command does not support get action.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances

`gcloud compute instances get --filter="zone:( us-central1-b )" and gcloud compute instances list --filter="zone:( europe-west1-d )" and combine the results.` **is not right.**
gcloud compute instances command does not support get action.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances

`gcloud compute instances list --filter="zone:( us-central1-b )" and gcloud compute instances list --filter="zone:( europe-west1-d )" and combine the results.` **is not right.**
The first command retrieves compute instances from us-central1-b and the second command retrieves compute instances from europe-west1-d. The output from the two statements can be combined to create a full list of instances from us-central1-b and europe-west1-d, however, this is not efficient as it is a manual activity. Moreover, gcloud already provides the ability to list and filter on multiple zones in a single command.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

`gcloud compute instances list --filter="zone:( us-central1-b europe-west1-d )".` **is the right answer.**
gcloud compute instances list - lists Google Compute Engine instances. The output includes internal as well as external IP addresses. The filter expression --filter="zone:(us-central1-b europe-west1-d)" is used to filter instances from zones us-central1-b and europe-west1-d.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
Here's a sample output of the command.

```
$gcloud compute instances list

NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS

gke-cluster-1-default-pool-8c599c87-16g9 us-central1-a n1-standard-1 10.128.0.
8 35.184.212.227 RUNNING

gke-cluster-1-default-pool-8c599c87-36xh us-central1-b n1-standard-1 10.129.0.
2 34.68.254.220 RUNNING

gke-cluster-1-default-pool-8c599c87-lprq us-central1-c n1-standard-1 10.130.0.
13 35.224.96.151 RUNNING



$gcloud compute instances list --filter="zone:( us-central1-b europe-west1-d )
"

NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS

gke-cluster-1-default-pool-8c599c87-36xhus-central1-bn1-standard-110.129.0.234
.68.254.220RUNNING
```

Question 28:

Skipped

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

- ○

  1. gcloud regions list

  2. gcloud compute images list

- ○

  1. gcloud compute regions list

  2. gcloud images list

- ○

  1. gcloud compute regions list

  2. gcloud compute images list

  (Correct)

- ○

  1. gcloud regions list

  2. gcloud images list

Explanation

`1. gcloud regions list.`

`2. gcloud images list.` **is not right.**

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

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

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

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

`1. gcloud compute regions list`

`2. gcloud images list.` **is not right.**

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

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

`1. gcloud regions list`

`2. gcloud compute images list.` **is not right.**

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

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

`1. gcloud compute regions list`

`2. gcloud compute images list.` **is the right answer.**

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

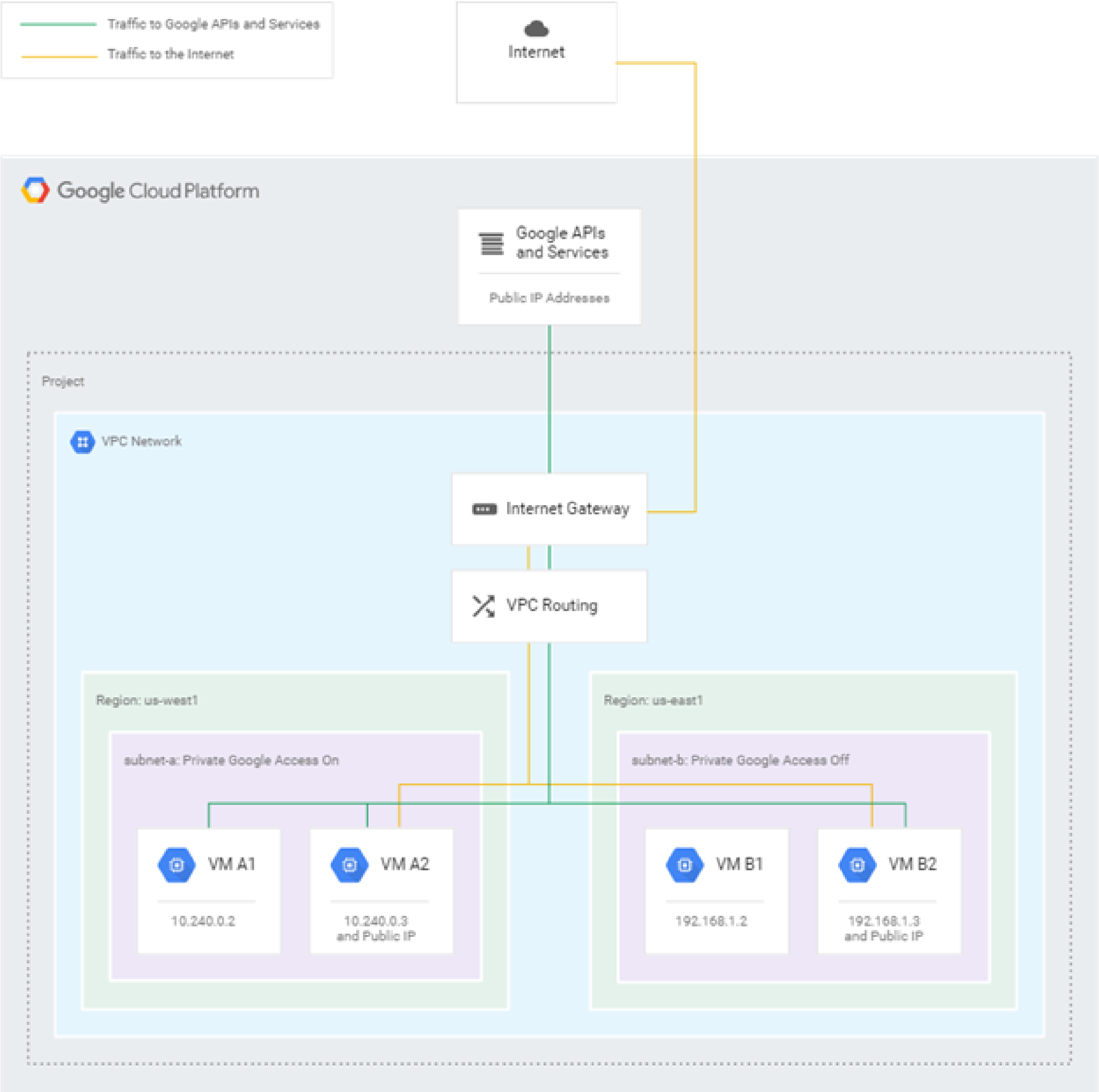
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/regions/list

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

Question 29:

Skipped

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



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

- ○

  VM A1, VM A2

- ○

  VM A1, VM A2, VM B1, VM B2

- ○

  VM A1, VM A2, VM B2

(Correct)

- ○

  VM A1, VM A2, VM B1

Explanation

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

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

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

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

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

Question 30:

Skipped

You deployed a number of services to Google App Engine Standard . The services are designed as microservices with several interdependencies between them. Most services have few version upgrades but some key services have over 20 version upgrades. You identified an issue with the service pt-createOrder and deployed a new version v3 for this service. You are confident this works and want this new version to receive all traffic for the service. You want to minimize effort and ensure availability of service. What should you do?

- ○

  Execute gcloud app versions stop v2 --service="pt-createOrder" and gcloud app versions start v3 --service="pt-createOrder"

- ○

  Execute gcloud app versions migrate v3 --service="pt-createOrder"

  (Correct)

- ○

Execute gcloud app versions stop v2 and gcloud app versions start v3

- ○

Execute gcloud app versions migrate v3

Explanation

`Execute gcloud app versions migrate v3.` **is not right.**

gcloud app versions migrate v3 migrates all services to version v3. In our scenario, we have multiple services with each service potentially being on a different version. We don't want to migrate all services to v3, instead, we only want to migrate the pt-createOrder service to v3.

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

`Execute gcloud app versions stop v2 --service="pt-createOrder" and gcloud app versions start v3 --service="pt-createOrder".` **is not right.**

Stopping version v2 and starting version v3 for pt-createOrder service would result in v3 receiving all traffic for pt-createOrder. While this is the intended outcome, stopping version v2 before starting version v3 results in service being unavailable until v3 is ready to receive traffic. As we want to "ensure availability", this option is not suitable.

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

`Execute gcloud app versions stop v2 and gcloud app versions start v3.` **is not right.**

Stopping version v2 and starting version v3 would result in migrating all services to version v3 which is undesirable. We don't want to migrate all services to v3, instead, we only want to migrate the pt-createOrder service to v3. Moreover, stopping version v2 before starting version v3 results in service being unavailable until v3 is ready to receive traffic. As we want to "ensure availability", this option is not suitable.

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

`Execute gcloud app versions migrate v3 --service="pt-createOrder".` **is the right answer.**

This command correctly migrates the service pt-createOrder to use version 3 and produces the intended outcome while minimizing effort and ensuring the availability of service.

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

Question 31:

Skipped

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

to connect to Google Cloud Storage and BigQuery and you want to do this in a secure way following Google recommended practices. What should you do?

- ○

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

- ○

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

- ○

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

- ○

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

  (Correct)

Explanation

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

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

Ref: https://cloud.google.com/compute/docs/access/service-accounts#default_service_account

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

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

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

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

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

The project editor role includes all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. Using a service account that

is over-privileged falls foul of the principle of least privilege. Google recommends you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Create a new service account, with editor permissions, generate and download a key. Use the key to authenticate inside the application.` **is not right.**
The project editor role includes all viewer permissions, plus permissions for actions that modify state, such as changing existing resources. Using a service account that is over-privileged falls foul of the principle of least privilege. Google recommends you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Create a new service account, grant it the least viable privileges to the required services, generate and download a JSON key. Use the JSON key to authenticate inside the application.` **is the right answer.**
Using a new service account with just the least viable privileges for the required services follows the principle of least privilege. To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. Once you have the key, you can use it in your application to authenticate connections to Cloud Storage and BigQuery.
Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys#creating_service_account_keys
Ref: https://cloud.google.com/iam/docs/recommender-overview

Question 32:
Skipped
You have asked your supplier to send you a purchase order and you want to enable them upload the file to a cloud storage bucket within the next 4 hours. Your supplier does not have a Google account. You want to follow Google recommended practices. What should you do?

- ○

  Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -m PUT -d 4h {JSON Key File} gs://{bucket}/.**

- ○

  Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 4h {JSON Key File} gs://{bucket}/.

- ○

Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m PUT -d 4h {JSON Key File} gs://{bucket}/.**

(Correct)

- ○

Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -httpMethod PUT -d 4h {JSON Key File} gs://{bucket}/.**

Explanation

`Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 4h {JSON Key File} gs://{bucket}/.` **is not right.**

This command creates signed URLs for retrieving existing objects. This command does not specify a HTTP method and in the absence of one, the default HTTP method is GET.

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

`Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -httpMethod PUT -d 4h {JSON Key File} gs://{bucket}/**.` **is not right.**

gsutil signurl does not accept -httpMethod parameter.

```
$ gsutil signurl -d 4h -httpMethod PUT keys.json gs://gcp-ace-lab-255520/*

CommandException: Incorrect option(s) specified. Usage:
```

The HTTP method can be provided through -m flag.

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

`Create a JSON key for the Default Compute Engine Service Account. Execute the command gsutil signurl -m PUT -d 4h {JSON Key File} gs://{bucket}/**.` **is not right.**

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

`Create a service account with just the permissions to upload files to the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -m PUT -d 4h {JSON Key File} gs://{bucket}/**.` **is the right answer.**

This command correctly creates a signed url that is valid for 4 hours and allows PUT

(through the -m flag) operations on the bucket. The supplier can then use the signed URL to upload a file to this bucket within 4 hours.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/signurl

Question 33:

Skipped

You developed an application that reads objects from a cloud storage bucket. You followed GCP documentation and created a service account with just the permissions to read objects from the cloud storage bucket. However, when your application uses this service account, it fails to read objects from the bucket. You suspect this might be an issue with the permissions assigned to the service account. You would like to authenticate a gsutil session with the service account credentials, reproduce the issue yourself and identify the root cause. How can you authenticate gsutil with service account credentials?

- ○

  Create JSON keys for the service account and execute gcloud auth service-account --key-file [KEY_FILE]

- ○

  Create JSON keys for the service account and execute gcloud authenticate activate-service-account --key-file [KEY_FILE]

- ○

  Create JSON keys for the service account and execute gcloud authenticate service-account --key-file [KEY_FILE]

- ○

  Create JSON keys for the service account and execute gcloud auth activate-service-account --key-file [KEY_FILE]

  (Correct)

Explanation

`Create JSON keys for the service account and execute gcloud authenticate activate-service-account --key-file [KEY_FILE].` **is not right.**
gcloud doesn't support using "authenticate" to grant/revoke credentials for Cloud SDK. The correct service is "auth".
Ref: https://cloud.google.com/sdk/gcloud/reference/auth

`Create JSON keys for the service account and execute gcloud authenticate service-account --key-file [KEY_FILE].` **is not right.**
gcloud doesn't support using "authenticate" to grant/revoke credentials for Cloud

SDK. The correct service is "auth".
Ref: https://cloud.google.com/sdk/gcloud/reference/auth

`Create JSON keys for the service account and execute gcloud auth service-account --key-file [KEY_FILE].` **is not right.**
gcloud auth does not support service-account action. The correct action to authenticate a service account is activate-service-account.
Ref: https://cloud.google.com/sdk/gcloud/reference/auth/activate-service-account

`Create JSON keys for the service account and execute gcloud auth activate-service-account --key-file [KEY_FILE].` **is the right answer.**
This command correctly authenticates access to Google Cloud Platform with a service account using its JSON key file. To allow gcloud (and other tools in Cloud SDK) to use service account credentials to make requests, use this command to import these credentials from a file that contains a private authorization key, and activate them for use in gcloud
Ref: https://cloud.google.com/sdk/gcloud/reference/auth/activate-service-account

Question 34:
Skipped
You have a web application deployed as a managed instance group. You noticed some of the compute instances are running low on memory. You suspect this is due to JVM memory leak and you want to restart the compute instances to reclaim the leaked memory. Your web application is currently serving live web traffic. You want to ensure that the available capacity does not go below 80% at any time during the restarts and you want to do this at the earliest. What would you do?

- ○

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

- ○

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

- ○

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

- ○

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

  (Correct)

Explanation

`Perform a rolling-action reboot with max-surge set to 20%.` **is not right.**
reboot is not a supported action for rolling updates. The supported actions are replace, restart, start-update and stop-proactive-update.
Ref: https://cloud.google.com/sdk/gcloud/reference/beta/compute/instance-groups/managed/rolling-action

`Perform a rolling-action replace with max-unavailable set to 20%.` **is not right.**
Performing a rolling-action replace - Replaces instances in a managed instance group. While this resolves the JVM memory leak issue, recreating the instances is a little drastic when the same result can be achieved with the simple restart action. One of our requirements is to "do this at the earliest " but recreating instances might take a lot of time depending on the number of instances and startup scripts; certainly more time than restart action.
Ref: https://cloud.google.com/sdk/gcloud/reference/beta/compute/instance-groups/managed/rolling-action

`Stop instances in the managed instance group (MIG) one at a time and rely on autohealing to bring them back up.` **is not right.**
While this would result in the same eventual outcome, it is manual, error-prone and time-consuming. One of our requirements is to "do this at the earliest" but stopping instances manually is time-consuming and could take a lot of time depending on the number of instances in the MIG. Also, relying on autohealing health checks to detect the failure and spin up the instance adds to the delay.

`Perform a rolling-action restart with max-unavailable set to 20%.` **is the right answer.**
This option achieves the outcome in the most optimal manner. The restart action restarts instances in a managed instance group. By performing a rolling restart with max-unavailable set to 20%, the rolling update restarts instances while ensuring there is at least 80% available capacity. The rolling update carries on restarting all the remaining instances until all instances in the MIG have been restarted.
Ref: https://cloud.google.com/sdk/gcloud/reference/alpha/compute/instance-groups/managed/rolling-action/restart

Question 35:

Skipped

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

- ○

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

- ○

Create a Read replica in a different region.

- ○

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

  (Correct)

- ○

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

Explanation

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

Read replicas do not provide failover capability. To provide failover capability, you need to configure Cloud SQL Instance for High Availability.
Ref: https://cloud.google.com/sql/docs/mysql/replication

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

Read replicas do not provide failover capability. To provide failover capability, you need to configure Cloud SQL Instance for High Availability.
Ref: https://cloud.google.com/sql/docs/mysql/replication

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

A Cloud SQL instance configured for HA is called a regional instance because it's primary and secondary instances are in the same region. They are located in different zones but within the same region. It is not possible to create a Failover replica in a different region.
Ref: https://cloud.google.com/sql/docs/mysql/high-availability

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

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

Question 36:

Skipped

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

```
$ gcloud config list

[component_manager]
disable_update_check = True
[compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False
project = gcp-ace-lab-266520
[metrics]
environment = devshell
```

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

- ○

  1. gcloud config set project gcp-ace-proj-266520

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

- ○

  1. gcloud compute instances delete instance1

  2. gcloud compute instances create instance1

- ○

  1. gcloud compute instances delete instance1

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

  3. gcloud compute instances create instance1

- ○

  1. gcloud compute instances delete instance1

  2. gcloud config set project gcp-ace-proj-266520

3. gcloud compute instances create instance1

(Correct)

Explanation

`1. gcloud compute instances delete instance1`

`2. gcloud compute instances create instance1.` **is not right.**

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

`1. gcloud config set project gcp-ace-proj-266520`

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

gcloud compute instances command doesn't support recreate action. It supports create/delete which is what we are supposed to use for this requirement.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances

`1. gcloud compute instances delete instance1`

`2. gcloud config set compute/project gcp-ace-proj-266520`

`3. gcloud compute instances create instance1.` **is not right.**

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

`1. gcloud compute instances delete instance1`

`2. gcloud config set project gcp-ace-proj-266520`

`3. gcloud compute instances create instance1.` **is the right answer.**

This sequence of commands correctly deletes the instance from gcp-ace-lab-266520 which is the default project in the active gcloud configuration, then modifies the current configuration to set the default project to gcp-ace-proj-266520, and finally creates the instance in the project gcp-ace-proj-266520 which is the default project in active gcloud configuration at the time of running the command. This produces the intended outcome of deleting the instance from gcp-ace-lab-266520 project and recreating it in gcp-ace-prod-266520
Ref: https://cloud.google.com/sdk/gcloud/reference/config/set
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/create
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/delete

Question 37:

Skipped

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

- ○

  gcloud app versions list --hide-no-traffic

  (Correct)

- ○

  gcloud app versions list --traffic

- ○

  gcloud app versions list

- ○

  gcloud app versions list --show-traffic

Explanation

`gcloud app versions list.` **is not right**

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

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

`gcloud app versions list --traffic.` **is not right**

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

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

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

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

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

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

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

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

Question 38:

Skipped

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

- ○

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

  2. gcloud app deploy --version=[NEW_VERSION]

  3. Validate [NEW_VERSION] in App Engine Flex

  4. gcloud app versions start [NEW_VERSION]

- ○

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

  2. gcloud app deploy --no-promote --version=[NEW_VERSION]

  3. Validate [NEW_VERSION] in App Engine Flex

  4. gcloud app versions start [NEW_VERSION]

- ○

  1. Set env: flex in app.yaml

  2. gcloud app deploy --version=[NEW_VERSION]

  3. Validate [NEW_VERSION] in App Engine Flex

  4. gcloud app versions migrate [NEW_VERSION]

- ○

  1. Set env: flex in app.yaml

  2. gcloud app deploy --no-promote --version=[NEW_VERSION]

  3. Validate [NEW_VERSION] in App Engine Flex

  4. gcloud app versions migrate [NEW_VERSION]

  (Correct)

Explanation

`1. Set env: flex in app.yaml`
`2. gcloud app deploy --version=[NEW_VERSION]`
`3. Validate [NEW_VERSION] in App Engine Flex`
`4. gcloud app versions migrate [NEW_VERSION].` **is not right.**

Executing gcloud app deploy --version=[NEW_VERSION] without --no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

`1. Set env: app-engine-flex in app.yaml`
`2. gcloud app deploy --version=[NEW_VERSION]`
`3. Validate [NEW_VERSION] in App Engine Flex`
`4. gcloud app versions start [NEW_VERSION]` **is not right.**

env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex. Also, Executing gcloud app deploy --version=[NEW_VERSION] without --no-promote would deploy the new version and immediately promote it to serve traffic. We don't want this version to receive traffic as we would like to validate the version first before sending it traffic.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

`1. Set env: app-engine-flex in app.yaml`
`2. gcloud app deploy --no-promote --version=[NEW_VERSION]`
`3. Validate [NEW_VERSION] in App Engine Flex`
`4. gcloud app versions start [NEW_VERSION]` **is not right.**

env: app-engine-flex is an invalid setting. The correct syntax for using the flex engine is env: flex.
Ref: https://cloud.google.com/sdk/gcloud/reference/app/versions/migrate

`1. Set env: flex in app.yaml`
`2. gcloud app deploy --no-promote --version=[NEW_VERSION]`
`3. Validate [NEW_VERSION] in App Engine Flex`
`4. gcloud app versions migrate [NEW_VERSION]` **is the right answer.**

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

Question 39:

Skipped

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

- ○

  Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --metadata-from-file startup-script=/scripts/install_app.sh

  (Correct)

- ○

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

- ○

  Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --startup-script=/scripts/install_app.sh

- ○

  Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --metadata-from-file startup-script-url=/scripts/install_app.sh

Explanation

`Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --startup-script=/scripts/install_app.sh.` **is not right.**

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

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

`Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --metadata-from-file startup-script-url=/scripts/install_app.sh.` **is not right.**

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

```
$ gcloud compute instance-templates create app-template --metadata-from-file s
tartup-script-url=/scripts/install_app.sh

ERROR: (gcloud.compute.instance-templates.create) Unable to read file [/script
s/install_app.sh]: [Errno 2] No such file or directory: '/scripts/install_app.
sh'
```

`Once the instance starts up, connect over SSH and install the application.` **is not right.**
The managed instances group has auto-scaling enabled. If we are to connect over SSH and install the application, we have to repeat this task on all current instances and on future instances the autoscaler adds to the group. This process is manual, error-prone, time consuming and should be avoided.

`Include a startup script to bootstrap the python application when creating instance template by running gcloud compute instance-templates create app-template --metadata-from-file startup-script=/scripts/install_app.sh.` **is the right answer.**
This command correctly provides the startup script using the flag metadata-from-file and providing a valid startup-script value. When creating compute engine images, the startup script can be provided through a special metadata key called startup-script which specifies a script that will be executed by the instances once they start running. For convenience, --metadata-from-file can be used to pull the value from a file.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instance-templates/create

Question 40:
Skipped
You have three gcloud configurations - one for each of development, test and production projects. You want to list all the configurations and switch to a new configuration. With the fewest steps possible, what's the fastest way to switch to the correct configuration?

- ○

  1. To list configurations - gcloud config configurations list

  2. To activate a configuration - gcloud config configurations activate.

  (Correct)

- ○

1. To list configurations - gcloud config list

2. To activate a configuration - gcloud config activate.

- ○

1. To list configurations - gcloud configurations list

2. To activate a configuration - gcloud configurations activate

- ○

1. To list configurations - gcloud configurations list

2. To activate a configuration - gcloud config activate

Explanation

`1. To list configurations - gcloud configurations list`
`2. To activate a configuration - gcloud configurations activate.` **is not right.**
gcloud configurations list does not list configurations. To list existing configurations, you need to execute gcloud config configurations list.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list gcloud configurations activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate

`1. To list configurations - gcloud config list`
`2. To activate a configuration - gcloud config activate.` **is not right.**
gcloud config list does not list configurations. It lists the properties of the existing configuration. To list existing configurations, you need to execute gcloud config configurations list.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list gcloud config activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate

`1. To list configurations - gcloud configurations list` `2. To activate a configuration - gcloud config activate.` **is not right.**
gcloud configurations list does not list configurations. To list existing configurations, you need to execute gcloud config configurations list.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list gcloud config activate does not activate a named configuration. To activate a configuration, you need to execute gcloud config configurations activate
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate

`1. To list configurations - gcloud config configurations list`
`2. To activate a configuration - gcloud config configurations activate.` **is the right answer.**

The two commands together achieve the intended outcome. gcloud config configurations list - lists existing named configurations and gcloud config configurations activate - activates an existing named configuration
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/list
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations/activate
See an example below

```
$ gcloud config configurations list

NAME IS_ACTIVE ACCOUNT PROJECT DEFAULT_ZONE DEFAULT_REGION

dev-configuration False gcp-ace-lab-dev

prod-configuration False gcp-ace-lab-prod

test-configuration True gcp-ace-lab-test


$ gcloud config configurations activate prod-configuration

Activated [prod-configuration].


$ gcloud config configurations list

NAME IS_ACTIVE ACCOUNT PROJECT DEFAULT_ZONE DEFAULT_REGION

dev-configuration False gcp-ace-lab-dev

prod-configuration True gcp-ace-lab-prod

test-configurationFalsegcp-ace-lab-test
```

Question 41:

Skipped

You have two Kubernetes resource configuration files.

```
1. deployment.yaml - creates a deployment
2. service.yaml - sets up a LoadBalancer service to expose the pods.
```

You don't have a GKE cluster in the development project and you need to provision one. Which of the commands below would you run in Cloud Shell to create a GKE cluster and deploy the yaml configuration files to create a deployment and service?

- ○

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

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

  3. gcloud gke apply -f deployment.yaml

4. gcloud gke apply -f service.yaml

- ○

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

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

  3. kubectl apply -f deployment.yaml

  4. kubectl apply -f service.yaml

  (Correct)

- ○

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

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

  3. kubectl deploy -f deployment.yaml

  4. kubectl deploy -f service.yaml

- ○

  1. kubectl container clusters create cluster-1 --zone=us-central1-a

  2. kubectl container clusters get-credentials cluster-1 --zone=us-central1-a

  3. kubectl apply -f deployment.yaml

  4. kubectl apply -f service.yaml

Explanation

`1. kubectl container clusters create cluster-1 --zone=us-central1-a`
`2. kubectl container clusters get-credentials cluster-1 --zone=us-central1-a`
`3. kubectl apply -f deployment.yaml`
`4. kubectl apply -f service.yaml.` **is not right.**

kubectl doesn't support kubectl container clusters create command. kubectl can not be used to create GKE clusters. To create a GKE cluster, you need to execute gcloud container clusters create command.
Ref: https://cloud.google.com/sdk/gcloud/reference/container/clusters/create

```
1. gcloud container clusters create cluster-1 --zone=us-central1-a
2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
3. kubectl deploy -f deployment.yaml
4. kubectl deploy -f service.yaml.
```

is not right.

kubectl doesn't support kubectl deploy command. The YAML file contains the cluster resource configuration. You don't create the configuration, instead, you apply the configuration to the cluster. The configuration can be applied by running kubectl apply command

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

```
1. gcloud container clusters create cluster-1 --zone=us-central1-a
2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
3. gcloud gke apply -f deployment.yaml
4. gcloud gke apply -f service.yaml.
```

is not right.

gcloud doesn't support gcloud gke apply command. The YAML file contains the cluster resource configuration. You don't create the configuration, instead, you apply the configuration to the cluster. The configuration can be applied by running kubectl apply command

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

```
1. gcloud container clusters create cluster-1 --zone=us-central1-a
2. gcloud container clusters get-credentials cluster-1 --zone=us-central1-a
3. kubectl apply -f deployment.yaml
4. kubectl apply -f service.yaml.
```

is the right answer.

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

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

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

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

Question 42:

Skipped

You have two workloads on GKE (Google Kubernetes Engine) - create-order and dispatch-order. create-order handles creation of customer orders; and dispatch-order handles dispatching orders to your shipping partner. Both create-order and

dispatch-order workloads have cluster autoscaling enabled. The create-order deployment needs to access (i.e. invoke web service of) dispatch-order deployment. dispatch-order deployment cannot be exposed publicly. How should you define the services?

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

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

When you create a Service of type LoadBalancer, the Google Cloud controller configures a network load balancer that is publicly available. Since we don't want our service to be publicly available, we shouldn't create a Service of type LoadBalancer
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/exposing-apps

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

When you create a Service of type LoadBalancer, the Google Cloud controller configures a network load balancer that is publicly available. Since we don't want our service to be publicly available, we shouldn't create a Service of type LoadBalancer
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/exposing-apps

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

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

`Create a Service of type ClusterIP for dispatch-order. Have create-order use the Service IP address.` **is the right answer.**
ClusterIP exposes the Service on a cluster-internal IP that is only reachable within the cluster. This satisfies our requirement that dispatch-order shouldn't be publicly accessible. create-order which is also located in the same GKE cluster can now access the ClusterIP of the service to reach dispatch-order.
Ref: https://kubernetes.io/docs/concepts/services-networking/service/

Question 43:
Skipped
Your company stores sensitive PII data in a cloud storage bucket. The objects are currently encrypted by Google-managed keys. Your compliance department has asked you to ensure all current and future objects in this bucket are encrypted by customer managed encryption keys. You want to minimize effort. What should you do?

- ○

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

  2. Existing objects encrypted by Google-managed keys can still be decrypted by the new Customer-managed key.

- ○

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

  2. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key.

  (Correct)

- ○

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

2. Delete all existing objects and upload them again so they use the new customer-supplied key for encryption.

- ○

  1. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key.

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

Explanation

`1. In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key. 2. Existing objects encrypted by Google-managed keys can still be decrypted by the new Customer-managed key.` **is not right.**
While changing the bucket encryption to use the Customer-managed key ensures all new objects use this key, existing objects are still encrypted by the Google-managed key. This doesn't satisfy our compliance requirements. Moreover, the customer managed key can't decrypt objects created by Google-managed keys.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

`1. In the bucket advanced settings, select customer-supplied key and then select a Cloud KMS encryption key. 2. Delete all existing objects and upload them again so they use the new customer-supplied key for encryption.` **is not right.**
The customer-supplied key is not an option when selecting the encryption method in the console. Moreover, we want to use customer-managed encryption keys and not customer-supplied encryption keys. This does not fit our requirements.

`1. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key. 2. In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key.` **is not right.**
While changing the bucket encryption to use the Customer-managed key ensures all new objects use this key, rewriting existing objects before changing the bucket encryption would result in the objects being encrypted by the encryption method in use at that point - which is still Google-managed.

`1. In the bucket advanced settings, select Customer-managed key and then select a Cloud KMS encryption key. 2. Rewrite all existing objects using gsutil rewrite to encrypt them with the new Customer-managed key.` **is the right answer.**

Changing the bucket encryption to use the Customer-managed key ensures all new objects use this key. Now that bucket encryption is changed to use the Customer-managed key, rewrite all existing objects using gsutil rewrite results in objects being encrypted by the new Customer-managed key. This is the only option that satisfies our requirements.
Ref: https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys#add-default-key

Question 44:

Skipped

You ran the following commands to create two compute instances.

```
gcloud compute instances create instance1
gcloud compute instances create instance2
```

Both compute instances were created in europe-west2-a zone but you want to create them in other zones. Your active gcloud configuration is as shown below.

```
$ gcloud config list

[component_manager]
disable_update_check = True
[compute]
gce_metadata_read_timeout_sec = 5
zone = europe-west2-a
[core]
account = gcp-ace-lab-user@gmail.com
disable_usage_reporting = False
project = gcp-ace-lab-266520
[metrics]
environment = devshell
```

You want to modify the gcloud configuration such that you are prompted for zone when you execute the create instance commands above. What should you do?

- ○

  gcloud config unset zone

- ○

  gcloud config set zone ""

- ○

  gcloud config unset compute/zone

  (Correct)

- ○

  gcloud config set compute/zone ""

Explanation

`gcloud config unset zone.` **is not right.**

gcloud config does not have a core/zone property. The syntax for this command is gcloud config unset SECTION/PROPERTY. If SECTION is missing from the command, SECTION is defaulted to core. We are effectively trying to run the command gcloud config unset core/zone but the core section doesn't have a property called zone, so this command fails.

```
$ gcloud config unset zone

ERROR: (gcloud.config.unset) Section [core] has no property [zone].
```

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

`gcloud config set zone "".` **is not right.**

gcloud config does not have a core/zone property. The syntax for this command is gcloud config set SECTION/PROPERTY VALUE. If SECTION is missing, SECTION is defaulted to core. We are effectively trying to run gcloud config set core/zone "" but the core section doesn't have a property called zone, so this command fails.

```
$ gcloud config set zone ""

ERROR: (gcloud.config.unset) Section [core] has no property [zone].
```

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

`gcloud config set compute/zone "".` **is not right.**

This command uses the correct syntax but it doesn't unset the compute/zone property correctly. Instead it sets it to "" in gcloud configuration. When the gcloud compute instances create command runs, it picks the zone value from this configuration property which is "" and attempts to create an instance in "" zone and fails because zone "" doesn't exist. gcloud doesn't treat "" zone as an unset value. The zone must be explicitly unset if it is to be removed from the configuration.

```
$ gcloud config set compute/zone ""

$ gcloud compute instances create instance1

Zone: Expected type (<type 'int'>, <type 'long'>) for field id, found projects
/compute-challenge-lab-266520/zones/ (type <type 'unicode'>)
```

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

`gcloud config unset compute/zone.` **is the right answer.**

This command uses the correct syntax and correctly unsets the zone in gcloud configuration. The next time gcloud compute instances create command runs, it knows there is no default zone defined in gcloud configuration and therefore prompts for a zone before the instance can be created.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/unset

Question 45:

Skipped

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

- ○

  The internal IP address is disabled.

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

`The compute instances have a static IP for their internal IP.` **is not right.**
Static internal IPs shouldn't be a reason for failed SSH connections. With all networking set up correctly, SSH works fine on Static internal IPs.
Ref: https://cloud.google.com/compute/docs/ip-addresses#networkaddresses

`The internal IP address is disabled.` **is not right.**
Every compute instance has one or more internal IP addresses so this option is not correct.

`The compute instances are not using the right cross-region SSH IAM permissions.` **is not right.**
There is no such thing as cross region SSH IAM permissions.

`The combination of compute instance network tags and VPC firewall rules allow SSH from 0.0.0.0 but denies SSH from the VPC subnets IP range.` **is the right answer.**
The combination of compute instance network tags and VPC firewall rules can certainly result in SSH traffic being allowed on the external IP range but disabled from subnets IP range. The firewall rule can be configured to allow SSH traffic from

0.0.0.0/0 but deny traffic from the VPC range e.g. 10.0.0.0/8. In this case, all SSH traffic from within the VPC is denied but external SSH traffic (i.e. on external IP) is allowed.
Ref: https://cloud.google.com/vpc/docs/using-firewalls

Question 46:
Skipped
You want to ingest and analyze large volumes of stream data from sensors in real time, matching the high speeds of IoT data to track normal and abnormal behavior. You want to run it through a data processing pipeline and store the results. Finally, you want to enable customers to build dashboards and drive analytics on their data in real time. What services should you use for this task?

- ○

  Cloud Pub/Sub, Cloud Dataflow, BigQuery

  (Correct)

- ○

  Cloud Pub/Sub, Cloud Dataflow, Cloud Dataproc

- ○

  Cloud Pub/Sub, Cloud Dataflow, Cloud Dataprep

- ○

  Stackdriver, Cloud Dataflow, BigQuery

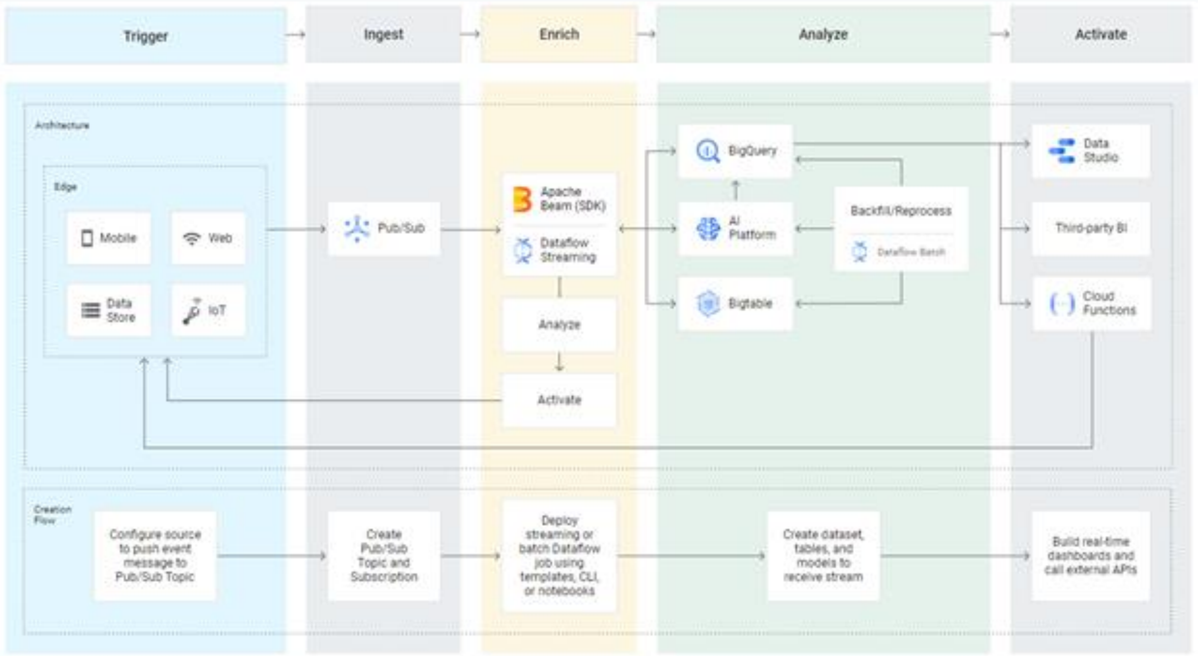
Explanation
You want to ingest large volumes of streaming data at high speeds. So you need to use Cloud Pub/Sub. Cloud Pub/Sub provides a simple and reliable staging location for your event data on its journey towards processing, storage, and analysis. Cloud Pub/Sub is serverless and you can ingest events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

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

Next, you want to store these results. BigQuery is an ideal place to store these results as BigQuery supports the querying of streaming data in real-time. This assists in real-time predictive analytics.
Ref: https://cloud.google.com/bigquery

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

Here’s more information from Google docs about the Stream analytics use case. Google recommends we use Dataflow along with Pub/Sub and BigQuery.
https://cloud.google.com/dataflow#section-6
Google’s stream analytics makes data more organized, useful, and accessible from the instant it’s generated. Built on Dataflow along with Pub/Sub and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights. This abstracted provisioning reduces complexity and makes stream analytics accessible to both data analysts and data engineers.


Trigger
Ingest
Enrich
Analyze
Activate
Architecture
Edge
Mobile
Web
Data Store
IoT
Pub/Sub
Apache Beam (SDK)
Dataflow Streaming
Analyze
Activate
BigQuery
AI Platform
Bigtable
Backfill/Reprocess
Dataflow Batch
Data Studio
Third-party BI
Cloud Functions
Creation Flow
Configure source to push event message to Pub/Sub Topic
Create Pub/Sub Topic and Subscription
Deploy streaming or batch Dataflow job using templates, CLI, or notebooks
Create dataset, tables, and models to receive stream
Build real-time dashboards and call external APIs

and
https://cloud.google.com/solutions/stream-analytics
Ingest, process, and analyze event streams in real time. Stream analytics from Google Cloud makes data more organized, useful, and accessible from the instant it’s generated. Built on the autoscaling infrastructure of Pub/Sub, Dataflow, and BigQuery, our streaming solution provisions the resources you need to ingest, process, and analyze fluctuating volumes of real-time data for real-time business insights.
Question 47:

Skipped

You created a kubernetes deployment by running kubectl run nginx --image=nginx --replicas=1. After a few days, you decided you no longer want this deployment. You identified the pod and deleted it by running kubectl delete pod. You noticed the pod got recreated. $ kubectl get pods NAME READY STATUS RESTARTS AGE nginx-84748895c4-nqqmt 1/1 Running 0 9m41s $ kubectl delete pod nginx-84748895c4-nqqmt pod "nginx-84748895c4-nqqmt" deleted $ kubectl get pods NAME READY STATUS RESTARTS AGE nginx-84748895c4-k6bzl 1/1 Running 0 25s What should you do to delete the deployment and avoid pod getting recreated?

- ○

  kubectl delete deployment nginx

  (Correct)

- ○

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

- ○

  kubectl delete nginx

- ○

  kubectl delete --deployment=nginx

Explanation

`kubectl delete pod nginx-84748895c4-k6bzl --no-restart.` **is not right.**
kubectl delete pod command does not support the flag --no-restart. The command fails to execute due to the presence of an invalid flag.

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

Error: unknown flag: --no-restart
```

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

`kubectl delete --deployment=nginx.` **is not right.**
kubectl delete command does not support the parameter --deployment. The command fails to execute due to the presence of an invalid parameter.

```
$ kubectl delete --deployment=nginx

Error: unknown flag: --deployment
```

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

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

```
$ kubectl delete nginx

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

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

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

```
$ kubectl delete deployment nginx

deployment.apps "nginx" deleted
```

Ref: https://kubernetes.io/docs/reference/kubectl/cheatsheet/#deleting-resources
Question 48:
Skipped
Your company has chosen to go serverless to enable developers to focus on writing code without worrying about infrastructure. You have been asked to identify a GCP Serverless service that does not limit your developers to specific runtimes. In addition, some of the applications need web sockets support. What should you suggest?

- ○

  Cloud Functions

- ○

  App Engine Standard

- ○

  Cloud Run for Anthos

  (Correct)

- ○

  Cloud Run

Explanation
`App Engine Standard.` **is not right.**
Google App Engine Standard offers a limited number of runtimes - Java, Node.js, Python, Go, PHP and Ruby; and at the same time doesn't offer support for Websockets.
Ref: https://cloud.google.com/appengine/docs/standard

`Cloud Functions.` **is not right.**
Like Google App Engine Standard, Cloud functions offer a limited number of runtimes - Node.js, Python, Go and Java; and doesn't offer support for Websockets.

Ref: https://cloud.google.com/blog/products/application-development/your-favorite-runtimes-now-generally-available-on-cloud-functions

`Cloud Run.` **is not right.**

Cloud Run lets you run stateless containers in a fully managed environment. As this is container-based, we are not limited to specific runtimes. Developers can write code using their favorite languages (Go, Python, Java, C#, PHP, Ruby, Node.js, Shell, and others). However, Cloud Run does not support Websockets.
Ref: https://cloud.google.com/run

`Cloud Run for Anthos.` **is the right answer.**

Cloud Run for Anthos leverage Kubernetes and serverless together using Cloud Run integrated with Anthos. As this is container-based, we are not limited to specific runtimes. Developers can write code using their favorite languages (Go, Python, Java, C#, PHP, Ruby, Node.js, Shell, and others). Cloud Run for Anthos is the only serverless GCP offering that supports WebSockets.
https://cloud.google.com/serverless-options

Question 49:

Skipped

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

- ○

  gcloud compute instances list

  (Correct)

- ○

  gcloud compute instances list-ip

- ○

  gcloud compute networks list

- ○

  gcloud compute networks list-ip

Explanation

`gcloud compute instances list-ip.` **is not right.**

"gcloud compute instances" doesn't support the action list-ip.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

`gcloud compute networks list-ip.` **is not right.**
"gcloud compute networks" doesn't support the action list-ip.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/networks/list

`gcloud compute networks list.` **is not right.**
"gcloud compute networks list" doesn't list the IP addresses. It is used for listing Google Compute Engine networks (i.e. VPCs)
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/networks/list
Here's a sample output of the command.

```
$ gcloud compute networks list

NAME SUBNET_MODE BGP_ROUTING_MODE IPV4_RANGE GATEWAY_IPV4

default AUTO REGIONAL

test-vpc CUSTOM REGIONAL
```

`gcloud compute instances list.` **is the right answer**
gcloud compute instances list - lists Google Compute Engine instances. The output includes internal as well as external IP addresses.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
Here's a sample output of the command.

```
$ gcloud compute instances list

NAME ZONE MACHINE_TYPE PREEMPTIBLE INTERNAL_IP EXTERNAL_IP STATUS

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

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

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

Question 50:
Skipped
You have files in a Cloud Storage bucket that you need to share with your suppliers. You want to restrict the time that the files are available to your suppliers to 1 hour. You want to follow Google recommended practices. What should you do?

- ○

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

- ○

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

- ○

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

- ○

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

  (Correct)

Explanation

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

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

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

CommandException: Incorrect option(s) specified. Usage:
```

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

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

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

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

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

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

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

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

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

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

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

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

`Create a service account with just the permissions to access files in the bucket. Create a JSON key for the service account. Execute the command gsutil signurl -d 1h {JSON Key File} gs://{bucket}/**.` **is the right answer.**
This command correctly specifies the duration that the signed url should be valid for by using the -d flag. The default is 1 hour so omitting the -d flag would have also resulted in the same outcome. Times may be specified with no suffix (default hours), or with s = seconds, m = minutes, h = hours, d = days. The max duration allowed is 7d.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/signurl

Question 1:

Skipped

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

- ○

  Transfer the data from Cloud Storage to BigQuery and advise the business analysts to run their SQL queries in BigQuery.

- ○

  Point a BigQuery external table at the Cloud Storage bucket and advise the business analysts to run their SQL queries in BigQuery.

  (Correct)

- ○

  Transfer the data from Cloud Storage to Cloud Datastore and advise the business analysts to run their SQL queries in Cloud Datastore.

- ○

  Transfer the data from Cloud Storage to HDFS. Configure an external table in Hive to point to HDFS and advise the business analysts to run their SQL queries in Hive.

Explanation

`Transfer the data from Cloud Storage to Cloud Datastore and advise the business analysts to run their SQL queries in Cloud Datastore.` **is not right.**
Datastore is a highly scalable NoSQL database, and although it supports SQL like queries, it doesn't support SQL. Moreover, there is no out of the box way for transforming the AVRO file from cloud storage into the Cloud Datastore entity. So we have to do in a bespoke way which adds to our cost and time.
Ref: https://cloud.google.com/datastore

`Transfer the data from Cloud Storage to HDFS. Configure an external table in Hive to point to HDFS and advise the business analysts to run their SQL queries in Hive.` **is not right.**
Like Cloud Datastore, Hive doesn't directly support SQL; it provides HiveQL (HQL) which is SQL-like.

`Transfer the data from Cloud Storage to BigQuery and advise the business analysts to run their SQL queries in BigQuery.` **is not right.**
Like the above two, while it is possible to build a solution that transforms and loads data into the target, BigQuery, which is not a trivial process and involves cost and time. GCP provides an out of the box way to query AVRO files from Cloud Storage, and this should be preferred.

`Point a BigQuery external table at the Cloud Storage bucket and advise the business analysts to run their SQL queries in BigQuery.` **is the right answer.**
BigQuery supports querying Cloud Storage data in several formats such as CSV, JSON, AVRO, etc. You do this by creating a Big Query external table that points to a Cloud Storage data source (bucket). This solution works out of the box, involves minimal effort, minimal cost, and is quick.
https://cloud.google.com/bigquery/external-data-cloud-storage

Question 2:
Skipped
Your finance department has asked you to provide their team access to view billing reports for all GCP projects. What should you do?

- ○

  Grant roles/billing.User IAM role to the finance group.

- ○

  Grant roles/billing.ProjectManager IAM role to the finance group.

- ○

  Grant roles/billing.Viewer IAM role to the finance group.

  (Correct)

- ○

  Grant roles/billing.Admin IAM role to the finance group.

Explanation
`Grant roles/billing.User IAM role to the finance group.` **is not right.**
This role has very restricted permissions, so you can grant it broadly, typically in combination with Project Creator. These two roles allow a user to create new projects linked to the billing account on which the role is granted.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

`Grant roles/billing.Admin IAM role to the finance group.` **is not right.**
This role is an owner role for a billing account. Use it to manage payment instruments, configure billing exports, view cost information, link and unlink projects, and manage other user roles on the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

`Grant roles/billing.ProjectManager IAM role to the finance group.` **is not right.**
This role allows a user to attach the project to the billing account, but does not grant any rights over resources. Project Owners can use this role to allow someone else to manage the billing for the project without granting them resource access.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

`Grant roles/billing.Viewer IAM role to the finance group.` **is the right answer.**
Billing Account Viewer access would usually be granted to finance teams; it provides access to spending information but does not confer the right to link or unlink projects or otherwise manage the properties of the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access

Question 3:

Skipped

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

- ○

  Have both the billing account export their billing data to a single BigQuery dataset.

- ○

  Move all projects from both organizations into a new GCP organization and link all the projects to a new billing account in the new GCP organization.

- ○

  Link all projects from production GCP organization to the billing account used by development GCP organization.

  (Correct)

- ○

Move all the projects from production GCP organization into development GCP organization and link them to the development billing account.

Explanation

`Have both the billing account export their billing data to a single BigQuery dataset.` **is not right.**

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

`Move all the projects from production GCP organization into development GCP organization and link them to the development billing account.` **is not right.**

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

`Move all projects from both organizations into a new GCP organization and link all the projects to a new billing account in the new GCP organization.` **is not right.**

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

`Link all projects from production GCP organization to the billing account used by development GCP organization.` **is the right answer.**

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

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

Question 4:

Skipped

Your company migrated its data warehousing solution from its on-premises data centre to Google Cloud 3 years ago. Since then, several teams have worked on different data warehousing and analytics needs, and have created numerous BigQuery datasets. The compliance manager is concerned at the possibility of PII data being present in these datasets and has asked you to identify all datasets that

contain us_social_security_number column. How can you most efficiently identify all datasets that contain us_social_security_number column?

- ○

  Write a custom script that uses bq commands to loop through all data sets and identify those containing us_social_security_number column.

- ○

  Search for us_social_security_number in Data Catalog.

  (Correct)

- ○

  Enable a Cloud Dataflow job that queries BigQuery INFORMATION_SCHEMA.TABLE_SCHEMA where COLUMN_NAME=us_social_security_number.

- ○

  Write a custom script that queries BigQuery INFORMATION_SCHEMA.TABLE_SCHEMA where COLUMN_NAME=us_social_security_number.

Explanation

`Search for us_social_security_number in Data Catalog.` **is the right answer.**
Data Catalog is a fully managed and scalable metadata management service that empowers organizations to discover quickly, understand, and manage all their data. It offers a simple and easy-to-use search interface for data discovery, a flexible and powerful cataloguing system for capturing both technical and business metadata, and a strong security and compliance foundation with Cloud Data Loss Prevention (DLP) and Cloud Identity and Access Management (IAM) integrations. The service automatically ingests technical metadata for BigQuery and Cloud Pub/Sub. It allows customers to capture business metadata in schematized format via tags, custom APIs, and the UI, offering a simple and efficient way to catalogue their data assets. You can perform a search for data assets from the Data Catalog home page in the Google Cloud Console.
See https://cloud.google.com/data-catalog/docs/how-to/search, for example.

All other options are manual, error-prone, time-consuming, and should be avoided.

Question 5:

Skipped

There has been an increased phishing email activity recently, and you deployed a new application on a GKE cluster to help scan and detect viruses in uploaded files. Each time the Finance or HR department receive an email with an attachment, they

use this application to scan the email attachment for viruses. The application pods open the email attachment in a sandboxed environment before initiating a virus scan. Some infected email attachments may run arbitrary phishing code with elevated privileges in the container. You want to ensure that the pods that run these scans do not impact pods of other applications running in the same GKE cluster. How can you achieve this isolation between pods?

- ○

  Create a new (non-default) node pool with sandbox type set to gvisor and configure the deployment spec with a runtimeClassName of gvisor.

  (Correct)

- ○

  Configure the pods to use containerd as the runtime by adding a node selector with key: cloud.google.com/gke-os-distribution and value:cos_containerd.

- ○

  Have your applications use trusted container images by enabling Binary Authorization.

- ○

  Detect vulnerabilities in the application container images in GCR repo by using the Container Analysis API.

Explanation

`Have your applications use trusted container images by enabling Binary Authorization.` **is not right.**

Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE). With Binary Authorization, you can require images to be signed by trusted authorities during the development process and then enforce signature validation when deploying. By enforcing validation, you can gain tighter control over your container environment by ensuring only verified images are integrated into the build-and-release process. This option doesn't help us with the requirement.

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

`Detect vulnerabilities in the application container images in GCR repo by using the Container Analysis API.` **is not right.**

Container Analysis is a service that provides vulnerability scanning and metadata storage for software artefacts. The scanning service performs vulnerability scans on images in Container Registry, then stores the resulting metadata and makes it

available for consumption through an API. Metadata storage allows storing information from different sources, including vulnerability scanning, other Cloud services, and third-party providers. This option doesn’t help us with the requirement.
Ref: https://cloud.google.com/container-registry/docs/container-analysis

`Configure the pods to use containerd as the runtime by adding a node selector with key: cloud.google.com/gke-os-distribution and value:cos_containerd.` **is not right.**
The cos_containerd and ubuntu_containerdimages let you use containerd as the container runtime in your GKE cluster. This option doesn't directly provide the isolation we require.
https://cloud.google.com/kubernetes-engine/docs/concepts/using-containerd

`Create a new (non-default) node pool with sandbox type set to gvisor and configure the deployment spec with a runtimeClassName of gvisor.` **is the right answer.**
GKE Sandbox provides an extra layer of security to prevent untrusted code from affecting the host kernel on your cluster nodes when containers in the Pod execute unknown or untrusted code. Multi-tenant clusters and clusters whose containers run untrusted workloads are more exposed to security vulnerabilities than other clusters. Examples include SaaS providers, web-hosting providers, or other organizations that allow their users to upload and run code. When you enable GKE Sandbox on a node pool, a sandbox is created for each Pod running on a node in that node pool. Also, nodes running sandboxed Pods are prevented from accessing other Google Cloud services or cluster metadata. Each sandbox uses its userspace kernel. With this in mind, you can make decisions about how to group your containers into Pods, based on the level of isolation you require and the characteristics of your applications.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/sandbox-pods#enabling-new
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/sandbox-pods#sandboxed-application

Question 6:
Skipped
The machine learning team at your company infrequently needs to use a GKE cluster with specific GPUs for processing a non-restartable and long-running job. How should you set up the GKE cluster for this requirement?

- ○

  Enable GKE cluster node auto-provisioning.

- ○

  Deploy the workload on a node pool with preemptible compute engine instances and GPUs attached to them.

- ○

  Deploy the workload on a node pool with non-preemptible compute engine instances and GPUs attached to them. Enable cluster autoscaling and set min-nodes to 1.

  (Correct)

- ○

  Enable Vertical Pod Autoscaling.

Explanation

`Enable GKE cluster node auto-provisioning.` **is not right.**

Node auto-provisioning automatically manages a set of node pools on the user's behalf. Without Node auto-provisioning, GKE considers starting new nodes only from the set of user-created node pools. With node auto-provisioning, new node pools can be created and deleted automatically. This in no way helps us with our requirements.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/node-auto-provisioning

`Enable Vertical Pod Autoscaling.` **is not right.**

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

`Deploy the workload on a node pool with preemptible compute engine instances and GPUs attached to them.` **is not right.**

You can use preemptible VMs in your GKE clusters or node pools to run batch or fault-tolerant jobs that are less sensitive to the ephemeral, non-guaranteed nature of preemptible VMs. In contrast, we have long-running and non-restartable jobs, so preemptible VMs aren't suitable for our requirement.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/preemptible-vms

`Deploy the workload on a node pool with non-preemptible compute engine instances and GPUs attached to them. Enable cluster autoscaling and set min-nodes to 1.` **is the right answer.**

A node pool is a group of nodes within a cluster that all have the same configuration. Our requirement is GPUs, so we create a node pool with GPU enabled and have the scientist's applications deployed to the cluster and use this node pool. At the same

time, you want to minimize cost, so you start with 1 instance and scale up as needed. It is important to note that the scale down needs to take into consideration if there are any running jobs; otherwise, the scale down may terminate the nonrestartable job.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/node-pools

Question 7:

Skipped

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

- ○

  Create an IAM user with the appropriate permissions and use the username and password in your on-premises application.

- ○

  Configure your on-premises application to use the service account username and password credentials.

- ○

  Configure the Direct interconnect to authenticate requests from your on-premises network automatically.

- ○

  Run gcloud iam service-accounts keys create to generate a JSON key file for the service account and configure your on-premises application to present the JSON key file.

  (Correct)

Explanation

`Configure your on-premises application to use the service account username and password credentials.` **is not right.**

Service accounts do not have passwords.
Ref: https://cloud.google.com/iam/docs/service-accounts

`Create an IAM user with the appropriate permissions and use the username and password in your on-premises application.` **is not right.**

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

Running workloads on virtual machines (VMs).

Running workloads from on-premises workstations that call Google APIs

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

Your application assumes the identity of the service account to call Google APIs so that the users aren't directly involved.
Ref: https://cloud.google.com/iam/docs/understanding-service-accounts

`Configure the Direct interconnect to authenticate requests from your on-premises network automatically.` **is not right.**
While setting up interconnect provides a direct physical connection between your on-premises network and Google’s network, it doesn't directly help us authenticate our application running in the data centre. You can configure Private Google Access for on-premises hosts by sending requests to restricted.googleapis.com and advertise a custom route on cloud router, but this only lets you reach Google API and doesn't help with authentication.
Ref: https://cloud.google.com/interconnect/docs/support/faq

`Run gcloud iam service-accounts keys create to generate a JSON key file for the service account and configure your on-premises application to present the JSON key file.` **is the right answer.**
To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. You can create a service account key using the Cloud Console, the gcloud tool, the serviceAccounts.keys.create() method, or one of the client libraries.
Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys

Question 8:
Skipped
You have developed an enhancement for a photo compression application running on the App Engine Standard service in Google Cloud Platform, and you want to canary test this enhancement on a small percentage of live users before completely switching off the old version. How can you do this?

- ○

  Deploy the enhancement in a GKE cluster and enable traffic splitting in GCP console.

- ○

  Deploy the enhancement in a GCE VM and enable traffic splitting in GCP console.

- ○

  Deploy the enhancement as a new version of the application and enable traffic splitting in GCP console.

  (Correct)

- ○

  Deploy the enhancement as a new application in App Engine Standard and enable traffic splitting in GCP console.

Explanation

`Deploy the enhancement in a GKE cluster and enable traffic splitting in GCP console.` **is not right.**
When you can achieve this natively in GCP app engine using versions, there is no need to do it outside App Engine.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

`Deploy the enhancement in a GCE VM and enable traffic splitting in GCP console.` **is not right.**
When you can achieve this natively in GCP app engine using versions, there is no need to do it outside App Engine.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

`Deploy the enhancement as a new application in App Engine Standard and enable traffic splitting in GCP console.` **is not right.**
You can achieve this natively in GCP app engine using versions, but App Engine doesn't let you split traffic between apps. If you need to do it between apps, you need to do this at the load balancer layer or the DNS layer, which ultimately increases the cost/complexity or introduces other problems such as caching issues.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

`Deploy the enhancement as a new version of the application and enable traffic splitting in GCP console.` **is the right answer.**
GCP App Engine natively offers traffic splitting functionality between versions. You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitting traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.
Ref: https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

Question 9:

Skipped

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

- ○

  Grant the Storage Object Viewer IAM role on the GCR Repo project to the service account used by GKE nodes in your project.

  (Correct)

- ○

  In the central GCR repo project, grant the Storage Object Viewer role on the Cloud Storage bucket that contains the container images to a service account and generate a P12 key for this service account. Configure the Kubernetes service account to use this key for imagePullSecrets.

- ○

  Enable full access to all Google APIs under Access Scopes when provisioning the GKE cluster.

- ○

  Update ACLs on each container image to provide read-only access to the service account used by GKE nodes in your project.

Explanation

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

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

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

`Update ACLs on each container image to provide read-only access to the service account used by GKE nodes in your project.` **is not right.**
As mentioned above, Container Registry ignores permissions set on individual objects within the storage bucket, so this isn't going to work.
Ref: https://cloud.google.com/container-registry/docs/access-control

`Enable full access to all Google APIs under Access Scopes when provisioning the GKE cluster.` **is not right.**
Selecting Allow full access to all Cloud APIs does not provide access to GCR images in a different project. Suppose the Google Kubernetes Engine cluster and the Container Registry storage bucket are in the same Google Cloud project. In that case, the Compute Engine default service account is configured with the appropriate permissions to push or pull images. But if the cluster is in a different project or if the VMs in the cluster use a different service account, you must grant the service account the appropriate permissions to access the storage bucket used by Container Registry.
Ref: https://cloud.google.com/container-registry/docs/using-with-google-cloud-platform
In this scenario, since there is no mention of the service account. Therefore, we have to assume we are using a default service account that hasn't been provided permissions to access the storage bucket used by Container Registry in another project, so the image pull isn't going to work. You would end up with an error like:

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

`In the central GCR repo project, grant the Storage Object Viewer role on the Cloud Storage bucket that contains the container images to a service account and generate a P12 key for this service account. Configure the Kubernetes service account to use this key for imagePullSecrets.` **is not right.**
It is technically possible to do it this way but using the JSON key and not P12 key as mentioned in this option. If you would like to understand how to do this, please look at these blogs.
Ref: https://medium.com/hackernoon/today-i-learned-pull-docker-image-from-gcr-google-container-registry-in-any-non-gcp-kubernetes-5f8298f28969 Ref: https://medium.com/@michaelmorrissey/using-cross-project-gcr-images-in-gke-1ddc36de3d42
Moreover, this approach is suitable for accessing GCR images in a non-Google Cloud Kubernetes environment. While it can be used in GKE too, it is not as secure as using Role Bindings since it involves downloading service account keys and setting them up as secret in Kubernetes.

`Grant the Storage Object Viewer IAM role on the GCR Repo project to the service account used by GKE nodes in your project.` **is the right answer.**

Granting the storage object viewer IAM role in the project where images are stored to the service account used by the Kubernetes cluster ensures that the nodes in the cluster can Read Images from the storage bucket. It would be ideal to restrict the role binding further to provide access just to the Cloud Storage bucket that is used as the underlying storage for container images. This approach aligns with the principle of least privilege. For more information about Storage Object Viewer IAM Role for GCR, refer:
https://cloud.google.com/container-registry/docs/access-control#permissions_and_roles

Question 10:

Skipped

The compliance manager asked you to provide an external auditor with a report of when Cloud Identity users in your company were granted IAM roles for Cloud Spanner. How should you retrieve this information?

- ○

  Retrieve the information from Cloud Logging console by filtering admin activity logs for Cloud Spanner IAM roles.

  (Correct)

- ○

  Retrieve the details from Cloud Spanner console.

- ○

  Retrieve the information from Cloud Monitoring console by filtering data logs for Cloud Spanner IAM roles.

- ○

  Retrieve the details from the policies section in the IAM console by filtering for Cloud Spanner IAM roles.

Explanation

`Retrieve the information from Cloud Monitoring console by filtering data logs for Cloud Spanner IAM roles.` **is not right.**

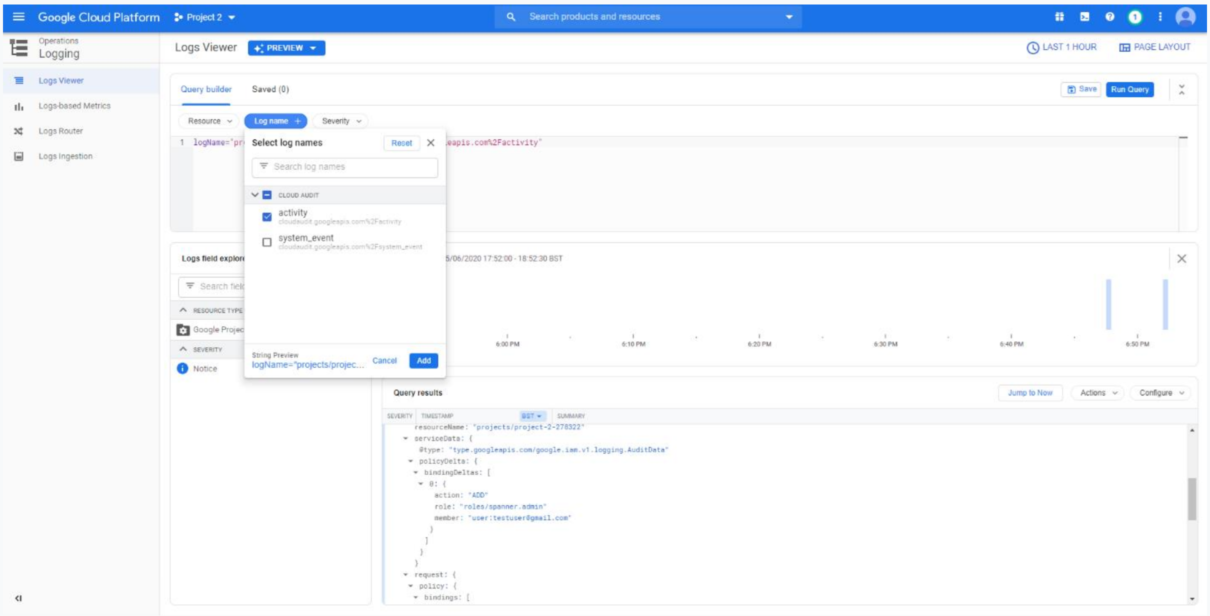
Monitoring collects metrics, events, and metadata from Google Cloud and lets you generate insights via dashboards, charts, and alerts. It can't provide information on when a role has been granted to a user.

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

`Retrieve the details from the policies section in the IAM console by filtering for Cloud Spanner IAM roles.` **is not right.**
You can't find the role bindings and the timestamps in the policies.
https://cloud.google.com/iam/docs/overview

`Retrieve the details from Cloud Spanner console.` **is not right.**
You manage cloud spanner instances in the console but you can't check when a role has been granted to a user.
Ref: https://cloud.google.com/spanner/docs/quickstart-console

`Retrieve the information from Cloud Logging console by filtering admin activity logs for Cloud Spanner IAM roles.` **is the right answer.**
Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Cloud Identity and Access Management permissions. Admin Activity audit logs are always written; you can't configure or disable them. There is no charge for your Admin Activity audit logs.
Ref: https://cloud.google.com/logging/docs/audit#admin-activity
See below a screenshot from GCP console showing this in action.



```
logName="pr…eapis.com%2Factivity"
```

☑ activity cloudaudit.googleapis.com%2Factivity
☐ system_event cloudaudit.googleapis.com%2Fsystem_event

5/06/2020 17:52:00 - 18:52:30 BST

String Preview
logName="projects/projec...

```
  resourceName: "projects/project-2-278322"
▾ serviceData: {
   @type: "type.googleapis.com/google.iam.v1.logging.AuditData"
 ▾ policyDelta: {
  ▾ bindingDeltas: [
   ▾ 0: {
      action: "ADD"
      role: "roles/spanner.admin"
      member: "user:testuser@gmail.com"
     }
    ]
   }
  }
▾ request: {
 ▾ policy: {
  ▾ bindings: [
```

Among other things, the payload contains

```
{
    action: "ADD"
    role: "roles/spanner.admin"
    member: "user:testuser@gmail.com"
}
```

Question 11:

Skipped

A mission-critical image processing application running in your on-premises data centre requires 64 virtual CPUs to execute all processes. You colleague wants to migrate this mission-critical application to Google Cloud Platform Compute Engine and has asked your suggestion for the instance size. What should you suggest?

- ○

  Use Xeon Scalable Processor (Skylake) as the CPU platform when provisioning the compute engine instance.

- ○

  Use n1-standard-64 machine type when provisioning the compute engine instance.

  (Correct)

- ○

  Provision the compute engine instance on the default settings, then modify it to have 64 vCPUs.

- ○

  Provision the compute engine instance on the default settings, then scale it as per sizing recommendations.

Explanation

`Provision the compute engine instance on the default settings, then modify it to have 64 vCPUs.` **is not right.**

You can't increase the vCPUs to 64 without changing the machine type. While it is possible to set machine type using gcloud, this would mean downtime for the mission-critical application while the upgrade happens, which is undesirable.

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

`Provision the compute engine instance on the default settings, then scale it as per sizing recommendations.` **is not right.**

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

`Use Xeon Scalable Processor (Skylake) as the CPU platform when provisioning the compute engine instance.` **is not right.**
Selecting an Intel Skylake CPU processor does not guarantee the compute engine instance 64 vCPUs.
Ref: https://cloud.google.com/compute/docs/cpu-platforms

`Use n1-standard-64 machine type when provisioning the compute engine instance.` **is the right answer.**
n1-standard-64 offers 64 vCPUs and 240 GB of memory. This machine type fits our requirements.
https://cloud.google.com/compute/docs/machine-types#n1_machine_type

Question 12:
Skipped
All development teams at your company share the same development GCP project, and this has previously resulted in some teams accidentally terminating compute engine resources of other teams, causing downtime and loss of productivity. You want to deploy a new application to the shared development GCP project, and you want to protect your instance from such issues. What should you do?

- ○

  Set the deletionProtection property on the VM.

  (Correct)

- ○

  Deploy the application on a Shielded VM.

- ○

  Deploy the application on VMs provisioned on sole-tenant nodes.

- ○

  Deploy the application on a Preemptible VM.

Explanation
`Deploy the application on a Shielded VM.` **is not right.**
Shielded VMs are virtual machines (VMs) on Google Cloud hardened by a set of security controls that help defend against rootkits and boot kits. Using Shielded VMs helps protect enterprise workloads from threats like remote attacks, privilege escalation, and malicious insiders. But shielded VMs don't offer protection for accidental termination of the instance.
Ref: https://cloud.google.com/shielded-vm

`Deploy the application on a Preemptible VM.` **is not right.**
A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage. Preemptible VMs don't offer protection for accidental termination of the instance.
Ref: https://cloud.google.com/compute/docs/instances/preemptible

`Deploy the application on VMs provisioned on sole-tenant nodes.` **is not right.**
Sole-tenancy lets you have exclusive access to a sole-tenant node, which is a physical Compute Engine server that is dedicated to hosting only your project's VMs. Use sole-tenant nodes to keep your VMs physically separated from VMs in other projects, or to group your VMs together on the same host hardware. Sole-tenant nodes don't offer protection for accidental termination of the instance.
Ref: https://cloud.google.com/compute/docs/nodes

`Set the deletionProtection property on the VM.` **is the right answer.**
As part of your workload, there might be certain VM instances that are critical to running your application or services, such as an instance running a SQL server, a server used as a license manager, and so on. These VM instances might need to stay running indefinitely, so you need a way to protect these VMs from being deleted. By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails. Only a user that has been granted a role with compute.instances.create permission can reset the flag to allow the resource to be deleted.
Ref: https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion

Question 13:

Skipped

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

- ○

  The deleted current version becomes a non-current version, and a lifecycle rule is applied to delete after 30 days. A lifecycle rule is applied on the deleted non-current version to delete after 30 days.

- ○

The deleted current version becomes a non-current version, and a lifecycle rule is applied to transition to Nearline Storage after 30 days. A lifecycle rule is applied on the deleted non-current version to transition to Nearline Storage after 30 days.

- ○

  The deleted current version is deleted permanently. The deleted non-current version is deleted permanently.

- ○

  The deleted current version becomes a non-current version. The deleted non-current version is deleted permanently.

  (Correct)

Explanation

`The deleted current version becomes a non-current version. The deleted non-current version is deleted permanently.` **is the right answer.**

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

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

Question 14:

Skipped

You developed a new mobile game that uses Cloud Spanner for storing user state, player profile and leaderboard. Data is always accessed by using the primary key. Your performance testing team identified latency issues in the application, and you suspect it might be related to table primary key configuration. You created the table by executing this DDL:

```
CREATE TABLE users {
  user_id INT64 NOT NULL,        // This is populated from a sequence
  user_name STRING (255),        // Game username
  …
  …
  email_address STRING (255)     // Email Address
} PRIMARY KEY (user_id)
```

What should you do to fix this read latency issue?

- ○

  Add another index on user_id column to speed up the data retrieval.

- ○

  Update the primary key (user_id) to not have sequential values.

(Correct)

- ○

  Make the table smaller by removing email_address and add another index on user_id column to speed up the data retrieval.

- ○

  Make the table smaller by removing email_address.

Explanation

`Update the primary key (user_id) to not have sequential values.` **is the right answer.**

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

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

All other options make no sense. The problem is with the sequentially increasing values in the primary key and removing email_address or adding another index isn't going to fix the problem.

Question 15:

Skipped

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

- ○

  Execute gcloud builds submit --tag gcr.io/app_prod/tranquillity:v1 from Cloud shell.

- ○

Execute gcloud builds submit --tag gcr.io/gcr_proj/tranquillity from Cloud shell.

- ○

  Execute gcloud builds submit --tag gcr.io/app_prod/tranquillity from Cloud shell.

- ○

  Execute gcloud builds submit --tag gcr.io/gcr_proj/tranquillity:v1 from Cloud shell.

  (Correct)

Explanation

`Execute gcloud builds submit --tag gcr.io/gcr_proj/tranquillity from Cloud shell.` **is not right.**
This command tags the image as tranquillity:latest, but we want to tag the image as tranquillity:v1.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

`Execute gcloud builds submit --tag gcr.io/app_prod/tranquillity from Cloud shell.` **is not right.**
This command tags the image as tranquillity: latest, but we want to tag the image as tranquillity:v1. This command also uploads the image to the wrong project.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

`Execute gcloud builds submit --tag gcr.io/app_prod/tranquillity:v1 from Cloud shell.` **is not right.**
This command uploads the image to the wrong project.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

`Execute gcloud builds submit --tag gcr.io/gcr_proj/tranquillity:v1 from Cloud shell.` **is the right answer.**
This command correctly tags the image as tranquillity:v1 and uploads the image to the gcr_proj project.
Ref: https://cloud.google.com/sdk/gcloud/reference/builds/submit

Question 16:

Skipped

To prevent accidental security breaches, the security team at your company has enabled Domain Restricted Sharing to limit resource sharing in your GCP organization to just your cloud identity domain. The compliance department has engaged an external auditor to carry out the annual audit, and the auditor requires

read access to all resources in the production project to fill out specific sections in the audit report. How can you enable this access?

- ○

  Grant the auditors’ Google account roles/iam.securityReviewer IAM role on the production project.

- ○

  Create a new Cloud Identity account for the auditor and grant them roles/viewer IAM role on the production project.

  (Correct)

- ○

  Grant the auditors’ Google account roles/viewer IAM role on the production project.

- ○

  Create a new Cloud Identity account for the auditor and grant them roles/iam.securityReviewer IAM role on the production project.

Explanation

`Grant the auditors’ Google account roles/viewer IAM role on the production project.` **is not right.**

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

`Grant the auditors’ Google account roles/iam.securityReviewer IAM role on the production project.` **is not right.**

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

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

`Create a new Cloud Identity account for the auditor and grant them roles/iam.securityReviewer IAM role on the production project.` **is not right.**
Creating a temporary account for the auditor in your cloud identity is the right approach as this makes the auditor part of the Cloud identity domain and the organization policy in place lets the auditor access resources. However, the role granted here is not suitable; it provides permissions to list all resources and Cloud IAM policies. Note that list permissions only allow you to list but not view resources. You need to get permission to view the resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#iam-roles

`Create a new Cloud Identity account for the auditor and grant them roles/viewer IAM role on the production project.` **is the right answer.**
The primitive viewer role provides permissions for read-only actions that do not affect the state, such as viewing (but not modifying) existing resources or data. This fits our requirements.
Also, adding the auditor to Cloud Identity ensures that Organization Policy for Domain Restricted Sharing doesn't block them from accessing resources.
Ref: https://cloud.google.com/iam/docs/understanding-roles#primitive_role_definitions

Question 17:

Skipped

Your production Compute workloads are running in a small subnet with a netmask 255.255.255.224. A recent surge in traffic has seen the production VMs struggle, but there are no free IP addresses for the Managed Instances Group (MIG) to autoscale. You anticipate requiring 30 additional IP addresses for the new VMs. All VMs within the subnet need to communicate with each other, and you want to do this without adding additional routes. What should you do?

- ○

  Create a new project and a new VPC. Share the new VPC with the existing project and configure all existing resources to use the new VPC.

- ○

  Create a new subnet with a bigger non-overlapping range. Move all instances to the new subnet and delete the old subnet.

- ○

  Expand the subnet IP range.

(Correct)

- ○

  Create a new subnet with a bigger overlapping range to automatically move all instances to the new subnet. Then, delete the old subnet.

Explanation

`Expand the subnet IP range.` **is the right answer.**

The subnet mask of the existing subnet is 255.255.255.224, which means the max possible addresses are 32. Therefore, the net prefix is /27, i.e. 5 bits free, so 2 to the power of 5 is 32 IP Addresses.

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

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

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

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

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

A prefix of 26 gives you 64 IP Addresses, i.e. 32 IP address more and we just need 30 more. So, expanding the subnet to a prefix of 26 should give us the required capacity. And GCP lets you do exactly that running a gcloud command https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range

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

Question 18:

Skipped

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

- ○

  Store new data in Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Coldline Storage Class.

(Correct)

- ○

  Store new data in Multi-Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Coldline Storage Class.

- ○

  Store new data in Multi-Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Nearline Storage Class.

- ○

  Store new data in Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Nearline Storage Class.

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

`Store new data in Multi-Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Coldline Storage Class.` **is not right.**
When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region. Moreover, this is expensive compared to standard Regional storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard

`Store new data in Multi-Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Nearline Storage Class.` **is not right.**
When used in a multi-region, Standard Storage is appropriate for storing data that is accessed around the world, such as serving website content, streaming videos, executing interactive workloads, or serving data supporting mobile and gaming applications. This is against our requirement of one region. Moreover, this is expensive compared to standard Regional storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#standard

`Store new data in Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Nearline Storage Class.` **is not right.**
While selecting Regional Storage is the right choice, archiving to Nearline is not the most optimal. We have a requirement to access data annually, whereas Nearline Storage is ideal for data you plan to read or modify on average once per month or

less. Nearline storage is more expensive than Coldline Storage which is more suitable for our requirements.
https://cloud.google.com/storage/docs/storage-classes#nearline

`Store new data in Regional Storage Class, and add a lifecycle rule to transition data older than 30 days to Coldline Storage Class.` **is the right answer.**
Regional Storage is the right fit for our requirements (one geographic region) and archiving to Coldline storage is the most cost-efficient solution. Coldline Storage is a very-low-cost, highly durable storage service for storing infrequently accessed data. Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Since we have a requirement to access data once a quarter and want to go with the most cost-efficient option, we should select Coldline Storage.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

Question 19:
Skipped
You work for a multinational conglomerate that has thousands of GCP projects and a very complex resource hierarchy that includes over 100 folders. An external audit team has requested to view this hierarchy to fill out sections of a report. You want to enable them to view the hierarchy while ensuring they can't do anything else. What should you do?

- ○

  Grant all individual auditors roles/iam.roleViewer IAM role.

- ○

  Add all individual auditors to an IAM group and grant the group roles/browser IAM role.

  (Correct)

- ○

  Grant all individual auditors roles/browser IAM role.

- ○

  Add all individual auditors to an IAM group and grant the group roles/iam.roleViewer IAM role.

Explanation

`Grant all individual auditors roles/iam.roleViewer IAM role.` **is not right.**
roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Add all individual auditors to an IAM group and grant the group roles/iam.roleViewer IAM role.` **is not right.**
roles/iam.roleViewer provides read access to all custom roles in the project and doesn't satisfy our requirement of viewing organization hierarchy.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Grant all individual auditors roles/browser IAM role.` **is not right.**
roles/browser provides read access to browse the hierarchy for a project, including the folder, organization, and Cloud IAM policy. This role doesn't include permission to view resources in the project. Although this is the role we require, you want to follow Google recommended practices which means we should instead add a group to the role and add users to the group instead of granting the role individually to users.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Add all individual auditors to an IAM group and grant the group roles/browser IAM role.` **is the right answer.**
roles/browser Read access to browse the hierarchy for a project, including the folder, organization, and Cloud IAM policy. This role doesn't include permission to view resources in the project. And you follow Google recommended practices by adding users to the group and group to the role. Groups are a convenient way to apply an access policy to a collection of users. You can grant and change access controls for a whole group at once instead of granting or changing access controls one at a time for individual users or service accounts. You can also easily add members to and remove members from a Google group instead of updating a Cloud IAM policy to add or remove users.
Ref: https://cloud.google.com/iam/docs/understanding-roles
Ref: https://cloud.google.com/iam/docs/overview

Question 20:

Skipped

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

- ○

Reuse an existing production GCP project of a different department for deploying the production resources.

- ○

Deploy the production resources in a new subnet within the existing GCP project.

- ○

In a new GCP project, enable the required GCP services and APIs, and deploy the necessary production resources.

(Correct)

- ○

Set up a shared VPC between test GCP project and production GCP project, and configure both test and production resources to use the shared VPC to achieve maximum isolation.

Explanation

`Set up a shared VPC between test GCP project and production GCP project, and configure both test and production resources to use the shared VPC to achieve maximum isolation.` **is not right.**

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

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

`Deploy the production resources in a new subnet within the existing GCP project.` **is not right.**

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

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

`Reuse an existing production GCP project of a different department for deploying the production resources.` **is not right.**
While this would technically isolate the test environment from the production environment, your production application is running in a project that is also hosting production applications of another division of your company. This goes against Google's recommended practices. You can use folders to isolate requirements for different departments and teams in the parent organization. And you have separate projects under the folders so as per Google recommendations we should be deploying the production application to a separate project that is just for one company division/department.
Ref: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#define-hierarchy

`In a new GCP project, enable the required GCP services and APIs, and deploy the necessary production resources.` **is the right answer.**
This aligns with Google's recommended practices. By creating a new project, we achieve complete isolation between test and production environments; as well as isolate this production application from production applications of other departments.
Ref: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#define-hierarchy

Question 21:

Skipped

Your company has accumulated terabytes of analytics data from clickstream logs and stores this data in BigQuery dataset in a central GCP project. Analytics teams from several departments in multiple GCP projects run queries against this data. The costs for BigQuery job executions have increased drastically in recent months, and your finance team has asked your suggestions for controlling these spiralling costs. What should you do? (Select two)

- ☐

  Enable BigQuery quota on a per-project basis.

- ☐

  Replicate the data in all GCP projects & have each department query data from their GCP project instead of the central BigQuery project.

- ☐

  Separate the data of each department and store it in BigQuery in their GCP project.

  (Correct)

- □

  Move to BigQuery flat rate and purchase the required number of query slots.

  (Correct)

- □

  Create a separate GCP project for each department and configure billing settings on each project to pick up the costs for queries ran by their analytics team.

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

`Create a separate GCP project for each department and configure billing settings on each project to pick up the costs for queries ran by their analytics team.` **is not right.**
The bytes scanned is not expected to go down by splitting the users into multiple projects so this wouldn't reduce/control the costs.
Ref: https://cloud.google.com/bigquery/pricing

`Replicate the data in all GCP projects & have each department query data from their GCP project instead of the central BigQuery project.` **is not right.**
Creating separate copies of the BigQuery data warehouse for each business unit is going to increase your costs. Not only is this expected to reduce the bytes scanned, but this is also going to increase the storage costs as we are now storing double the amount of data.
Ref: https://cloud.google.com/bigquery/pricing

`Enable BigQuery quota on a per-project basis.` **is not right.**
BigQuery limits the maximum rate of incoming requests and enforces appropriate quotas on a per-project basis. You can set various limits to control costs such as Concurrent rate limit for interactive queries, Concurrent rate limit for interactive queries against Bigtable external data sources, Concurrent rate limit for legacy SQL queries that contain UDFs, Cross-region federated querying, Daily query size limit, etc. Setting limits controls costs but comes with an expense - analysts wouldn’t be

able to run any more queries once the limits are hit and this affects business operations.
https://cloud.google.com/bigquery/quotas

`Separate the data of each department and store it in BigQuery in their GCP project.` **is the right answer.**
By splitting the dataset into multiple datasets per department, the bytes scanned during the query execution is smaller and this significantly reduces the costs. Splitting the data might actually result in duplicating some data across multiple data sets, but as pointed out in the Big Cost Optimization article, the storage costs are insignificant compared to the data retrieval costs.
Ref: https://cloud.google.com/bigquery/pricing
Ref: https://cloud.google.com/bigquery/docs/best-practices-costs#materialize_query_results_in_stages

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

Question 22:
Skipped
You want to identify a cost-efficient storage class for archival of audit logs in Google Cloud Storage. Some of these audit logs may need to be retrieved during the quarterly audit. What Storage Class should you use to minimize costs?

- ○

  Regional Storage Class.

- ○

  Coldline Storage Class.

  (Correct)

- ○

Disaster Recovery Storage Class.

- ○

  Nearline Storage Class.

Explanation

`Nearline Storage Class.` **is not right.**

Nearline Storage is a low-cost, highly durable storage service for storing infrequently accessed data. Nearline Storage is ideal for data you plan to read or modify on average once per month or less. Nearline storage is more expensive than Coldline Storage which is more suitable for our requirements.
https://cloud.google.com/storage/docs/storage-classes#nearline

`Regional Storage Class.` **is not right.**

While this would certainly let you access your files once a quarter, it would be too expensive compared to Coldline storage which is more suitable for our requirement.
https://cloud.google.com/storage/docs/storage-classes#standard

`Disaster Recovery Storage Class.` **is not right.**

There is no such storage class.
https://cloud.google.com/storage/docs/storage-classes

`Coldline Storage Class.` **is the right answer.**

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

Question 23:

Skipped

Your finance team owns two GCP projects – one project for payroll applications and another project for accounts. You need the VMs in the payroll project in one VPC to communicate with VMs in accounts project in a different VPC and vice versa. How should you do it?

- ○

  Ensure you have the Administrator role on both projects and move all instances to a single new VPC.

- ○

  Create a new VPC and move all VMs to the new VPC. Ensure both projects belong to the same GCP organization.

- ○

  Ensure you have the Administrator role on both projects and move all instances to two new VPCs.

- ○

  Share the VPC from one of the projects and have the VMs in the other project use the shared VPC. Ensure both projects belong to the same GCP organization.

  (Correct)

Explanation

`Share the VPC from one of the projects and have the VMs in the other project use the shared VPC. Ensure both projects belong to the same GCP organization.` **is the right answer.**

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

All other options make no sense.

Question 24:

Skipped

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

- ○

  Trigger a Cloud Function whenever the topic receives a new message. From the Cloud Function, invoke Cloud Run.

- ○

  Assign roles/run.invoker role (Cloud Run Invoker role) on your Cloud Run application to a service account. Set up a Cloud Pub/Sub subscription on the topic and configure it to use the service account to push the message to your Cloud Run application.

  (Correct)

- ○

  Deploy your application to Google Cloud Run on GKE. Set up a Cloud Pub/Sub subscription on the topic and deploy a sidecar container in the same GKE cluster to consume the message from the topic and push it to your application.

- ○

  Assign roles/pubsub.subscriber role (Pub/Sub Subscriber role) to the Cloud Run service account. Set up a Cloud Pub/Sub subscription on the topic and configure the application to pull messages.

Explanation

`Trigger a Cloud Function whenever the topic receives a new message. From the Cloud Function, invoke Cloud Run.` **is not right.**
Both Cloud functions and Cloud Run are serverless offerings from GCP, and they are both capable of integrating with Cloud Pub/Sub. It is pointless to invoking Cloud Function from Cloud Run.

`Assign roles/pubsub.subscriber (Pub/Sub Subscriber role) role to the Cloud Run service account. Set up a Cloud Pub/Sub subscription on the topic and configure the application to pull messages.` **is not right.**
You need to provide Cloud Run Invoker role to that service account for your Cloud Run application.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub

`Deploy your application to Google Cloud Run on GKE. Set up a Cloud Pub/Sub subscription on the topic and deploy a sidecar container in the same GKE cluster to consume the message from the topic and push it to your application.` **is not right.**
Like above, you need cloud Run Invoker role on the service account.
Ref: https://cloud.google.com/run/docs/tutorials/pubsub
Also, our question states the application on Cloud Run processes messages from a Cloud Pub/Sub topic; whereas in this option, we are utilizing a separate container to process messages from the topic. So this doesn't satisfy our requirements.

`Assign roles/run.invoker role (Cloud Run Invoker role) on your Cloud Run application to a service account. Set up a Cloud Pub/Sub subscription on the topic and configure it to use the service account to push the message to your Cloud Run application.` **is the right answer.**
This exact process is described in
https://cloud.google.com/run/docs/tutorials/pubsub
You create a service account.

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

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

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

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

 --member=serviceAccount:cloud-run-pubsub-invoker@PROJECT_ID.iam.gserviceaccou
nt.com \

 --role=roles/run.invoker
```

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

```
 gcloud pubsub subscriptions create myRunSubscription --topic myRunTopic \

 --push-endpoint=SERVICE-URL/ \

 --push-auth-service-account=cloud-run-pubsub-invoker@PROJECT_ID.iam.gservicea
ccount
```

Question 25:

Skipped

Your colleague is learning about docker images, containers and Kubernetes, and has recently deployed a sample application to a GKE You deployed a demo application on a GKE cluster that uses preemptible nodes. The deployment has 2 replicas, and although the demo application is responding to requests, the output from Cloud Shell shows one of the pods is pending state.

```
kubectl get pods -l app=demo

NAME                               READY     STATUS       RESTART       AGE
demo-deployment-8998dab376-brm68       0/1      Pending      0             29m
demo-deployment-8998dab376-kpg18       1/1      Running      0             29m
```

What is the most likely explanation for this behaviour?

- ○

  Cluster autoscaling is not enabled, and the existing (only) node doesn't have enough resources for provisioning the pod.

  (Correct)

- ○

  The pod in the pending state is too big to fit on a single preemptible VM. The node pool needs to be recreated with a bigger machine type.

- ○

  The node got preempted before the pod could be started fully. GKE cluster master is provisioning a new node.

- ○

The pod in the pending state is unable to download the docker image.

Explanation

`The node got preempted before the pod could be started fully. GKE cluster master is provisioning a new node.` **is not right.**

Our question states that we provisioned a Google Kubernetes Engine cluster with preemptible node pool. If the node is pre-empted, the status wouldn't be pending, it would be terminating/terminated.

`The pod in the pending state is unable to download the docker image.` **is not right.**

If the node pool has permission issues when pulling the container image, the other pod would not be in Running status. And the status would have been ImagePullBackOff if there was a problem pulling the image.

`The pod in the pending state is too big to fit on a single preemptible VM. The node pool needs to be recreated with a bigger machine type.` **is not right.**

If the resource requests in Pod specification are too large to fit on the node, the other pod would not be in Running status, i.e. both pods should have been in pending status if this was the case.

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

`Cluster autoscaling is not enabled, and the existing (only) node doesn’t have enough resources for provisioning the pod.` **is the right answer.**

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

```
kubectl describe pod myapp-deployment-58ddbbb995-lp86m

Events:

Type     Reason            Age                  From               Message

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

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

Question 26:

Skipped

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

- ○

  Configure a job in BigQuery to fetch all Compute Engine logs from Stackdriver. Set up Cloud Scheduler to trigger a Cloud Function every day at midnight. Grant the Cloud Function the BigQuery jobUser role on the pt-logs dataset and trigger the BigQuery job from Cloud Function.

- ○

  Add a metadata tag with key: logs-destination and value: bq://pt-logs, and grant the VM service accounts BigQuery Data Editor role on the pt-logs dataset.

- ○

  Create an export for all logs in Cloud Logging and set up a Cloud Pub/Sub topic as the sink destination. Have a Cloud Function trigger based on the messages in the topic and configure it to send logs Compute Engine service to BigQuery pt-logs dataset.

- ○

  Create an export for Compute Engine logs in Cloud Logging and set up BigQuery pt-logs dataset as sink destination.

  (Correct)

Explanation

`Add a metadata tag with key: logs-destination and value: bq://pt-logs, and grant the VM service accounts BigQuery Data Editor role on the pt-logs dataset.` **is not right.**

Among other things, roles/bigquery.dataEditor lets you Create, update, get, and delete the dataset's tables. However, setting a metadata tag logs-destination to bq://pt-logs does not affect how the logs are generated or forwarded. The stack driver agent is already installed, so the logs are forwarded to stack driver logging and not to the BigQuery dataset. Metadata entries are key-value pairs and do not influence this behaviour.
Ref: https://cloud.google.com/compute/docs/storing-retrieving-metadata

`Create an export for all logs in Cloud Logging and set up a Cloud Pub/Sub topic as the sink destination. Have a Cloud Function trigger based on the messages in the topic and configure it to send logs Compute Engine service to BigQuery pt-logs dataset.` **is not right.**

While the result meets our requirement, this option involves more steps; it is inefficient and expensive. Triggering a cloud function for each log message and then dropping messages that are not relevant (i.e. not compute engine logs) is inefficient.

We are paying for cloud function execution for all log entries when we are only interested in compute engine logs. Secondly, triggering a cloud function and then have that insert into the BigQuery dataset is also inefficient and expensive when the same can be achieved directly by configuring BigQuery as the sink destination - we don't pay for cloud function executions. Using this option, we are unnecessarily paying for Cloud Pub/Sub and Cloud Functions.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2
Ref: https://cloud.google.com/logging/docs/view/advanced-queries

`Configure a job in BigQuery to fetch all Compute Engine logs from Stackdriver. Set up Cloud Scheduler to trigger a Cloud Function every day at midnight. Grant the Cloud Function the BigQuery jobUser role on the pt-logs dataset and trigger the BigQuery job from Cloud Function.` **is not right.**
The role roles/bigquery.user provides permissions to run jobs, including queries, within the project. A cloud function with this role can execute queries in BigQuery; however, BigQuery can not query the compute engine logs.
Ref: https://cloud.google.com/bigquery/docs/access-control

`Create an export for Compute Engine logs in Cloud Logging and set up BigQuery pt-logs dataset as sink destination.` **is the right answer.**
In stack driver logging, it is possible to create a filter just to query the compute engine logs which is what we are interested.
Ref: https://cloud.google.com/logging/docs/view/advanced-queries
You can then export these logs into a sink that has the BigQuery dataset configured as the destination.
https://cloud.google.com/logging/docs/export/configure_export_v2
This way, just the logs that we need are exported to BigQuery. This option is the most efficient of all options and uses features provided by GCP out of the box.

Question 27:

Skipped

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

- ○

  Block project-wide public SSH keys from the instance to restrict SSH only through instance-level keys. Use ssh-keygen to generate a key for each analyst, distribute the keys to the analysts and ask them to SSH to the instance with their key from putty.

- ○

Block project-wide public SSH keys from the instance to restrict SSH only through instance-level keys. Use ssh-keygen to generate a single key for all analysts, distribute the key to the analysts and ask them to SSH to the instance with the key from putty.

- ○

  Enable OS Login by adding a metadata tag to the instance with key: enable-oslogin and value: TRUE, and grant roles/compute.osLogin role to the analysts group. Ask the analysts to SSH to the instance through Cloud Shell.

  (Correct)

- ○

  Enable OS Login by adding a metadata tag to the instance with key: enable-oslogin and value: TRUE. Ask the analysts to SSH to the instance through Cloud Shell.

Explanation

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

`Block project-wide public SSH keys from the instance to restrict SSH only through instance-level keys. Use ssh-keygen to generate a key for each analyst, distribute the keys to the analysts and ask them to SSH to the instance with their key from putty.` **is not right.**

Generating SSH keys for users is fine, but unless the SSH keys are added to the instance, users would not be able to SSH to the server. If you need your instance to ignore project-wide public SSH keys and use only the instance-level keys, you can block project-wide public SSH keys from the instance. This option only allows users whose public SSH key is stored in instance-level metadata to access the instance.
Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#edit-ssh-metadata

`Block project-wide public SSH keys from the instance to restrict SSH only through instance-level keys. Use ssh-keygen to generate a single key for all analysts, distribute the key to the analysts and ask them to SSH to the instance with the key from putty.` **is not right.**

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

`Enable OS Login by adding a metadata tag to the instance with key: enable-oslogin and value: TRUE. Ask the analysts to SSH to the instance through Cloud Shell.` **is not right.**

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

`Enable OS Login by adding a metadata tag to the instance with key: enable-oslogin and value: TRUE, and grant roles/compute.osLogin role to the analysts group. Ask the analysts to SSH to the instance through Cloud Shell.` **is the right answer.**

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

Question 28:

Skipped

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

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: demo-deployment
spec:
  selector:
    matchLabels:
      app: demo
  replicas: 2
  template:
    metadata:
      labels:
        app: demo
    spec:
      containers:
      - name:  demo
```

```
        image:  demo:2.7
        ports:
        - containerPort: 8080
```

```
apiVersion: v1
kind: Service
metadata:
  name: demo-service
spec:
  ports:
  - port:  80
    targetPort:  8080
    protocol: TCP
  selector:
    app: demo
```

```
kubectl get pods -l app=demo

NAME                               READY     STATUS        RESTART       AGE
demo-deployment-8998dab376-brm68       0/1      Pending      0             29m
demo-deployment-8998dab376-kpg18       1/1      Running      0             29m
```

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

- ○

  Check for error messages from demo-service Service object.

- ○

  Check logs of the container in demo-deployment-8998dab376-brm68 Pod.

- ○

  Check for error messages from demo-deployment Deployment object.

- ○

  Check for warning messages from demo-deployment-8998dab376-brm68 Pod.

  (Correct)

Explanation

`Check for error messages from demo-service Service object.` **is not right.**

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

`Check logs of the container in demo-deployment-8998dab376-brm68 Pod.` **is not right.**

Since the pod hasn't moved to Running state, the logs of the container would be empty. So running kubectl logs pod/demo-deployment-8998dab376-brm68 to check the logs of the pod isn't of much use.

`Check for error messages from demo-deployment Deployment object.` **is not right.**

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

Here's a sample output of this use case.

```
kubectl describe deployment demo-deployment

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

Events:

Type Reason Age From Message

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

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

`Check for warning messages from demo-deployment-8998dab376-brm68 Pod.` **is the right answer.**

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

```
kubectl describe pod demo-deployment-8998dab376-brm68

Events:

Type Reason Age From Message

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

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

Question 29:

Skipped

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

- ○

  GKE with horizontal pod autoscaling and cluster autoscaler enabled.

- ○

  Cloud Run on GKE.

- ○

  App Engine Flexible.

- ○

  Cloud Run.

  (Correct)

Explanation

`Cloud Run on GKE.` **is not right.**
Cloud Run on GKE can scale the number of pods to zero. The number of nodes per cluster cannot scale to zero, and these nodes are billed in the absence of requests.
Ref: https://cloud.google.com/serverless-options

`GKE with horizontal pod autoscaling and cluster autoscaler enabled.` **is not right.**
Like above, while you can set up the pod autoscaler to scale back the pods to zero, the number of nodes per cluster cannot scale to zero, and these nodes are billed in the absence of requests. If you specify the minimum node pool size of zero nodes, an idle node pool can scale down completely. However, at least one node must always be available in the cluster to run system Pods.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-autoscaler

`App Engine Flexible.` **is not right.**
App Engine flexible environment instances are Compute Engine virtual machines, and you can't truly scale down to zero and compute instances are billed in the absence of requests.
Ref: https://cloud.google.com/appengine/docs/flexible

`Cloud Run.` **is the right answer.**
Cloud Run is a fully managed compute platform that automatically scales your stateless containers. Cloud Run is serverless. Cloud Run abstracts away all infrastructure management. It automatically scales up and down from zero depending on traffic almost instantaneously. Cloud Run only charges you for the exact resources you use.
Ref: https://cloud.google.com/run

Question 30:

Skipped

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

- ○

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

- ○

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

  (Correct)

- ○

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

- ○

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

Explanation

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

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

`Have a single person from the procurement team access the document signing system with the service account credentials.` **is not right.**
While this would prevent password reuse, it goes against our requirements and results in a single person dependency.

`Register the application as a password vaulted app and set the credentials to the service account credentials.` **is the right answer.**
As a G Suite or Cloud Identity administrator, the password vaulted apps service enables you to manage access to some of the apps that don't support federation and that are available to users on the User Dashboard. The password vaulted apps service saves login credential sets for applications and assigns those credential sets to users through group association. When a user has access to one of these applications through a group, they can sign in to the application through the user dashboard, or they can sign in directly from the specific application. This functionality is possible by leveraging Chrome or Firefox extensions/plugins. When adding an app to the password vaulted apps service, you can search and choose from the available web-based applications in the app library, or you can add a custom app. You can then manage usernames and passwords safely while providing users in your organization with quick one-click access to all of the apps they already use.
Ref: https://support.google.com/cloudidentity/answer/9178974?hl=en

Question 31:
Skipped
Your company is migrating its on-premises data centre to Google Cloud Platform in several phases. The current phase requires the migration of the LDAP server onto a Compute Engine instance. However, several legacy applications in your on-premises data centre and few third-party applications still depend on the LDAP server for user authentication. How can you ensure the LDAP server is publicly reachable via TLS on UDP port 636?

- ○

  Add default-allow-udp network tag to the LDAP server Compute Engine Instance.

- ○

  Configure a firewall route called default-allow-udp and have the next hop as the LDAP server Compute Engine Instance.

- ○

  Configure a firewall rule to allow inbound (ingress) UDP traffic on port 636 from 0.0.0.0/0 for the network tag allow-inbound-udp-636, and add this network tag to the LDAP server Compute Engine Instance.

(Correct)

- ○

  Configure a firewall rule to allow outbound (egress) UDP traffic on port 636 to 0.0.0.0/0 for the network tag allow-outbound-udp-636, and add this network tag to the LDAP server Compute Engine Instance.

Explanation

`Configure a firewall route called default-allow-udp and have the next hop as the LDAP server Compute Engine Instance.` **is not right.**
Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations. These destinations can be inside your Google Cloud Virtual Private Cloud (VPC) network (for example, in another VM) or outside it. Routes aren't a suitable solution for our requirement as we need to enable EXTERNAL clients to reach our VM on port 636 using UDP.
Ref: https://cloud.google.com/vpc/docs/routes

`Add default-allow-udp network tag to the LDAP server Compute Engine Instance.` **is not right.**
Tags enable you to make firewall rules and routes applicable to specific VM instances, but default-allow-udp is not a network tag that GCP provides. The default network tags provided by GCP are default-allow-icmp, default-allow-internal, default-allow-RDP and default-allow-ssh. In this scenario, we are assigning a tag to the instance with no network rules, so there would be no difference in the firewall behaviour.
Ref: https://cloud.google.com/vpc/docs/add-remove-network-tags

`Configure a firewall rule to allow outbound (egress) UDP traffic on port 636 to 0.0.0.0/0 for the network tag allow-outbound-udp-636, and add this network tag to the LDAP server Compute Engine Instance.` **is not right.**
We are interested in enabling inbound traffic to our VM, whereas egress firewall rules control outgoing connections from target instances in your VPC network.
Ref: https://cloud.google.com/vpc/docs/firewalls#egress_cases

`Configure a firewall rule to allow inbound (ingress) UDP traffic on port 636 from 0.0.0.0/0 for the network tag allow-inbound-udp-636, and add this network tag to the LDAP server Compute Engine Instance.` **is the right answer.**
This option fits all the requirements. Ingress firewall rules control incoming connections from a source to target instances in your VPC network. We can create an ingress firewall rule to allow UDP port 636 for a network tag. And when we assign this network tag to the instance, the firewall rule applies to the instances, so traffic is accepted on port 636 using UDP. Although not specified in this option, it has to be assumed that the source for the firewall rule is set to 0.0.0.0/0, i.e. all IP ranges so

that external clients are allowed to connect to this VM.
Ref: https://cloud.google.com/vpc/docs/firewalls#ingress_cases

Question 32:
Skipped
Your company has a Citrix Licensing Server in a Windows VM in your on-premises data centre and needs to migrate this to Google Cloud Platform. You have provisioned a new Windows VM in a brand new Google project, and you want to RDP to the instance to install and register the licensing server. What should you do?

- ○

  Generate a JSON key for the default GCE service account and RDP with this key.

- ○

  Retrieve the RDP credentials by executing gcloud compute reset-windows-password and RDP with the credentials.

  (Correct)

- ○

  RDP to the VM with your Google Account.

- ○

  Add a metadata tag to the instance with key: windows-password and password as the value, and RDP with these details.

Explanation
`Add a metadata tag to the instance with key: windows-password and password as the value, and RDP with these details.` **is not right.**
It is not possible to specify a windows password at the time of creating windows VM instance. You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. Alternatively, you can generate passwords programmatically with API commands, but all these methods assume that you have an existing windows instance.
Ref: https://cloud.google.com/compute/docs/instances/windows/creating-passwords-for-windows-instances#gcloud

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

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

`Generate a JSON key for the default GCE service account and RDP with this key.` **is not right.**
This option is not a supported method of authentication for logging into the VM. You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. Alternatively, you can generate passwords programmatically with API commands.
Ref: https://cloud.google.com/compute/docs/instances/windows/creating-passwords-for-windows-instances#gcloud

`Retrieve the RDP credentials by executing gcloud compute reset-windows-password and RDP with the credentials.` **is the right answer.**
You can generate Windows passwords using either the Google Cloud Console or the gcloud command-line tool. This option uses the right syntax to reset the windows password.

```
gcloud compute reset-windows-password windows-instance
```

Ref: https://cloud.google.com/compute/docs/instances/windows/creating-passwords-for-windows-instances#gcloud
Question 33:
Skipped
You created a deployment manager template to automate the provisioning of a production Google Kubernetes Engine (GKE) cluster. The GKE cluster requires a monitoring pod running on each node (DaemonSet) in daemon-system namespace, and your manager has asked you to identify if it is possible to automate the provisioning of the monitoring pod along with the cluster using the least number of resources. How should you do this?

- ○

  Update the deployment manager template to add a metadata tag with key: daemon-system and value: DaemonSet manifest YAML.

- ○

  Have the Runtime Configurator create a RuntimeConfig resource with the DaemonSet definition.

- ○

  Add a new type provider in Deployment Manager for Kubernetes APIs and use the new type provider to create the DaemonSet resource.

  (Correct)

- ○

  Update the deployment manager template to provision a preemptable compute engine instance and configure its startup script to use kubectl to create the DaemonSet.

Explanation

`Update the deployment manager template to add a metadata tag with key: daemon-system and value: DaemonSet manifest YAML.` **is not right.**
Metadata entries are key-value pairs and do not influence this behaviour.
Ref: https://cloud.google.com/compute/docs/storing-retrieving-metadata

`Update the deployment manager template to provision a preemptable compute engine instance and configure its startup script to use kubectl to create the DaemonSet.` **is not right.**
It is possible to spin up a compute engine instance with a startup script that executes kubectl to create a DaemonSet deployment.

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

Ref: https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/
But this involves using the compute engine service, which is an additional service. We require to achieve using the fewest possible services, and as you'll notice later, the correct answer uses fewer services.

`Have the Runtime Configurator create a RuntimeConfig resource with the DaemonSet definition.` **is not right.**
You can configure the GKE nodes (provisioned by Deployment manager) to report their status to the Runtime Configurator, and when they are UP, you can run a task to create a DaemonSet. While this is possible, it involves one additional service - to run a task, e.g. using Cloud Functions, etc. We require to achieve using the fewest possible services, and as you'll notice later, the correct answer uses fewer services. Here is some more info about Runtime Configurator. The Runtime Configurator feature lets you define and store data as a hierarchy of key-value pairs in Google Cloud Platform. You can use these key-value pairs as a way to:

Dynamically configure services

Communicate service states

Send notification of changes to data

Share information between multiple tiers of services

For example, imagine a scenario where you have a cluster of nodes that run a startup procedure. During startup, you can configure your nodes to report their status to the

Runtime Configurator, and then have another application query the Runtime Configurator and run specific tasks based on the status of the nodes.

The Runtime Configurator also offers a Watcher service and a Waiter service. The Watcher service watches a specific key pair and returns when the value of the key pair changes, while the Waiter service waits for a specific end condition and returns a response once that end condition has been met.
Ref: https://cloud.google.com/deployment-manager/runtime-configurator

`Add a new type provider in Deployment Manager for Kubernetes APIs and use the new type provider to create the DaemonSet resource.` **is the right answer.**
A type provider exposes all resources of a third-party API to Deployment Manager as base types that you can use in your configurations. If you have a cluster running on Google Kubernetes Engine, you could add the cluster as a type provider and access the Kubernetes API using Deployment Manager. Using these inherited API, you can create a DaemonSet. This option uses just the Deployment Manager to create a DaemonSet and is, therefore, the right answer.
Ref: https://cloud.google.com/deployment-manager/docs/configuration/type-providers/creating-type-provider

Question 34:

Skipped

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

- ○

  Grant the user roles/iam.securityAdmin IAM role.

- ○

  Grant the user roles/iam.serviceAccountUser IAM role.

- ○

  Grant the user roles/iam.roleAdmin IAM role.

- ○

  Grant the user roles/iam.serviceAccountAdmin IAM role.

  (Correct)

Explanation

`Grant the user roles/iam.roleAdmin IAM role.` **is not right.**
roles/iam.roleAdmin is an administrator role that provides access to all custom roles in the project. This role doesn't include permissions needed to manage service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#roles-roles

`Grant the user roles/iam.securityAdmin IAM role.` **is not right.**
roles/iam.securityAdmin role is a Security admin role, with permissions to get and set any IAM policy. This role is too broad, i.e. includes too many permissions and goes against the principle of least privilege. Moreover, although this role provides iam.serviceAccounts.get/list, it doesn't provide iam.serviceAccounts.create, iam.serviceAccounts.delete and iam.serviceAccounts.update permissions that are needed for managing service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#iam-roles

`Grant the user roles/iam.serviceAccountUser IAM role.` **is not right.**
roles/iam.serviceAccountUser is a service Account User role which is used for running operations as the service account. This role does not provide the permissions iam.serviceAccounts.create, iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list which are required for managing service accounts.
Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

`Grant the user roles/iam.serviceAccountAdmin IAM role.` **is the right answer.**
roles/iam.serviceAccountAdmin is a Service Account Admin role that lets you Create and manage service accounts. This grants all the required permissions for managing service accounts (iam.serviceAccounts.create iam.serviceAccounts.delete, iam.serviceAccounts.update, iam.serviceAccounts.get/list etc) and therefore fits our requirements.
Ref: https://cloud.google.com/iam/docs/understanding-roles#service-accounts-roles

Question 35:

Skipped

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

- ○

  Configure a lifecycle rule to transition non-current versions to Nearline Storage Class after 30 days.

(Correct)

- ○

  Configure a lifecycle rule to transition objects from Regional Storage Class to Coldline Storage Class after 30 days.

- ○

  Configure a lifecycle rule to transition non-current versions to Coldline Storage Class after 30 days.

- ○

  Configure a lifecycle rule to transition objects from Regional Storage Class to Nearline Storage Class after 30 days.

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

`Configure a lifecycle rule to transition non-current versions to Coldline Storage Class after 30 days.` **is not right.**
Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Our requirement states we need to read or modify every month, so Coldline Storage is not an ideal storage class for our requirement.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

`Configure a lifecycle rule to transition objects from Regional Storage Class to Coldline Storage Class after 30 days.` **is not right.**
Coldline Storage is ideal for data you plan to read or modify at most once a quarter. Our requirement states we need to read or modify every month, so Coldline Storage is not an ideal storage class for our requirement. Moreover, we don't want to archive live versions; we want to archive just the noncurrent versions.
Ref: https://cloud.google.com/storage/docs/storage-classes#coldline

`Configure a lifecycle rule to transition objects from Regional Storage Class to Nearline Storage Class after 30 days.` **is not right.**
While Nearline Storage is ideal for data you plan to read or modify on average once per month or less, we don't want to archive live versions, we want to archive just the noncurrent versions.
Ref: https://cloud.google.com/storage/docs/storage-classes#nearline

`Configure a lifecycle rule to transition non-current versions to Nearline Storage Class after 30 days.` **is the right answer.**

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

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

Question 36:

Skipped

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

- ○

  Create a Kubernetes deployment from Redis image and run it in a GKE Cluster on a node pool with a single n1-standard-32 instance.

- ○

  Use Cloud Memorystore for Redis instance replicated across two zones and configured for 32 GB in-memory cache.

  (Correct)

- ○

  Run Redis on a single Google Compute Engine instance of type n1-standard-1, and configure Redis to use 32GB SSD persistent disk as caching backend.

- ○

  Set up Redis on a custom compute engine instance with 32 GB RAM and 6 virtual CPUs.

Explanation
Requirements

1. latency sensitive

2. 30 GB in-memory cache

3. 2 GB for rest of processes

4. Cost-effective

`Run Redis on a single Google Compute Engine instance of type n1-standard-1, and configure Redis to use 32GB SSD persistent disk as caching backend.` **is not right.**
Fetching data from disk is slower compared to fetching from in-memory. Our requirements state we need 30GB in-memory cache for a latency-sensitive website and a compute engine with disk can't provide in-memory cache.

`Set up Redis on a custom compute engine instance with 32 GB RAM and 6 virtual CPUs.` **is not right.**
While this option provides us with 32 GB of memory, a part of it used by the compute engine operating system as well as the reverse proxy process leaving us with less than 32GB which does not satisfy our requirements. Also, the reverse proxy consumes almost no CPU so having 6vCPUs is a waste of resources and money. Finally, setting up Redis on a custom compute engine instance makes no sense when you can provision a GCP Memorystore Service that does the same out of the box with minimal configuration and no-ops.

`Create a Kubernetes deployment from Redis image and run it in a GKE Cluster on a node pool with a single n1-standard-32 instance.` **is not right.**
Without going into details of the feasibility of this option, let's assume for now that this option is possible. But this option is quite expensive. An instance with machine type n1-standard-32 is over-provisioned for this requirement with 32 vCPUs and 120 GB Memory. At the time of writing, just the compute cost for a single n1-standard-32 instance is $1.5200 per hour in the Iowa region.
Ref: https://cloud.google.com/compute/all-pricing
In comparison, the cost of GCP Cloud Memorystore is $0.023 per GB-hr or $0.736 for 32GB per hour. Plus, you need to take into consideration the Cluster charges for GKE, setting up high availability as a single instance is a single point of failure etc. which shoots up the costs.
Ref: https://cloud.google.com/memorystore.

`Use Cloud Memorystore for Redis instance replicated across two zones and configured for 32 GB in-memory cache.` **is the right answer.**
This option is the only one that fits the requirements. Cloud Memorystore is a fully managed in-memory data store service for Redis built on scalable, secure, and highly available infrastructure managed by Google. Use Memorystore to build application caches that provide sub-millisecond data access.
Ref: https://cloud.google.com/memorystore
Memorystore for Redis instance pricing is charged per GB-hour, and you can scale as needed. You can also specify eviction (maxmemory) policies to restrict the rest of

processes to 2GB or the reverse proxy to 30GB or both; you can select a suitable maxmemory policy to handle scenarios when memory is full.
Ref: https://cloud.google.com/memorystore/docs/reference/redis-configs#maxmemory_policies

Question 37:

Skipped

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

- ○

  Local SSD, Snapshot Storage and Persistent disk storage.

  (Correct)

- ○

  GPU, Snapshot Storage and Persistent disk storage.

- ○

  Local SSD and GKE Cluster Management Fee.

- ○

  GPU and GKE Cluster Management Fee.

Explanation

`Local SSD and GKE Cluster Management Fee.` **is not right.**

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

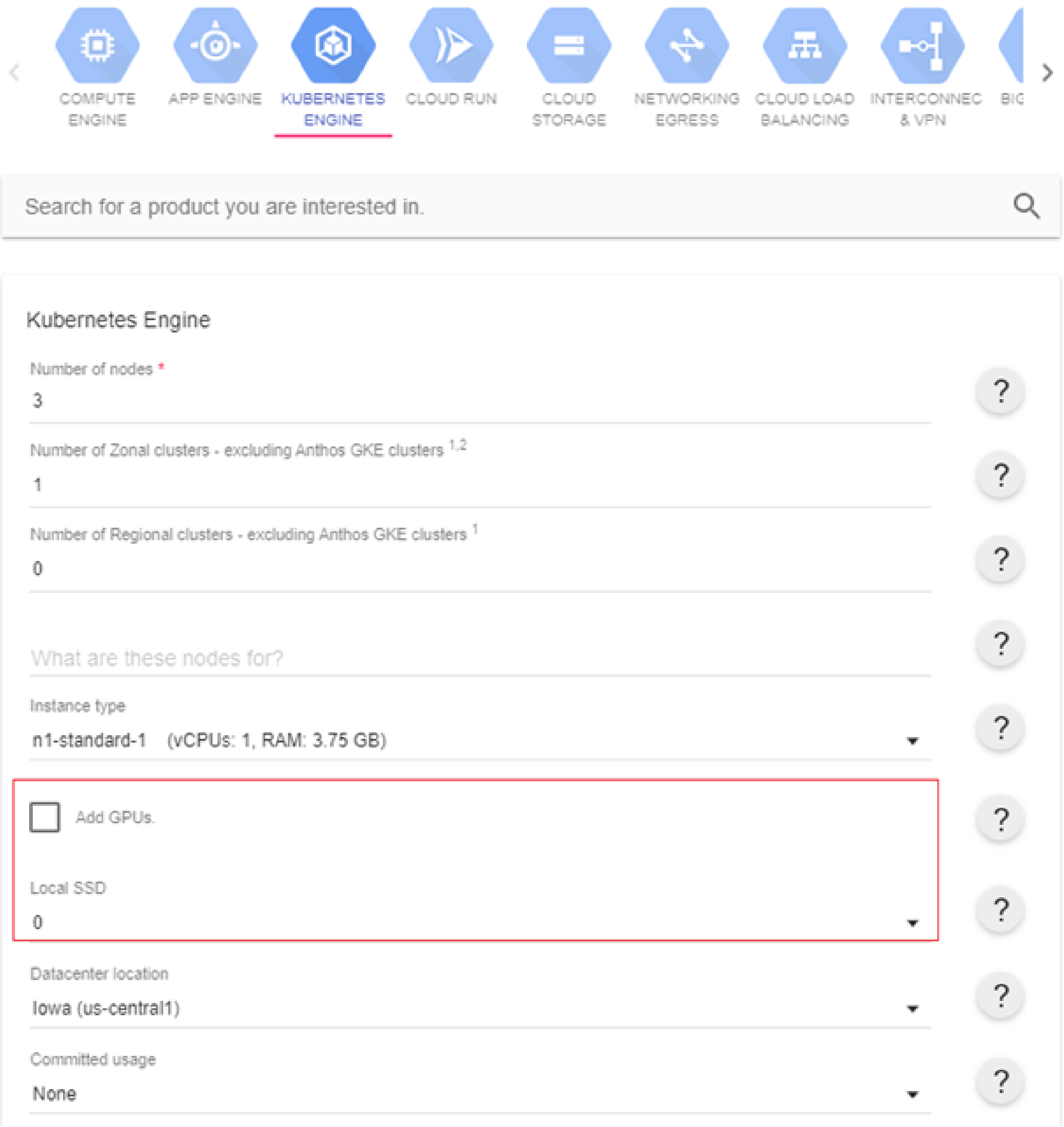
`GPU and GKE Cluster Management Fee.` **is not right.**

You don't need to add an estimated cost for cluster management as the calculator automatically applies this. At the time of writing this, GKE clusters accrue a management fee of $0.10 per cluster per hour, irrespective of cluster size or

topology. One zonal cluster per billing account is free. GKE cluster management fees do not apply to Anthos GKE clusters.
Ref: https://cloud.google.com/kubernetes-engine/pricing

`GPU, Snapshot Storage and Persistent disk storage.` **is not right.**
GPUs don't help us with our requirement of high IOPS. Compute Engine provides graphics processing units (GPUs) that you can add to your virtual machine instances to accelerate specific workloads on your instances such as machine learning and data processing. But this doesn't help increase IOPS.
Ref: https://cloud.google.com/compute/docs/gpus

`Local SSD, Snapshot Storage and Persistent disk storage.` **is the right answer.**
The pricing calculator for Kubernetes Engine offers us the ability to add GPUs as well as specify Local SSD requirements for estimation. GPUs don't help us with our requirement of high IOPS, but Local SSD does.
Ref: https://cloud.google.com/products/calculator



Search for a product you are interested in.

Kubernetes Engine

Number of nodes * 3

Number of Zonal clusters - excluding Anthos GKE clusters [1,2] 1

Number of Regional clusters - excluding Anthos GKE clusters [1] 0

What are these nodes for?

Instance type n1-standard-1 (vCPUs: 1, RAM: 3.75 GB)

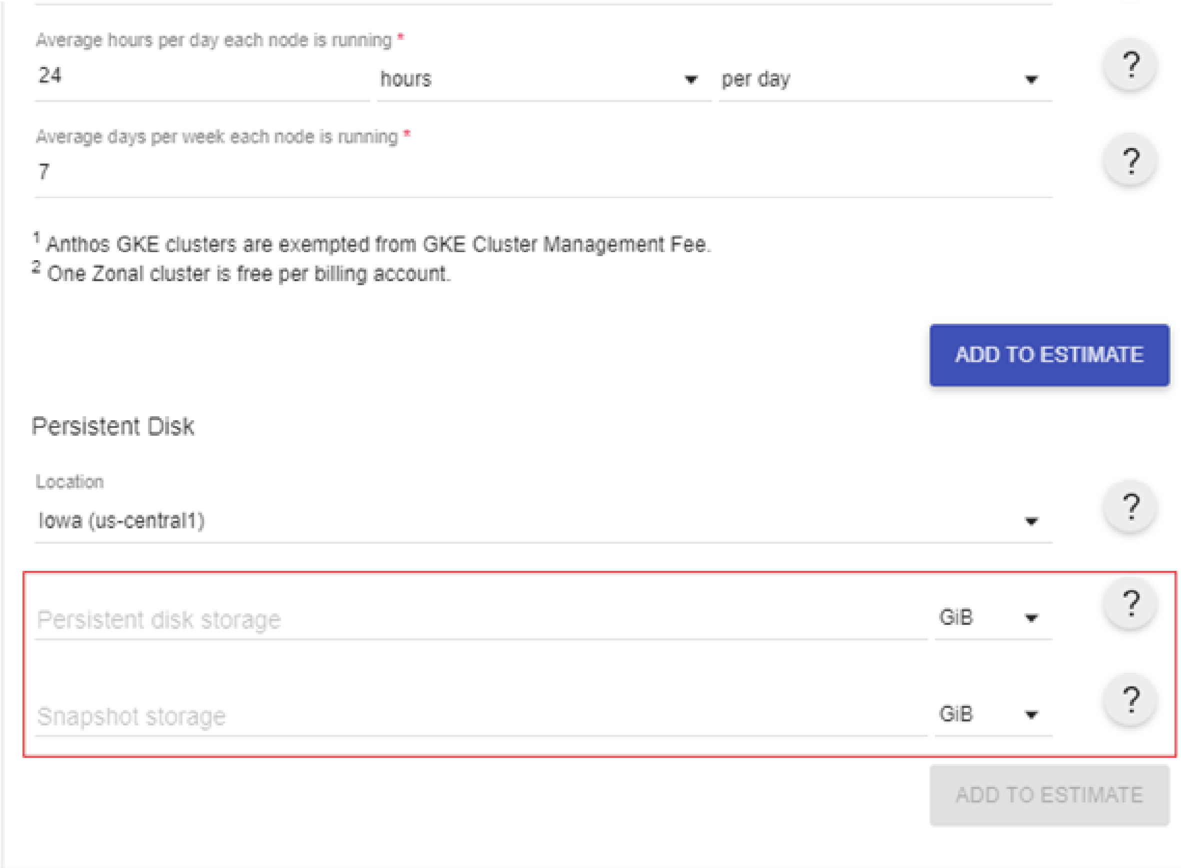
□ Add GPUs.

Local SSD 0

Datacenter location Iowa (us-central1)

Committed usage None

GKE offers always-encrypted local solid-state drive (SSD) block storage. Local SSDs are physically attached to the server that hosts the virtual machine instance for very high input/output operations per second (IOPS) and very low latency compared to persistent disks. Ref: https://cloud.google.com/kubernetes-engine Once you fill in the local SSD requirement, you can fill in persistent disk storage and snapshot storage.



Average hours per day each node is running *
24 hours per day

Average days per week each node is running *
7

[1] Anthos GKE clusters are exempted from GKE Cluster Management Fee.
[2] One Zonal cluster is free per billing account.

Question 38:

Skipped

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

- ○

  Use gcloud to set up two gcloud configurations – one for each project. Write a script to activate the development gcloud configuration, retrieve the list of compute engine instances, then activate production gcloud configuration and retrieve the list of compute engine instances. Schedule the script using cron.

  (Correct)

- ○

  Use gsutil to set up two gcloud configurations – one for each project. Write a script to activate the development gcloud configuration, retrieve the list of compute engine instances, then activate production gcloud configuration and retrieve the list of compute engine instances. Schedule the script using cron.

- ○

  Have your operations engineer export this information from GCP console to Cloud Datastore every day just before midnight.

- ○

  Have your operations engineer execute a script in Cloud Shell to export this information to Cloud Storage every day just before midnight.

Explanation

`Have your operations engineer execute a script in Cloud Shell to export this information to Cloud Storage every day just before midnight.` **is not right.**
You want an automated process, but this is a manual activity that needs to be executed daily.

`Have your operations engineer export this information from GCP console to Cloud Datastore every day just before midnight.` **is not right.**
You want an automated process, but this is a manual activity that needs to be executed daily.

`Use gsutil to set up two gcloud configurations – one for each project. Write a script to activate the development gcloud configuration, retrieve the list of compute engine instances, then activate production gcloud configuration and retrieve the list of compute engine instances. Schedule the script using cron.` **is not right.**
The gsutil config command applies to users who have installed gsutil as a standalone tool and is used for obtaining access credentials for Cloud Storage and writes a boto/gsutil configuration file containing the obtained credentials along with several other configuration-controllable values.
Ref: https://cloud.google.com/storage/docs/gsutil/commands/config
It is not used for creating gcloud configurations. You use gcloud config to do that.
https://cloud.google.com/sdk/gcloud/reference/config/configurations/create

`Use gcloud to set up two gcloud configurations – one for each project. Write a script to activate the development gcloud configuration, retrieve the list of compute engine instances, then activate production gcloud configuration and retrieve the list of compute engine instances. Schedule the script using cron.` **is the right answer.**
You can create two configurations - one for the development project and another for the production project. And you do that by running "gcloud config configurations create" command.
https://cloud.google.com/sdk/gcloud/reference/config/configurations/create

In your custom script, you can load these configurations one at a time and execute gcloud compute instances list to list Google Compute Engine instances in the project that is active in the gcloud configuration.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
Once you have this information, you can export it in a suitable format to a suitable target, e.g. export as CSV or export to Cloud Storage/BigQuery/SQL, etc.

Question 39:
Skipped
Your organization has several applications in the on-premises data centre that depend on Active Directory for user identification and authorization. Your organization is planning a migration to Google Cloud Platform and requires complete control over the Cloud Identity accounts used by staff to access Google Services and APIs. Where possible, you want to re-use Active Directory as the source of truth for identification and authorization. What should you do?

- ○

  Ask your operations team to export identities from active directory into a comma-separated file and use GCP console to import them into Cloud Identity daily.

- ○

  Create a custom script that synchronizes identities between Active Directory and Cloud Identity. Use Google Cloud Scheduler to run the script regularly.

- ○

  Ask all staff to create Cloud Identity accounts using their Google email address and require them to re-use their AD password for Cloud Identity account.

- ○

  Synchronize users in Google Cloud Identity with identities in Active directory by running Google Cloud Directory Sync (GCDS).

  (Correct)

Explanation
`Create a custom script that synchronizes identities between Active Directory and Cloud Identity. Use Google Cloud Scheduler to run the script regularly.` **is not right.**
You could do this, but this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

`Ask your operations team to export identities from active directory into a comma-separated file and use GCP console to import them into Cloud Identity daily.` **is not right.**
You could do this, but like above this process is manual, error-prone, time-consuming, and should be avoided especially when there is a service/tool that does it out of the box with minimal configuration.

`Ask all staff to create Cloud Identity accounts using their Google email address and require them to re-use their AD password for Cloud Identity account.` **is not right.**
If you let employees create accounts, your organization no longer has full control over the Google accounts used. This approach has several other issues concerning creating/managing user accounts and should be avoided.

`Synchronize users in Google Cloud Identity with identities in Active directory by running Google Cloud Directory Sync (GCDS).` **is the right answer.**
Since we already have user identities in Active Directory, it makes sense to reuse this directory as the source of truth for identities. But for GCP, you need identities either in G Suite or Google Cloud Identity. Cloud Directory Sync is a tool that enables you to synchronize users, groups, and other data from an Active Directory/LDAP service to their Google Cloud domain directory. This performs a one-way synchronization and ensures Cloud Identity users match that of your Active Directory. This also helps with our requirement of the organization having full control over the accounts used by employees.
Ref: https://tools.google.com/dlpage/dirsync/
Ref: https://support.google.com/a/answer/106368?hl=en#:~:text=With%20Google%20Cloud%20Directory%20Sync,files)%20to%20your%20Google%20Account.

Question 40:
Skipped
A Data Support Engineer at your company accidentally disclosed customer PII data in a support case in Google Cloud Console. Your compliance team wants to prevent this from occurring again and has asked you to set them up as approvers for cases raised by support teams. You want to follow Google Best Practices. What IAM access should you grant them?

- ○

  Grant roles/accessapproval.approver IAM role to the compliance team group.

  (Correct)

- ○

Grant roles/accessapproval.approver IAM role to all members of the compliance team.

- ○

Grant roles/iam.roleAdmin IAM role to all members of the compliance team.

- ○

Grant roles/iam.roleAdmin IAM role to the compliance team group.

Explanation

`Grant roles/iam.roleAdmin IAM role to all members of the compliance team.` **is not right.**

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

`Grant roles/iam.roleAdmin IAM role to the compliance team group.` **is not right.**

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

`Grant roles/accessapproval.approver IAM role to all members of the compliance team.` **is not right.**

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

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

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

`Grant roles/accessapproval.approver IAM role to the compliance team group.` **is the right answer.**

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

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

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

Question 41:

Skipped

Your company has terabytes of audit logs and analytics data in multiple BigQuery datasets. Some of these data sets need to be retained long term for audit purposes. You want to ensure analysts do not delete this data. What should you do?

- ○

  Grant roles/bigquery.user IAM role to the analysts' group.

  (Correct)

- ○

  Grant a custom role with just the required query permissions to all the analysts.

- ○

  Grant a custom role with just the required query permissions to the analysts' group.

- ○

  Grant roles/bigquery.dataOwner IAM role to the analysts' group.

Explanation

`Grant roles/bigquery.dataOwner IAM role to the analysts' group.` **is not right.**
roles/bigquery.dataEditor is a BigQuery Data Editor role which when applied to a dataset provides permissions to read the dataset's metadata and to list tables in the dataset; Create, update, get, and delete the dataset's tables. When applied at the project or organization level, this role can also create new datasets. We want to grant users query access but not modify/delete.

`Grant a custom role with just the required query permissions to all the analysts.` **is not right.**
This option might work, but this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

`Grant a custom role with just the required query permissions to the analysts' group.` **is not right.**
This option might work, but like above this is a manual, error-prone, time-consuming, and adds to operational overhead. If GCP provides a primitive role that is fit for purpose, this should be preferred over creating custom roles.

`Grant roles/bigquery.user IAM role to the analysts’ group.` **is the right answer.**

roles/bigquery.user is a BigQuery User role, which when applied to a project provides the ability to run jobs, including queries, within the project. A member with this role can enumerate their jobs, cancel their jobs, and enumerate datasets within a project.
Ref: https://cloud.google.com/iam/docs/understanding-roles#bigquery-roles

Question 42:

Skipped

Your compliance officer has requested you to provide an external auditor view, but not edit, access to all project resources. What should you do?

- ○

  Add the auditors’ account to the predefined project viewer IAM role.

  (Correct)

- ○

  Add the auditors’ account to a custom IAM role that has view-only permissions on all the project services.

- ○

  Add the auditors’ account to the predefined service viewer IAM role.

- ○

  Add the auditors’ account to a custom IAM role that has view-only permissions on all the project resources.

Explanation

`Add the auditors’ account to the predefined project viewer IAM role.` **is the right answer**

The primitive role roles/viewer provides read access to all resources in the project. The permissions in this role are limited to Get and list access for all resources. As we have an out of the box role that exactly fits our requirement, we should use this.
Ref: https://cloud.google.com/resource-manager/docs/access-control-proj
It is advisable to use the existing GCP provided roles over creating custom roles with similar permissions as this becomes a maintenance overhead. If GCP modifies how permissions are handled, or adds/removes permissions, the default GCP provided roles are automatically updated. However, the responsibility is with us for custom IAM roles, which adds to the operational overhead and should be avoided.

Question 43:

Skipped

You want to provide an operations engineer access to a specific GCP project. Everyone at your company has G Suite accounts. How should you grant access?

- ○

  Run G Suite to Cloud Identity migration tool to convert G Suite Accounts into Cloud Identity accounts. Grant the necessary roles to the Cloud Identity account.

- ○

  Disable G Suite Sign in, enable Cloud Identity Sign in, and add their email address to Cloud Identity. Grant the necessary roles to the Cloud Identity account.

- ○

  Assign the necessary roles to their G Suite email address.

  (Correct)

- ○

  Add the operations engineer to the gcp-console-access group in your G Suite domain and grant the necessary roles to the group.

Explanation

`Assign the necessary roles to their G Suite email address.` **is the right answer.**

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

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

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

Question 44:

Skipped

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

- ○

Update the SAML integrations on the existing third-party apps to use Google as the Identity Provider (IdP).

- ○

Configure a SAML SSO integration with Okta as the Identity Provider (IdP) and Google as the Service Provider (SP).

(Correct)

- ○

Enable OAuth 2.0 with Okta OAuth Authorization Server for web applications.

- ○

Enable OAuth 2.0 with Okta OAuth Authorization Server for desktop and mobile applications.

Explanation

`Update the SAML integrations on the existing third-party apps to use Google as the Identity Provider (IdP).` **is not right.**
The question states that you want to use the company's existing Identity provider for SSO, not Google.
Ref: https://cloud.google.com/identity/solutions/enable-sso

`Enable OAuth 2.0 with Okta OAuth Authorization Server for desktop and mobile applications.` **is not right.**
OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow.
See https://oauth.net/2/ for more information about OAuth 2.0, which is quite a popular protocol for SSO. Enabling OAuth 2.0 for mobile and desktop apps does not affect how users login into GCP console.
Ref: https://cloud.google.com/identity/solutions/enable-sso

`Enable OAuth 2.0 with Okta OAuth Authorization Server for web applications.` **is not right.**
OAuth 2.0 credentials are needed for an OAuth 2.0 flow, not SAML flow.
See https://oauth.net/2/ for more information about OAuth 2.0, which is quite a popular protocol for SSO. Enabling OAuth 2.0 for Web apps does not affect how users login into GCP console.
Ref: https://cloud.google.com/identity/solutions/enable-sso

`Configure a SAML SSO integration with Okta as the Identity Provider (IdP) and Google as the Service Provider (SP).` **is the right answer.**
This option fits the requirement. You configure applications (service providers) to accept SAML assertions from the company's existing identity provider and users in

Cloud Identity can sign in to various applications through the third-party single sign-on (SSO) identity provider. It is important to note that user authentication occurs in the third-party IdP, so the absence of a Gmail login is not an issue for signing in.
Ref: https://cloud.google.com/identity/solutions/enable-sso
If you have a third-party IdP, you can still configure SSO for third-party apps in the Cloud Identity catalogue. User authentication occurs in the third-party IdP, and Cloud Identity manages the cloud apps.
To use Cloud Identity for SSO, your users need Cloud Identity accounts. They sign in through your third-party IdP or using a password on their Cloud Identity accounts.

Question 45:

Skipped

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

- ○

  Configure a ClusterIP service for the application and set up a DNS A record on the application DNS to point to the IP service.

- ○

  Configure a NodePort service for the application and use an Ingress service to open it to the public.

  (Correct)

- ○

  Configure an HAProxy service for the application and set up a DNS A records on the application DNS to the public IP address of the node that runs HAProxy.

- ○

  Configure a NodePort service on port 443 for the application and set up a dynamic pool of DNS A records on the application DNS to achieve round-robin load balancing.

Explanation

`Configure a ClusterIP service for the application and set up a DNS A record on the application DNS to point to the IP service.` **is not right.**

Kubernetes Service of type ClusterIP exposes the Service on a cluster-internal IP. Choosing this value makes the Service only reachable from within the cluster so you

can not route external traffic to this IP.
Ref: https://kubernetes.io/docs/concepts/services-networking/service/

`Configure an HAProxy service for the application and set up a DNS A records on the application DNS to the public IP address of the node that runs HAProxy.` **is not right.**
HAProxy is a popular Kubernetes ingress controller. An Ingress object is an independent resource, apart from Service objects, that configures external access to a service's pods. Ingress Controllers still need a way to receive external traffic. You can do this by exposing the Ingress Controller as a Kubernetes service with either NodePort or LoadBalancer type. You can't use public IP of the node the HAProxy is running on as this may be running in any node in the Kubernetes Cluster. In a majority of scenarios, these nodes do not have public IPs. They are meant to be private, and the pods/deployments are accessed through Service objects.
Ref: https://www.haproxy.com/blog/dissecting-the-haproxy-kubernetes-ingress-controller/

`Configure a NodePort service on port 443 for the application and set up a dynamic pool of DNS A records on the application DNS to achieve round-robin load balancing.` **is not right.**
Kubernetes Service of type NodePort uses a port in the range 30000-32767, we can't configure it for port 443. This option also requires downstream clients to have an awareness of all of your nodes' IP addresses, since they will need to connect to those addresses directly. In other words, they won't be able to connect to a single, proxied IP address. And this is against our requirement of "a public IP address".
Ref: https://kubernetes.io/docs/concepts/services-networking/service/
Ref: https://www.haproxy.com/blog/dissecting-the-haproxy-kubernetes-ingress-controller/

`Configure a NodePort service for the application and use an Ingress service to open it to the public.` **is the right answer.**
This option meets all the requirements. When you create an Ingress object, the GKE Ingress controller creates a Google Cloud HTTP(S) Load Balancer and configures it according to the information in the Ingress and its associated Services. You have a choice between an Internal HTTP(s) Load Balancer and External HTTP(s) Load Balancer, and as we require to expose the service to the public, we need to use external HTTP(s) Load Balancer.
Ref: https://cloud.google.com/kubernetes-engine/docs/concepts/ingress#overview
With (Global) Cloud Load Balancing, a single anycast IP front-ends all your backend instances in regions around the world. It provides cross-region load balancing, including automatic multi-region failover, which gently moves traffic in fractions if backends become unhealthy.
Ref: https://cloud.google.com/load-balancing/
The ingress accepts traffic from the cloud load balancer and can distribute the traffic across the pods in the cluster.
Ref: https://kubernetes.io/docs/concepts/services-networking/ingress/

Some additional info: To deploy an external load balancer in Ingress, you use the gce ingress class. (For an internal load balancer, you would use gce-internal ingress class.)
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/load-balance-ingress#creating_an_ingress
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/internal-load-balance-ingress#step_4_deploy_ingress

Question 46:
Skipped
Your runs several applications on the production GKE cluster. The machine learning team runs their training models in the default GKE cluster node pool, but the processing is slower and is delaying their analysis. You want the ML jobs to run on NVIDIA® Tesla® K80: nvidia-tesla-k80 GPU for better performance and increased throughput. What should you do?

- ○

  Create a dedicated GKE cluster with GPU enabled node pool as per the required specifications, and migrate the ML jobs to the new cluster.

- ○

  Terminate all existing nodes in the node pools and create new nodes with the required GPUs attached.

- ○

  Add a metadata tag to the pod specification with key: accelerator and value: tesla-gpu.

- ○

  Create a new GPU enabled node pool with the required specification, and configure node selector on the pods with key: cloud.google.com/gke-accelerator and value: nvidia-tesla-k80.

  (Correct)

Explanation
`Add a metadata tag to the pod specification with key: accelerator and value: tesla-gpu.` **is not right.**

There are two issues with this approach. One - the syntax is invalid. Two - You cannot add GPUs to existing node pools.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus

`Terminate all existing nodes in the node pools and create new nodes with the required GPUs attached.` **is not right.**
There are two issues with this approach.
One - recreating all nodes to enable GPUs makes the cluster very expensive. Only the ML team needs access to GPUs to train their models. Recreating all nodes to enable GPUs helps your ML team use them, but they are left unused for all other workloads yet cost you money.
Two - Even though your nodes have GPUs enabled, you still have to modify pod specifications to request GPU. This step isn't performed in this option.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus

`Create a dedicated GKE cluster with GPU enabled node pool as per the required specifications, and migrate the ML jobs to the new cluster.` **is not right.**
While this works, it increases the cost as you now pay the Kubernetes cluster management fee for two clusters instead of one. GKE clusters accrue a management fee that is per cluster per hour, irrespective of cluster size or topology.
Ref: https://cloud.google.com/kubernetes-engine/pricing

`Create a new GPU enabled node pool with the required specification, and configure node selector on the pods with key: cloud.google.com/gke-accelerator and value: nvidia-tesla-k80.` **is the right answer.**
This option is the most optimal solution for the requirement. Rather than recreating all nodes, you create a new node pool with GPU enabled. You then modify the pod specification to target particular GPU types by adding node selector to your workload's Pod specification. You still have a single cluster, so you pay Kubernetes cluster management fee for just one cluster, thus minimizing the cost.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/gpus
Ref: https://cloud.google.com/kubernetes-engine/pricing

Example:

```
apiVersion: v1
kind: Pod
metadata:
name: my-gpu-pod
spec:
containers:
- name: my-gpu-container
    image: nvidia/cuda:10.0-runtime-ubuntu18.04
    command: ["/bin/bash"]
    resources:
```

```
    limits:

    nvidia.com/gpu: 2

nodeSelector:

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

Question 47:

Skipped

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

- ○

  Ask your finance department to grant you the Project Billing Manager IAM role. Set up a budget and an alert in the billing account.

- ○

  Ask your finance department to grant you the Billing Account Administrator IAM role. Set up a budget and an alert for the test project in the billing account.

  (Correct)

- ○

  Ask your finance department to grant you the Billing Account Administrator IAM role. Set up a budget and an alert in the billing account.

- ○

  Ask your finance department to grant you the Project Billing Manager IAM role. Set up a budget and an alert for the test project in the billing account.

Explanation

`Ask your finance department to grant you the Project Billing Manager IAM role. Set up a budget and an alert for the test project in the billing account.` **is not right.**

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

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

`Ask your finance department to grant you the Project Billing Manager IAM role. Set up a budget and an alert in the billing account.` **is not right.**
Project Billing Manager role allows a user to attach the project to the billing account, but does not grant any rights over resources. This role does not provide user permissions to view spending, create budgets and alerts.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam

`Ask your finance department to grant you the Billing Account Administrator IAM role. Set up a budget and an alert in the billing account.` **is not right.**
Billing Account Administrator role enables a user to view the spend and set budget alerts. But the budget here isn't scoped to the test project. Since the single billing account is linked to all three projects, this results in budget alerts being triggered for Compute Engine usage on all three projects - which is against our requirements.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

`Ask your finance department to grant you the Billing Account Administrator IAM role. Set up a budget and an alert for the test project in the billing account.` **is the right answer.**
Billing Account Administrator role enables a user to view the spend and set budget alerts. Also, the budget here is scoped to a single project. Therefore, when the compute engine costs exceed the threshold in the project, we send an alert, and this only works for the scoped project, and not all projects linked to the billing account.
Ref: https://cloud.google.com/billing/docs/how-to/billing-access#overview-of-cloud-billing-roles-in-cloud-iam
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

Question 48:
Skipped
An external partner working on a production issue has asked you to share a list of all GCP APIs enabled for your GCP production project – production_v1. How should you retrieve this information?

- ○

  Execute gcloud info to retrieve the account information and execute gcloud services list --account {Account} to retrieve a list of all services enabled for the project.

- ○

  Execute gcloud services list --available to retrieve a list of all services enabled for the project.

- ○

  Execute gcloud init production_v1 to set production_v1 as the current project in gcloud configuration and execute gcloud services list --available to retrieve a list of all services enabled for the project.

- ○

  Execute gcloud projects list --filter='name:production_v1' to retrieve the ID of the project, and execute gcloud services list --project {project ID} to retrieve a list of all services enabled for the project.

  (Correct)

Explanation

`Execute gcloud init production_v1 to set production_v1 as the current project in gcloud configuration and execute gcloud services list --available to retrieve a list of all services enabled for the project.` **is not right.**

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

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

Also, to set the current project, you need to use gcloud config set project {project id}

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

gcloud init is used for initializing or reinitializing gcloud configurations.

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

`Execute gcloud info to retrieve the account information and execute gcloud services list --account {Account} to retrieve a list of all services enabled for the project.` **is not right.**

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

```
gcloud services list --account {account_id}
```

Errors with the following error.

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

To set your project, run:

```
$ gcloud config set project PROJECT_ID
```

or to unset it, run:

```
$ gcloud config unset project
```

`Execute gcloud services list --available to retrieve a list of all services enabled for the project.` **is not right.**
--available return the services available to the project to enable and not the services that are enabled. This list will include any services that the project has already enabled plus the services that the project can enable.
Ref: https://cloud.google.com/sdk/gcloud/reference/services/list

`Execute gcloud projects list --filter='name:production_v1' to retrieve the ID of the project, and execute gcloud services list --project {project ID} to retrieve a list of all services enabled for the project.` **is the right answer.**
gcloud projects list lists all the projects accessible by the active account. Adding the filter with name criteria retrieves just the project with the specific name. For the gcloud services list command, --enabled is the default. So running

```
gcloud services list --project {project ID}
```

is the same as running

```
gcloud services list --project {project ID} --enabled
```

which would get all the enabled services for the project.
Question 49:

Skipped

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

- ○

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

  (Correct)

- ○

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

- ○

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

- ○

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

Explanation

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

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

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

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

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

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

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

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

Question 50:

Skipped

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

- ○

Add bastion hosts in GCP as well as on-premises network and set up a proxy tunnel between the bastion hosts in GCP and the bastion hosts in the on-premises network. Allow applications in the data centre to scale to Google Cloud through the proxy tunnel.

- ○

Create a new GCP project and a new VPC and enable VPC peering between the new VPC and networks in the data centre.

- ○

Create a new VPC in GCP with a non-overlapping IP range and configure Cloud VPN between the on-premises network and GCP. Allow applications in the data centre to scale to Google Cloud through the VPN tunnel.

(Correct)

- ○

Create a new GCP project and a new VPC and make this a shared VPC with the on-premises network. Allow applications in the data centre to scale to Google Cloud on the shared VPC.

Explanation

`Create a new GCP project and a new VPC and make this a shared VPC with the on-premises network. Allow applications in the data centre to scale to Google Cloud on the shared VPC.` **is not right.**

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

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

`Create a new GCP project and a new VPC and enable VPC peering between the new VPC and networks in the data centre.` **is not right.**

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

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

`Add bastion hosts in GCP as well as on-premises network and set up a proxy tunnel between the bastion hosts in GCP and the bastion hosts in the on-premises network. Allow applications in the data centre to scale to Google Cloud through the proxy tunnel.` **is not right.**
Bastion hosts provide an external facing point of entry into a network containing private network instances. Bastion hosts are primarily for end users so they can connect to an instance that does not have an external IP address through a bastion host.
Ref: https://cloud.google.com/compute/docs/instances/connecting-advanced

`Create a new VPC in GCP with a non-overlapping IP range and configure Cloud VPN between the on-premises network and GCP. Allow applications in the data centre to scale to Google Cloud through the VPN tunnel.` **is the right answer.**
Cloud VPN securely connects your on-premises network to your Google Cloud (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection.
Ref: https://cloud.google.com/vpn/docs/concepts/overview

Question 1:

Skipped

You are deploying an application on the Google Compute Engine, and you want to minimize network egress costs. The organization has a policy that requires you to block all but essential egress traffic. What should you do?

- ○

  Enable a firewall rule at priority 100 to block all egress traffic, and another firewall rule at priority 65534 to allow essential egress traffic.

- ○

  Enable a firewall rule at priority 65534 to block all egress traffic, and another firewall rule at priority 100 to allow essential egress traffic.

  (Correct)

- ○

  Enable a firewall rule at priority 100 to allow ingress and essential egress traffic.

- ○

  Enable a firewall rule at priority 100 to allow essential egress traffic.

Explanation

`Enable a firewall rule at priority 100 to allow essential egress traffic.` **is not right.**

This option would enable all egress traffic. Every VPC network has two implied firewall rules, one of which is the implied allow egress rule. This egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. Since we want to restrict egress on all but required traffic, you can't rely on just the high priority rules to allow specific traffic.
Ref: https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules

`Enable a firewall rule at priority 100 to allow ingress and essential egress traffic.` **is not right.**

There is no relation between ingress and egress, and they both work differently. Like above, this would enable all egress traffic. Every VPC network has two implied firewall rules, one of which is the implied allow egress rule. This egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. Since we want to restrict egress on all but required traffic, you can't rely on

just the high priority rules to allow specific traffic.
Ref: https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules

`Enable a firewall rule at priority 100 to block all egress traffic, and another firewall rule at priority 65534 to allow essential egress traffic.` **is not right.**
The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. The highest priority rule applicable for a given protocol and port definition takes precedence over others. In this scenario, having a deny all traffic at priority 100 takes effect over all other egress rules that allow traffic at a lower priority resulting in all outgoing traffic being blocked.
Ref: https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

`Enable a firewall rule at priority 65534 to block all egress traffic, and another firewall rule at priority 100 to allow essential egress traffic.` **is the right answer.**
The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. The highest priority rule applicable for a given protocol and port definition takes precedence over others. The relative priority of a firewall rule determines whether it is applicable when evaluated against others. In this scenario, the allow rule at priority 100 is evaluated first, and this allows the required egress traffic. The deny rule at 65534 priority is executed last and denies all other traffic that is not allowed by previous allow rules.
Ref: https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

Question 2:
Skipped
You work for a multinational delivery services company that uses Apache Cassandra DB as the backend store for its delivery track and trace system. The existing on-premises data centre is out of space. To cope with an anticipated increase in requests in the run-up to Christmas, you want to move this application rapidly to Google Cloud with minimal effort whilst ensuring you can spin up multiple stacks (development, test, production) and isolate them from each other. How can you do this?

- ○

  Launch Cassandra DB from Cloud Marketplace.

  (Correct)

- ○

  Install an instance of Cassandra DB on Google Cloud Compute Engine, take a snapshot of this instance and use the snapshot to spin up additional instances of Cassandra DB.

- ○

  Download the installation guide for Cassandra on GCP and follow the instructions to install the database.

- ○

  Install an instance of Cassandra DB on Google Cloud Compute Engine, take a snapshot of this instance and upload to Google Cloud Storage bucket. Every time you need a new instance of Cassandra DB, spin up a new compute engine instance from the snapshot.

Explanation

`Download the installation guide for Cassandra on GCP and follow the instructions to install the database.` **is not right.**

There is a simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to follow the installation guide to install it.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

`Install an instance of Cassandra DB on Google Cloud Compute Engine, take a snapshot of this instance and use the snapshot to spin up additional instances of Cassandra DB.` **is not right.**

Like above, there is a simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

`Install an instance of Cassandra DB on Google Cloud Compute Engine, take a snapshot of this instance and upload to Google Cloud Storage bucket. Every time you need a new instance of Cassandra DB, spin up a new compute engine instance from the snapshot.` **is not right.**

Like above, there is a simple and straightforward way to deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. You don't need to do this in a convoluted way.

Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud

Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

`Launch Cassandra DB from Cloud Marketplace.` **is the right answer.**
You can deploy Cassandra as a Service, called Astra, on the Google Cloud Marketplace. Not only do you get a unified bill for all GCP services, but you can also create Cassandra clusters on Google Cloud in minutes and build applications with Cassandra as a database as a service without the operational overhead of managing Cassandra. Each instance is deployed to a separate set of VM instances (at the time of writing this, 3 x VM instance: 4 vCPUs + 26 GB memory (n1-highmem-4) + 10-GB Boot Disk) which are all isolated from the VM instances for other Cassandra deployments.
Ref: https://cloud.google.com/blog/products/databases/open-source-cassandra-now-managed-on-google-cloud
Ref: https://console.cloud.google.com/marketplace/details/click-to-deploy-images/cassandra?filter=price:free&filter=category:database&id=25ca0967-cd8e-419e-b554-fe32e87f04be&pli=1

Question 3:
Skipped
You work for a startup company where every developer has a dedicated development GCP project linked to a central billing account. Your finance lead is concerned that some developers may leave some services running unnecessarily or may not understand the cost implications of turning on specific services in Google Cloud Platform. They want to be alerted when a developer spends more than 750$ per month in their GCP project. What should you do?

- ○

  Export Billing data from each development GCP projects to a separate BigQuery dataset. On each dataset, use a Data Studio dashboard to plot the spending.

- ○

  Export Billing data from all development GCP projects to a single BigQuery dataset. Use a Data Studio dashboard to plot the spend.

- ○

  Set up a budget for each development GCP projects. For each budget, trigger an email notification when the spending exceeds $750.

  (Correct)

- ○

Set up a single budget for all development GCP projects. Trigger an email notification when the spending exceeds $750 in the budget.

Explanation

`Set up a single budget for all development GCP projects. Trigger an email notification when the spending exceeds $750 in the budget.` **is not right.**

A budget enables you to track your actual Google Cloud spend against your planned spend. After you've set a budget amount, you set budget alert threshold rules that are used to trigger email notifications. Budget alert emails help you stay informed about how your spend is tracking against your budget. But since a single budget is created for all projects, it is not possible to identify if a developer has spent more than $750 per month on their development project.

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

`Export Billing data from each development GCP projects to a separate BigQuery dataset. On each dataset, use a Data Studio dashboard to plot the spending.` **is not right.**

This option does not alert the finance team if any of the developers have spent above $750.

`Export Billing data from all development GCP projects to a single BigQuery dataset. Use a Data Studio dashboard to plot the spend.` **is not right.**

This option does not alert the finance team if any of the developers have spent above $750.

`Set up a budget for each development GCP projects. For each budget, trigger an email notification when the spending exceeds $750.` **is the right answer.**

A budget enables you to track your actual Google Cloud spend against your planned spend. After you've set a budget amount, you set budget alert threshold rules that are used to trigger email notifications. Budget alert emails help you stay informed about how your spend is tracking against your budget. As the budget is created per project, the alert triggers whenever spent in the project is more than $750 per month.

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

Question 4:

Skipped

You want to drive efficiency through automation and reduce the operational burden of maintaining large fleets of Compute Engine VMs in your Google Cloud project. What should you do to manually set up VM Manager?

- ○

  Enable OS Config API and Container Analysis API in your project.

If your VM does not have public internet access, enable Private Google Access.

- ○

Enable OS Config API in your project.

Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.

If your VM does not have public internet access, enable Private Google Access.

- ○

Enable OS Config API in your project.

Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.

Enable Container Analysis API in your project.

Verify that all VMs have an attached service account. Ensure your VMs are in a private VPC network with no public internet access.

- ○

Enable OS Config API in your project.

Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.

Enable Container Analysis API in your project.

Verify that all VMs have an attached service account. If your VM does not have public internet access, enable Private Google Access.

(Correct)

Explanation

`1. Enable OS Config API in your project.`
`2. Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.`
`3. If your VM does not have public internet access, enable Private Google Access.` **is not right**

All steps above are valid. In addition, you need to ensure all VMs have an attached service account. If your VM does not have public internet access, you need to enable Private Google Access.
Ref: https://cloud.google.com/compute/docs/manage-os#overview

`1. Enable OS Config API in your project.`
`2. Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.`
`3. Enable Container Analysis API in your project.`
`4. Ensure your VMs are in a private VPC network with no public internet access.` **is not right**

The first three steps above are valid. In addition, you need to ensure all VMs have an attached service account. Also, there is no need to have your VMs in a private VPC network. If your VM does not have public internet access, you need to enable Private Google Access.
Ref: https://cloud.google.com/compute/docs/manage-os#overview

`1. Enable OS Config API and Container Analysis API in your project.`
`2. If your VM does not have public internet access, enable Private Google Access.` **is not right**

There's a whole load of steps missing here such as ensuring all VMs have an attached service account, enabling Private Google Access if needed, setting instance metadata on the OS config agent etc.
Ref: https://cloud.google.com/compute/docs/manage-os#overview

`1. Enable OS Config API in your project.`
`2. Ensure OS config agent is installed on all VMs and set instance metadata for the OS config agent.`

`3. Enable Container Analysis API in your project.`
`4. Verify that all VMs have an attached service account. If your VM does not have public internet access, enable Private Google Access.` **is the right answer**

This has all the steps needed to enable VM manager manually. To manually set up VM Manager, complete the following steps:

In your Google Cloud project, enable the OS Config API.

In your Google Cloud project, enable the Container Analysis API.

On each VM, check if the OS Config agent is installed. If the agent is not already installed, install the OS Config agent.

On either your project or on each VM, set instance metadata for the OS Config agent. This step is needed to make the OS Config agent active in your VM or project.

Verify that all VMs have an attached service account. You do not need to grant any IAM roles to this service account. VM Manager uses this service account to sign requests to the API service.

If your VM is running within a private VPC network and does not have public internet access, enable Private Google Access.

Ref: https://cloud.google.com/compute/docs/manage-os#overview

Question 5:

Skipped

All departments at your company have their own Google Cloud Projects. You got transferred into a new department that doesn't have a project yet, and you are ready to deploy a new application onto a Compute Engine Instance. What should you do?

- ○

  In the GCP Console, enable the Compute Engine API. Run gcloud compute instances create with --project flag to automatically create the new project and a compute engine instance.

- ○

  In the GCP Console, enable the Compute Engine API. When creating a new instance in the console, select the checkbox to create the instance in a new GCP project and provide the project name and ID.

- ○

Run gcloud compute instances create with --project flag to automatically create the new project and a compute engine instance. When prompted to enable the Compute Engine API, select Yes.

- ○

  Use gcloud commands first to create a new project, then to enable the Compute Engine API and finally, to launch a new compute engine instance in the project.

  (Correct)

Explanation

`In the GCP Console, enable the Compute Engine API. Run gcloud compute instances create with --project flag to automatically create the new project and a compute engine instance.` **is not right.**

You can't create the instance without first creating the project. The --project flag in gcloud compute create instances command is used to specify an existing project.
https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

```
--project=PROJECT_ID
```

The Google Cloud Platform project ID 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.
Ref: https://cloud.google.com/sdk/gcloud/reference#--project

`Run gcloud compute instances create with --project flag to automatically create the new project and a compute engine instance. When prompted to enable the Compute Engine API, select Yes.` **is not right.**

You can't create the instance without first creating the project. The --project flag in gcloud compute create instances command is used to specify an existing project.
https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

```
--project=PROJECT_ID
```

The Google Cloud Platform project ID 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.
Ref: https://cloud.google.com/sdk/gcloud/reference#--project

`In the GCP Console, enable the Compute Engine API. When creating a new instance in the console, select the checkbox to create the instance in a new GCP project and provide the project name and ID.` **is not right.**

In Cloud Console, when you create a new instance, you don't get an option to select

the project. The compute engine instance is always created in the currently active project.
Ref: https://cloud.google.com/compute/docs/instances/create-start-instance

`Use gcloud commands first to create a new project, then to enable the Compute Engine API and finally, to launch a new compute engine instance in the project.` **is the right answer.**
This option does it all in the correct order. You first create a project using gcloud projects create, then enable the compute engine API and finally create the VM instance in this project by using the --project flag or by creating an instance in this project in Cloud console.
https://cloud.google.com/sdk/gcloud/reference/compute/instances/create

```
--project=PROJECT_ID
```

The Google Cloud Platform project ID 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.
Ref: https://cloud.google.com/sdk/gcloud/reference#--project
Question 6:
Skipped
Your compliance team has asked you to set up an external auditor access to logs from all GCP projects for the last 60 days. The auditor wants to combine, explore and analyze the contents of the logs from all projects quickly and efficiently. You want to follow Google Recommended practices. What should you do?

- ○

  Set up a Cloud Scheduler job to trigger a Cloud Function that reads and export logs from all the projects to a BigQuery dataset. Configure the table expiration on the dataset to 60 days. Ask the auditor to query logs from the dataset.

- ○

  Set up a BigQuery sink destination to export logs from all the projects to a dataset. Configure the table expiration on the dataset to 60 days. Ask the auditor to query logs from the dataset.

  (Correct)

- ○

  Ask the auditor to query logs from Cloud Logging.

- ○

Set up a Cloud Storage sink destination to export logs from all the projects to a bucket. Configure a lifecycle rule to delete objects older than 60 days. Ask the auditor to query logs from the bucket.

Explanation

`Ask the auditor to query logs from Cloud Logging.` **is not right.**
Log entries are held in Stackdriver Logging for a limited time known as the retention period - which is 30 days (default configuration). After that, the entries are deleted. To keep log entries longer, you need to export them outside of Stackdriver Logging by configuring log sinks. Also, it's not easy to combine logs from all projects using this option.
https://cloud.google.com/blog/products/gcp/best-practices-for-working-with-google-cloud-audit-logging

`Set up a Cloud Scheduler job to trigger a Cloud Function that reads and export logs from all the projects to a BigQuery dataset. Configure the table expiration on the dataset to 60 days. Ask the auditor to query logs from the dataset.` **is not right.**
While this works, it makes no sense to use Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery when Google provides a feature (export sinks) that does the same thing and works out of the box.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2

`Set up a Cloud Storage sink destination to export logs from all the projects to a bucket. Configure a lifecycle rule to delete objects older than 60 days. Ask the auditor to query logs from the bucket.` **is not right.**
You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud Storage, BigQuery, and Pub/Sub.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2
Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to export logs from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud organization.
https://cloud.google.com/logging/docs/export/aggregated_sinks
Either way, we now have the data in Cloud Storage, but querying logs information from Cloud Storage is harder than Querying information from BigQuery dataset. For this reason, we should prefer BigQuery over Cloud Storage.

`Set up a BigQuery sink destination to export logs from all the projects to a dataset. Configure the table expiration on the dataset to 60 days. Ask the auditor to query logs from the dataset.` **is the right answer.**
You can export logs by creating one or more sinks that include a logs query and an export destination. Supported destinations for exported log entries are Cloud

Storage, BigQuery, and Pub/Sub.
Ref: https://cloud.google.com/logging/docs/export/configure_export_v2
Sinks are limited to exporting log entries from the exact resource in which the sink was created: a Google Cloud project, organization, folder, or billing account. If it makes it easier to export logs from all projects of an organization, you can create an aggregated sink that can export log entries from all the projects, folders, and billing accounts of a Google Cloud organization.
https://cloud.google.com/logging/docs/export/aggregated_sinks
Either way, we now have the data in a BigQuery Dataset. Querying information from a Big Query dataset is easier and quicker than analyzing contents in Cloud Storage bucket. As the requirement is to "Quickly analyze the log contents", we should prefer Big Query over Cloud Storage.

Also, You can control storage costs and optimize storage usage by setting the default table expiration for newly created tables in a dataset. If you set the property when the dataset is created, any table created in the dataset is deleted after the expiration period. If you set the property after the dataset is created, only new tables are deleted after the expiration period.

For example, if you set the default table expiration to 7 days, older data is automatically deleted after 1 week.
Ref: https://cloud.google.com/bigquery/docs/best-practices-storage

Question 7:

Skipped

You are managing an application running on a Google Compute engine instance. While the application is not critical for live operations, any outage affects your big development team. You want to minimize from regular infrastructure maintenance and upgrades, and you want to achieve this at the lowest possible cost. What should you do?

- ○

  Set onHostMaintenance availability policy to MIGRATE. Set automaticRestart policy to true.

  (Correct)

- ○

  Deploy your application to a regional managed instance group spread across two availability zones and set the minimum required VM instances to 2. In the event of downtime affecting one instance, the other instance continues to serve traffic.

- ○

Set onHostMaintenance availability policy to TERMINATE. Set automaticRestart policy to false.

- ○

  Deploy your application to a zonal managed instance group and set the minimum required VM instances to 2. In the event of downtime affecting one instance, the other instance continues to serve traffic.

Explanation

`Deploy your application to a zonal managed instance group and set the minimum required VM instances to 2. In the event of downtime affecting one instance, the other instance continues to serve traffic.` **is not right**

This certainly works but you are doubling the cost by increasing the compute engine instances to 2.

`Deploy your application to a regional managed instance group spread across two availability zones and set the minimum required VM instances to 2. In the event of downtime affecting one instance, the other instance continues to serve traffic.` **is not right**

Like above, this works as well but you are doubling the cost by increasing the compute engine instances to 2.

`Set onHostMaintenance availability policy to TERMINATE. Set automaticRestart policy to false.` **is not right**

This has the exact opposite effect of what we need. Setting the onHostMaintenance availability policy to TERMINATE stops a VM instead of migrating it. And setting automaticRestart policy to false does not restart a VM if the VM crashes or is stopped.

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

`Set onHostMaintenance availability policy to MIGRATE. Set automaticRestart policy to true.` **is the right answer**

For shielding your application from regular infrastructure maintenance and upgrades, this option gives you what you need with the lowest possible cost. You still have a single VM instance. Setting onHostMaintenance availability policy to MIGRATE causes Compute Engine to live migrate an instance when there is a maintenance event. Live migration keeps your virtual machine instances running even when a host system event, such as a software or hardware update, occurs. Compute Engine live migrates your running instances to another host in the same zone instead of requiring your VMs to be rebooted. This allows Google to perform maintenance that is integral to keeping infrastructure protected and reliable without interrupting any of your VMs.

Ref: https://cloud.google.com/compute/docs/instances/live-migration

In addition, setting automaticRestart to true restarts an instance if the instance

crashes or is stopped. This ensures the application is back available should the VM crash.
Ref: https://cloud.google.com/compute/docs/instances/setting-instance-scheduling-options

Question 8:

Skipped

You work for a multinational car insurance company that specializes in rewarding safer drivers with cheaper premiums. Your company does this by installing black box IoT devices in its 2 million insured drivers' cars. These devices capture driving behaviours such as acceleration/deceleration, speed compared to speed limits, and types of driving, such as commuting on freeway compared to commuting on surface streets etc. You expect to receive hundreds of events per minute from every device. You need to store this data and retrieve data consistently based on the event time, and both operations should be atomic. How should you store this data?

- ○

  Store the data in Cloud BigTable. Have a row key based on the ingestion timestamp.

  (Correct)

- ○

  Store the data in Cloud Datastore. Have an entity group per device.

- ○

  Store the data in Cloud Filestore. Have a file per IoT device and append new data to the file.

- ○

  Store the data in Cloud Storage. Have a file per IoT device and append new data to the file.

Explanation

`Store the data in Cloud Storage. Have a file per IoT device and append new data to the file.` **is not right.**

Terrible idea!! Cloud Storage Objects are immutable, which means that an uploaded object cannot change throughout its storage lifetime. In practice, this means that you cannot make incremental changes to objects, such as append operations. However, it is possible to overwrite objects that are stored in Cloud Storage, and doing so happens atomically — until the new upload completes the old version of the object will be served to the readers, and after the upload completes the new version

of the object will be served to readers. So for each update, the clients (construction equipment)) will have to read the full object, append a single row and upload the full object again. With the high frequency of IoT data here, different clients may read different data while the updates happen, and this can mess things up big time.
Ref: https://cloud.google.com/storage/docs/key-terms#immutability

`Store the data in Cloud Filestore. Have a file per IoT device and append new data to the file.` **is not right.**
Like above, there is no easy way to append data to a file in Cloud Filestore. For each update, the clients will have to read the full file, append a single row and upload the full file again. A client has to lock the file before updating, and this prevents other clients from modifying the file. With the high frequency of IoT data here, this design is impractical.
Ref: https://cloud.google.com/filestore/docs/limits#file_locks

`Store the data in Cloud Datastore. Have an entity group per device.` **is not right.**
Cloud Datastore isn't suitable for ingesting IoT data. It is more suitable for Gaming leaderboard/player profile data, or where direct client access and real-time sync to clients is required.
Ref: https://cloud.google.com/products/databases
Also, storing data in an entity group based on the device means that the query has to iterate through all entities and look at the timestamp value to arrive at the result which isn't the best design.

`Store the data in Cloud BigTable. Have a row key based on the ingestion timestamp.` **is the right answer.**
Cloud Bigtable provides a scalable NoSQL database service with consistent low latency and high throughput, making it an ideal choice for storing and processing time-series vehicle data.
Ref: https://cloud.google.com/solutions/designing-connected-vehicle-platform#data_ingestion
By creating a row key based on the event timestamp, you can easily/fetch data based on the time of the event, which is our requirement.
Ref: https://cloud.google.com/bigtable/docs/schema-design-time-series

Question 9:

Skipped

You manage an overnight batch job that uses 20 VMs to transfer customer information from a CRM system to BigQuery dataset. The job can tolerate some VMs going down. The current high cost of the VMs make the overnight job not viable, and you want to reduce the costs. What should you do?

- ○

  Use a fleet of f1-micro instances behind a Managed Instances Group (MIG) with autoscaling and minimum nodes set to 1.

- ○

  Use tiny f1-micro instances to reduce cost.

- ○

  Use preemptible compute engine instances to reduce cost.

  (Correct)

- ○

  Use a fleet of f1-micro instances behind a Managed Instances Group (MIG) with autoscaling. Set minimum and maximum nodes to 20.

Explanation

`Use preemptible compute engine instances to reduce cost.` **is the right answer.**

Since the batch workload is fault-tolerant, i.e. can tolerate some of the VMs being terminated, you should use preemptible VMs. A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might stop (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 stop during processing, the job slows but does not entirely 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 regular instances.

Ref: https://cloud.google.com/compute/docs/instances/preemptible#what_is_a_preemptible_instance

Question 10:

Skipped

Your company has a massive quantity of unstructured data in text, Apache AVRO and PARQUET files in the on-premise data centre and wants to transform this data using a Dataflow job and migrate cleansed/enriched data to BigQuery. How should you make the on-premise files accessible to Cloud Dataflow?

- ○

  Migrate the data from the on-premises data centre to Cloud Spanner by using the upload files function.

- ○

Migrate the data from the on-premises data centre to Cloud Storage by using a custom script with gsutil commands.

(Correct)

- ○

Migrate the data from the on-premises data centre to BigQuery by using a custom script with bq commands.

- ○

Migrate the data from the on-premises data centre to Cloud SQL for MySQL by using the upload files function.

Explanation
The key to answering this question is "unstructured data".

`Migrate the data from the on-premises data centre to BigQuery by using a custom script with bq commands.` **is not right.**
The bq load command is used to load data in BigQuery from a local data source, i.e. local file, but the data has to be in a structured format.

```
bq --location=LOCATION load \
--source_format=FORMAT \
PROJECT_ID:DATASET.TABLE \
PATH_TO_SOURCE \
SCHEMA
```

where schema: a valid schema. The schema can be a local JSON file, or it can be typed inline as part of the command. You can also use the --autodetect flag instead of supplying a schema definition.
Ref: https://cloud.google.com/bigquery/docs/loading-data-local#bq

`Migrate the data from the on-premises data centre to Cloud SQL for MySQL by using the upload files function.` **is not right.**
Fully managed relational database service for MySQL, PostgreSQL, and SQL Server. As this is a relational database, it is for structured data and not fit for unstructured data.
Ref: https://cloud.google.com/sql

`Migrate the data from the on-premises data centre to Cloud Spanner by using the upload files function.` **is not right.**
Cloud Spanner is the first scalable, enterprise-grade, globally-distributed, and strongly consistent database service built for the cloud specifically to combine the

benefits of relational database structure with non-relational horizontal scale. Although Google claims Cloud Spanner is the best of the relational and non-relational worlds, it also says "With Cloud Spanner, you get the best of relational database structure and non-relational database scale and performance with external strong consistency across rows, regions, and continents.". Cloud spanner is for structured data and not fit for unstructured data.
Ref: https://cloud.google.com/spanner

`Migrate the data from the on-premises data centre to Cloud Storage by using a custom script with gsutil commands.` **is the right answer.**
Cloud storage imposes no such restrictions; you can store large quantities of unstructured data in different file formats. Cloud Storage provides globally unified, scalable, and highly durable object storage for developers and enterprises. Also, Dataflow can query Cloud Storage filesets as described in this article
Ref: https://cloud.google.com/dataflow/docs/guides/sql/data-sources-destinations#querying-gcs-filesets

Question 11:
Skipped
You want to optimize the storage costs for long term archival of logs. Logs are accessed frequently in the first 30 days and only retrieved after that if there is any special requirement in the annual audit. The auditors may need to look into log entries of the previous three years. What should you do?

- ○

  Store the logs in Standard Storage Class and set up a lifecycle policy to transition the files older than 30 days to Archive Storage Class.

  (Correct)

- ○

  Store the logs in Standard Storage Class and set up lifecycle policies to transition the files older than 30 days to Coldline Storage Class, and files older than 1 year to Archive Storage Class.

- ○

  Store the logs in Nearline Storage Class and set up a lifecycle policy to transition the files older than 30 days to Archive Storage Class.

- ○

  Store the logs in Nearline Storage Class and set up lifecycle policies to transition the files older than 30 days to Coldline Storage Class, and files older than 1 year to Archive Storage Class.

Explanation

`Store the logs in Nearline Storage Class and set up a lifecycle policy to transition the files older than 30 days to Archive Storage Class.` **is not right.**

Nearline Storage is ideal for data you plan to read or modify on average once per month or less, and there are costs associated with data retrieval. Since we require to access data frequently for 30 days, we should avoid Nearline and prefer Standard Storage which is suitable for frequently accessed ("hot" data).

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

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

`Store the logs in Nearline Storage Class and set up lifecycle policies to transition the files older than 30 days to Coldline Storage Class, and files older than 1 year to Archive Storage Class.` **is not right.**

Nearline Storage is ideal for data you plan to read or modify on average once per month or less, and there are costs associated with data retrieval. Since we require to access data frequently for 30 days, we should avoid Nearline and prefer Standard Storage which is suitable for frequently accessed ("hot" data).

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

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

`Store the logs in Standard Storage Class and set up lifecycle policies to transition the files older than 30 days to Coldline Storage Class, and files older than 1 year to Archive Storage Class.` **is not right.**

Since we require to access data frequently for 30 days, we should use Standard Storage which is suitable for frequently accessed ("hot" data).

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

However, transitioning to Coldline is unnecessary as there is no requirement to access data after that so we might as well transition all data to archival storage which offers the lowest cost option for archiving data.

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

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

`Store the logs in Standard Storage Class and set up a lifecycle policy to transition the files older than 30 days to Archive Storage Class.` **is the right answer.**

Since we require to access data frequently for 30 days, we should use Standard Storage which is suitable for frequently accessed ("hot" data).

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

And since there is no requirement to access data after that, we can transition all data to archival storage which offers the lowest cost option for archiving data.

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

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

Question 12:

Skipped

You are running a big fleet of virtual machines in your Google Cloud project running Windows and Linux on Google Compute Engine. You have been asked to identify ways to drive efficiency through automation and reduce the operational burden of maintaining these VM fleets. You need to apply on-demand and scheduled patches, collect and review operating system information, and install, remove, and auto-update software packages. What should you do?

- ○

  Enable VM Fleet Organizer in your Cloud project.

- ○

  Enable VM Manager in your Cloud project.

  (Correct)

- ○

  Enable VM Fleet Manager in your Cloud project.

- ○

  Enable VM Fleet in your Cloud project.

Explanation

`Enable VM Fleet Organizer in your Cloud project.` **is not right.**

There is no such service - VM Fleet Organizer

`Enable VM Fleet in your Cloud project.` **is not right.**

There is no such service - VM Fleet

`Enable VM Fleet Manager in your Cloud project.` **is not right.**

There is no such service - VM Fleet Manager

`Enable VM Manager in your Cloud project.` **is the right answer.**

VM Manager is a suite of tools that can be used to manage operating systems for large virtual machine (VM) fleets running Windows and Linux on Compute Engine. VM Manager helps drive efficiency through automation and reduces the operational burden of maintaining these VM fleets. VM Manager supports projects in VPC Service Controls service perimeters. The following services are available as part of the VM Manager suite:

OS patch management: use this service to apply on-demand and scheduled patches. You can also use OS patch management for patch compliance reporting in your environment.

OS inventory management: use this service to collect and review operating system information.

OS configuration management: use this service to install, remove, and auto-update software packages.

Ref: https://cloud.google.com/compute/docs/vm-manager

Question 13:

Skipped

You want to run an application in Google Compute Engine in the app-tier GCP project and have it export data from Cloud Bigtable to daily-us-customer-export Cloud Storage bucket in the data-warehousing project. You plan to run a Cloud Dataflow job in the data-warehousing project to pick up data from this bucket for further processing. How should you design the IAM access to enable the compute engine instance push objects to daily-us-customer-export Cloud Storage bucket in the data-warehousing project?

- ○

  Ensure both the projects are in the same GCP folder in the resource hierarchy.

- ○

  Grant the service account used by the compute engine in app-tier GCP project roles/storage.objectCreator IAM role on app-tier GCP project.

- ○

  Grant the service account used by the compute engine in app-tier GCP project roles/storage.objectCreator IAM role on the daily-us-customer-export Cloud Storage bucket.

  (Correct)

- ○

  Update the access control on daily-us-customer-export Cloud Storage bucket to make it public. Create a subfolder inside the bucket with a randomized name and have the compute engine instance push objects to this folder.

Explanation

`Ensure both the projects are in the same GCP folder in the resource hierarchy.` **is not right.**

Folder resources provide an additional grouping mechanism and isolation

boundaries between projects. They can be seen as sub-organizations within the Organization. Folders can be used to model different legal entities, departments, and teams within a company. For example, the first level of folders could be used to represent the main departments in your organization. Since folders can contain projects and other folders, each folder could then include other sub-folders, to represent different teams. Each team folder could contain additional sub-folders to represent different applications.
Ref: https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy
Although it is possible to move both projects under the same folder, unless the relevant permissions are assigned to the VM service account, it can't push the exports to the cloud storage bucket in a different project.

`Grant the service account used by the compute engine in app-tier GCP project roles/storage.objectCreator IAM role on app-tier GCP project.` **is not right.**
The bucket daily-us-customer-export is in the data-warehousing so the VMs service account must the assigned the role on data-warehousing and not app-tier.

`Update the access control on daily-us-customer-export Cloud Storage bucket to make it public. Create a subfolder inside the bucket with a randomized name and have the compute engine instance push objects to this folder.` **is not right.**
Making the bucket public compromises security. It doesn't matter that the folder has a pseudo-randomized suffix name. Anyone can check the contents of a public bucket.

`Grant the service account used by the compute engine in app-tier GCP project roles/storage.objectCreator IAM role on the daily-us-customer-export Cloud Storage bucket.` **is the right answer.**
Since the VM needs to access the bucket daily-us-customer-export which is in the data-warehousing, its service account needs to be granted the required permissions (Storage Object Creator) on the bucket daily-us-customer-export in the data-warehousing.

Question 14:
Skipped
Your company has deployed all its production applications in a single Google Cloud Project and uses several GCP projects for development and test environments. The operations team requires access to all production services in this project to debug live issues and deploy enhancements. Your security team prevents the creation of IAM roles that automatically broaden to include new permissions/services in future. How should you design the IAM role for operations team?

- ○

Grant the Project Editor role on the production GCP project to all members of the operations team.

- ○

Create a custom role with the necessary permissions and grant the role on the production GCP project to all members of the operations team.

(Correct)

- ○

Create a custom role with the necessary permissions and grant the role at the organization level to all members of the operations team.

- ○

Grant the Project Editor role at the organization level to all members of the operations team.

Explanation

`Grant the Project Editor role on the production GCP project to all members of the operations team.` **is not right.**

You want to prevent Google Cloud product changes from broadening their permissions in the future. So you shouldn't use predefined roles, e.g. Project Editor. Predefined roles are created and maintained by Google. Their permissions are automatically updated as necessary, such as when new features or services are added to Google Cloud.

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

`Grant the Project Editor role at the organization level to all members of the operations team.` **is not right.**

You want to prevent Google Cloud product changes from broadening their permissions in the future. So you shouldn't use predefined roles, e.g. Project Editor. Predefined roles are created and maintained by Google. Their permissions are automatically updated as necessary, such as when new features or services are added to Google Cloud.

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

`Create a custom role with the necessary permissions and grant the role at the organization level to all members of the operations team.` **is not right.**

Unlike predefined roles, the permissions in custom roles are not automatically updated when Google adds new features or services. So the custom role is the right choice.

Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic_concepts
However, granting the custom role at the organization level grants the DevOps team access to not just the production project but also testing and development projects which go against the principle of least privilege and should be avoided.
Ref: https://cloud.google.com/iam/docs/understanding-roles

`Create a custom role with the necessary permissions and grant the role on the production GCP project to all members of the operations team.` **is the right answer.**
Unlike predefined roles, the permissions in custom roles are not automatically updated when Google adds new features or services. So the custom role is the right choice.
Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#basic_concepts
Granting the custom role at the production project level grants the DevOps team access to just the production project and not testing and development projects which aligns with the principle of least privilege and should be preferred.
Ref: https://cloud.google.com/iam/docs/understanding-roles

Question 15:

Skipped

You plan to deploy an application to Google Compute Engine instance, and it relies on making connections to a Cloud SQL database for retrieving information about book publications. To minimize costs, you are developing this application on your local workstation, and you want it to connect to a Cloud SQL instance. Your colleague suggested setting up Application Default Credentials on your workstation to make the transition to Google Cloud easier. You are now ready to move the application to Google Compute Engine instance. You want to follow Google recommended practices to enable secure IAM access. What should you do?

- ○

  Grant the necessary IAM roles to a service account, download the JSON key file and package it with your application.

- ○

  Grant the necessary IAM roles to a service account, store its credentials in a config file and package it with your application.

- ○

  Grant the necessary IAM roles to a service account and configure the application running on Google Compute Engine instance to use this service account.

- ○

  Grant the necessary IAM roles to the service account used by Google Compute Engine instance.

  (Correct)

Explanation

`Grant the necessary IAM roles to a service account, download the JSON key file and package it with your application.` **is not right.**
To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. Since our application is running inside Google Cloud, Google's recommendation is to assign the required permissions to the service account and not use the service account keys.
Ref: https://cloud.google.com/iam/docs/creating-managing-service-account-keys

`Grant the necessary IAM roles to a service account, store its credentials in a config file and package it with your application.` **is not right.**
For application to application interaction, Google recommends the use of service accounts. A service account is an account for an application instead of an individual end-user. When you run code that's hosted on Google Cloud, the code runs as the account you specify. You can create as many service accounts as needed to represent the different logical components of your application.
Ref: https://cloud.google.com/iam/docs/overview#service_account

`Grant the necessary IAM roles to a service account and configure the application running on Google Compute Engine instance to use this service account.` **is not right.**
Using Application Default Credentials ensures that the service account works seamlessly. When testing on your local machine, it uses a locally-stored service account key, but when running on Compute Engine, it uses the project's default Compute Engine service account. So we have to provide access to the service account used by the compute engine VM and not the service account used by the application.
Ref: https://cloud.google.com/iam/docs/service-accounts#application_default_credentials

`Grant the necessary IAM roles to the service account used by Google Compute Engine instance.` **is the right answer.**
Using Application Default Credentials ensures that the service account works seamlessly. When testing on your local machine, it uses a locally-stored service account key, but when running on Compute Engine, it uses the project's default Compute Engine service account. So we have to provide access to the service account used by the compute engine VM.

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

Question 16:

Skipped

Your company deployed its applications across hundreds of GCP projects that use different billing accounts. The finance team is struggling to add up all production Cloud Opex costs and has requested your assistance for enabling/providing a single pane of glass for all costs incurred by all applications in Google Cloud. You want to include new costs as soon as they become available. What should you do?

- ○

  Use Cloud Scheduler to trigger a Cloud Function every hour. Have the Cloud Function download the CSV from the Cost Table page and upload the data to BigQuery. Ask the finance team to use Google Data Studio to visualize the data.

- ○

  Use Google pricing calculator for all the services used in all GCP projects and pass the estimated cost to finance team every month.

- ○

  Enable Billing Export from all GCP projects to BigQuery and ask the finance team to use Google Data Studio to visualize the data.

  (Correct)

- ○

  Ask the finance team to check reports view section in Cloud Billing Console.

Explanation

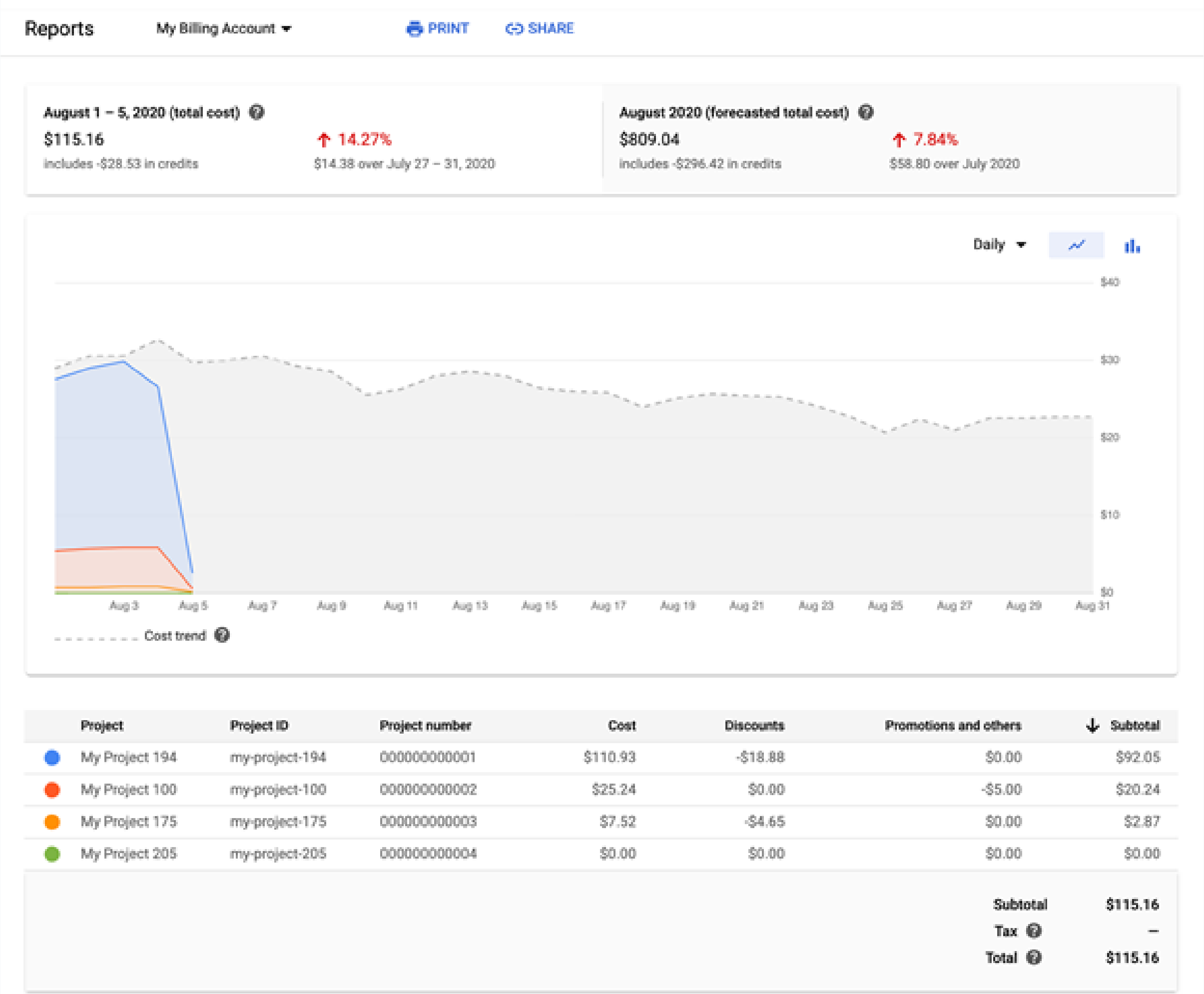
`Use Google pricing calculator for all the services used in all GCP projects and pass the estimated cost to finance team every month.` **is not right.**

We are interested in the costs incurred, not estimates.

`Use Cloud Scheduler to trigger a Cloud Function every hour. Have the Cloud Function download the CSV from the Cost Table page and upload the data to BigQuery. Ask the finance team to use Google Data Studio to visualize the data.` **is not right.**

The question states "You want to include new costs as soon as they become available" but exporting CSV is a manual process, i.e. not automated, so you don't get new cost data as soon as it becomes available.

`Ask the finance team to check reports view section in Cloud Billing Console.` **is not right.**
If all projects are linked to the same billing account, then the billing report would have provided this information in a single screen with a visual representation that can be customized based on different parameters. However, in this scenario, projects are linked to different billing accounts and viewing the billing information of all these projects in a single visual representation is not possible in the Reports View section in Cloud Billing Console.



August 1 – 5, 2020 (total cost)
$115.16
includes -$28.53 in credits
↑ 14.27%
$14.38 over July 27 – 31, 2020

August 2020 (forecasted total cost)
$809.04
includes -$296.42 in credits
↑ 7.84%
$58.80 over July 2020

	Project	Project ID	Project number	Cost	Discounts	Promotions and others	↓ Subtotal
●	My Project 194	my-project-194	000000000001	$110.93	-$18.88	$0.00	$92.05
●	My Project 100	my-project-100	000000000002	$25.24	$0.00	-$5.00	$20.24
●	My Project 175	my-project-175	000000000003	$7.52	-$4.65	$0.00	$2.87
●	My Project 205	my-project-205	000000000004	$0.00	$0.00	$0.00	$0.00
						Subtotal	$115.16
						Tax	–
						Total	$115.16

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

`Enable Billing Export from all GCP projects to BigQuery and ask the finance team to use Google Data Studio to visualize the data.` **is the right answer.**
Cloud Billing export to BigQuery enables you to export detailed Google Cloud billing data (such as usage, cost estimates, and pricing data) automatically throughout the day to a BigQuery dataset that you specify. Then you can access your Cloud Billing data from BigQuery for detailed analysis, or use a tool like Google Data Studio to

visualize your data and provide cost visibility to the finance department. All projects can be configured to export their data to the same billing dataset. As the export happens automatically throughout the day, this satisfies our "as soon as possible" requirement.
Ref: https://cloud.google.com/billing/docs/how-to/export-data-bigquery

Question 17:

Skipped

You deployed an application on a general-purpose Google Cloud Compute Engine instance that uses a persistent zonal SSD of 300 GB. The application downloads large Apache AVRO files from Cloud Storage, retrieve customer details from them and saves a text file on local disk for each customer before pushing all the text files to a Google Storage Bucket. These operations require high disk I/O, but you find that the read and write operations on the disk are always throttled. What should you do to improve the throughput while keeping costs to a minimum?

- ○

  Bump up the CPU allocated to the general-purpose Compute Engine instance.

- ○

  Bump up the size of its SSD persistent disk to 1 TB.

- ○

  Replace Zonal Persistent SSD with a Regional Persistent SSD.

- ○

  Replace Zonal Persistent SSD with a Local SSD.

  (Correct)

Explanation

`Replace Zonal Persistent SSD with a Regional Persistent SSD.` **is not right.**
Migrating to a regional SSD would actually make it worse. At the time of writing, the Read IOPS for a Zonal standard persistent disk is 7,500, and the Read IOPS reduces to 3000 for a Regional standard persistent disk, which reduces the throughput.
Ref: https://cloud.google.com/compute/docs/disks/performance

`Bump up the size of its SSD persistent disk to 1 TB.` **is not right.**
The performance of SSD persistent disks scales with the size of the disk.
Ref: https://cloud.google.com/compute/docs/disks/performance#cpu_count_size
However, no guarantee increasing the disk to 1 TB will increase the throughput in this scenario as disk performance also depends on the number of vCPUs on VM

instance.
Ref: https://cloud.google.com/compute/docs/disks/performance#ssd_persistent_disk_performance_by_disk_size
Ref: https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits
For example, consider a 1,000 GB SSD persistent disk attached to an instance with an N2 machine type and 4 vCPUs. The read limit based solely on the size of the disk is 30,000 IOPS. However, because the instance has 4 vCPUs, the read limit is restricted to 15,000 IOPS.

`Bump up the CPU allocated to the general-purpose Compute Engine instance.` **is not right.**
In Compute Engine, machine types are grouped and curated for different workloads. Each machine type is subject to specific persistent disk limits per vCPU. Increasing the vCPU count increases the Read IOPS
https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits
However, no guarantee increasing CPU will increase the throughput in this scenario as disk performance could be limited by disk size.
Ref: https://cloud.google.com/compute/docs/disks/performance#ssd_persistent_disk_performance_by_disk_size
Ref: https://cloud.google.com/compute/docs/disks/performance#machine-type-disk-limits
For example, consider a 1,000 GB SSD persistent disk attached to an instance with an N2 machine type and 48 vCPUs. The read limit based solely on the vCPU count is 60,000 IOPS. However, because the instance has 1000 GB SSD, the read limit is restricted to 30,000 IOPS.

`Replace Zonal Persistent SSD with a Local SSD.` **is the right answer.**
Local SSDs are physically attached to the server that hosts your VM instance. Local SSDs have higher throughput and lower latency than standard persistent disks or SSD persistent disks. The performance gains from local SSDs require trade-offs in availability, durability, and flexibility. Because of these trade-offs, Local SSD storage isn't automatically replicated, and all data on the local SSD might be lost if the instance terminates for any reason.
Ref: https://cloud.google.com/compute/docs/disks#localssds
Ref: https://cloud.google.com/compute/docs/disks/performance#type_comparison

Question 18:
Skipped
The operations manager has asked you to identify the IAM users with Project Editor role on the GCP production project. What should you do?

- ○

  Turn on IAM Audit logging and build a Cloud Monitoring dashboard to display this information.

- ○

  Extract all project-wide SSH keys.

- ○

  Execute gcloud projects get-iam-policy to retrieve this information.

  (Correct)

- ○

  Check the permissions assigned in all Identity Aware Proxy (IAP) tunnels.

Explanation

`Extract all project-wide SSH keys.` **is not right.**
Project-wide SSH keys provide the ability to connect to most instances in your project. It can't be used to identify who has been granted the project editor role.
Ref: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#edit-ssh-metadata

`Check the permissions assigned in all Identity Aware Proxy (IAP) tunnels.` **is not right.**
Identity Aware Proxy is for controlling access to your cloud-based and on-premises applications and VMs running on Google Cloud. It can't be used to gather who has been granted the project editor role.
Ref: https://cloud.google.com/iap

`Turn on IAM Audit logging and build a Cloud Monitoring dashboard to display this information.` **is not right.**
Once enabled, new users signing in with a project editor role are recorded in logs, and you can query this information, but these logs don't give you a full list of all users who currently have Project editors role but have not logged in.

`Execute gcloud projects get-iam-policy to retrieve this information.` **is the right answer.**
gcloud projects get-iam-policy lets you retrieve IAM policy for a project. You can combine this with various flags to retrieve the required information. e.g.

```
gcloud projects get-iam-policy $PROJECT_ID --filter="bindings.role:roles/owner
"
```

Question 19:

Skipped

Your company wants to migrate all compute workloads from the on-premises data centre to Google Cloud Compute Engine. A third-party team provides operational support for your production applications outside business hours. Everyone at your

company has a Gsuite account, but the support team do not. How should you grant them access to the VMs?

- ○

  Set up a Cloud VPN tunnel between the third-party network and your production GCP project.

- ○

  Use Cloud Identity Aware Proxy (IAP) to enable SSH tunnels to the VMs and add the third-party team as a tunnel user.

  (Correct)

- ○

  Set up a firewall rule to open SSH port (TCP:22) to the IP range of the third-party team.

- ○

  Add all the third party teams’ SSH keys to the production compute engine instances.

Explanation

`Set up a firewall rule to open SSH port (TCP:22) to the IP range of the third-party team.` **is not right.**
This option a terrible way to enable access - the SSH connections may be happening over untrusted networks, i.e. no encryption and you can't SSH to the instances without adding an SSH public key.

`Set up a Cloud VPN tunnel between the third-party network and your production GCP project.` **is not right.**
A step forward but you can't SSH without adding SSH public keys to the instances and opening the firewall ports to allow traffic from the operations partner IP range.

`Add all the third party teams’ SSH keys to the production compute engine instances.` **is not right.**
Like above, you haven't opened the firewall to allow traffic from the operations partner IP range, and the SSH connections may be happening over untrusted networks, i.e. no encryption.

`Use Cloud Identity Aware Proxy (IAP) to enable SSH tunnels to the VMs and add the third-party team as a tunnel user.` **is the right answer.**

This option is the preferred approach, given that the operations partner does not use Google accounts. IAP lets you

- Control access to your cloud-based and on-premises applications and VMs running on Google Cloud

- Verify user identity and use context to determine if a user should be granted access

- Work from untrusted networks without the use of a VPN

- Implement a zero-trust access model

To set up SSH tunnels using IAP, see:
https://cloud.google.com/iap/docs/using-tcp-forwarding#tunneling_ssh_connections

Question 20:

Skipped

Your gaming backend uses Cloud Spanner to store leaderboard and player profile data. You want to scale the spanner instances based on predictable usage patterns. What should you do?

- ○

  Configure alerts in Cloud Monitoring to alert Google Operations Support team and have them use their scripts to scale up or scale down the spanner instance as necessary.

- ○

  Configure a Cloud Scheduler job to invoke a Cloud Function that reviews the relevant Cloud Monitoring metrics and resizes the Spanner instance as necessary.

- ○

  Configure alerts in Cloud Monitoring to alert your operations team and have them manually scale up or scale down the spanner instance as necessary.

- ○

  Configure alerts in Cloud Monitoring to trigger a Cloud Function via webhook, and have the Cloud Function scale up or scale down the spanner instance as necessary.

  (Correct)

Explanation

`Configure a Cloud Scheduler job to invoke a Cloud Function that reviews the relevant Cloud Monitoring metrics and resizes the Spanner instance as necessary.` **is not right.**
While this works and does it automatically, it does not follow Google's recommended practices.
Ref: https://cloud.google.com/spanner/docs/instances
"Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

`Configure alerts in Cloud Monitoring to alert your operations team and have them manually scale up or scale down the spanner instance as necessary.` **is not right.**
This option does not follow Google's recommended practices.
Ref: https://cloud.google.com/spanner/docs/instances
"Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

`Configure alerts in Cloud Monitoring to alert Google Operations Support team and have them use their scripts to scale up or scale down the spanner instance as necessary.` **is not right.**
This option does not follow Google's recommended practices.
Ref: https://cloud.google.com/spanner/docs/instances
"Note: You can scale the number of nodes in your instance based on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions."

`Configure alerts in Cloud Monitoring to trigger a Cloud Function via webhook, and have the Cloud Function scale up or scale down the spanner instance as necessary.` **is the right answer.**
For scaling the number of nodes in Cloud spanner instance, Google recommends implementing this base on the Cloud Monitoring metrics on CPU or storage utilization in conjunction with Cloud Functions.
Ref: https://cloud.google.com/spanner/docs/instances

Question 21:
Skipped
You run a business-critical application in a Google Cloud Compute Engine instance, and you want to set up a cost-efficient solution for backing up the data on the boot disk. You want a solution that: • minimizes operational overhead • backs up boot disks daily • allows quick restore of the backups when needed, e.g. disaster scenarios • deletes backups older than a month automatically. What should you do?

- ○

Deploy a Cloud Function to initiate the creation of instance templates for all instances daily

- ○

  Enable Snapshot Schedule on the disk to enable automated snapshots per schedule.

  (Correct)

- ○

  Set up a cron job with a custom script that uses gcloud APIs to create a new disk from existing instance disk for all instances daily.

- ○

  Configure a Cloud Task to initiate the creation of images for all instances daily and upload them to Cloud Storage.

Explanation

`Deploy a Cloud Function to initiate the creation of instance templates for all instances daily.` **is not right.**
This option does not fulfil our requirement of allowing quick restore and automatically deleting old backups.

`Set up a cron job with a custom script that uses gcloud APIs to create a new disk from existing instance disk for all instances daily.` **is not right.**
This option does not fulfil our requirement of allowing quick restore and automatically deleting old backups.

`Configure a Cloud Task to initiate the creation of images for all instances daily and upload them to Cloud Storage.` **is not right.**
This option does not fulfil our requirement of allowing quick restore and automatically deleting old backups.

`Enable Snapshot Schedule on the disk to enable automated snapshots per schedule.` **is the right answer.**
Create snapshots to periodically back up data from your zonal persistent disks or regional persistent disks. To reduce the risk of unexpected data loss, consider the best practice of setting up a snapshot schedule to ensure your data is backed up on a regular schedule.
Ref: https://cloud.google.com/compute/docs/disks/create-snapshots
You can also delete snapshots on a schedule by defining a snapshot retention policy. A snapshot retention policy defines how long you want to keep your snapshots. If you choose to set up a snapshot retention policy, you must do so as

part of your snapshot schedule.
Ref: https://cloud.google.com/compute/docs/disks/scheduled-snapshots#retention_policy

Question 22:
Skipped
Your company runs most of its compute workloads in Google Compute Engine in the europe-west1-b zone. Your operations team use Cloud Shell to manage these instances. They want to know if it is possible to designate a default compute zone and not supply the zone parameter when running each command in the CLI. What should you do?

- ○

  Add a metadata entry in the Compute Engine Settings page with key: compute/zone and value: europe-west1-b.

- ○

  In GCP Console set europe-west1-b zone in the default location in Compute Engine Settings.

  (Correct)

- ○

  Run gcloud config to set europe-west1-b as the default zone.

- ○

  Update the gcloud configuration file ~/config.ini to set europe-west1-b as the default zone.

Explanation
`Update the gcloud configuration file ~/config.ini to set europe-west1-b as the default zone.` **is not right.**
gcloud does not read configurations from default.conf
Ref: https://cloud.google.com/sdk/gcloud/reference/config/configurations
Ref: https://cloud.google.com/sdk/docs/configurations

`Run gcloud config to set europe-west1-b as the default zone.` **is not right.**
Using gcloud config set, you can set the zone in your active configuration only. This setting does not apply to other gcloud configurations and does not become the default for the project.
Ref: https://cloud.google.com/sdk/gcloud/reference/config/set

```
gcloud config set compute/zone europe-west1-b
```

`Add a metadata entry in the Compute Engine Settings page with key: compute/zone and value: europe-west1-b.` **is not right.**
You could achieve this behaviour by running the following in gcloud.
https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud

```
gcloud compute project-info add-metadata \

--metadata google-compute-default-region=europe-west1,google-compute-default-z
one=europe-west1-b
```

As shown above, the key to be used is google-compute-default-zone and not compute/zone.

`In GCP Console set europe-west1-b zone in the default location in Compute Engine Settings.` **is the right answer.**
Ref: https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud
The default region and zone settings affect only client tools, such as the gcloud command-line tool and the Google Cloud Console. When you use these tools to construct your requests, the tools help you manage resources by automatically selecting the default region and zone. When you use the Cloud Console to create regional or zonal resources like addresses and instances, Compute Engine sets the region and zone fields for you. You can accept the pre-populated values, or explicitly change one or both of the values. When you use the gcloud tool, omit setting the --region and --zone flags to use the default region and zone properties for the new project. You can always change the default region and zone settings in the metadata server, override the default region and zone locally for the gcloud tool or override the settings manually for each request in either the gcloud tool and the Cloud Console.

You could also achieve this behaviour by running the following in gcloud.
https://cloud.google.com/compute/docs/regions-zones/changing-default-zone-region#gcloud

```
gcloud compute project-info add-metadata \

--metadata google-compute-default-region=europe-west1,google-compute-default-z
one=europe-west1-b
```

After you update the default metadata by using any method, run the gcloud init command to reinitialize your default configuration. The gcloud tool refreshes the default region and zone settings only after you run the gcloud init command.
Question 23:

Skipped

Your company uses Google Cloud for all its compute workloads. One of the applications that you developed has passed unit testing, and you want to use Jenkins to deploy the application in User Acceptance Testing (UAT) environment. Your manager has asked you to automate Jenkins installation as quickly and efficiently as possible. What should you do?

- ○

  Use GCP Marketplace to provision Jenkins.

  (Correct)

- ○

  Deploy Jenkins on a fleet of Google Cloud Compute Engine VMs in a Managed Instances Group (MIG) with autoscaling.

- ○

  Deploy Jenkins on a GKE Cluster.

- ○

  Deploy Jenkins on a Google Compute Engine VM.

Explanation

`Deploy Jenkins on a Google Compute Engine VM.` **is not right.**
While this can be done, this involves a lot more work than installing the Jenkins server through GCP Marketplace.

`Deploy Jenkins on a GKE Cluster.` **is not right.**
While this can be done, this involves a lot more work than installing the Jenkins server through GCP Marketplace.

`Deploy Jenkins on a fleet of Google Cloud Compute Engine VMs in a Managed Instances Group (MIG) with autoscaling.` **is not right.**
Like the above options, this can be done, but it involves a lot more work than installing the Jenkins server through GCP Marketplace.

`Use GCP Marketplace to provision Jenkins.` **is the right answer.**
The simplest way to launch a Jenkins server is from GCP Market place. GCP market place has several builds available for Jenkins:
https://console.cloud.google.com/marketplace/browse?q=jenkins.
All you need to do is spin up an instance from a suitable market place build, and you have a Jenkins server in a few minutes with just a few clicks.

Question 24:

Skipped

You are migrating a complex on-premises data warehousing solution to Google Cloud. You plan to create a fleet of Google Compute Engine instances behind a Managed Instances Group (MIG) in the app-tier project, and BigQuery in the data-warehousing project. How should you configure the service accounts used by Compute Engine instances to allow them query access to BigQuery datasets?

- ○

  Grant the compute engine service account roles/owner on data-warehousing GCP project and roles/bigquery.dataViewer role on the app-tier GCP project.

- ○

  Grant the BigQuery service account roles/owner on app-tier GCP project.

- ○

  Grant the compute engine service account roles/bigquery.dataViewer role on the data-warehousing GCP project.

  (Correct)

- ○

  Grant the compute engine service account roles/owner on data-warehousing GCP project.

Explanation

`Grant the BigQuery service account roles/owner on app-tier GCP project.` **is not right.**

The requirement is to identify the access needed for the service account in the app-tier project, not the service account in the data-warehousing project.

`Grant the compute engine service account roles/owner on data-warehousing GCP project.` **is not right.**

The primitive project owner role provides permissions to manage all resources within the project. For this scenario, the service account in the app-tier project needs access to BigQuery datasets in the data-warehousing project. Granting the project owner role would fall foul of least privilege principle.
Ref: https://cloud.google.com/iam/docs/recommender-overview

`Grant the compute engine service account roles/owner on data-warehousing GCP project and roles/bigquery.dataViewer role on the app-tier GCP project.` **is not right.**

The primitive project owner role provides permissions to manage all resources within the project. For this scenario, the service account in the app-tier project needs access to BigQuery datasets in the data-warehousing project. Granting the project owner role would fall foul of least privilege principle.
Ref: https://cloud.google.com/iam/docs/recommender-overview

`Grant the compute engine service account roles/bigquery.dataViewer role on the data-warehousing GCP project.` **is the right answer.**

bigquery.dataViewer role provides permissions to read the dataset's metadata and list tables in the dataset as well as Read data and metadata from the dataset's tables. This role is what we need to fulfil this requirement and follows the least privilege principle.
Ref: https://cloud.google.com/iam/docs/understanding-roles#bigquery-roles

Question 25:

Skipped

You developed an application on App Engine Service to read data from a BigQuery dataset and convert the data to PARQUET format. The application is using the default app-engine service account in the app-tier GCP project. The data team owns the BigQuery dataset in the data-warehousing project. What IAM Access should you grant to the default app-engine service account in app-tier GCP project?

- ○

  Grant the service account in the data-warehousing GCP project roles/bigquery.jobUser role on the app-tier project.

- ○

  Grant the default app-engine service account in the app-tier GCP project roles/bigquery.jobUser role on data-warehousing project.

- ○

  Grant the default app-engine service account in the app-tier GCP project roles/bigquery.dataViewer role on the same project.

- ○

  Grant the default app-engine service account in the app-tier GCP project roles/bigquery.dataViewer role on the data-warehousing project.

  (Correct)

Explanation

`Grant the default app-engine service account in the app-tier GCP project roles/bigquery.jobUser role on the data-warehousing project.` **is not right.**
Granting jobUser IAM role lets your App engine service create and run jobs including "query jobs" but doesn't give access to read data, i.e. query the data directly from the datasets. The role that you need for reading data from datasets is dataViewer!!
Ref: https://cloud.google.com/bigquery/docs/access-control#bigquery

`Grant the service account in the data-warehousing GCP project roles/bigquery.jobUser role on the app-tier project.` **is not right.**
If you grant the role from your project, you are granting the permissions for BigQuery

instance in your project. Since the requirement is for the app engine service to read data from the BigQuery dataset in a different project, this wouldn't work. Moreover, granting jobUser IAM role lets you run jobs including "query jobs" but doesn't give access to read data, i.e. query the data directly from the datasets. The role that you need for reading data from datasets is dataViewer!!
Ref: https://cloud.google.com/bigquery/docs/access-control#bigquery

`Grant the default app-engine service account in the app-tier GCP project` `roles/bigquery.dataViewer role on the same project.` **is not right.**
If you grant the role from your project, you are granting the permissions for BigQuery instance in your project. Since the requirement is for the app engine service to read data from the BigQuery dataset in a different project, these permissions are insufficient.

`Grant the default app-engine service account in the app-tier GCP project` `roles/bigquery.dataViewer role on the data-warehousing project.` **is the right answer.**
Since the data resides in the other project, the role must be granted in the other project to the App Engine service account. And since you want to read the data from BigQuery datasets, you need dataViewer role.
Ref: https://cloud.google.com/bigquery/docs/access-control#bigquery

Question 26:
Skipped
You are running a business-critical application in a GKE cluster in a subnet with cluster autoscaling enabled. A massive surge in demand for your company's products has seen the GKE cluster node pool scale-up until there were no more free IP addresses available for new VMs in the subnet. What should you do to fix this issue?

- ○

  Add a new VPC and set up VPC sharing between the new and existing VPC.
- ○

  Add a secondary (alias) IP range to the existing subnet.
- ○

  Add a new subnet to the same region.
- ○

  Expand the range of the existing subnet.

  (Correct)

Explanation

`Add a new subnet to the same region.` **is not right.**

When you create a regional (private) GKE cluster, it automatically creates a private cluster subnet, and you can't change this/add a second subnet.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#view_subnet

`Add a secondary (alias) IP range to the existing subnet.` **is not right.**

Since there are no more primary IP Address available in the VPC, it is not possible to provision new VMs. You cannot create a VM with just a secondary (alias) IP. All subnets have a primary CIDR range, which is the range of internal IP addresses that define the subnet. Each VM instance gets its primary internal IP address from this range. You can also allocate alias IP ranges from that primary range, or you can add a secondary range to the subnet and allocate alias IP ranges from the secondary range.
Ref: https://cloud.google.com/vpc/docs/alias-ip#subnet_primary_and_secondary_cidr_ranges

`Add a new VPC and set up VPC sharing between the new and existing VPC.` **is not right.**

You can't split a GKE cluster across two VPCs. You can't use shared VPC either as Google Kubernetes Engine does not support converting existing clusters to the Shared VPC model.
https://cloud.google.com/kubernetes-engine/docs/how-to/cluster-shared-vpc#overview

`Expand the range of the existing subnet.` **is the right answer.**

Since there are no more IPs available in the IP range, you need to expand the primary IP range of an existing subnet by modifying its subnet mask, setting the prefix length to a smaller number. Expanding the subnet adds more IP addresses to the subnet IP range and lets the GKE cluster spin up more nodes as needed.
Ref: https://cloud.google.com/vpc/docs/using-vpc#expand-subnet

Question 27:

Skipped

Your production applications are distributed across several Google Cloud Platform (GCP) projects, and your operations team want to efficiently manage all the production projects and applications using gcloud SDK on Cloud Shell. What should you recommend they do to achieve this in the fewest possible steps?

- ○

  Use the default gcloud configuration on cloud shell. To manage resources of a particular project, activate the relevant gcloud configuration.

- ○

Create a gcloud configuration for each production project. To manage resources of a particular project, run gcloud init to update and initialize the relevant gcloud configuration.

- ○

  Create a gcloud configuration for each production project. To manage resources of a particular project, activate the relevant gcloud configuration.

  (Correct)

- ○

  Use the default gcloud configuration on cloud shell. To manage resources of a particular project, run gcloud init to update and initialize the relevant gcloud configuration.

Explanation

`Create a gcloud configuration for each production project. To manage resources of a particular project, activate the relevant gcloud configuration.` **is the right answer.**

gcloud configurations enable you to manage multiple projects in gcloud CLI using the fewest possible steps,
Ref: https://cloud.google.com/sdk/gcloud/reference/config

For example, we have two projects.

```
$ gcloud projects list

PROJECT_ID NAME PROJECT_NUMBER

project-1-278333 project-1-278333 85524215451

project-2-278333 project-2-278333 25349885274
```

We create a configuration for each project. For project-2-278333,

```
$ gcloud config configurations create project-1-config

$ gcloud config set project project-1-278333
```

And for project-2-278333,

```
$ gcloud config configurations create project-2-config

$ gcloud config set project project-2-278333
```

We now have two configurations, one for each project.

```
$ gcloud config configurations list

NAME IS_ACTIVE ACCOUNT PROJECT COMPUTE_DEFAULT_ZONE COMPUTE_DEFAULT_REGION

cloudshell-4453 False

project-1-config False project-1-278333
```

```
project-2-config True project-2-278333
```

To activate configuration for project-1,

```
$ gcloud config configurations activate project-1-config

Activated [project-1-config].

$ gcloud config get-value project

Your active configuration is: [project-1-config]

project-1-278333
```

To activate configuration for project-2,

```
$ gcloud config configurations activate project-2-config

Activated [project-2-config].

$ gcloud config get-value project

Your active configuration is: [project-2-config]

project-2-278333
```

Question 28:

Skipped

You run a batch job every month in your on-premises data centre that downloads clickstream logs from Google Cloud Storage bucket, enriches the data and stores them in Cloud BigTable. The job runs for 32 hours on average, is fault-tolerant and can be restarted if interrupted, and must complete. You want to migrate this batch job onto a cost-efficient GCP compute service. How should you deploy it?

- ○

  Deploy the batch job in a GKE Cluster with preemptible VM node pool.

  (Correct)

- ○

  Deploy the batch job on a Google Cloud Compute Engine Preemptible VM.

- ○

  Deploy the batch job on a Google Cloud Compute Engine non-preemptible VM. Restart instances as required.

- ○

  Deploy the batch job on a fleet of Google Cloud Compute Engine preemptible VM in a Managed Instances Group (MIG) with autoscaling.

Explanation

`Deploy the batch job on a Google Cloud Compute Engine Preemptible VM.` **is not right.**
A preemptible VM is an instance that you can create and run at a much lower price than regular 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. Since our batch process must be restarted if interrupted, a preemptible VM by itself is not sufficient.
https://cloud.google.com/compute/docs/instances/preemptible#what_is_a_preemptible_instance

`Deploy the batch job on a Google Cloud Compute Engine non-preemptible VM. Restart instances as required.` **is not right.**
Stopping and starting instances as needed is a manual activity and incurs operational expenditure. Since we require to minimize cost, we shouldn't do this.

`Deploy the batch job on a fleet of Google Cloud Compute Engine preemptible VM in a Managed Instances Group (MIG) with autoscaling.` **is not right.**
Our requirement is not to scale up or scale down based on target CPU utilization.

`Deploy the batch job in a GKE Cluster with preemptible VM node pool.` **is the right answer.**
Preemptible VMs are Compute Engine VM instances that last a maximum of 24 hours and provide no availability guarantees. Preemptible VMs are priced lower than standard Compute Engine VMs and offer the same machine types and options. You can use preemptible VMs in your GKE clusters or node pools to run batch or fault-tolerant jobs that are less sensitive to the ephemeral, non-guaranteed nature of preemptible VMs.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/preemptible-vms
GKE's autoscaler is very smart and always tries to first scale the node pool with cheaper VMs. In this case, it scales up the preemptible node pool. The GKE autoscaler then scales up the default node pool—but only if no preemptible VMs are available.
Ref: https://cloud.google.com/blog/products/containers-kubernetes/cutting-costs-with-google-kubernetes-engine-using-the-cluster-autoscaler-and-preemptible-vms

Question 29:

Skipped

Your company stores an export of its Customer PII data in a multi-regional Google Cloud storage bucket. Your legal and compliance department has asked you to record all operations/requests on the data in this bucket. What should you do?

- ○

  Use the Identity Aware Proxy API to record this information.

- ○

  Enable the default Cloud Storage Service account exclusive access to read all operations and record them.

- ○

  Use the Data Loss Prevention API to record this information.

- ○

  Turn on data access audit logging in Cloud Storage to record this information.

  (Correct)

Explanation

`Use the Identity Aware Proxy API to record this information.` **is not right.**

Identity Aware Proxy is for controlling access to your cloud-based and on-premises applications and VMs running on Google Cloud. It can't be used to record/monitor data access in Cloud Storage bucket.
Ref: https://cloud.google.com/iap

`Use the Data Loss Prevention API to record this information.` **is not right.**
Cloud Data Loss Prevention is a fully managed service designed to help you discover, classify, and protect your most sensitive data. It can't be used to record/monitor data access in Cloud Storage bucket.
Ref: https://cloud.google.com/dlp

`Enable the default Cloud Storage Service account exclusive access to read all operations and record them.` **is not right.**
You need access logs, and service account access has no impact on that. Moreover, there is no such thing as a default Cloud Storage service account.
Ref: https://cloud.google.com/storage/docs/access-logs

`Turn on data access audit logging in Cloud Storage to record this information.` **is the right answer.**
Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data.
Ref: https://cloud.google.com/logging/docs/audit#data-access
You can enable data access audit logs at multiple levels as described here.
Ref: https://cloud.google.com/logging/docs/audit/configure-data-access#configuration_overview

Question 30:

Skipped

Your business-critical application deployed on a compute engine instance in us-west1-a zone suffered an outage due to GCP zone failure. You want to modify the application to be immune to zone failures while minimizing costs. What should you do?

- ○

  Ensure you have hourly snapshots of the disk in Google Cloud Storage. In the unlikely event of a zonal outage, use the snapshots to provision a new Compute Engine Instance in a different zone.

- ○

  Replace the single instance with a Managed Instance Group (MIG) and autoscaling enabled. Configure a health check to detect failures rapidly.

- ○

  Provision another compute engine instance in us-west1-b and balance the traffic across both zones.

  (Correct)

- ○

  Direct the traffic through a Global HTTP(s) Load Balancer to shield your application from GCP zone failures.

Explanation

`Ensure you have hourly snapshots of the disk in Google Cloud Storage. In the unlikely event of a zonal outage, use the snapshots to provision a new Compute Engine Instance in a different zone.` **is not right.**

This option wouldn't eliminate downtime, the solution doesn't support the failure of a single Compute Engine zone, and the solution involves manual intervention which adds to the overall cost.

`Direct the traffic through a Global HTTP(s) Load Balancer to shield your application from GCP zone failures.` **is not right.**

The VMs are still in a single zone, so this solution doesn't support the failure of a single Compute Engine zone.

`Replace the single instance with a Managed Instance Group (MIG) and autoscaling enabled. Configure a health check to detect failures rapidly.` **is not right.**

The VMs are still in a single zone, so this solution doesn't support the failure of a single Compute Engine zone.

`Provision another compute engine instance in us-west1-b and balance the traffic across both zones.` **is the right answer.**

Creating Compute Engine resources in us-west1-b and balancing the load across both zones ensures that the solution supports the failure of a single Compute Engine zone and eliminates downtime. Even if one zone goes down, the application can continue to serve requests from the other zone.

Question 31:

Skipped

Your company plans to migrate all applications from the on-premise data centre to Google Cloud Platform and requires a monthly estimate of the cost of running these applications in GCP. How can you provide this estimate?

- ○

  Migrate all applications to GCP and run them for a week. Use Cloud Monitoring to identify the costs for this week and use it to derive the monthly cost of running all applications in GCP.

- ○

  For all GCP services/APIs you are planning to use, use the GCP pricing calculator to estimate the monthly costs.

  (Correct)

- ○

  For all GCP services/APIs you are planning to use, capture the pricing from the products pricing page and use an excel sheet to estimate the monthly costs.

- ○

  Migrate all applications to GCP and run them for a week. Use the costs from the Billing Report page for this week to extrapolate the monthly cost of running all applications in GCP.

Explanation

`Migrate all applications to GCP and run them for a week. Use the costs from the Billing Report page for this week to extrapolate the monthly cost of running all applications in GCP.` **is not right.**

By provisioning the solution on GCP, you are going to incur costs. We are required to

estimate the costs, and this can be done by using Google Cloud Pricing Calculator.
Ref: https://cloud.google.com/products/calculator

`Migrate all applications to GCP and run them for a week. Use Cloud Monitoring to identify the costs for this week and use it to derive the monthly cost of running all applications in GCP.` **is not right.**
By provisioning the solution on GCP, you are going to incur costs. We are required to estimate the costs, and this can be done by using Google Cloud Pricing Calculator.
Ref: https://cloud.google.com/products/calculator

`For all GCP services/APIs you are planning to use, capture the pricing from the products pricing page and use an excel sheet to estimate the monthly costs.` **is not right.**
This option would certainly work but is a manual task. Why use this when you can use Google Cloud Pricing Calculator to achieve the save?
Ref: https://cloud.google.com/products/calculator

`For all GCP services/APIs you are planning to use, use the GCP pricing calculator to estimate the monthly costs.` **is the right answer.**
You can use the Google Cloud Pricing Calculator to total the estimated monthly costs for each GCP product. You don't incur any charges for doing so.
Ref: https://cloud.google.com/products/calculator

Question 32:

Skipped

You deployed the Finance teams' Payroll application to Google Compute Engine, and this application is used by staff during regular business hours. The operations team want to backup the VMs daily outside the business hours and delete images older than 50 days to save costs. They need an automated solution with the least operational overhead and the least number of GCP services. What should they do?

- ○

  Use Cloud Scheduler to trigger a Cloud Function that creates snapshots of the disk daily. Use Cloud Scheduler to trigger another Cloud Function that iterates over the snapshots and deletes snapshots older than 50 days.

- ○

  Navigate to the Compute Engine Disk section of your VM instance in the GCP console and enable a snapshot schedule for automated creation of daily snapshots. Set Auto-Delete snapshots after to 50 days.

  (Correct)

- ○

Add a metadata tag on the Google Compute Engine instance to enable snapshot creation. Add a second metadata tag to specify the snapshot schedule, and a third metadata tag to specify the retention period.

- ○

Use AppEngine Cron service to trigger a custom script that creates snapshots of the disk daily. Use AppEngine Cron service to trigger another custom script that iterates over the snapshots and deletes snapshots older than 50 days.

Explanation

`Add a metadata tag on the Google Compute Engine instance to enable snapshot creation. Add a second metadata tag to specify the snapshot schedule, and a third metadata tag to specify the retention period.` **is not right.**

Adding these metadata tags on the instance does not affect snapshot creation/automation.

`Use Cloud Scheduler to trigger a Cloud Function that creates snapshots of the disk daily. Use Cloud Scheduler to trigger another Cloud Function that iterates over the snapshots and deletes snapshots older than 50 days.` **is not right.**

You want to fulfil this requirement by using the least number of services. While this works, it involves the use of Cloud Functions and Cloud Scheduler, and we should look at doing this using the least number of services.

`Use AppEngine Cron service to trigger a custom script that creates snapshots of the disk daily. Use AppEngine Cron service to trigger another custom script that iterates over the snapshots and deletes snapshots older than 50 days.` **is not right.**

Bash scripts and crontabs add a lot of operational overhead. You want to fulfil this requirement with the least management overhead so you should avoid this.

`Navigate to the Compute Engine Disk section of your VM instance in the GCP console and enable a snapshot schedule for automated creation of daily snapshots. Set Auto-Delete snapshots after to 50 days.` **is the right answer.**

Google recommends you use Use snapshot schedules as a best practice to back up your Compute Engine workloads.

Ref: https://cloud.google.com/compute/docs/disks/scheduled-snapshots

Question 33:

Skipped

You want to migrate a legacy application from your on-premises data centre to Google Cloud Platform. The application serves SSL encrypted traffic from worldwide clients on TCP port 443. What GCP Loadbalancing service should you use to minimize latency for all clients?

- ○

  Internal TCP/UDP Load Balancer.

- ○

  Network TCP/UDP Load Balancer.

- ○

  External HTTP(S) Load Balancer.

- ○

  SSL Proxy Load Balancer.

  (Correct)

Explanation

`Internal TCP/UDP Load Balancer.` **is not right.**

Internal TCP Load Balancing is a regional load balancer that enables you to run and scale your services behind an internal load balancing IP address that is accessible only to your internal virtual machine (VM) instances. Since we need to serve public traffic, this load balancer is not suitable for us.

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

`Network TCP/UDP Load Balancer.` **is not right.**

Google Cloud external TCP/UDP Network Load Balancing is a regional, non-proxied load balancer. Since this is a regional load balancer, its endpoint is regional, and this means that the traffic for this load balancer must traverse through the internet to reach the regional endpoint. Not a problem for clients located closer to this region but traversing through the internet can add a lot of latency to connections from other regions. In this scenario, clients are located all over the world; therefore, Network Load Balancer is not a suitable option.

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

`External HTTP(S) Load Balancer.` **is not right.**

External HTTP(S) Load Balancer is a Layer 7 load balancer suitable for HTTP/HTTPS traffic and is not suited for TCP traffic.

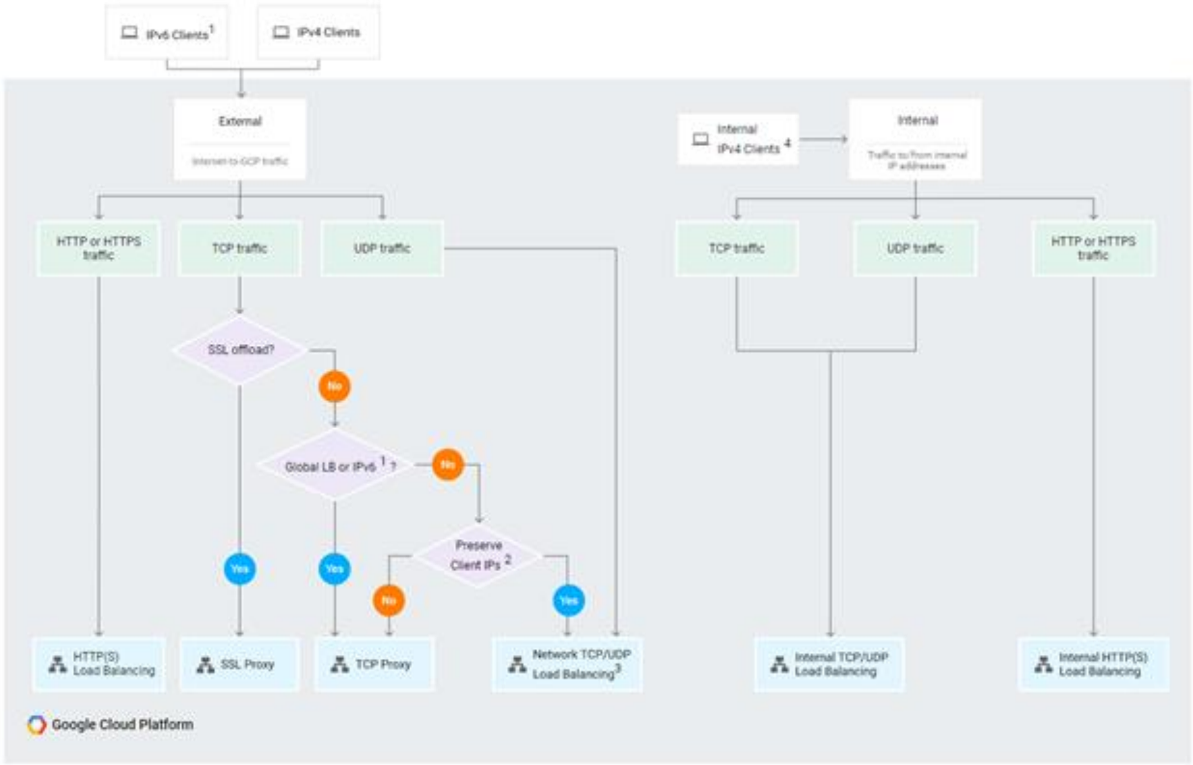
Ref: https://cloud.google.com/load-balancing/docs/choosing-load-balancer#summary-of-google-cloud-load-balancers

`SSL Proxy Load Balancer.` **is the right answer.**

By using Google Cloud SSL Proxy Load Balancing for your SSL traffic, you can terminate user SSL (TLS) connections at the load balancing layer. You can then balance the connections across your backend instances by using the SSL (recommended) or TCP protocols. The SSL proxy load balancer terminates TLS in locations that are distributed globally, to minimize latency between clients and the load balancer.

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

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



[1] IPv6 clients are supported for TCP traffic if you configure the load balancer in Premium Tier. IPv6 clients aren't supported for UDP traffic.

[2] Another reason to choose Network TCP/UDP Load Balancing is if you need to ensure that the load balancer is located in a particular region.

[3] Network TCP/UDP load balancers use regional external IP addresses that are accessible by clients anywhere.

[4] Clients in a VPC network or in a network connected to a VPC network.

Question 34:

Skipped

Your company's compute workloads are split between the on-premises data centre and Google Cloud Platform. The on-premises data centre is connected to Google Cloud network by Cloud VPN. You have a requirement to provision a new non-publicly-reachable compute engine instance on a c2-standard-8 machine type in australia-southeast1-b zone. What should you do?

- ○

  Provision the instance in a subnetwork that has all egress traffic disabled.

- ○

  Provision the instance without a public IP address.

  (Correct)

- ○

  Configure a route to route all traffic to the public IP of compute engine instance through the VPN tunnel.

- ○

  Provision the instance in a subnet that has Google Private Access enabled.

Explanation

`Provision the instance in a subnet that has Google Private Access enabled.` **is not right.**

VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access to external IP addresses of Google APIs and services. Private Google Access has no effect on instances with Public IPs as they are always publicly reachable irrespective of the private google access setting.

Ref: https://cloud.google.com/vpc/docs/private-access-options#pga

`Provision the instance in a subnetwork that has all egress traffic disabled.` **is not right.**

An egress firewall rule prevents traffic from leaving the VPC network, but does not prevent traffic coming in. If the instance has a public IP address, then the instance is still publicly reachable despite creating a deny-all egress firewall rule.

`Configure a route to route all traffic to the public IP of compute engine instance through the VPN tunnel.` **is not right.**

You can not create routes for public IP addresses. Routes within the VPC are applicable only to traffic on the internal IP range.

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

`Provision the instance without a public IP address.` **is the right answer.**

Public IP addresses are internet routable. But Private IP addresses are internal and cannot be internet routable, such as RFC 1918 addresses. So creating the instance without a public IP address ensures that no internet traffic can reach it.

Ref: https://cloud.google.com/vpc/docs/ip-addresses

Question 35:

Skipped

An auditor requires specific access on certain GCP services in your Cloud project. You have developed the the first version of a custom IAM role to enable this

access. The compliance team wants to test this role in a test GCP project and has asked you to share with them the role and its lifecycle stage. What should you do?

- ○

  1. Set the custom IAM role lifecycle stage to BETA while you test the role in the test GCP project.

  2. Restrict the custom IAM role to use permissions with TESTING support level.

- ○

  1. Set the custom IAM role lifecycle stage to BETA while you test the role in the test GCP project.

  2. Restrict the custom IAM role to use permissions with SUPPORTED support level.

- ○

  1. Set the custom IAM role lifecycle stage to ALPHA while you test the role in the test GCP project.

  2. Restrict the custom IAM role to use permissions with TESTING support level.

- ○

  1. Set the custom IAM role lifecycle stage to ALPHA while you test the role in the test GCP project.

  2. Restrict the custom IAM role to use permissions with SUPPORTED support level.

  (Correct)

Explanation
When setting support levels for permissions in custom roles, you can set to one of **SUPPORTED**, **TESTING** or **NOT_SUPPORTED**. **SUPPORTED** -The permission is fully supported in custom roles. **TESTING** - The permission is being tested to check its compatibility with custom roles. You can include the permission in custom roles, but you might see unexpected behaviour. Such permissions are not recommended for production use.
Ref: https://cloud.google.com/iam/docs/custom-roles-permissions-support Since we want the role to be suitable for production use, **we need "SUPPORTED" and not "TESTING".**

In terms of role stage, the stage transitions from **ALPHA --> BETA --> GA**
Ref: https://cloud.google.com/iam/docs/understanding-custom-roles#testing_and_deploying Since this is the first version of the custom role, **we start with "ALPHA"**.

The only option that satisfies "ALPHA" stage with "SUPPORTED" support level is

`1. Set the custom IAM role lifecycle stage to ALPHA while you test the role in the test GCP project.`
`2. Restrict the custom IAM role to use permissions with SUPPORTED support level.` **is the right answer**

Question 36:
Skipped
Your production Compute workloads are running in a subnet with a range 192.168.20.128/25. A recent surge in traffic has seen the production VMs struggle, and you want to add more VMs, but all IP addresses in the subnet are in use. All new and old VMs need to communicate with each other. How can you do this with the fewest steps?

- ○

  Create a new non-overlapping Alias range in the existing VPC and Configure the VMs to use the alias range.

- ○

  Update the subnet range to 192.168.20.0/24.

  (Correct)

- ○

  Create a new VPC network and a new subnet with IP range 192.168.21.0/24. Enable VPC Peering between the old VPC and new VPC.

- ○

  Create a new VPC and a new subnet with IP range 192.168.21.0/24. Enable VPC Peering between the old VPC and new VPC. Configure a custom Route exchange.

Explanation
`Create a new non-overlapping Alias range in the existing VPC and Configure the VMs to use the alias range.` **is not right.**
Since there isn't any more primary IP Address available in the VPC, it is not possible

to provision new VMs. You cannot create a VM with just a secondary (alias) IP. All subnets have a primary CIDR range, which is the range of internal IP addresses that define the subnet. Each VM instance gets its primary internal IP address from this range. You can also allocate alias IP ranges from that primary range, or you can add a secondary range to the subnet and allocate alias IP ranges from the secondary range.
Ref: https://cloud.google.com/vpc/docs/alias-ip#subnet_primary_and_secondary_cidr_ranges

`Create a new VPC and a new subnet with IP range 192.168.21.0/24. Enable VPC Peering between the old VPC and new VPC. Configure a custom Route exchange.` **is not right.**
Subnet routes that don't use privately reused public IP addresses are always exchanged between peered networks. You can also exchange custom routes, which include static and dynamic routes, and routes for subnets that use privately reused public IP addresses if network administrators in both networks have the appropriate peering configurations. But in this case, there is no requirement to exchange custom routes.
Ref: https://cloud.google.com/vpc/docs/vpc-peering?&_ga=2.257174475.-1345429276.1592757751#importing-exporting-routes

`Create a new VPC network and a new subnet with IP range 192.168.21.0/24. Enable VPC Peering between the old VPC and new VPC.` **is not right.**
This approach works but is more complicated than expanding the subnet range.
Ref: https://cloud.google.com/vpc/docs/vpc-peering

`Update the subnet range to 192.168.20.0/24.` **is the right answer.**
Since there are no private IP addresses available in the subnet, the most appropriate action is to expand the subnet. Expanding the range to 192.168.21.0/24 gives you 128 additional IP addresses. You could you gcloud compute networks subnets expand-ip-range to expand a subnet.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/networks/subnets/expand-ip-range

Question 37:

Skipped

You migrated a mission-critical application from the on-premises data centre to Google Kubernetes Engine (GKE) which uses e2-standard-2 machine types. You want to deploy additional pods on c2-standard-16 machine types. How can you do this without causing application downtime?

- ○

  Update the existing cluster to add a new node pool with c2-standard-16 machine types and deploy the pods.

(Correct)

- ○

  Create a new GKE cluster with node pool instances of type c2-standard-16. Deploy the application on the new GKE cluster and delete the old GKE Cluster.

- ○

  Create a new GKE cluster with two node pools – one with e2-standard-2 machine types and other with c2-standard-16 machine types. Deploy the application on the new GKE cluster and delete the old GKE Cluster.

- ○

  Run gcloud container clusters upgrade to move to c2-standard-16 machine types. Terminate all existing pods.

Explanation

`Create a new GKE cluster with node pool instances of type c2-standard-16. Deploy the application on the new GKE cluster and delete the old GKE Cluster.` **is not right.**

This option results in the extra cost of running two clusters in parallel until the cutover happens. Also, creating a single node pool with just n2-highmem-16 nodes might result in inefficient use of resources and subsequently extra costs.

`Create a new GKE cluster with two node pools – one with e2-standard-2 machine types and other with c2-standard-16 machine types. Deploy the application on the new GKE cluster and delete the old GKE Cluster.` **is not right.**

Having two node pools - one based on n1-standard-2 and the other based on n2-highmem-16 is the right idea. The relevant pods can be deployed to the respective node pools. However, you are incurring the extra cost of running two clusters in parallel while the cutover happens.

`Run gcloud container clusters upgrade to move to c2-standard-16 machine types. Terminate all existing pods.` **is not right.**

gcloud container clusters upgrade - is used to upgrade the Kubernetes version of an existing container cluster.

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

`Update the existing cluster to add a new node pool with c2-standard-16 machine types and deploy the pods.` **is the right answer.**

This option is the easiest and most practical of all options. Having two node pools -

one based on e2-standard-2 and the other based on c2-standard-16 is the right idea. Also, adding the node pools to the existing cluster does not affect the existing node pool and therefore no downtime.

Question 38:

Skipped

A compute engine instance that runs one of your critical application has live migration enabled. You want to learn when a maintenance event will occur so that you can perform some backups before the live migration kicks in. What should you do?

- ○

  Query the maintenance event metadata key periodically by running `curl http://metadata.google.internal/computeMetadata/v1/instance/maintenance-event -H "Metadata-Flavor: Google"`**.**

  (Correct)

- ○

  Set up an alert on guest/system/live-migrat-event metric in Cloud Monitoring.

- ○

  Set up an alert on guest/system/maintenance-event metric in Cloud Monitoring.

- ○

  Query the live migration events periodically by running `curl http://metadata.google.internal/computeMetadata/v1/instance/live-migrate-event -H "Metadata-Flavor: Google"`**.**

Explanation

`Set up an alert on guest/system/maintenance-event metric in Cloud Monitoring.` **is not right**

There is no such metric in Cloud monitoring for compute service.
Ref: https://cloud.google.com/monitoring/api/metrics_gcp#gcp-compute

`Set up an alert on guest/system/live-migrat-event metric in Cloud Monitoring.` **is not right**

There is no such metric in Cloud monitoring for compute service.
Ref: https://cloud.google.com/monitoring/api/metrics_gcp#gcp-compute

`Query the live migration events periodically by running curl http://metadata.google.internal/computeMetadata/v1/instance/live-migrate-event -H "Metadata-Flavor: Google"`. **is not right**
live-migrate-event metadata key isn't available.
Ref: https://cloud.google.com/compute/docs/metadata/getting-live-migration-notice

`Query the maintenance event metadata key periodically by running curl http://metadata.google.internal/computeMetadata/v1/instance/maintenance-event -H "Metadata-Flavor: Google".` **is the right answer**
You can learn when a maintenance event will occur by querying the maintenance-event metadata key periodically. The maintenance-event metadata key is populated for maintenance events only if you have set your VM's scheduling option to migrate or if your VM has a GPU attached. The value of this metadata key changes 60 seconds before a maintenance event starts, giving your application code a way to trigger any tasks you want to perform prior to a maintenance event, such as backing up data or updating logs. To query the maintenance-event metadata key on Linux VMs, run the following command:

```
curl http://metadata.google.internal/computeMetadata/v1/instance/maintenance-event -H "Metadata-Flavor: Google"
```

Ref: https://cloud.google.com/compute/docs/metadata/getting-live-migration-notice

Question 39:

Skipped

You deployed a mission-critical application on Google Compute Engine. Your operations team have asked you to enable measures to prevent engineers from accidentally destroying the instance. What should you do?

- ○

  Uncheck “Delete boot disk when instance is deleted” option when provisioning the compute engine instance.

- ○

  Enable automatic restart on the instance.

- ○

  Turn on deletion protection on the compute engine instance.

  (Correct)

- ○

  Deploy the application on a preemptible compute engine instance.

Explanation

`Deploy the application on a preemptible compute engine instance.` **is not right.**

A preemptible VM is an instance that you can create and run at a much lower price than normal instances. However, Compute Engine might terminate (preempt) these instances if it requires access to those resources for other tasks. Preemptible instances are excess Compute Engine capacity, so their availability varies with usage. This option wouldn't help with our requirement - to prevent anyone from accidentally destroying the instance.

Ref: https://cloud.google.com/compute/docs/instances/preemptible

`Uncheck “Delete boot disk when instance is deleted” option when provisioning the compute engine instance.` **is not right.**

You can automatically delete read/write persistent zonal disks when the associated VM instance is deleted. Enabling/Disabling the flag impacts disk deletion but not the instance termination.

Ref: https://cloud.google.com/compute/docs/disks/add-persistent-disk#updateautodelete

`Enable automatic restart on the instance.` **is not right.**

The restart behaviour determines whether the instance automatically restarts if it crashes or gets terminated. This setting does not prevent anyone from accidentally destroying the instance.

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

`Turn on deletion protection on the compute engine instance.` **is the right answer.**

By setting the deletionProtection flag, a VM instance can be protected from accidental deletion. If a user attempts to delete a VM instance for which you have set the deletionProtection flag, the request fails.

Ref: https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion

Question 40:

Skipped

Your compliance team wants to review the audit logs and data access logs in the production GCP project. You want to follow Google recommended practices. What should you do?

- ○

Export logs to Cloud Storage and grant the compliance team roles/logging.privateLogViewer IAM role.

- ○

Grant the compliance team roles/logging.privateLogViewer IAM role. Let the compliance team know they can also query IAM policy changes in Cloud Logging.

(Correct)

- ○

Export logs to Cloud Storage and grant the compliance team a custom IAM role that has logging.privateLogEntries.list permission.

- ○

Grant the compliance team a custom IAM role that has logging.privateLogEntries.list permission. Let the compliance team know they can also query IAM policy changes in Cloud Logging.

Explanation
Google Cloud provides Cloud Audit Logs, which is an integral part of Cloud Logging. It consists of two log streams for each project: Admin Activity and Data Access, which are generated by Google Cloud services to help you answer the question of "who did what, where, and when?" within your Google Cloud projects.
Ref: https://cloud.google.com/iam/docs/job-functions/auditing#scenario_external_auditors

To view Admin Activity audit logs, you must have one of the following Cloud IAM roles in the project that contains your audit logs:

- Project Owner, Project Editor, or Project Viewer.

- The Logging Logs Viewer role.

- A custom Cloud IAM role with the logging.logEntries.list Cloud IAM permission.
https://cloud.google.com/iam/docs/audit-logging#audit_log_permissions

To view Data Access audit logs, you must have one of the following roles in the project that contains your audit logs:

- Project Owner.

- Logging's Private Logs Viewer role.

- A custom Cloud IAM role with the logging.privateLogEntries.list Cloud IAM permission.
https://cloud.google.com/iam/docs/audit-logging#audit_log_permissions

`Export logs to Cloud Storage and grant the compliance team a custom IAM role that has logging.privateLogEntries.list permission.` **is not right.**
logging.privateLogEntries.list provides permissions to view Data Access audit logs but this does not grant permissions to view Admin activity logs.
Ref: https://cloud.google.com/logging/docs/access-control#console_permissions

`Grant the compliance team a custom IAM role that has logging.privateLogEntries.list permission. Let the compliance team know they can also query IAM policy changes in Cloud Logging.` **is not right.**
logging.privateLogEntries.list provides permissions to view Data Access audit logs but this does not grant permissions to view Admin activity logs.
Ref: https://cloud.google.com/logging/docs/access-control#console_permissions

`Export logs to Cloud Storage and grant the compliance team roles/logging.privateLogViewer IAM role.` **is not right.**
The IAM role roles/logging.privateLogViewer is the right role. It includes roles/logging.viewer permissions (everything in logging except access transparency and data access audit logs) plus: logging.privateLogEntries.list permissions (access transparency and data access audit logs). Together, they let the compliance team review the admin activity logs and data access logs. But exporting logs to Cloud Storage indicates that we want the compliance team to review logs from Cloud Storage and not the logs within Cloud Logging console. In this scenario, unless the compliance team is also assigned a role that lets them access the relevant cloud storage buckets, they wouldn't be able to view log information in the buckets.

`Grant the compliance team roles/logging.privateLogViewer IAM role. Let the compliance team know they can also query IAM policy changes in Cloud Logging.` **is the right answer.**
The IAM role roles/logging.privateLogViewer is the right role. It includes roles/logging.viewer permissions (everything in logging except access transparency and data access audit logs) plus: logging.privateLogEntries.list permissions (access transparency and data access audit logs). Together, they let the compliance team review the admin activity logs and data access logs. This role lets them access the logs in Cloud Logging console.
Ref: https://cloud.google.com/logging/docs/access-control

Question 41:

Skipped

You want to monitor resource utilization (RAM, Disk, Network, CPU, etc.) for all applications in development, test and production GCP projects in a single dashboard. What should you do?

- ○

  Make use of the default Cloud Monitoring dashboards in all the projects.

- ○

  Grant roles/monitoring.admin to development, test and production GCP projects.

- ○

  Create a Cloud Monitoring workspace in the production project and add development and test projects to it.

  (Correct)

- ○

  In Cloud Monitoring, share charts from development, test and production GCP projects.

Explanation

`In Cloud Monitoring, share charts from development, test and production GCP projects.` **is not right.**

This option involves a lot of work. You can share charts from development, test and production projects by enabling Cloud Monitoring as a data source for Grafana
Ref: https://cloud.google.com/monitoring/charts/sharing-charts
and then follow the instructions
at https://grafana.com/docs/grafana/latest/features/datasources/cloudmonitoring/
to build Grafana dashboards.

`Grant roles/monitoring.admin to development, test and production GCP projects.` **is not right.**
You don’t grant roles to projects, and this doesn’t help you get a unified view in a single dashboard.
Rer: https://cloud.google.com/monitoring/access-control

`Make use of the default Cloud Monitoring dashboards in all the projects.` **is not right.**
Possibly, but this doesn't satisfy the requirement "single pane of glass".

`Create a Cloud Monitoring workspace in the production project and add development and test projects to it.` **is the right answer.**
A Workspace is a tool for monitoring resources contained in one or more Google

Cloud projects or AWS accounts. A Workspace accesses metric data from its monitored projects, but the metric data remains in those projects. You can configure Production project to be the host project and the development and test projects as the monitored projects. You can now build dashboards in the Cloud Monitoring workspace and view monitoring information for all projects in a "single pane of glass".
Ref: https://cloud.google.com/monitoring/workspaces

Question 42:
Skipped
You deployed an application using Apache Tomcat server on a single Google Cloud VM. Users are complaining of intermittent issues accessing a specific page in the application, and you want to look at the logs on the local disk. What should you do?

- ○

  Check logs in the Serial Console.

- ○

  Install the Cloud Logging Agent on the VM and configure it to send logs to Cloud Logging. Check logs in Cloud Logging.

  (Correct)

- ○

  Configure a health check on the instance to identify the issue and email you the logs when the application experiences the issue.

- ○

  Check logs in Cloud Logging.

Explanation
`Check logs in Cloud Logging.` **is not right.**
The application writes logs to disk, but we don't know if these logs are forwarded to Cloud Logging. Unless you install Cloud logging agent (which this option doesn't talk about) and configure to stream the application logs, the logs don't get to Cloud logging.
Ref: https://cloud.google.com/logging/docs/agent

`Check logs in the Serial Console.` **is not right.**
You would interact with instance's serial console to debug boot and networking issues, troubleshoot malfunctioning instances, interact with the GRand Unified Bootloader (GRUB), and perform other troubleshooting tasks. Since the issues being reported are with the application, analysing and debugging in the instances' serial

console doesn't help.
Ref: https://cloud.google.com/compute/docs/instances/interacting-with-serial-console

`Configure a health check on the instance to identify the issue and email you the logs when the application experiences the issue.` **is not right.**
We don’t know what the issue is, and we want to look at the logs to identify the problem, so it is not possible to create a health check without first identifying what the issue is.

`Install the Cloud Logging Agent on the VM and configure it to send logs to Cloud Logging. Check logs in Cloud Logging.` **is the right answer.**
It is a best practice to run the Logging agent on all your VM instances. In its default configuration, the Logging agent streams logs from common third-party applications and system software to Logging; review the list of default logs. You can configure the agent to stream additional logs; go to Configuring the Logging agent for details on agent configuration and operation. As logs are now streamed to Cloud Logging, you can view your logs in Cloud logging and diagnose the problem.
Ref: https://cloud.google.com/logging/docs/agent

Question 43:

Skipped

You have an application in your on-premises data centre with an API that is triggered when a new file is created or updated in a NAS share. You want to migrate this solution to Google Cloud Platform and have identified Cloud Storage as the replacement service for NAS. How should you deploy the API?

- ○

  Trigger a Cloud Function whenever files in Cloud Storage are created or updated.

  (Correct)

- ○

  Deploy the API on GKE cluster and use Cloud Scheduler to trigger the API to look for files in Cloud Storage there were created or update since the last run.

- ○

  Configure Cloud Pub/Sub to capture details of files created/modified in Cloud Storage. Deploy the API in App Engine Standard and use Cloud Scheduler to trigger the API to fetch information from Cloud Pub/Sub.

- ○

Trigger a Cloud Dataflow job whenever files in Cloud Storage are created or updated.

Explanation

`Configure Cloud Pub/Sub to capture details of files created/modified in Cloud Storage. Deploy the API in App Engine Standard and use Cloud Scheduler to trigger the API to fetch information from Cloud Pub/Sub.` **is not right.**

Cloud Scheduler lets you run your batch and big data jobs on a recurring schedule. Since it doesn't work real-time, you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.
Ref: https://cloud.google.com/scheduler

`Deploy the API on GKE cluster and use Cloud Scheduler to trigger the API to look for files in Cloud Storage there were created or update since the last run.` **is not right.**

You can use CronJobs to run tasks at a specific time or interval. Since it doesn't work real-time, you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.
Ref: https://cloud.google.com/kubernetes-engine/docs/how-to/cronjobs

`Trigger a Cloud Dataflow job whenever files in Cloud Storage are created or updated.` **is not right.**

Dataflow is Unified stream and batch data processing that's serverless, fast, and cost-effective. Batch processing is not real-time, so you can't execute a code snippet whenever a new file is uploaded to a Cloud Storage bucket.
Ref: https://cloud.google.com/dataflow

`Trigger a Cloud Function whenever files in Cloud Storage are created or updated.` **is the right answer.**

Cloud Functions can respond to change notifications emerging from Google Cloud Storage. These notifications can be configured to trigger in response to various events inside a bucket—object creation, deletion, archiving and metadata updates.
Ref: https://cloud.google.com/functions/docs/calling/storage

Question 44:

Skipped

Your company updated its business operating model recently and no longer need the applications deployed in the data-analytics-v1 GCP project. You want to turn off all GCP services and APIs in this project. You want to do this efficiently using the least number of steps while following Google recommended practices. What should you do?

- ○

Ask an engineer with Organization Administrator IAM role to locate the project and shut down.

- ○

Ask an engineer with Organization Administrator IAM role to identify all resources in the project and delete them.

- ○

Ask an engineer with Project Owner IAM role to identify all resources in the project and delete them.

- ○

Ask an engineer with Project Owner IAM role to locate the project and shut down.

(Correct)

Explanation

`Ask an engineer with Organization Administrator IAM role to locate the project and shut down.` **is not right.**
Organization Admin role provides permissions to get and list projects but not shutdown projects.
Ref: https://cloud.google.com/iam/docs/understanding-roles#resource-manager-roles

`Ask an engineer with Organization Administrator IAM role to identify all resources in the project and delete them.` **is not right.**
Organization Admin role provides permissions to get and list projects but not delete projects.
Ref: https://cloud.google.com/iam/docs/understanding-roles#resource-manager-roles

`Ask an engineer with Project Owner IAM role to identify all resources in the project and delete them.` **is not right.**
The primitive Project Owner role provides permissions to delete project
https://cloud.google.com/iam/docs/understanding-roles#primitive_roles
But locating all the resources and deleting them is a manual task, time-consuming and error-prone. Our goal is to accomplish the same but with fewest possible steps.

`Ask an engineer with Project Owner IAM role to locate the project and shut down.` **is the right answer.**
The primitive Project Owner role provides permissions to delete project
https://cloud.google.com/iam/docs/understanding-roles#primitive_roles

You can shut down projects using the Cloud Console. When you shut down a project, this immediately happens: All billing and traffic serving stops, You lose access to the project, The owners of the project will be notified and can stop the deletion within 30 days, The project will be scheduled to be deleted after 30 days. However, some resources may be deleted much earlier.
Ref: https://cloud.google.com/resource-manager/docs/creating-managing-projects#shutting_down_projects

Question 45:

Skipped

EU GDPR requires you to respond to a Subject Access Request (SAR) within one month. To be compliant, your company deployed an application that uses Apache WebServer to provide SAR archive (tar) files back to customers requesting them. Your compliance team has asked you to send them an email notification when the network egress charges for this server in the GCP project exceeds 250 dollars per month. What should you do?

- ○

  Configure a budget with the scope set to the project, the amount set to $250, threshold rule set to 100% of actual cost & trigger email notifications when spending exceeds the threshold.

- ○

  Export the project billing data to a BigQuery dataset and deploy a Cloud Function to extract and sum up the network egress costs from the BigQuery dataset for the Apache server for the current month, and send an email notification when spending exceeds $250.

  (Correct)

- ○

  Configure a budget with the scope set to the billing account, the amount set to $250, threshold rule set to 100% of actual cost & trigger email notifications when spending exceeds the threshold.

- ○

  Export the logs from Apache server to Cloud Logging and deploy a Cloud Function to parse the logs, extract and sum up the size of response payload for all requests during the current month; and send an email notification when spending exceeds $250.

Explanation

`Configure a budget with the scope set to the project, the amount set to $250, threshold rule set to 100% of actual cost & trigger email notifications when spending exceeds the threshold.` **is not right.**
This budget alert is defined for the project, which means it includes all costs and not just the egress network costs - which goes against our requirements. It also contains costs across all applications and not just the Compute Engine instance containing the Apache webserver. While it is possible to set the budget scope to include the Product (i.e. Google Compute Engine) and a label that uniquely identifies the specific compute engine instance, the option doesn't mention this.
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

`Configure a budget with the scope set to the billing account, the amount set to $250, threshold rule set to 100% of actual cost & trigger email notifications when spending exceeds the threshold.` **is not right.**
Like above, but worse as this budget alert includes costs from all projects linked to the billing account. And like above, while it is possible to scope an alert down to Project/Product/Labels, the option doesn't mention this.
Ref: https://cloud.google.com/billing/docs/how-to/budgets#budget-scope

`Export the logs from Apache server to Cloud Logging and deploy a Cloud Function to parse the logs, extract and sum up the size of response payload for all requests during the current month; and send an email notification when spending exceeds $250.` **is not right.**
You can't arrive at the exact egress costs with this approach. You can configure apache logs to include the response object size.
Ref: https://httpd.apache.org/docs/1.3/logs.html#common
And you can then do what this option says to arrive at the combined size of all the responses, but this is not 100% accurate as it does not include header sizes. Even if we assume the header size is insignificant compare to the large files published on the apache web server, our question asks us to do this the Google way "as measured by Google Cloud Platform (GCP)". GCP does not look at the response sizes in the Apache log files to determine the egress costs. The GCP egress calculator takes into consideration the source and destination (source = the region that hosts the Compute Engine instance running Apache Web Server; and the destination is the destination region of the packet). The egress cost is different for different destinations, as shown in this pricing reference.
Ref: https://cloud.google.com/vpc/network-pricing#internet_egress
The Apache logs do not give you the destination information, and without this information, you can't accurately calculate the egress costs.

`Export the project billing data to a BigQuery dataset and deploy a Cloud Function to extract and sum up the network egress costs from the BigQuery dataset for the Apache server for the current month, and send an email notification when spending exceeds $250.` **is the right answer.**

This option is the only one that satisfies our requirement. We do it the Google way by (re)using the Billing Data that GCP uses. And we scope down the costs to just egress network costs for the apache web server. Finally, we schedule this to run hourly and send an email if the costs exceed 250 dollars.

Question 46:

Skipped

You are running an application on a Google Compute Engine instance. You want to create multiple copies of this VM to handle the burst in traffic. What should you do?

- ○

  Create a snapshot of the compute engine instance disk, create custom images from the snapshot to handle the burst in traffic.

- ○

  Create a snapshot of the compute engine instance disk and create images from this snapshot to handle the burst in traffic.

- ○

  Create a snapshot of the compute engine instance disk, create a custom image from the snapshot, create instances from this image to handle the burst in traffic.

  (Correct)

- ○

  Create a snapshot of the compute engine instance disk and create instances from this snapshot to handle the burst in traffic.

Explanation

`Create a snapshot of the compute engine instance disk and create images from this snapshot to handle the burst in traffic.` **is not right.**

You can't process additional traffic with images. It would be best if you spun up new compute engine VM instances.

Ref: https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots

`Create a snapshot of the compute engine instance disk, create custom images from the snapshot to handle the burst in traffic.` **is not right.**

You can't process additional traffic with images. It would be best if you spun up new compute engine VM instances.

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

`Create a snapshot of the compute engine instance disk and create instances from this snapshot to handle the burst in traffic.` **is not right.**
The documentation states you can do this.
Ref: https://cloud.google.com/compute/docs/instances/create-start-instance#restore_boot_snapshot
But, further down in step 7, you see that you are creating a new disk which will be used by the compute engine instance. You can't directly create a VM from a snapshot without the disk. You can use the snapshot to create a disk for the new instance, but you can't create the instance directly from a snapshot without the disk.

Ref: https://cloud.google.com/compute/docs/instances/create-start-instance#creating_a_vm_from_a_custom_image

Also, Google says if you plan to create many instances from the same boot disk snapshot, consider creating a custom image and creating instances from that image instead. Custom images can create the boot disks for your instances more quickly and efficiently than snapshots.

`Create a snapshot of the compute engine instance disk, create a custom image from the snapshot, create instances from this image to handle the burst in traffic.` **is the right answer.**
To create an instance with a custom image, you must first have a custom image. You can create custom images from source disks, images, snapshots, or images stored in Cloud Storage. You can then use the custom image to create one or more instances as needed.
Ref: https://cloud.google.com/compute/docs/instances/create-start-instance#creating_a_vm_from_a_custom_image
Ref: https://cloud.google.com/compute/docs/images
These additional instances can be used to handle the burst in traffic.

Question 47:
Skipped
Your team creates/updates the infrastructure for all production requirements. You need to implement a new change to the current infrastructure and want to preview the update to the rest of your team before committing the changes. You want to follow Google-recommended practices. What should you?

- ○

  Clone the production environment to create a staging environment and deploy the proposed changes to the staging environment. Execute gcloud compute instances list to view the changes and store the results in a Google Cloud Storage bucket.

- ○

Preview the updates using Deployment Manager and store the results in a Google Cloud Storage bucket.

(Correct)

- ○

  Clone the production environment to create a staging environment and deploy the proposed changes to the staging environment. Execute gcloud compute instances list to view the changes and store the results in a Google Cloud Source Repository.

- ○

  Preview the updates using Deployment Manager and store the results in a Google Cloud Source Repository.

Explanation

`Clone the production environment to create a staging environment and deploy the proposed changes to the staging environment. Execute gcloud compute instances list to view the changes and store the results in a Google Cloud Storage bucket.` **is not right.**

gcloud compute instances list - lists Google Compute Engine instances. The infrastructure changes may include much more than compute engine instances, e.g. firewall rules, VPC, subnets, databases etc. The output of this command is not sufficient to describe the proposed changes. Moreover, you want to share the proposed changes, not the changes after applying them.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

`Clone the production environment to create a staging environment and deploy the proposed changes to the staging environment. Execute gcloud compute instances list to view the changes and store the results in a Google Cloud Source Repository.` **is not right.**

gcloud compute instances list - lists Google Compute Engine instances. The infrastructure changes may include much more than compute engine instances, e.g. firewall rules, VPC, subnets, databases etc. The output of this command is not sufficient to describe the proposed changes. Moreover, you want to share the proposed changes, not the changes after applying them.
Ref: https://cloud.google.com/sdk/gcloud/reference/compute/instances/list

`Preview the updates using Deployment Manager and store the results in a Google Cloud Source Repository.` **is not right.**

With deployment manager, you can preview the update you want to make before committing any changes, with the gcloud command-line tool or the API. The Deployment Manager service previews the configuration by expanding the full

configuration and creating "shell" resources. Deployment Manager does not instantiate any actual resources when you preview a configuration, allowing you to see the deployment before committing to it.
Ref: https://cloud.google.com/deployment-manager However, saving the proposed changes to Cloud Source Repositories is not a great idea. Cloud source repositories is a private Git repository in GCP and is not a suitable place for such content.
Ref: https://cloud.google.com/source-repositories

`Preview the updates using Deployment Manager and store the results in a Google Cloud Storage bucket.` **is the right answer.**
With deployment manager, you can preview the update you want to make before committing any changes, with the gcloud command-line tool or the API. The Deployment Manager service previews the configuration by expanding the full configuration and creating "shell" resources. Deployment Manager does not instantiate any actual resources when you preview a configuration, allowing you to see the deployment before committing to it.
Ref: https://cloud.google.com/deployment-manager
Cloud Storage bucket is an ideal place to upload the information and share it with the rest of the team.

Question 48:
Skipped
Your company is building a mobile application that enables users to upload and share images with their friends. Your company places a high value on security, prefers minimal maintenance (no-op), and wants to optimize costs where possible. You are designing the backend for the app based on these requirements: - Enable users to upload images for only 30 minutes, - Enable users to retrieve their images and share their images with their friends, - Delete images older than 50 days. You have very little time to design the solution and take it to production. What should you do (Choose two)?

- □

  Enable lifecycle policy on the bucket to delete objects older than 50 days.

  (Correct)

- □

  Have the mobile application use signed URLs to enabled time-limited upload to Cloud Storage.

  (Correct)

- □

Write a cron script that checks for objects older than 50 days and deletes them.

- □

Have the mobile application send the images to an SFTP server.

- □

Use Cloud Scheduler to trigger a Cloud Function to check for objects older than 50 days and delete them.

Explanation

`Have the mobile application send the images to an SFTP server.` **is not right.**
It is possible to set up an SFTP server so that your suppliers can upload files but building an SFTP solution is not something you would do when the development cycle is short. It would help if you instead looked for off the shelf solutions that work with minimal configuration. Moreover, this option doesn't specify where the uploaded files are stored. Nor does it talk about how the files are secured and how the expiration is handled.

`Use Cloud Scheduler to trigger a Cloud Function to check for objects older than 50 days and delete them.` **is not right.**
Sure can be done, but this is unnecessary when GCP already provides lifecycle management for the same. You are unnecessarily adding cost and complexity by doing this using Cloud functions.

`Write a cron script that checks for objects older than 50 days and deletes them.` **is not right.**
Like above, sure can be done but this is unnecessary when GCP already provides lifecycle management for the same. You are unnecessarily adding cost and complexity by doing it this way.

`Have the mobile application use signed URLs to enabled time-limited upload to Cloud Storage.` **is the right answer.**
When we generate a signed URL, we can specify an expiry (30 mins), and users can only upload for the specified time "30 minutes". Also, only users with the signed URL can view/download the objects so we share individual signed URLs so that "suppliers can access only their data". Finally, all objects in Google Cloud Storage are encrypted, which takes care of one of the primary goal "data security".
Ref: https://cloud.google.com/storage/docs/access-control/signed-urls

`Enable lifecycle policy on the bucket to delete objects older than 50 days.` **is the right answer.**
Since you don't need data older than 50 days, deleting such data is the right approach. You can set a lifecycle policy to delete objects older than 50 days. The

policy is valid on current as well as future objects and doesn't need any human intervention. This option also takes care of the other primary goal "expiration of aged data" and ensures that we "Delete data that is over 50 days old.".
Ref: https://cloud.google.com/storage/docs/lifecycle

Question 49:

Skipped

You want to deploy a business-critical application on a fleet of compute engine instances behind an autoscaled Managed Instances Group (MIG). You created an instance template, configured a MIG to use the instance template and set up the scaling policies, however, the creation of compute engine VM instance fails. How should you debug this issue?

- ○

  1. Ensure you don’t have any persistent disks with the same name as the VM instance.

  2. Ensure the disk autodelete property is turned on (disks.autoDelete set to true).

  3. Ensure instance template syntax is valid.

  (Correct)

- ○

  1. Ensure instance template syntax is valid.

  2. Ensure the instance template, instance and the persistent disk names do not conflict.

- ○

  1. Ensure the instance template, instance and the persistent disk names do not conflict.

  2. Ensure the disk autodelete property is turned on (disks.autoDelete set to true).

- ○

  1. Ensure you don’t have any persistent disks with the same name as the VM instance.

  2. Ensure instance template syntax is valid.

Explanation

`1. Ensure you don’t have any persistent disks with the same name as the VM instance.`
`2. Ensure the disk autodelete property is turned on (disks.autoDelete set to true).`
`3. Ensure instance template syntax is valid.` **is the right answer.**

As described in this article, "My managed instance group keeps failing to create a VM. What's going on?"
https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances#troubleshooting
The likely causes are

- A persistent disk already exists with the same name as VM Instance

- disks.autoDelete option is set to false

- instance template might be invalid

Therefore, **we need to ensure that the instance template is valid, disks.autoDelete is turned on, and that there are no existing persistent disks with the same name as VM instance.**

Question 50:

Skipped

A finance analyst at your company is suspended pending an investigation into alleged financial misconduct. However, their Gsuite account was not disabled immediately. Your compliance team has asked you to find out if the suspended employee has accessed any audit logs or BigQuery datasets after their suspension. What should you do?

- ○

  Search for users’ Cloud Identity username (email address) as the principal in system event logs in Cloud Logging.

- ○

  Search for users’ service account as the principal in data access logs in Cloud Logging.

- ○

  Search for users’ Cloud Identity username (email address) as the principal in data access logs in Cloud Logging.

  (Correct)

- ○

Search for users’ service account as the principal in admin activity logs in Cloud Logging.

Explanation

`Search for users’ service account as the principal in admin activity logs in Cloud Logging.` **is not right.**

Admin Activity logs do not contain log entries for reading resource data. Admin Activity audit logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources.
Ref: https://cloud.google.com/logging/docs/audit#admin-activity

`Search for users’ Cloud Identity username (email address) as the principal in system event logs in Cloud Logging.` **is not right.**

System Event audit logs do not contain log entries for reading resource data. System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. Google systems generate system Event audit logs; they are not driven by direct user action.
Ref: https://cloud.google.com/logging/docs/audit#system-event

`Search for users’ service account as the principal in data access logs in Cloud Logging.` **is not right.**

System Event audit logs do not contain log entries for reading resource data. System Event audit logs contain log entries for Google Cloud administrative actions that modify the configuration of resources. Google systems generate system Event audit logs; they are not driven by direct user action.
Ref: https://cloud.google.com/logging/docs/audit#system-event

`Search for users’ Cloud Identity username (email address) as the principal in data access logs in Cloud Logging.` **is the right answer.**

Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data.
Ref: https://cloud.google.com/logging/docs/audit#data-access