Aldovelio Castremonte's 1000 Practice Questions to Master the GCP Google Cloud Certified Associate Cloud Engineer Exam

Aldovelio Castremonte's 1000 Practice Questions to Master the GCP Google Cloud Certified Associate Cloud Engineer Exam

Aldovelio Castremonte

2024-05-01

Preface

It is with immense pleasure that I introduce to you, my latest work titled "Aldovelio Castremonte's 1000 Practice Questions to Master the GCP Google Cloud Certified Associate Cloud Engineer Exam." Over the past few years, the world has shifted its focus towards cloud computing, and among the industry leaders is Google Cloud Platform (GCP). GCP has brought cutting-edge innovation to a plethora of organizations and individuals, helping them streamline their processes and optimize their digital storage requirements. As the demand for GCP services increases, so does the need for qualified professionals who possess the necessary skills and knowledge to use GCP effectively and efficiently. This book is designed as a comprehensive study guide for those who aspire to ace the Google Cloud Certified Associate Cloud Engineer Exam.

The GCP Google Cloud Certified Associate Cloud Engineer exam has been an essential yardstick to assess one's proficiency in cloud technology and specifically Google Cloud Platform. This professional certification, once acquired, is the hallmark for an individual's competence in using Google Cloud Platform to its maximum potential. With ever-changing requirements and new features being added, keeping up to date with GCP advancements becomes essential for any aspiring cloud engineer.

In authoring this book, my team and I have carefully analyzed the exam objectives and formulated questions that closely represent the problems and scenarios faced during the exam. These 1000 practice questions ensure that you are well equipped with the requisite knowledge to tackle any kind of question that comes your way during the certification examination. As you proceed through this book, you will develop a clear understanding of the intricate aspects of the GCP ecosystem, which will make you a valuable asset in your professional endeavors.

The book is structured into several sections, each covering different domains of the GCP Google Cloud Certified Associate Cloud Engineer exam. These sections are further divided into chapters containing questions that span various sub-domains, in line with the exam blueprint. To maximize your learning, we recommend solving these questions in the order they have been presented. This way, your learning progresses naturally, and you can gradually build upon the knowledge you have acquired. Moreover, we have included detailed explanations for every question, which not only validate the correct choice but also provide valuable insight into the concepts that underlie the question.

Moreover, at the end of each section, you will find a set of reinforcing exercises designed to reinforce the knowledge you have gained so far. We encourage you to study the concepts diligently, practice the exercises rigorously, and review the explanations carefully to gain a holistic understanding of GCP. Also, do not hesitate to revisit questions and explanations to solidify your understanding of the concepts covered in the book.

This learning journey will not be without challenges, but I am confident that with dedication and commitment, you will overcome these hurdles and emerge victoriously. While we have made every effort to ensure the accuracy of the content, it is essential to keep an eye on the official GCP documentation and exam updates, as they might influence the exam requirements over time. However, this book remains a reliable resource for developing a strong foundation of essential GCP concepts and good practice for the exam.

In closing, allow me to wish you great success, not just in your pursuit of the GCP Google Cloud Certified Associate Cloud Engineer certification, but also in your future professional endeavors. I firmly believe that this book will become your trusted companion on your journey to mastering the GCP Google Cloud Certified Associate Cloud Engineer exam.

Aldovelio Castremonte

Practice Exam 1

Question 1: As a software engineer at a leading tech company, you are tasked with updating a web application that has been running successfully on Cloud Run for Anthos. You want to test the new version with a specific percentage of your production users through a canary deployment. What should you do?

A. Create a new version of the application in a separate Google Cloud Project and use VPC peering to route traffic between the two projects.

B. Create a new service with the new version of the application. Split traffic between this version and the version that is currently running.

C. Create a new Cloud Function with the new version of the application. Use Cloud Pub/Sub to split traffic between the two versions.

D. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

Question 2: As an IT manager in a large corporation, you've recently developed a comprehensive organizational structure on Google Cloud consisting of numerous folders and projects. To maintain security, you want to limit access to view this hierarchical structure to only a few team members. What approach should you take to assign minimum permissions to these members while adhering to Google's best practices?

A. Add the users to roles/storage.admin role.

B. Add the users to a group, and add this group to roles/browser.

C. Add the users to a group, and add this group to roles/bigquery.dataViewer.

D. Add the users to a group, and add this group to roles/iam.roleViewer role.

Question 3: As a software engineer at a tech company, you have been assigned the task of ensuring that the support team is automatically notified if users experience high latency for at least 5 minutes in your company's web application running on Compute Engine. You need to implement a solution recommended by Google without incurring any development cost. What should you do?

A. Use Cloud Profiler to monitor the latency of your web application and send notifications when the threshold is exceeded.

B. Configure a custom logging solution in Compute Engine instances to monitor high latency and send notifications.

C. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

D. Enable VPC Flow Logs and analyze traffic patterns to detect high latency issues.

Question 4: As a developer working for a software company specializing in the finance industry, you are running Linux workloads on Compute Engine instances. Your company is planning to collaborate with a new operations partner that does not have Google Accounts. In order to maintain the installed tools on these instances, you need to grant the operations partner access. How should you proceed?

A. Configure Compute Engine instances to use an external metadata server and grant the operations partner access to that server.

B. Ask the operations partner to generate SSH key pairs, and add the public keys to the VM instances.

C. Enable Cloud NAT and grant the operations partner access to the Cloud NAT gateway to allow traffic redirection.

D. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

Question 5: As a financial analyst working in the tech industry, your company manages multiple projects linked to a single billing account in Google Cloud. You are required to create visualizations that display the costs with customized metrics calculated based on your company's specific requirements. You also need to ensure that the process is automated. What approach should you take to achieve this?

A. Configure Cloud Billing export to Firestore, and use Google Charts to create custom visualizations based on the exported data.

B. In the Google Cloud console, use the export functionality of the Cost table. Create a Looker Studio dashboard on top of the CSV export.

C. Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery export.

D. Utilize Google Data Studio to directly connect to the Cloud Billing reports and create custom visualizations.

Question 6: As a software engineer at a data analytics company, you are tasked with setting up permissions for a group of Compute Engine instances to enable them to write data into a specific Cloud Storage bucket, while adhering to Google-recommended practices. What is the most appropriate action to take?

A. Create a service account and add it to the IAM role 'compute.admin' for that bucket.

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

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

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

Question 7: At your tech company, the finance department needs access to view billing reports for various projects, but you want to avoid granting them unnecessary permissions. What action should you take?

A. Add the group for the finance team to roles/pubsub admin role.

B. Add the group for the finance team to roles/storage admin role.

C. Add the group for the finance team to roles/billing viewer role.

D. Add the group for the finance team to roles/appengine admin role.

Question 8: As a cloud specialist in a financial services company, you are tasked with assisting an external auditor who is interested in reviewing who accessed the data in your organization's Google Cloud Storage buckets. How can you help the auditor obtain the necessary information?

A. Use the export logs API to provide the Admin Activity Audit Logs in the format they want.

B. Use Cloud Dataflow to process and analyze the data access logs in real-time.

C. Assign the appropriate permissions, and then create a Data Studio report on Admin Activity Audit Logs.

D. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

Question 9: Working in a tech company, your sales team has a project called Sales Data Digest with the ID acme-data-digest, which involves Google Cloud resources. You have been tasked with setting up similar resources for the marketing team, but you need to ensure that their resources are organized independently from the sales team. What should you do?

A. Use Shared VPC to connect the Marketing team resources to acme-data-digest.

B. Create a separate organization for the Marketing team and migrate the acme-data-digest project there.

C. Create a billing account for the Marketing team and link it to the acme-data-digest project.

D. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

Question 10: You're working as a network engineer for a company that relies heavily on Cloud services. You need to configure Cloud DNS for the company's domain to ensure that home.mydomain.com, mydomain.com, and www.mydomain.com all point to the IP address of your Google Cloud load balancer. How should you proceed?

A. Create one CNAME record to point mydomain.com to the load balancer, and create two A records to point WWW and HOME to mydomain.com respectively.

B. Create one CNAME record to point mydomain.com to the load balancer, and create two AAAA records to point WWW and HOME to mydomain.com respectively.

C. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively. Most Voted

D. Create one A record to point mydomain.com to the load balancer, and create two NS records to point WWW and HOME to mydomain.com respectively.

Question 11: As an engineer in a software development company, you are tasked with utilizing Deployment Manager to create a Google Kubernetes Engine cluster. Furthermore, within the same Deployment Manager deployment, you need to create a DaemonSet in the kube-system namespace of the cluster, while ensuring the solution requires the least number of services. What approach should you take?

A. Use Anthos Config Management to create a config that sets up the DaemonSet in the kube-system namespace, and reference this config in the Deployment Manager template.

B. Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

C. Use the Deployment Manager to create a Cloud Run service that deploys the DaemonSet to the kube-system namespace when triggered by an HTTP request.

D. In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value.

Question 12: You are working in a global tech company that is developing a mobile app to connect users worldwide. As part of the development team, your task is to create a database solution to store relational data from millions of potential users. Your team leader emphasizes the importance of implementing a storage solution that can easily scale with user growth and requires minimal configuration changes. Which storage solution should you use?

A. Cloud Filestore

B. Firestore IN-dataSTORE-mode

C. Cloud Spanner

D. Cloud Storage

Question 13: You're working as a Cloud Architect at a software development company and are responsible for granting access to the Google Cloud Platform resources. You need to configure an SSH connection for the dev1 group members

to connect to a single Compute Engine instance within a specific project, without allowing them access to other resources. How should you proceed in this case?

A. Create a Kubernetes Engine Cluster and grant the dev1 group the container.developer role. Direct them to use the Cloud Shell to ssh to that instance.

B. Create a Cloud SQL instance and grant the dev1 group the cloudsql.client role. Direct them to use the Cloud Shell to ssh to that instance.

C. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.InstanceAdmin role. Direct them to use the Cloud Console to ssh to that instance.

D. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

Question 14: As a financial analyst at a tech company that manages multiple business units, you are responsible for tracking the costs of various resources created in several Google Cloud projects. Each project is linked to different billing accounts, and you wish to have a single visual representation of all costs incurred to evaluate future charges more effectively. Additionally, you want to include new cost data as quickly as possible. How can you achieve this goal?

A. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

B. Fill all resources in the Pricing Calculator to get an estimate of the monthly cost.

C. Use the Cloud Billing API to fetch the costs from each project and compile them into a single file for visualization in Excel.

D. Install Stackdriver Monitoring Agent on each resource and use Stackdriver Monitoring to visualize the costs.

Question 15: As a software engineer at an innovative tech company, you are tasked with deploying an application on Cloud Run to process messages from a Cloud Pub/Sub topic while following Google-recommended practices. What should be your approach?

A. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

B. 2. Use Cloud Scheduler to periodically trigger your Cloud Run application, which then reads and processes messages from the Pub/Sub topic.

C. 7. Use Cloud IoT Core to subscribe to the Cloud Pub/Sub topic and then configure it to push messages to your Cloud Run application using the REST API.

D. 3. Create an App Engine service that subscribes to the Cloud Pub/Sub topic and then HTTP requests to your Cloud Run application for each message.

Question 16: As a network administrator in a tech company, you need to confirm the IAM users and roles assigned within a GCP project called my-project for security purposes. How should you proceed?

A. Run gcloud projects describe my-project. Review the output section.

B. Use Cloud Audit Logs to review IAM activity for my-project.

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

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

Question 17: As a database administrator for a prominent financial company, you're tasked with implementing an archival solution using Cloud Storage to store critical information. In order to comply with regulatory requirements, the company's employees must access this data once every quarter. To optimize costs, which storage option should you choose?

A. Google Cloud Filestore

B. Datastore

C. Durable Reduced Availability Storage

D. Cold Storage

Question 18: You are working for a company in the healthcare industry that stores its medical images in an on-premises data room. The company wants to utilize Cloud Storage for archival storage of these images and is looking for an automated process to upload any new medical images to the Cloud Storage. How should you design and implement a solution for this requirement?

A. Create a Bigtable instance and store the medical images as rows, then use an export job to transfer the images to Cloud Storage.

B. Use Cloud Transfer Service to schedule a transfer from the on-premises storage to Cloud Storage.

C. Deploy an App Engine service to sync the medical images from the on-premises storage to Cloud Storage using Cloud Endpoints.

D. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

Question 19: As a software engineer at a multinational company, you are responsible for deploying a globally distributed application using Cloud Spanner for data storage. Before creating a Cloud Spanner instance, what is the first step you should take to prepare?

A. Enable the Cloud Spanner API.

B. Enable Cloud Storage API for the project.

C. Configure your Cloud Spanner instance to be multi-regional.

D. Create a new VPC network with subnetworks in all desired regions.

Question 20: As an IT manager at a software development company, you have been asked to establish application performance monitoring for Google Cloud projects A, B, and C with a single, unified view of CPU, memory, and disk usage. What should you do to achieve this efficiently?

A. Use Firebase Performance Monitoring to track metrics across the three projects.

B. Set up Google Kubernetes Engine for projects A, B, and C with a single dashboard.

C. Enable API and connect projects A, B, and C to Cloud SQL for monitoring purposes.

D. Enable API, create a workspace under project A, and then add projects B and C.

Question 21: As a DevOps engineer at a software development company, you are tasked with setting up a new Google Kubernetes Engine (GKE) cluster while ensuring it always runs on a supported and stable version of Kubernetes. What is the most appropriate step to take?

A. Enable the "Stackdriver Monitoring" for your GKE cluster.

B. Use "Windows Server" as a node image for your GKE cluster.

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

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

Question 22: You are working as a Cloud Administrator in a tech company, and your task is to find out when users were added to Cloud Spanner Identity Access Management (IAM) roles on your Google Cloud Platform (GCP) project. What should you do in the GCP Console to get this information?

A. Open the BigQuery console, and check audit logs for Cloud Spanner IAM roles.

B. Go to the Stackdriver Monitoring console and set up dashboards for Cloud Spanner IAM roles.

C. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

D. Go to the Cloud Functions console and create a function that monitors IAM roles in Cloud Spanner.

Question 23: As a cloud administrator for an e-commerce company, you've been tasked with managing the service accounts within a specific project, named proj-sa. Your responsibility is to use a service account from this project to take snapshots of VMs in another department's project called proj-vm. What should you do?

A. Use IAM Conditions to restrict the service account's access to proj-vm only.

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

C. Use gcloud command to copy the service account from proj-sa project to proj-vm project.

D. Grant the service account the IAM Role of Project Viewer in the project called proj-vm.

Question 24: As an IT specialist at a software development company, you are assigned to implement a continuous integration and delivery (CI/CD) pipeline on Compute Engine instances to streamline the deployment process. The pipeline should be responsible for managing the entire cloud infrastructure through code while adhering to security best practices. What strategy should you employ to ensure that the pipeline has the appropriate permissions without compromising security?

A. • Create multiple service accounts, one for each pipeline with the appropriate minimal Identity and Access Management (IAM) permissions. • Use a secret manager service to store the key files of the service accounts. • Allow the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline.

B. • Add a step for human approval to the CI/CD pipeline before the execution of the infrastructure provisioning. • Use the human approvals IAM account for the provisioning.

C. Create individual user accounts for each pipeline and use them for respective infrastructure provisioning.

D. Use Compute Engine default service account for provisioning resources.

Question 25: As a software engineer in a retail company, you have been tasked with migrating an on-premises e-commerce application to a serverless Google Cloud solution. The current application has multiple Python microservices, each running on Docker containers with configurations being managed through environment variables. How should you deploy the existing application to Google Cloud while ensuring a seamless transition?

A. Migrate the code to App Engine Flexible Environment and deploy each microservice as separate services. Update the configurations and the required endpoints.

B. Use the existing CI/CD pipeline. Use the generated Docker images and deploy them to Compute Engine instances. Use the same configuration as on-premises.

C. Use the existing codebase and deploy each service as a separate Cloud Function. Update the configurations and the required endpoints.

D. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

Question 26: As a software developer working in a tech company, you are tasked with streamlining the process of generating and managing numerous Google Cloud resources utilizing Infrastructure as Code. The goal is to reduce the redundant code required to maintain the environment. What approach should you adopt?

A. Develop templates for the environment using Cloud Deployment Manager.

B. Create a bash script that contains all requirement steps as gcloud commands.

C. Use Google Cloud Pub/Sub to implement message-based asynchronous resource management.

D. Manually use the gcloud command-line tool to manage all resources interactively.

Question 27: As a data engineer in a tech company, you manage a Dataproc cluster that runs within a single Virtual Private Cloud (VPC) network in a single subnetwork with range 172.16.20.128/25. There are no private IP addresses left in the subnetwork. Your task is to add new virtual machines to communicate with the cluster using the least number of steps. What should you do?

A. Create a new subnetwork in the existing VPC with a range of 172.16.20.192/26 and configure the VMs to use that subnetwork.

B. Configure a VPN between the existing VPC network and a new VPC network for the VMs. Create a new subnetwork in the new VPC network and configure the VMs to use that subnetwork.

C. Modify the existing subnet range to 172.16.20.0/24.

D. Create a new VPC network for the VMs with a subnet of 172.16.20.0/25. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

Question 28: As a software architect at a rapidly growing tech company, you are responsible for managing a Google Kubernetes Engine (GKE) cluster that allows various teams within the company to run non-production workloads. The Machine Learning (ML) team requires access to Nvidia Tesla P100 GPUs for training their models more efficiently. To ensure minimal effort and cost, what should be your course of action?

A. Ask your ML team to add the accelerator: gpu annotation to their pod specification.

B. Manually install Nvidia Tesla P100 GPUs on the cluster's nodes for your ML team.

C. Enable GPUs on the existing nodes, but don't create a dedicated node pool.

D. Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

Question 29: You are working as a DevOps engineer in a software development company, and you have developed an application that is packaged into a Docker image. Now, your task is to deploy the Docker image as a workload on Google Kubernetes Engine. What steps should you follow to achieve this?

A. Upload the image to Cloud Storage and create a Kubernetes Service referencing the image.

B. Upload the image to Artifact Registry and create a Kubernetes Service referencing the image.

C. Upload the image to Cloud Storage and create a Kubernetes DaemonSet referencing the image.

D. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image.

Question 30: As a data analyst in a tech company, you have to execute a crucial query in BigQuery, which will likely return a large number of records. To determine the cost of running the query using on-demand pricing, which step should you take?

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

B. Run the query in multiple parts and pay for each part separately.

C. Use the BigQuery UI to estimate the cost without actually running the query.

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

Question 31: As a cloud architect in a leading software company, you have made significant modifications to a complex Deployment Manager template. You want to ensure that all dependencies of the resources defined in the template are met before committing it to the main project. For the quickest feedback on your changes, what approach should you take?

A. Leverage a custom Cloud Function to validate the Deployment Manager template's resource dependencies before executing it.

B. Simulate the Deployment Manager template changes in the Cloud Shell before applying it to the project.

C. Execute the Deployment Manager template against a separate project with the same configuration, and monitor for failures.

D. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

Question 32: As an IT specialist at a software company, you are responsible for managing a virtual machine that is currently configured with 2 vCPUs and 4 GB of memory. The VM is experiencing memory shortage issues, and your manager requests an upgrade to 8 GB of memory. What is the appropriate course of action to achieve this?

A. Stop the VM, increase the memory to 8 GB, and start the VM.

B. Use Cloud Functions to handle memory intensive tasks.

C. Use Cloud Storage Bucket to store the excess data and offload memory usage.

D. Upgrade the Cloud SDK to allow for increased memory usage.

Question 33: As an IT manager at a software development company, you need to set a budget alert for the use of Compute Engineer services in one of the three Google Cloud Platform projects that you manage, which are all linked to a single billing account. What should you do?

A. Verify that you are the project billing administrator. Select the associated billing account and create a budget and a custom alert.

B. Verify that you have owner role at the organization level. Select the associated billing account and create a budget and alert for the appropriate project.

C. Verify that you are the project billing administrator. Select the associated billing account and create a budget for Compute Engine only.

D. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

Question 34: You are working as a DevOps engineer at a software company and have recently deployed a new application in your Google Kubernetes Engine cluster using a specific YAML file. Upon inspecting the status of the deployed pods, you notice that one of them is still in PENDING status. To determine the reason behind the pod's pending status, what should you do?

A. View logs of the myapp-deployment Deployment object and check for warning messages.

B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

C. Review details of the myapp-service Service object and check for error messages.

D. View logs of the container in myapp-deployment-58ddbbb995-lp86m pod and check for error messages.

Question 35: You are working as a developer at a tech company, and you have completed a development project where you defined the appropriate IAM roles. Now, you are creating a new production project and want to replicate the same IAM roles from the previous project, using the fewest possible steps. What should you do?

A. Use gcloud projects update command to merge both projects and migrate IAM roles.

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

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

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

Question 36: You are working at a software development company that recently developed a highly important application that requires deployment on Kubernetes. This application is vital for your business operations, and it's essential to ensure the utmost reliability. To set up a Kubernetes cluster, you plan to adhere to Google's recommended practices. What steps should you take?

A. Create a GKE standard cluster with no availability preference. Enroll the cluster in the rapid release channel.

B. Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

C. Create a GKE standard cluster with no availability preference. Enroll the cluster in the stable release channel.

D. Create a zonal GKE standard cluster. Enroll the cluster in the stable release channel.

Question 37: As a software engineer at a tech company, you've recently developed an application that is packaged into a Docker image. To deploy this Docker image as a workload on Google Kubernetes Engine within the company's infrastructure, what is the appropriate course of action to take?

A. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

B. Upload the image to BigQuery and create a Kubernetes Deployment referencing the image.

C. Upload the image to Firestore and create a Kubernetes Deployment referencing the image.

D. Upload the image to Cloud Storage and create a Kubernetes Service referencing the image.

Question 38: You work at a software development company that relies on G Suite for communication and collaboration among team members. All employees have a G Suite account. You now need to provide certain G Suite users with access to your company's Cloud Platform project. What course of action should you take?

A. Create a new GCP project for each G Suite user and share the resources individually.

B. Use the Cloud SDK to create a new user role and assign it to each G Suite user's email address.

C. In the GCP Console, create an Organization Policy restricting access to specific G Suite users by listing their email addresses.

D. Grant them the required IAM roles using their G Suite email address.

Question 39: You are working as a cloud engineer for a company that has a web application deployed on Cloud Run with several hundred users. Some users have reported that the initial web page takes significantly longer to load compared to subsequent pages. In order to address this issue while adhering to Google's recommendations, what action should you take?

A. Change the Cloud Run memory allocation to a larger value.

B. Set the concurrency number to 1 for your Cloud Run service.

C. Decrease the request timeout for your Cloud Run service.

D. Set the minimum number of instances for your Cloud Run service to 3.

Question 40: In your company's marketing department, you're tasked with deploying a specific content management system (CMS) solution to Google Cloud for your team. You need a quick and simple way to install it. What should you do?

A. Manually install the CMS on a new App Engine standard environment instance.

B. Deploy the CMS solution using Kubernetes Engine and manually configure the solution using the YAML files.

C. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

D. Use Datastore to store the CMS files and deploy the solution using a custom Cloud Function.

Question 41: As a system administrator in a technology company, you need to set up 10 Compute Engine instances to ensure high availability during mainte-

nance periods and automatically restart if they crash. How should you proceed with this configuration?

A. Create an instance group for the instances. Set the 'Autohealing' health check to healthy (HTTP).

B. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

C. Create a Google Kubernetes Engine cluster and deploy the instances using Kubernetes Deployments, ensuring automatic restart and high availability during system maintenance.

D. Create an instance group for the instance. Verify that the 'Advanced creation options' setting for 'do not retry machine creation' is set to off.

Question 42: You are working for a company in the financial industry that has a vast amount of unstructured data in various file formats. You need to conduct ETL transformations on this data and make it available on Google Cloud for further processing by a Dataflow job. Which method should you use to accomplish this task?

A. Upload the data to Cloud Storage using the gsutil command line tool.

B. Upload the data to Cloud Bigtable using the cbt command line tool.

C. Upload the data to Cloud Firestore using the Firestore module in the Google Cloud Client Libraries.

D. Upload data to Google Drive using the Google Drive API.

Question 43: As a cloud architect working at a fast-growing company, you have decided to utilize Google Kubernetes Engine to deploy a new application with autoscaling enabled. You aim to make this application accessible to the public using HTTPS on a public IP address. What is the recommended method to achieve this?

A. Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluster. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing.

B. Create a Kubernetes Service of type NodePort for your application, then use a Google Cloud Armor policy to expose it with a public IP address.

C. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

D. Create a HAProxy pod in the cluster to load-balance the traffic to all the pods of the application. Forward the public traffic to HAProxy with an iptable rule. Configure the DNS name of your application using the public IP of the node HAProxy is running on.

Question 44: As an IT professional working in a software development company, you have been assigned to optimize costs while deploying an application on Google Kubernetes Engine. The application has critical components that require constant availability, while other parts are non-critical and can afford downtime. How should you configure the Google Kubernetes Engine cluster to achieve the desired balance?

A. Create a cluster with a single node-pool by using Balanced Persistent Disks. Label the critical Deployments as disk_balanced_false.

B. Create a cluster with a single node-pool by using Preemptible VMs. Label the fault-tolerant Deployments as preemptible_true.

C. Create a cluster with both a Spot VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Spot VM node pool.

D. Create a cluster with both a Shielded VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Shielded VM node pool.

Question 45: You are working as an IT administrator at a company that is transitioning to Google Cloud Identity. Some of your colleagues have existing personal Google accounts, and you'd like to add them to the system without causing any conflicting accounts. What is the recommended approach to achieve this?

A. Tell the user to share their existing account credentials with the GCP admin to resolve the conflict.

B. Tell the user to remove all personal email from the existing account.

C. Create a new Google account for each user.

D. Invite the user to transfer their existing account.

Question 46: You are working as an application administrator in a software company and, after analyzing user feedback, discover that there's a sharp increase in a specific error. Upon investigation, you find out that the error is caused by a Service Account having insufficient permissions. You manage to fix the issue, but you want to be alerted if this problem arises again in the future. What action should you take in this situation?

A. Disable and enable the Service Account to reset permissions.

B. Implement a use of Dead-letter topic in Pub/Sub to handle errors.

C. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

D. Export logs to Cloud Storage and analyze them using Dataflow.

Question 47: As a software engineer at a fast-growing company, you have been tasked with migrating the firm's current on-premises workloads to Google Cloud to reduce operational costs. The existing workloads include a Flask web application, a backend API, and a scheduled, long-running background job for ETL and reporting. Which serverless solutions on Google Cloud should you adopt in accordance with Google-recommended practices for each workload component?

A. Run the web application on a Cloud Storage bucket and the backend API on Cloud Functions. Use Cloud Tasks to run your background job on Kubernetes Engine.

B. Migrate the web application to Kubernetes Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

C. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Compute Engine.

D. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

Question 48: You are working as a project lead in a renowned software company that ventured into the cloud computing industry 6 months ago. As your company acquires more clients and handles larger projects, your reliance on Google Cloud services is on the rise. You want to streamline the process of allowing all engineers to create new projects without requiring their credit card information. What is the most appropriate solution?

A. Create an organization-wide Google Cloud Platform free trial account for all engineers to use.

B. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

C. Request Google Cloud to provide a corporate credit card for the entire engineering team.

D. Create separate billing accounts for each engineer and associate their individual credit cards.

Question 49: As an IT manager in a leading tech company, you have a crucial Compute Engine workload. To ensure the data on the workload's boot disk is regularly backed up, you need a fast disaster recovery solution and want older backups to be automatically removed to minimize costs. Following Google-recommended practices, what should you do?

A. Configure a Data Transfer Service job to save disk data to BigQuery periodically.

B. Create a cron job to create a new disk from the disk using gcloud.

C. Create a snapshot schedule for the disk using the desired interval.

D. Create a Managed Instance Group using the existing instance as a template.

Question 50: As a Data Analyst working in a company with multiple Google Cloud Platform (GCP) projects, you have been asked to gather and analyze logs from the past 60 days across all projects. To do this efficiently and in line with Google-recommended practices, how should you obtain the combined logs for all projects?

A. Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

B. Configure a Cloud Function to read from Stackdriver Logging and write the logs to Cloud Spanner. Set the retention policy to 60 days for the database.

C. Use gsutil to manually copy logs from Stackdriver Logging to BigQuery every day. Configure the table expiration to 60 days.

D. Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days.

Practice Exam 1 Solutions

Solution to Question 1: D

The correct answer is D, and here's why:

When updating a web application running on Cloud Run for Anthos, the best strategy to perform a canary deployment is to create a new revision with the new version of the application and then split the traffic between the two versions (the old version and the new revision). This approach allows you to gradually introduce the changes to your user base, test the stability and performance of the new version while keeping the old version active, and minimize any potential negative impact on the end users during the testing phase.

Now, let's analyze why the other options will not work:

Option A: Creating a new version of the application in a separate Google Cloud Project and using VPC peering to route traffic between the two projects introduces unnecessary complexity to the deployment process, and does not help to achieve the desired controlled rollout process that canary deployments are supposed to provide. Additionally, managing resources across two different projects can be challenging and can lead to higher operational costs and difficulties in managing access controls.

Option B: Creating a new service with the new version of the application does offer traffic splitting, but it also requires managing two separate services which adds unnecessary overhead and can lead to confusion. By creating a new revision within the existing service, you can take advantage of the built-in traffic splitting functionality of Cloud Run in a more efficient and streamlined manner.

Option C: Creating a new Cloud Function with the new version of the application and using Cloud Pub/Sub to split traffic between the two versions is not a suitable solution in this context because we are discussing a web application running on Cloud Run for Anthos, not a Cloud Function. Mixing two different deployment platforms like Cloud Functions and Cloud Run would add significant complexity and potential points of failure, making it less suitable for a simple canary test.

Solution to Question 2: B

The correct answer is B: Add the users to a group, and add this group to roles/browser.

Explanation: The roles/browser role, or Browser role, is designed specifically for providing the minimum necessary permissions to allow users to browse and view the metadata of resources within the hierarchical structure of Google Cloud. This role grants users read-only access to see an organization's Google Cloud resource hierarchy, including folders and projects, without granting access to the data or allowing any modification to the resources.

Here's why the other options are not suitable for the given scenario:

A. Adding the users to roles/storage.admin role would be inappropriate as this role provides admin access to Cloud Storage resources which are beyond the required permission level to view an organization's hierarchical structure.

C. Adding the users to a group and adding this group to roles/bigquery.dataViewer is unnecessary for this situation as this role grants users access to view datasets and tables in BigQuery. This role does not provide the ability to view the overall hierarchical structure of Google Cloud resources.

D. Adding the users to a group and adding this group to roles/iam.roleViewer role is insufficient since this role gives users permission to view the available predefined Identity and Access Management (IAM) roles within the organization but not the Google Cloud resource hierarchy itself.

In conclusion, based on the given scenario, the best approach to maintaining security and assigning minimum permissions is to add the users to a group and add this group to roles/browser, which is designed to provide the required level of access.

Solution to Question 3: C

The correct answer is C: Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

Explanation:

Option A is not correct because Cloud Profiler is used for analyzing and optimizing application performance, not for monitoring real-time user experience. It will not be able to provide immediate notifications to the support team in case of high latency.

Option B is not correct because configuring a custom logging solution in Compute Engine instances would require development effort, which goes against the requirement of not incurring any development cost. Additionally, this option would not be a recommended Google solution as it involves manual implementation.

Option C is the correct answer because creating an alert policy in Google Cloud Monitoring will allow you to configure the conditions that should trigger a notification based on specific metrics, such as HTTP response latency. This solution is recommended by Google, requires no additional development, and directly addresses the problem of notifying the support team when users experience high latency.

Option D is not correct because VPC Flow Logs are used to capture information about the traffic flowing within a VPC. They are typically more focused on network security and are not designed to monitor application latency. Analyzing traffic patterns with VPC Flow Logs would not be an efficient solution for detecting and notifying the support team of high latency issues in real-time.

Solution to Question 4: D

The correct answer is D. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

Explanation:

D is the correct answer because Identity-Aware Proxy (Cloud IAP) allows you to establish a secure connection to your Compute Engine instances without the need for the operations partner to have a Google account. By adding the operations partner as a Cloud IAP Tunnel User, they can access the instances securely using the IAP tunneling feature without causing any security concerns.

Option A is incorrect. Configuring Compute Engine instances to use an external metadata server does not directly grant the operations partner access to the instances; rather, it only allows them to access the metadata. Additionally, this method may involve substantial overhead and complexity for managing metadata access.

Option B is not ideal. Although adding the partner's public SSH keys to the VM instances will grant them access, it does not offer sufficient control, auditing, or security features that Cloud IAP provides to ensure long-term secure access. Moreover, the new partner's users would need Google Accounts to access the instances, which is not a feasible option in this scenario.

Option C is incorrect. Enabling Cloud NAT and granting access to the Cloud NAT gateway is unrelated to granting access to Compute Engine instances. Cloud NAT deals with providing outbound internet access and IP address translation for instances without external IPs, rather than secure access for third-party partners.

Therefore, the best option to grant the operations partner access to the Compute Engine instances without requiring Google Accounts is to enable Cloud IAP (Identity-Aware Proxy) and add them as a Cloud IAP Tunnel User.

Solution to Question 5: C

The correct answer is C. You should configure Cloud Billing data export to BigQuery for the billing account and create a Looker Studio dashboard on top of the BigQuery export. This approach allows you to create custom visualizations and calculations based on your company's specific requirements. BigQuery offers seamless integration with Google Cloud's billing data, and Looker Studio enables effortless data visualization and reporting on top of that data. This approach also lets you automate the process, as the billing data is continuously exported to BigQuery.

Option A is incorrect because Firestore is a NoSQL database designed for real-time data synchronization, making it less suitable for large-scale data analysis and visualization. Additionally, Google Charts is mainly used for rendering simple charts based on client-side data and is not as powerful as Looker Studio in creating advanced custom visualizations.

Option B is not appropriate because exporting data to a CSV file from the Cost table is a manual process, which does not allow you to automate the process effectively. Furthermore, using a CSV export is also less efficient as it doesn't benefit from the real-time scalability and advanced features of BigQuery.

Option D is incorrect because, while Google Data Studio is a powerful data visualization tool, it does not allow you to create custom calculations based on specific company metrics directly from Cloud Billing reports. With Data Studio, you will be limited to visualizing pre-defined metrics and dimensions without the flexibility to tailor them according to your company's needs. Using BigQuery and Looker Studio, as in Option C, provides more flexibility for custom calculations and reporting.

Solution to Question 6: C

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

Here's the explanation for why the answer should be C, and why other options will not work:

A. Creating a service account and adding it to the 'compute.admin' role for the bucket is not correct because 'compute.admin' is a Compute Engine role, and it provides extensive permissions to resources within the compute engine. However, it does not grant the necessary permissions for writing data into Cloud Storage buckets.

B. Creating a service account and adding it to the 'storage.legacyBucketReader' role is not correct because this role only allows the service account to read data from the bucket. It doesn't grant permission to write data, which is the requirement for this scenario.

C. Creating a service account and adding it to the 'storage.objectCreator' role for the bucket is the most appropriate action to take. This is because the 'storage.objectCreator' role grants permission for the service account to create new objects (i.e., write data) in the Cloud Storage bucket without providing access to edit or delete the existing objects. This follows Google-recommended practices of granting the least privilege necessary for a specific task.

D. Creating a service account with an access scope using the 'https://www.googleapis.com/auth/cloud-platform' is not recommended in this case. This access scope gives the service account broad permissions on all Google Cloud services, which is not necessary and may lead to potential security risks. Following the principle of least privilege, the service account should only have permission to write data in the specific Cloud Storage bucket, which is provided by option C.

Solution to Question 7: C

The correct answer is C: Add the group for the finance team to roles/billing viewer role.

Explanation: The finance department needs to view billing reports, which requires access to billing-related information. The billing viewer role provides the necessary permissions to view the cost, usage, and other billing details without granting them access to modify any data or configurations. This helps to maintain the principle of least privilege, where users are only given the minimum permissions necessary to perform their job responsibilities.

Option A: Adding the finance team to the pubsub admin role would provide unnecessary access to manage and configure Pub/Sub resources, which are irrelevant to their job responsibilities in reviewing billing information.

Option B: Granting the finance team the storage admin role would give them access to manage and control storage resources within the project, which goes beyond their need to view billing information.

Option D: Assigning the finance team the appengine admin role would provide them with broad administrative permissions on App Engine resources, which are not needed for their finance-related tasks.

In conclusion, the best approach is option C, as it provides the finance team with the necessary access to view billing reports while maintaining the principle of least privilege by not granting them unnecessary permissions.

Solution to Question 8: D

The correct answer is D. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

The reason why option D is the best choice is that Data Access Logs specifically capture access to user data, which is the information the auditor wants to review. By enabling Data Access Logs for the relevant Google Cloud Storage buckets, you will be able to collect the data access information required by the auditor. Furthermore, using the built-in log viewer to filter the logs based on Cloud Storage will make it easier for the auditor to review the data and find the information they need.

Option A is not the ideal solution because exporting Admin Activity Audit Logs may not provide granular enough data to show who specifically accessed the data in the cloud storage buckets. Admin Activity Audit Logs focus more on the administrative actions performed in the cloud environment, rather than data access events.

Option B, using Cloud Dataflow to process and analyze the data access logs in real-time, is not the best choice for this scenario. While Cloud Dataflow could enable real-time log analysis, it would require additional setup, development, and technical expertise to create the required data pipeline. Moreover, the auditor may not necessarily need real-time analysis of the data access logs, making this an over-complicated solution.

Option C, creating a Data Studio report on Admin Activity Audit Logs, is not the correct choice as it wouldn't provide specific information about who accessed

the data in the storage buckets, as mentioned earlier. Additionally, using Data Studio would require spending extra time and effort in creating and adjusting a report that may not meet the auditor's requirements.

Solution to Question 9: D

The correct answer is D: Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

Explanation: Creating another project for the marketing team with a different project ID, such as acme-marketing-data-digest, allows for independent and organized management of all the Marketing team's Google Cloud resources. This separation ensures better accountability and tracking of resources used by each team, leading to efficient resource allocation and budget management.

Now, let's discuss why the other options will not work in this scenario:

A. Use Shared VPC to connect the Marketing team resources to acme-data-digest: Shared VPC allows for sharing network resources like subnetworks across multiple projects. However, it does not provide a solution to organize the marketing team's resources independently of the sales team. The resources would still be tied to the acme-data-digest project, leading to a lack of separation between the two teams.

B. Create a separate organization for the Marketing team and migrate the acme-data-digest project there: This option would involve creating an entirely new organization for the marketing team, which is unnecessary and time-consuming. Additionally, migrating the acme-data-digest project to the new organization would result in both the Sales and Marketing teams sharing the same resources, which violates the requirement for independent organization and resource allocation.

C. Create a billing account for the Marketing team and link it to the acme-data-digest project: Creating a separate billing account for the marketing team would allow for better budget management. However, it would not address the problem of organizing the marketing team's resources independently from the sales team, as the resources would still be connected to the acme-data-digest project.

Solution to Question 10: C

The correct answer is C. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

Here's why the other options don't work:

Option A: Create one CNAME record to point mydomain.com to the load balancer, and create two A records to point WWW and HOME to mydomain.com respectively. This option is incorrect because you cannot create a CNAME record for the root domain (mydomain.com) to point the domain to the load

balancer as doing so would conflict with other mandatory DNS records such as NS and SOA records. The appropriate record type for mapping a domain to an IP address is an A record.

Option B: Create one CNAME record to point mydomain.com to the load balancer, and create two AAAA records to point WWW and HOME to mydomain.com respectively. This option is incorrect because AAAA records are used for IPv6 addresses, not IPv4 addresses. The question refers to an IPv4 address (as no specific type requirement was mentioned, IPv4 is the default assumption). Also, similar to option A, you cannot create a CNAME record for the root domain.

Option D: Create one A record to point mydomain.com to the load balancer, and create two NS records to point WWW and HOME to mydomain.com respectively. This option is incorrect because NS (Name Server) records are used to specify the authoritative DNS servers for a domain and are not meant to point subdomains to a specific IP address such as a load balancer. Instead, CNAME records should be used to map the subdomains WWW and HOME to mydomain.com, as indicated in the correct answer (Option C).

In summary, the correct answer (Option C) ensures that all three domains - mydomain.com, www.mydomain.com, and home.mydomain.com - point to the Google Cloud load balancer IP address by using an A record for the root domain and CNAME records for the subdomains.

Solution to Question 11: B

The correct approach to take in this scenario is option B: Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet. This is because Deployment Manager allows you to create custom type providers that interact directly with the Kubernetes API. By creating a new Type Provider, you can manage Kubernetes resources, such as a DaemonSet, within the same Deployment Manager deployment. This approach ensures that the solution requires the least number of services, unlike the other options offered.

Option A is not a suitable approach because Anthos Config Management is used for managing configurations across multiple Kubernetes clusters and is not integrated with Deployment Manager. In this case, you are asked to use Deployment Manager to create the cluster and DaemonSet within a single deployment.

Option C won't work effectively because it involves creating a Cloud Run service, which adds an additional layer of complexity and requires more services. Moreover, this method would necessitate an HTTP request to trigger the deployment of the DaemonSet to the kube-system namespace, which is not the most efficient approach.

Option D is not a recommended approach because adding metadata to the cluster's definition in Deployment Manager will not create a DaemonSet in the kube-system namespace. Metadata is only used to provide key-value pairs

that can be accessed by applications running on the cluster. It is not the appropriate method for defining Kubernetes resources in a Deployment Manager deployment.

In summary, option B is the most appropriate approach for creating a Google Kubernetes Engine cluster and DaemonSet in the kube-system namespace, using Deployment Manager, while minimizing the number of services required.

Solution to Question 12: C

The correct answer is C, Cloud Spanner, and here is an explanation for why each of the other options would not be the best choice:

A. Cloud Filestore: Cloud Filestore is a managed file storage service that is best suited for applications that require shared access to a file system, such as content management systems, file analytics, data processing pipelines, and media rendering. It would not be the ideal solution for a mobile app aimed at connecting users worldwide, as it might not scale optimally with user growth and it does not handle relational data as efficiently as a dedicated database storage solution.

B. Firestore IN-dataSTORE-mode: Firestore is a cloud-native NoSQL database and would work well for storing unstructured or semi-structured data. However, the question specifies that the storage solution must be designed to handle relational data, which means a SQL-like interface and transactional consistency are required. While Firestore IN-dataSTORE-mode supports some SQL-like features, it is designed for a specific data model and does not meet the requirements of handling large-scale relational data.

D. Cloud Storage: Cloud Storage is an object storage solution meant for storing large amounts of unstructured data like media content, backups, and log files. It is best utilized for providing access to objects via HTTP/HTTPS or serving as a storage backend for applications. Since our requirement is to store relational data for millions of users, Cloud Storage would not be the best solution for this task.

C. Cloud Spanner (correct answer): Cloud Spanner is a fully managed, globally distributed relational database service designed to scale horizontally with minimal configuration changes. It supports real-time transactions, which ensures consistency across all users' data. Additionally, Cloud Spanner allows for strong asset transaction guarantees across regions, making it the ideal choice for the storage solution in this mobile app scenario connecting users worldwide.

Solution to Question 13: D

The correct answer is D. You should set the metadata to enable-oslogin=true for the instance, grant the dev1 group the compute.osLogin role, and direct them to use the Cloud Shell to ssh to that instance.

Here's why each of the other options will not work:

Option A: Creating a Kubernetes Engine Cluster and granting the dev1 group the container.developer role is not relevant in this case. It is useful for managing Kubernetes resources, and it doesn't address this specific need– which is to connect to a Compute Engine instance using SSH.

Option B: Creating a Cloud SQL instance and granting the dev1 group the cloudsql.client role also doesn't address the requirement. The cloudsql.client role is for managing Cloud SQL instances, not for connecting to Compute Engine instances using SSH.

Option C: By setting the metadata enable-oslogin=true and granting the dev1 group the compute.InstanceAdmin role, you are giving them additional permissions beyond the needed SSH access. The compute.InstanceAdmin role provides broad permissions to manage instances, including starting, stopping, and deleting them, which is not necessary in this situation.

Option D meets the requirement by enabling OS Login and granting the dev1 group the correct role – compute.osLogin – providing them with the necessary access to connect to the instance using SSH without granting unnecessary permissions. The Cloud Shell allows group members to access the instance through an SSH connection in a browser-based terminal, making it an ideal choice.

Solution to Question 14: A

The correct answer is A: Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

Reasoning for A: Exporting billing data to BigQuery allows for storage, management, and analysis of your Google Cloud costs in one place. BigQuery is updated daily with new billing data (or near real-time with a separate configuration), ensuring that new cost data is promptly included in your analysis. Looker Studio provides a powerful visualization tool for BigQuery data, enabling you to easily explore, analyze, and visualize your Google Cloud costs across all your projects. This option fulfills the requirement of having a single visual representation alongside the quick inclusion of new cost data.

Reasons for not choosing other options:

B: The Pricing Calculator is a tool for estimating the costs of Google Cloud resources based on potential usage and configuration. It does not reflect the exact actual cost of resources being used in the organization's multiple business units across different billing accounts. Therefore, it cannot be used to evaluate real-time costs incurred for future charge consideration.

C: While the Cloud Billing API allows fetching the cost information from each project, it is less efficient and requires additional manual effort to compile the costs into a single file, such as an Excel spreadsheet. This option is not as seamless as exporting data to BigQuery and visualizing it in Looker Studio. Furthermore, the Cloud Billing API only provides daily cost data, which might not be granular enough for some workloads.

D: Stackdriver Monitoring Agent is primarily designed to collect metrics on resource utilization, such as CPU, memory, and disk usage. It does not have a direct relation to costs incurred by Google Cloud Resources. Stackdriver Monitoring cannot provide a single visual representation of the costs and might not update as quickly as needed for evaluating future charges.

Solution to Question 15: A

The correct answer is A, based on the following explanation:

A. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

This is the recommended approach:

1. A service account is required for proper security and authentication between Google Cloud components like Cloud Pub/Sub and Cloud Run.
2. Assigning the Cloud Run Invoker role to the service account ensures that the service account has the necessary permissions to invoke the Cloud Run application.
3. Creating a Cloud Pub/Sub subscription that uses the service account and your Cloud Run application as the push endpoint creates a secure link between the Pub/Sub topic and your Cloud Run application, allowing it to process incoming messages.

Now let's see why the other options won't work effectively:

B. Use Cloud Scheduler to periodically trigger your Cloud Run application, which then reads and processes messages from the Pub/Sub topic.

Cloud Scheduler is not recommended for this purpose because it will create unnecessary delays and overhead. It requires you to set a specific time interval to trigger the Cloud Run application, even if there are no messages in the Pub/Sub topic, and will not provide real-time processing of messages as they arrive.

C. Use Cloud IoT Core to subscribe to the Cloud Pub/Sub topic and then configure it to push messages to your Cloud Run application using the REST API.

Cloud IoT Core is primarily designed for device management and communication from IoT devices to Google Cloud Platform. It is not the recommended solution for processing Cloud Pub/Sub messages in a Cloud Run application, as it adds unnecessary complexity and is not designed for this purpose.

D. Create an App Engine service that subscribes to the Cloud Pub/Sub topic and then HTTP requests to your Cloud Run application for each message.

Using App Engine to subscribe to the Pub/Sub topic and send messages to your Cloud Run application adds an extra layer of complexity that is not needed. The

direct connection between Cloud Pub/Sub and Cloud Run in option A provides a simpler, more efficient, and recommended solution.

Solution to Question 16: D

The correct answer is D, as the question asks to confirm the IAM users and roles assigned within a GCP project called my-project for security purposes. The best way to achieve this is to navigate to the project and then to the IAM section in the GCP Console. After that, you can review the members and their assigned roles. This will provide a clear and up-to-date overview of the users and their permissions within your project.

Option A is not correct because running "gcloud projects describe my-project" does not provide information about IAM users and roles. It displays basic project information, such as the project name, project ID, and project number.

Option B is also incorrect because, although Cloud Audit Logs allows you to review various activities within a project, it does not display the current IAM assignments. It will only show you the changes and activities related to IAM, so you might need to search through various logs, which might be time-consuming and less efficient compared to directly viewing the IAM section in the GCP Console.

Finally, Option C is not a suitable choice as it focuses on the Roles section in the GCP Console. While this section does provide information about the roles, it does not show the members assigned to those roles. Thus, it does not offer complete information on IAM users' and roles' assignment within the project.

Solution to Question 17: D

The correct answer is D. Cold Storage.

Explanation:

D. Cold Storage

Cold Storage is designed for storing infrequently accessed data, which makes it an optimal solution in this scenario. Since the company's employees are required to access the data once every quarter, this meets the conditions for infrequent access. Additionally, Cold Storage offers lower costs compared to other storage classes, which helps optimize expenses for the company. Google Cloud Storage options such as Nearline, Coldline, and Archive storage classes fall under Cold Storage.

Other Options:

A. Google Cloud Filestore

Google Cloud Filestore is a fully managed, high-performance file storage service, optimized for applications that require low latency and a shared file system. Although it provides easy access to data, it is not the most cost-effective solution

for rarely accessed data that only needs to be accessed once every quarter, as required in this scenario.

B. Datastore

Datastore is a NoSQL database service for web and mobile applications, which is optimized for querying complex data structures and horizontal scaling. It is mainly designed for storing unstructured data and isn't the most suitable choice for storing critical archival information that's accessed infrequently at a low cost.

C. Durable Reduced Availability Storage

Durable Reduced Availability (DRA) Storage is no longer an actively supported Google Cloud Storage offering and has been replaced by Regional storage class. This storage class is designed for storing data redundantly across multiple locations within a region, useful when data access is more frequent and low latency is a priority. This option is not a cost-effective solution for infrequent access, as required in this scenario, making it a poor choice for storing critical archival data.

Solution to Question 18: D

The correct answer is D, and here's why:

Option A is not suitable because Bigtable is a real-time, scalable, NoSQL database service designed for large analytical and operational workloads, and not intended for storing medical images. Also, exporting the images from Bigtable to Cloud Storage adds an unnecessary extra step in the process.

Option B is incorrect because Cloud Transfer Service is a managed service for transferring data from or to cloud storage services like Amazon S3 or Google Cloud Storage but it does not directly deal with on-premises storage.

Option C is not appropriate because App Engine and Cloud Endpoints are application development platforms and APIs management tools, respectively. They provide scalable infrastructure for your applications but do not directly provide the required file synchronization capabilities between on-premises storage and Cloud Storage.

Option D is the correct choice because the gsutil command line interface (CLI) is a useful tool for performing a wide range of operations on Cloud Storage like uploading, downloading, and synchronizing files. By creating a script that utilizes gsutil to sync the on-premises storage with Cloud Storage and scheduling the script as a cron job, you will automate the process of uploading new medical images to Cloud Storage, meeting the company's requirements in the healthcare industry. This solution is easy to implement and satisfies the requirement for an automated process to transfer medical images from on-premises storage to Cloud Storage.

Solution to Question 19: A

The correct answer is A. Enable the Cloud Spanner API.

Explanation for choosing A: Before creating a Cloud Spanner instance, you should first enable the Cloud Spanner API. This is because the API is the primary interface for interacting with Cloud Spanner, allowing you to manage your instances, databases, and data. Enabling the Cloud Spanner API ensures that your project has access to all the required features and functionalities of Cloud Spanner to deploy a globally distributed application.

Reasons why other options are incorrect: B. Enable Cloud Storage API for the project: While Cloud Storage can be used for storing files such as images, logs, and backups, it is unrelated to Cloud Spanner, which is a globally distributed and horizontally scalable database service. Enabling the Cloud Storage API does not directly impact the deployment of an application using Cloud Spanner as the data storage solution.

C. Configure your Cloud Spanner instance to be multi-regional: While configuring a Cloud Spanner instance to be multi-regional is essential for deploying a globally distributed application, it is not the first step. Before creating the instance and configuring it as multi-regional, you need to enable the Cloud Spanner API to interact with the Cloud Spanner service.

D. Create a new VPC network with subnetworks in all desired regions: Although setting up a VPC network and subnetworks in desired regions is important for ensuring connectivity between different parts of the application, it is not directly related to using Cloud Spanner for data storage. The first step regarding Cloud Spanner is enabling its API, as mentioned in option A.

Solution to Question 20: D

The correct answer is option D: Enable API, create a workspace under project A, and then add projects B and C.

Explanation for choosing option D: Application performance monitoring in Google Cloud Platform requires the use of Google Cloud Monitoring, which is a part of Google Cloud Operations Suite (formerly Stackdriver). In this scenario, you need a single, unified view of CPU, memory, and disk usage across multiple projects. By creating a workspace under project A and adding projects B and C to it, you can collect and display the monitoring data for all three projects in a single dashboard, providing the efficient and comprehensive solution you are looking for.

Why other options won't work:

A. Use Firebase Performance Monitoring to track metrics across the three projects. Firebase Performance Monitoring is a separate service primarily focused on monitoring mobile applications, and it does not offer a comprehensive solution for Google Cloud projects as required in the scenario. Furthermore, Firebase Performance Monitoring does not include CPU, memory, or disk usage in its metrics, meaning it would not fulfill the monitoring requirements

specified.

B. Set up Google Kubernetes Engine for projects A, B, and C with a single dashboard. Google Kubernetes Engine (GKE) is an orchestration service for managing containerized applications in Kubernetes. Although GKE does offer its own performance monitoring and logging features, it is designed to manage containerized applications, not to provide monitoring for multiple Google Cloud projects. In this scenario, using GKE would not provide the needed functionality for a unified view of application performance monitoring across multiple projects.

C. Enable API and connect projects A, B, and C to Cloud SQL for monitoring purposes. Cloud SQL is a Google Cloud Platform service that provides managed SQL databases. It does not offer application performance monitoring for other cloud resources such as CPU, memory, and disk usage. Connecting projects A, B, and C to Cloud SQL would only provide monitoring for database usage, and it would not meet the requirements of monitoring for multiple projects with a single, unified view.

Solution to Question 21: C

The correct answer is C. Enable the Node Auto-Upgrades feature for your GKE cluster.

Here's the explanation for why this is the best choice and why the other options are not suitable:

A. Enable the "Stackdriver Monitoring" for your GKE cluster: Stackdriver Monitoring is a useful feature for collecting metrics and logs from your containerized applications and infrastructure, but it does not ensure that your cluster is always running on a supported and stable version of Kubernetes. Therefore, this option does not fulfill the requirement stated in the question.

B. Use "Windows Server" as a node image for your GKE cluster: Windows Server is an operating system supported by GKE for running Windows containers, but choosing this as the node image does not guarantee that your cluster will always run on a supported and stable version of Kubernetes. Additionally, using Windows Server as a node image will not provide any automated capability to upgrade the cluster.

C. Enable the Node Auto-Upgrades feature for your GKE cluster: This is the correct answer because enabling the Node Auto-Upgrades feature ensures that your GKE cluster's nodes are always running on versions of Kubernetes supported by Google. This feature automatically upgrades the nodes in your cluster without any intervention, keeping them on the latest stable version and preventing potential compatibility and security issues.

D. Enable the Node Auto-Repair feature for your GKE cluster: Node Auto-Repair is another beneficial GKE feature designed to automatically repair nodes that fail health checks. While this option is advantageous for maintaining a

healthy cluster, it does not guarantee that your cluster will always run on a supported and stable version of Kubernetes.

Solution to Question 22: C

The correct answer is C: Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

Here's why option C is correct and the others are not:

Option A: BigQuery is a fully managed data warehouse and analytics platform, not an auditing and logging tool. Cloud Spanner audit logs won't be found in the BigQuery Console. So, this answer is incorrect.

Option B: Stackdriver Monitoring is a tool for monitoring the performance, uptime, and overall health of applications and infrastructure. While Stackdriver Monitoring can create dashboards for different aspects of Cloud Spanner, it doesn't provide IAM role audit logs. This option is also incorrect.

Option C: Stackdriver Logging (also known as Cloud Logging) is the correct tool for reviewing audit logs in Google Cloud Platform. Reviewing admin activity logs and filtering them for Cloud Spanner IAM roles in Stackdriver Logging console allows you to find information about when users were added to these roles. Therefore, this answer is correct.

Option D: Cloud Functions is a serverless compute platform that allows you to run small code parts when specific events are triggered. It's not intended for monitoring IAM roles in Cloud Spanner, making this answer incorrect.

Solution to Question 23: B

The correct answer is B. Grant the service account the IAM Role of Compute Storage Admin in the project called proj-vm.

Explanation: As a cloud administrator for an e-commerce company, you are required to manage service accounts within a specific project (proj-sa). You need a service account within that project to take snapshots of VMs in another department's project (proj-vm). To achieve this, you should grant the service account the IAM Role of Compute Storage Admin in the project called proj-vm. This role provides the necessary permissions to create and manage VM disk snapshots.

Reasons why other options will not work:

A. Use IAM Conditions to restrict the service account's access to proj-vm only. - IAM conditions do not grant necessary permissions but only give an additional level of control over the granted permissions. Thus, you need to grant the appropriate role first to provide the service account with the required permissions.

C. Use gcloud command to copy the service account from proj-sa project to proj-vm project. - Service accounts cannot be copied across projects. Instead, you can grant the service account from one project the necessary IAM Role in

another project, allowing it to access resources and perform actions in the target project.

D. Grant the service account the IAM Role of Project Viewer in the project called proj-vm. - The Project Viewer role provides only read access to all resources within the project. It does not grant any write or management permissions needed to take snapshots of VMs in the project. Thus, this role is not suitable for the given task.

Solution to Question 24: A

The correct answer for this scenario is option A. The strategy involves creating multiple service accounts, one for each pipeline, with the appropriate minimal Identity and Access Management (IAM) permissions. This ensures that the CI/CD pipeline has the required permissions without over-provisioning access. Using a secret manager service to store the key files of the service accounts enables secure storage and retrieval of sensitive data. Allowing the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline ensures that the required access permissions are available only on-demand, reducing the potential for unauthorized access.

Option B is not the best solution because adding a step for human approval to the CI/CD pipeline before infrastructure provisioning introduces delays and potential bottlenecks. Using a human approvals IAM account for the provisioning concentrates excessive permissions in a single account, which is against security best practices of segregating duties and granting least privilege.

Option C is not ideal because creating individual user accounts for each pipeline is not a scalable solution, especially for a company implementing multiple pipelines. Furthermore, using individual user accounts for provisioning infrastructure leads to difficulty in managing the deployed resources while increasing the attack surface and potential for unauthorized access.

Option D is not recommended as using the Compute Engine default service account for provisioning resources is against security best practices. Default service accounts have broad permissions, increasing the risk of unauthorized operations or data breaches. It is always advisable to use custom service accounts with the least privilege principle for better security management.

Solution to Question 25: D

The correct answer is D:

D. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

Explanation:

In this scenario, the goal is to migrate a containerized Python microservices application to a serverless Google Cloud solution. Cloud Run is an ideal choice

as it provides a fully managed serverless environment to run Docker containers with automatic scaling, which aligns with the serverless requirement. By doing so, you can keep using your existing CI/CD pipeline, Docker images, and manage configurations through environment variables, ensuring minimal changes during the migration process. Updating the configurations and the required endpoints is necessary to adapt the application to the new infrastructure.

Why other options will not work:

A. Migrating to App Engine Flexible Environment is not the ideal choice compared to Cloud Run because it will require you to make changes to your application's codebase, deployment process, and configuration management, thus increasing overall migration efforts. Additionally, App Engine Flexible Environment is not fully serverless and may have limitations on automatic scaling compared to Cloud Run.

B. Deploying the generated Docker images to Compute Engine instances does not provide a serverless environment. Compute Engine instances require manual scaling and management, which may result in more administrative overhead and complications during the application's migration.

C. Deploying each service as a separate Cloud Function will require significant changes to the existing codebase because Cloud Functions are designed to serve event-driven applications, not containerized microservices applications. Converting an existing containerized app to functions will require re-architecting the whole application, increasing migration complexity, and affecting the seamless transition.

Solution to Question 26: A

The correct answer is A. Develop templates for the environment using Cloud Deployment Manager.

Explanation:

A. Develop templates for the environment using Cloud Deployment Manager: Using Cloud Deployment Manager to create templates is the most suitable option for managing numerous Google Cloud resources in a streamlined manner. These templates enable you to define your infrastructure as code, meaning you can treat the infrastructure the same way you would treat software code. This approach promotes reusability, maintainability, and version control, ultimately reducing the redundant code and making the management process more efficient.

B. Create a bash script that contains all requirement steps as gcloud commands: Although creating a bash script might help automate some tasks, it is not the best option, as it is not specifically designed for managing Google Cloud resources. This approach lacks the flexibility, reusability, and maintainability provided by Cloud Deployment Manager. Moreover, it would be more challenging and time-consuming to maintain the infrastructure using bash scripts.

C. Use Google Cloud Pub/Sub to implement message-based asynchronous resource management: Google Cloud Pub/Sub is a messaging service, not an Infrastructure-as-Code solution. It allows you to send and receive messages between independently written applications, but it is not designed for managing cloud resources systematically. Hence, this option is not suitable for the task at hand.

D. Manually use the gcloud command-line tool to manage all resources interactively: Using the gcloud command-line tool interactively is a manual and labor-intensive process, prone to human error. This approach does not streamline the management of numerous Google Cloud resources, nor does it promote efficiency, reusability, or maintainability. Therefore, this option is not suitable for the task.

Solution to Question 27: C

The correct answer is C: Modify the existing subnet range to 172.16.20.0/24.

Explanation:

Option A is not the best approach because creating a new subnetwork in the existing VPC with a range of 172.16.20.192/26 would overlap with the current subnetwork range (172.16.20.128/25). This would cause IP address conflicts in the VPC network and would not be a proper solution to the problem.

Option B would not be the most efficient solution because configuring a VPN between the existing VPC network and a new VPC network requires more complex setup steps than modifying the existing subnet range. It would also introduce potential latency and additional costs due to the VPN setup.

Option D is not the best approach because creating a new VPC network and enabling VPC Peering introduces more complexity and increases the number of steps compared to simply modifying the existing subnet range. This also involves more configuration steps and may introduce additional costs for the VPC Peering setup.

The optimal solution, option C, is to modify the existing subnet range to 172.16.20.0/24, which would increase the available private IP address space within the same subnetwork without causing overlapping IP address ranges or introducing any additional configuration steps. This is the most efficient and least complex approach to fulfilling the task.

Solution to Question 28: D

The correct answer should be D: Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

Here's why answer D is the appropriate choice, while the other options will not work:

A. Adding the accelerator: gpu annotation to the pod specification may appear to be the right direction, but it is insufficient. This only defines the GPU requirement in the pod but does not guarantee that the required GPUs are attached to the nodes in your cluster. In order to launch pods, the appropriate GPU-enabled nodes must be in your cluster first.

B. Manually installing Nvidia Tesla P100 GPUs on the cluster's nodes is not an optimal solution. This approach would require significant manual effort and would not adhere to infrastructure-as-code practices. In addition, you would need to maintain the GPUs and ensure their compatibility with GKE. With GKE, you can use native support for GPUs, which automatically takes care of installing necessary drivers and adding GPU resources to your nodes.

C. Enabling GPUs on existing nodes without creating a dedicated node pool is not recommended. A separate node pool allows you to isolate workloads, manage costs more effectively, and scale the resources readilly when needed. Furthermore, many ML workloads are resource-intensive and may interfere with other workloads running on the same nodes, causing performance issues.

D. Creating a new, GPU-enabled node pool to the GKE cluster allows you to separate the GPU-intensive workloads of your ML team from other workloads in the cluster. Using the provided nodeSelector in their pod specification, the ML team can ensure that their pods run on nodes with the desired GPUs. This approach requires minimal manual effort, adheres to infrastructure-as-code practices, and allows you to scale and manage resources more efficiently.

Solution to Question 29: D

The correct answer is D because Google Kubernetes Engine (GKE) requires a container image to be hosted in a container registry so that it can be pulled and deployed as a workload. Google Cloud Artifact Registry works as the managed solution for hosting container images on Google Cloud Platform (GCP).

Option A is incorrect, as images must be hosted in a container registry such as Artifact Registry or Container Registry, not in Cloud Storage. Cloud Storage is a scalable object storage solution for different types of data but is not suitable for storing container images.

Option B is incorrect, as creating a Kubernetes Service just to reference the image isn't the correct approach. A Kubernetes Service is designed to provide network services to your application components running in a cluster. In this case, you need to deploy the workload before creating a service to expose it.

Option C is incorrect for two reasons. Firstly, like Option A, it mentions uploading the image to Cloud Storage, which is not suitable for storing container images. Secondly, it suggests creating a Kubernetes DaemonSet, which is not the best choice for deploying an application on GKE. DaemonSets are used to ensure that a single copy of a specific Pod runs on every (or some specific) node(s) in a cluster, typically for monitoring, logging, or other system-level services.

Option D is correct because it involves uploading the container image to Artifact Registry, which is the appropriate container registry for GCP. After uploading the image, you create a Kubernetes Deployment that references the image. Kubernetes Deployments are responsible for managing the desired state of application instances and ensuring the specified number of replicas is always available. This is the recommended way of deploying and scaling applications on GKE.

Solution to Question 30: A

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

The reason behind choosing option A is that a dry run query allows you to estimate the number of bytes read without actually executing the query. This enables you to have an idea of the cost associated with running the query. Then, you can use the Pricing Calculator to convert the bytes estimate to dollars, thus providing you with the cost estimate for running the query using on-demand pricing.

Option B, to run the query in multiple parts and pay for each part separately, is not an optimal solution. It may cause inconsistencies, and managing the fragmented data can become challenging. Additionally, splitting the query will not provide an accurate cost estimation, as the sum of each part will still be the total cost.

Option C, using the BigQuery UI to estimate the cost without actually running the query, is not a viable solution as the BigQuery UI does not offer an in-built feature to provide cost estimation without executing the query. In order to accurately determine the cost, you need to perform a dry run query using the command line, as mentioned in option A.

Option D, which involves switching to Flat-Rate pricing for just one query and then moving back to on-demand pricing, is not a feasible solution. It can be time-consuming and complicated, as you will have to modify your pricing model and then revert it back after executing this single query. Furthermore, altering the pricing structure may not be allowed by the pricing policy.

In conclusion, option A provides the best approach to determine the cost of running a large query on BigQuery with on-demand pricing. Using a dry run query, you can estimate the number of bytes read and convert that to dollars with the Pricing Calculator, ensuring an accurate cost estimation.

Solution to Question 31: D

The correct answer is D. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

Explanation:

Option A does not work because leveraging a custom Cloud Function might not provide the quickest feedback on the modifications made to the Deployment Manager template. A custom function would require additional coding, testing, and possibly troubleshooting, which would delay the validation process.

Option B is not suitable because simulating the Deployment Manager template changes in the Cloud Shell does not guarantee that all dependencies will be met in the actual environment. There could be discrepancies between the simulation and the actual project, which could lead to undetected issues.

Option C is not the best choice either, as executing the Deployment Manager template against a separate project with the same configuration may take longer, and it could lead to cleanup efforts if the changes have unwanted consequences in the separate project. This may not provide the quickest feedback as desired.

Option D is the best choice because executing the Deployment Manager template using the "-preview" option allows you to observe the state of interdependent resources without actually committing the changes in the same project. It provides quick feedback, ensuring that all dependencies are met before committing the template will minimize the risk of breaking the existing configuration.

Solution to Question 32: A

The correct answer to this question is A: Stop the VM, increase the memory to 8 GB, and start the VM. This is because the main issue presented in the question is a memory shortage on the virtual machine. By stopping the VM and increasing its memory allocation to 8 GB, you are directly addressing the root cause of the problem and providing the requested upgrade to resolve the memory shortage. After increasing the memory, starting the VM will ensure access to the new memory allocation.

Option B, using Cloud Functions, is not the appropriate solution because Cloud Functions are used for single-purpose, stateless functions that respond to cloud events. This does not address the memory shortage issue that the virtual machine is currently experiencing.

Option C, using Cloud Storage Bucket, is also not suitable for this situation. While it can store excess data, it does not help in solving the memory shortage of the virtual machine. Cloud Storage Bucket is more useful for storing static objects like images or binary data, and it doesn't solve the specific problem of increasing available memory for the VM.

Option D, upgrading the Cloud SDK, is not viable because upgrading the Cloud SDK would not directly impact the VM's memory allocation. The Cloud SDK is a set of development tools for managing resources on Google Cloud Platform, and its version doesn't relate to fixing memory shortage issues on a VM.

Solution to Question 33: D

The correct answer is D: Verify that you are the project billing administrator.

Select the associated billing account and create a budget and alert for the appropriate project.

Explanation:

Option A is incorrect because it mentions creating a custom alert without specifying for which project the budget and alert should be created. As an IT manager, you need to set a budget alert specifically for one of the three projects, not a custom alert for the whole billing account.

Option B is incorrect because having the owner role at the organization level is unnecessary for this task. The project billing administrator role is sufficient to create a budget and alert for a specific project. Moreover, there is no need to select the "associated billing account" at the organization level, as you simply need to manage the budget for one project within that account.

Option C is incorrect because although it mentions creating a budget for Compute Engine only, it does not mention setting an alert, which is a crucial part of the question. Creating a budget without an alert will not notify you when the budget threshold is reached, defeating the purpose of the task.

Option D is the correct answer because it covers all requirements mentioned in the question. First, you verify that you are the project billing administrator, which provides the authority to manage budgets for the associated billing account. Next, you select the billing account and create a budget specifically for the appropriate project, ensuring that the budget and alert are tailored to that project's needs. This solution satisfies the objective of setting a budget alert for the use of Compute Engineer services in the relevant project while managing multiple projects under a single billing account.

Solution to Question 34: B

The correct answer is B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

The reason for this is because the issue lies within the specific pod (myapp-deployment-58ddbbb995-lp86m), which is stuck in the PENDING status. By reviewing the pod details and looking for warning messages, you can identify the possible causes of the issue, such as insufficient resources or scheduling conflicts.

Option A is not the correct choice because the Deployment object logs will not provide specific information about the status of individual pods. Deployments manage the desired state of the application, and their logs would not necessarily contain specific information about the pod's issue.

Option C is not the correct choice as the myapp-service Service object is responsible for providing network access to the application, and the issue at hand is related to a specific pod's status. If there were issues with the Service object, it would likely impact all pods and not just a single one.

Option D is not the correct choice because when a pod is in the PENDING

status, the container has not started yet, and thus, there will be no logs available. The PENDING status indicates that Kubernetes has not yet scheduled the pod onto a node or has not been able to create a container. Viewing container logs will not provide any insights into the underlying cause of the issue.

Solution to Question 35: D

The correct answer is D: Use gcloud iam roles copy and specify the production project as the destination project.

Explanation:

When you want to replicate the same IAM roles from one project to another, using gcloud iam roles copy is the most efficient method. This command can efficiently copy roles from one project to another while minimizing the number of steps needed.

Why other options will not work:

A: Using the gcloud projects update command to merge both projects and migrate IAM roles is not an appropriate solution. This command is used for updating the metadata of a project, not merging two separate projects or transferring IAM roles between them. Additionally, merging projects would not be recommended in this case, as it's essential to separate development and production environments.

B: In the Google Cloud Platform Console, using the 'create role' functionality and selecting all applicable permissions would be too manual and time-consuming. This approach requires you to recreate the roles manually in the new project, instead of simply replicating them from the previous one. It also opens the possibility of human errors resulting from the manual process.

C: Using gcloud iam roles copy and specifying the development project as the destination project would be incorrect because you want to replicate the IAM roles into the new production project, not the previous development project. This option would merely create duplicate roles within the same development project, rather than transferring the roles to the production project.

In conclusion, the most appropriate solution is to use gcloud iam roles copy and specify the production project as the destination project (Option D) because it efficiently replicates the IAM roles between projects with the fewest steps possible.

Solution to Question 36: B

The best option for this scenario would be Option B: Create a GKE Autopilot cluster and enroll the cluster in the stable release channel.

Explanation for Option B: GKE Autopilot is designed to provide a managed Kubernetes experience focused on simplicity and reliability. Autopilot clusters automatically manage and scale your Kubernetes infrastructure for you, which allows you to focus solely on your application. Furthermore, the stable release

channel is recommended for production use as it provides the most recent, thoroughly tested, and reliable Kubernetes version. This ensures that the vital application will have the utmost reliability while adhering to Google's recommended practices.

Why other options don't work:

Option A: This option suggests using the rapid release channel, which includes the latest Kubernetes versions with new features and improvements. However, the rapid release channel might not be as stable and reliable as the stable release channel, and may contain untested features, making it less suitable for an application that is vital for business operations.

Option C: While this option suggests enrolling in the stable release channel, it does not have any availability preference set. This could potentially lead to less reliability, as it does not ensure optimal node distribution or regional availability in the cluster.

Option D: A zonal GKE standard cluster is limited to a single zone, which might not be suitable for an application that requires utmost reliability. If the zone experiences failure, it could result in downtime for the entire cluster, which could impact business operations. Additionally, there is less redundancy and high availability compared to regional clusters.

Solution to Question 37: A

The correct answer is A: Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Explanation for answer A: Uploading the Docker image to Google Container Registry (GCR) is the appropriate action because it's designed to store and manage container images. Once the image is uploaded to GCR, you can create a Kubernetes Deployment that refers to the image using the image's URL. This will instruct Kubernetes to pull the image from the registry and create containers based on the image. This is the standard method to deploy containerized applications on Google Kubernetes Engine (GKE) and generally recommended.

Explanation for why other options will not work:

Option B: Upload the image to BigQuery and create a Kubernetes Deployment referencing the image. This option is not suitable because BigQuery is a fully-managed data warehouse and analytics platform. It's meant to store structured data and process queries, not designed for storing and serving container images. Therefore, using BigQuery for this purpose would be inappropriate and technically unfeasible.

Option C: Upload the image to Firestore and create a Kubernetes Deployment referencing the image. This option is also incorrect because Firestore is a managed NoSQL database service. It is designed to store and synchronize data across applications, not to store and serve container images. Like BigQuery,

it's unsuitable and technically infeasible for storing Docker images and creating a Kubernetes deployment.

Option D: Upload the image to Cloud Storage and create a Kubernetes Service referencing the image. This option is incorrect because, while Cloud Storage can store various types of data, it's not suitable for storing container images and is not deeply integrated with GKE the way Container Registry is. Additionally, creating a Kubernetes Service referencing an image doesn't make sense because a Service is responsible for exposing running containers to the network, while a Deployment ensures the desired number of replicas are running. To correctly deploy the image, you would need to create a Kubernetes Deployment, not a Service, and use Container Registry, not Cloud Storage.

Solution to Question 38: D

The correct answer is D, which requires you to grant the required IAM roles using the G Suite users' email addresses. This approach ensures that the users are granted access to the company's Cloud Platform project in a quick, organized, and secure manner without creating redundant resources.

Let's delve into why the other options are not appropriate:

Option A suggests creating a new GCP project for each G Suite user and sharing the resources individually. This method is impractical, as it entails creating and managing potentially numerous separate GCP projects. This process will not only slow down overall productivity but also consume more resources, making it an inefficient solution.

Option B proposes using the Cloud SDK to create a new user role and assign it to each G Suite user's email address. While this appears plausible, the recommended approach when granting access in GCP is to use IAM roles, which are a collection of permissions that form the basis of fine-grained access control. Creating a new user role, in this case, is unnecessary and could introduce potential security risks if not managed appropriately.

Option C involves creating an Organization Policy in the GCP Console to restrict access to specific G Suite users by listing their email addresses. While Organization Policies offer a way to manage resource access, they are designed primarily for company-wide management and configuration, not granting individual users access to a project. Using IAM roles (Option D) is a more straightforward and effective solution for this particular use case.

Solution to Question 39: D

The correct answer is D, which involves setting the minimum number of instances for your Cloud Run service to 3. Here's why this is the best choice and why the other options are not appropriate.

Option A suggests changing the Cloud Run memory allocation to a larger value, but this is not recommended because it will just increase the overall resource usage instead of addressing the issue of the initial page load times. If your

application's performance is slower during the initial operation but fine afterwards, it is a strong indication that the problem is related to instance scaling, not memory allocation.

Option B proposes setting the concurrency number to 1 for your Cloud Run service. Decreasing concurrency, however, will cause your service to handle fewer requests simultaneously thus increasing the response time, which is the exact opposite of what you need to optimize.

Option C recommends decreasing the request timeout for your Cloud Run service. This is not a suitable solution because it could lead to premature termination of some requests and negatively impact user experience. This might not address the problem of the initial page load times being longer than the subsequent ones.

Option D is the correct choice because setting the minimum number of instances for your Cloud Run service to 3 will ensure that there are always three instances running ready to accept incoming requests, as per Google's recommendations. This will reduce the time it takes to spin up a new instance if needed, overcoming the issue of the initial page load taking longer when new instances are being created. This option leads to faster loading times for users without negatively impacting other aspects of the service.

Solution to Question 40: C

The correct answer is C. You should search for the CMS solution in Google Cloud Marketplace and deploy the solution directly from Cloud Marketplace. This option provides a seamless deployment process, quick setup, and is less prone to manual configuration errors.

Other options are not the best solution for the given scenario for the following reasons:

A. Manually installing the CMS on a new App Engine standard environment instance would require a longer setup process and would be more prone to human error from manual configuration. App Engine is designed primarily for web apps, and not all CMS solutions are built to run on App Engine; hence, this may lead to additional complications.

B. Deploying the CMS solution using Kubernetes Engine and manually configuring the solution using the YAML files is not a quick and simple approach as requested in the scenario. This option would require substantial knowledge of Kubernetes and YAML, and it could lead to complications if not set up correctly.

D. Using Datastore to store the CMS files and deploying the solution using a custom Cloud Function would not only require custom scripting but also additional configuration, making it a time-consuming process. Besides, this approach does not take advantage of Google Cloud's more efficient deployment methods available through the Cloud Marketplace.

Solution to Question 41: B

The correct answer is B because it involves creating an instance template for the instances, which is necessary for setting up identical Compute Engine instances within an instance group. By setting 'Automatic Restart' to on, the instances will automatically restart if they crash, fulfilling that part of the requirement. Additionally, setting 'On-host maintenance' to Migrate VM instance ensures high availability during maintenance periods, as instances will be moved to another host instead of being terminated or paused.

Option A is not correct because it only involves creating an instance group and setting the 'Autohealing' health check to healthy (HTTP). While this can be useful for monitoring instance health, it does not ensure high availability during maintenance periods or automatically restart instances upon crashing.

Option C is not appropriate for this scenario as it involves creating a Google Kubernetes Engine cluster and deploying instances using Kubernetes Deployments. While Kubernetes can help ensure high availability and automatic restarts, it's unnecessary for this particular use case, where Compute Engine instances are the primary requirement.

Option D is also incorrect because it creates an instance group but focuses on the 'Advanced creation options' setting for 'do not retry machine creation'. This setting does not fulfill the requirement of ensuring high availability during maintenance periods or automatically restarting instances if they crash.

Solution to Question 42: A

The correct answer is A: Upload the data to Cloud Storage using the gsutil command line tool.

Explanation:

A: This is the best option among all the choices, as Google Cloud Storage is designed to store and manage large amounts of unstructured data. It supports a variety of file formats and offers seamless integration with other GCP services, including Dataflow. The gsutil command line tool simplifies the process of uploading data to Cloud Storage, making it the most appropriate method for this scenario.

B: Cloud Bigtable is a NoSQL database intended for real-time, high-throughput read and write workloads. While Cloud Bigtable could be beneficial for specific use cases, it might not suit a situation dealing with unstructured data, various file formats, and ETL processes. Moreover, the cbt command line tool is not designed specifically for data uploads and may lack the desired efficiency.

C: Cloud Firestore is a NoSQL, serverless, fully managed, real-time database solution for web and mobile applications to store and sync their data. While it is a powerful service for specific use cases, Firestore is not ideal for storing and managing vast amounts of unstructured data in various formats. Additionally,

the Firestore module in the Google Cloud Client Libraries is not as simple and straightforward as the gsutil command line tool.

D: Google Drive is a file storage and synchronization solution, commonly used for personal and team storage. While Drive does offer storage capabilities, it is not designed to handle large, unstructured datasets for use in GCP services, like Dataflow. The Google Drive API is intended for integration with other applications, not for storing and managing massive ETL processes for a large financial industry company. Thus, uploading the data to Google Drive may lead to inefficiency and suboptimal performance.

Solution to Question 43: C

The correct answer is C. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer. This option is the recommended method because it allows you to expose your autoscaled application to the public using an HTTPS endpoint on a public IP address. By using a Kubernetes Ingress, you can configure SSL/TLS certificates and manage the routing to your NodePort service. Additionally, Ingress integrates seamlessly with Cloud Load Balancer, which provides global load balancing and greater availability for your application.

Option A is incorrect because although creating a Kubernetes Service of type NodePort does expose the application on port 443, manually configuring the public DNS name with the IP of every node of the cluster is not an efficient method for achieving load balancing. This approach would require constant updating of DNS records as nodes are added and removed, as well as the potential for uneven load distribution and increased maintenance effort.

Option B is incorrect because Google Cloud Armor is a security service designed to protect applications from Distributed Denial of Service (DDoS) attacks and other web application vulnerabilities, not for exposing a public IP address. While the Kubernetes Service of type NodePort does allow external access, relying on Google Cloud Armor for exposure is not its primary purpose and would not provide the needed routing and load balancing features.

Option D is incorrect because creating an HAProxy pod and forwarding traffic with an iptable rule is not an ideal solution for load balancing in Google Kubernetes Engine environment. This approach lacks proper integration with the platform and creates a single point of failure with the HAProxy instance running on a single node. In contrast, using a Kubernetes Ingress with a Cloud Load Balancer ensures greater redundancy, scalability, and easier management.

Solution to Question 44: C

The correct answer is C, and here's why:

Option A is not suitable because Balanced Persistent Disks are used to optimize storage costs and performance, not the availability of the applications.

Also, labeling critical deployments as disk_balanced_false doesn't provide any meaningful configuration changes for availability.

Option B is incorrect because configuring the entire cluster with Preemptible VMs doesn't guarantee continuous availability for the critical components of the application. Preemptible VMs are short-lived instances that could be terminated at any moment, which is not ideal for critical deployments.

Option C is correct because it provides an optimal cost-availability balance. By creating a cluster consisting of two node pools (one with Spot VMs and the other with standard VMs), you can deploy the critical components on the more reliable standard VM node pool, while non-critical, fault-tolerant components can take advantage of the cost savings from Spot VMs.

Option D is not ideal because Shielded VMs are used to ensure the security of the VMs, not their availability. Deploying fault-tolerant deployments on Shielded VMs will not optimize costs and doesn't balance the availability requirements specified for the application components.

In conclusion, option C is the best approach to achieve the desired balance between cost optimization and availability for the application components deployed on Google Kubernetes Engine.

Solution to Question 45: D

Answer D, inviting the user to transfer their existing account, is the most recommended approach to avoid conflicting accounts when adding colleagues with personal Google accounts to your company's Google Cloud Identity. This is because:

1. It ensures a smooth and seamless transition for users without causing data loss or requiring reconfiguration of their Google services and products, which in turn increases user satisfaction and productivity.
2. The process of transferring existing accounts allows users to maintain their email addresses, contacts, calendar events, files, and other essential data.
3. Inviting users to transfer accounts also ensures compliance with your organization's standards and security policies, providing a reduced risk of unauthorized access or data breaches.

The other options are not recommended for the following reasons:

Option A - Telling the user to share their existing account credentials with the Google Cloud Platform (GCP) admin can lead to severe security risks and violates Google's terms of service. It doesn't address the conflicting accounts issue and exposes potential vulnerabilities associated with sharing personal credentials.

Option B - Telling the user to remove all personal email from the existing account might not prevent conflicting accounts, and could result in an unnecessary loss of personal data and information. Moreover, it could cause confusion and

frustration for the user, as they will need to manage both their personal and professional data with an unclear separation.

Option C - Creating a new Google account for each user compels them to start from scratch without any previous data, resulting in an inefficient use of their time. It doesn't leverage the existing account data, leading to a potential loss of important information and contacts. Additionally, users might have to manage two separate accounts, which can be cumbersome and time-consuming.

Solution to Question 46: C

The correct answer is C: Create a custom log-based metric for the specific error to be used in an Alerting Policy.

The explanation for why the answer should be C is as follows:

By creating a custom log-based metric for the specific error, you will be able to monitor the occurrence of that particular error in real-time. You can then create an alerting policy based on this custom metric, which will notify you whenever the error arises again. This proactive approach will allow you to address the problem as soon as it appears, rather than reacting after gathering user feedback.

Now let's discuss why other options are not correct:

A. Disabling and enabling the Service Account to reset permissions isn't a suitable solution because it doesn't address the core issue of monitoring the error. While resetting permissions might have helped fix the problem this time, there is no guarantee that the issue won't arise again in the future.

B. Implementing a use of Dead-letter topic in Pub/Sub to handle errors doesn't target the specific error caused by the Service Account. The Dead-letter topic approach is primarily for handling undeliverable messages in a Pub/Sub system. While it may help you track errors, it's not tailored to alert you about the specific problem concerning the Service Account's permissions.

D. Exporting logs to Cloud Storage and analyzing them using Dataflow involves a significant time delay between when an error occurs and when you identify it. This reactive approach is not ideal, as it doesn't allow you to address issues promptly. By waiting for logs to be exported to Cloud Storage and then analyzing them, you lose the opportunity to resolve the problem as soon as it arises.

In conclusion, option C is the best solution to address the problem of being alerted to the specific error caused by a Service Account having insufficient permissions in the future.

Solution to Question 47: D

The correct answer is D - Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

Reasoning:

A. Running the web application on a Cloud Storage bucket and the backend API on Cloud Functions has some drawbacks:

1. Cloud Storage isn't meant for hosting dynamic Flask web applications; it's primarily for static web content.
2. Although Cloud Functions are a serverless solution for the backend API, the combination mentioned here isn't recommended for all workload components.

B. Using Kubernetes Engine for both the web application and the backend API doesn't align with Google-recommended practices for a serverless migration:

1. Kubernetes Engine requires more manual management and maintenance compared to App Engine and Cloud Run.
2. It doesn't take full advantage of Google Cloud's serverless offerings for these workloads.

C. Using Compute Engine to run the background job is not the best fit:

1. Compute Engine is not a serverless solution and requires VM management.
2. Integrating Cloud Tasks with Compute Engine doesn't leverage the same serverless benefits as using Cloud Run.

D. This option is the best choice based on the requirement to migrate all components to serverless Google Cloud solutions:

1. App Engine is designed for web applications without the need for infrastructure management.
2. Cloud Run enables you to run stateless containers for your backend API and is fully managed.
3. Cloud Tasks provide a serverless solution to handle scheduled or long-running background tasks and can trigger Cloud Run services.

Thus, answer D is the ideal choice for implementing Google-recommended serverless practices for each workload component.

Solution to Question 48: B

The most appropriate solution is B. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

Option B is the best choice because it centralizes the costs and allows project creators to bypass entering their credit card information. By creating a single billing account and associating a payment method, it streamlines project management while empowering engineers to create projects as needed. It also makes tracking expenses related to Google Cloud Services easier and provides better control over the budget.

Option A is not suitable because the Google Cloud Platform free trial account is intended for individual use, offers limited resources, and will expire after a period of time. It's not ideal for a growing company handling larger projects and requires engineers to create a new account once the trial ends.

Option C is not feasible because Google Cloud doesn't provide corporate credit cards. Moreover, it would not address the underlying issue - streamlining the process of creating projects without requiring credit card information from individuals.

Option D is impractical because creating separate billing accounts for each engineer would complicate the process. It would require individual credit card information from each engineer, which lacks efficiency, and make it challenging for the company to oversee costs and manage multiple billing accounts. This option would create unnecessary administrative tasks and make it harder to maintain budget control.

In conclusion, Option B is the most appropriate solution because it simplifies project creation and expense management while providing the necessary financial flexibility for company growth.

Solution to Question 49: C

The correct answer is C. Create a snapshot schedule for the disk using the desired interval.

Explanation:

Option A is not suitable because Data Transfer Service and BigQuery are primarily designed for data analytics and not for backing up disk data. Therefore, this approach will not be efficient or cost-effective.

Option B might work, but creating a new disk from the existing one using a cron job will not be an ideal workflow for backing up disk data. Moreover, it will not provide the desired automated older backup removal, which will lead to increased costs.

Option C is the recommended solution because creating a snapshot schedule ensures that the boot disk is backed up regularly at specified intervals. Snapshots can be created faster and have an incremental nature, making them more efficient than creating an entire new disk. Additionally, Google automatically removes older snapshots based on your defined retention policy, effectively minimizing costs.

Option D is not relevant for ensuring regular backups since Managed Instance Groups are mainly used for horizontal scaling and distributing workloads across instances. While they might use a template derived from the existing instance's disk, they do not focus on regular backup and disaster recovery solutions.

Solution to Question 50: A

The answer should be A: Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

Explanation:

Option A is the best solution for gathering and analyzing logs from multiple Google Cloud Platform projects because it uses Stackdriver Logging, which is specifically designed to aggregate logs from various GCP services. By creating an export with a Sink destination to a BigQuery dataset, you can efficiently store and analyze the combined logs for all projects in a flexible and scalable way. Configuring the table expiration to 60 days meets the requirement of gathering logs from the past 60 days.

Reasons why other options will not work:

Option B: Configuring a Cloud Function to read from Stackdriver Logging and write the logs to Cloud Spanner may work as a solution to collect logs, but it is not recommended by Google. Cloud Spanner is better suited for serving large-scale, high-throughput transactional workloads, rather than analyzing and storing logs. Furthermore, it may introduce unnecessary complexity and management overhead.

Option C: Using gsutil to manually copy logs from Stackdriver Logging to BigQuery every day is not a scalable or efficient solution. It requires manual intervention, which is prone to errors and not the recommended practice for automating log processing in GCP. Using this approach may also lead to duplicate logs or missed log data.

Option D: Configuring a Cloud Scheduler job may be a solution to periodically process logs, but it is not the most efficient way to obtain and analyze logs in GCP. Using Stackdriver Logging Export (option A) is a more direct and reliable method for managing logs, whereas Cloud Scheduler would introduce additional complexity and potential failure points with no real added benefits.

Practice Exam 2

Question 1: In your data analytics company, you need to provide team members with the ability to query datasets in BigQuery while ensuring they don't accidentally delete these datasets. To achieve this in compliance with Google-recommended practices, what action should you take?

A. Create a custom role by removing delete permissions, and add users to that role only.

B. Create a custom role by removing delete permissions. Add users to the group, and then.add the group to the custom role.

C. Create a custom role by adding only read permissions, and add users to that role only.

D. Enable Data Loss Prevention (DLP) on the datasets, instead of modifying user roles.

Question 2: As a developer at a software company, you have been working on a project that utilizes Google Cloud services. Initially, you used your personal credit card for the expenses and later got reimbursed by your company. However, your company now wants to directly handle the billing for these services in their monthly invoice. What should you do to make this happen?

A. Use Google Cloud Pub/Sub to send billing notifications to your finance team.

B. Change the billing account of your projects to the billing account of your company.

C. Enable Google Cloud Monitoring alerts for billing thresholds to notify your financial team.

D. Share your credit card details with your financial team and have them add it to a new billing account.

Question 3: As a software engineer working at a tech company, you've built an application comprising multiple microservices, each in its own Docker container image. To deploy the entire application on Google Kubernetes Engine and allow individual scaling for each microservice, what should you do?

A. Create and deploy a Function per microservice.

B. Create and deploy a Firestore Database per microservice.

C. Create and deploy a Docker Compose File.

D. Create and deploy a Deployment per microservice.

Question 4: You are working as a cloud architect in a software development company, and you have been assigned a task to deploy a single binary application on Google Cloud Platform. The company wants the application to scale

automatically based on the underlying infrastructure's CPU usage while adhering to the organizational policies of using virtual machines directly. Your goal is to ensure that the application scaling is both operationally efficient and completed as quickly as possible. What should you do?

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

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

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

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

Question 5: As a security expert at a leading tech company, you are tasked with storing sensitive client information in a Cloud Storage bucket. To comply with legal requirements, you must record all requests that access any of the stored data. How can you ensure your company fulfills these requirements?

A. Enable Cloud Storage Object Lifecycle Management.

B. Enable Data Access audit logs for the Cloud Storage API.

C. Scan the bucket using the Data Loss Prevention API.

D. Encrypt the bucket data with Cloud KMS.

Question 6: As a database administrator for a rapidly growing tech company, you have been tasked with migrating the following on-premises data management solutions to Google Cloud in order to maximize scalability and minimize operational and infrastructure management:

• One MySQL cluster for your company's primary database • Apache Kafka for your company's event streaming platform • One Cloud SQL for PostgreSQL database for your company's analytical and reporting needs

Which Google-recommended solutions should you implement for the migration?

A. Migrate from MySQL to Cloud SQL, from Kafka to Dataflow, and from Cloud SQL for PostgreSQL to Cloud Bigtable.

B. Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

C. Migrate from MySQL to Cloud SQL, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

D. Migrate from MySQL to Firestore, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to Bigtable.

Question 7: As an IT manager in a multinational corporation, you have been tasked to cut down on GCP service costs for a specific department within the company. Your objective is to shut down all configured services in an ongoing GCP project using the least number of steps. What should you do?

A. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Switch to the project in the GCP console, locate the resources, and assign them to an external user to delete.

B. 1. Verify that you are assigned the Project Billing Administrator IAM role for this project. 2. Locate the project in the GCP console, click on billing and pause billing for the project.

C. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Switch to the project in the GCP console, locate the resources and delete them.

D. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID.

Question 8: As part of a software company, your development team requires a new Jenkins server for their upcoming project. To make the deployment process efficient, what strategy should you utilize to deploy the server with the least number of steps?

A. Use GCP Marketplace to launch the Jenkins solution.

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

C. Deploy Jenkins as an API Gateway with an API key.

D. Create a Jenkins instance using Cloud Functions.

Question 9: As a network engineer for a large organization, you are tasked with transitioning the company's workload to Google Cloud's Compute Engine. The infrastructure has a mix of servers that need to be connected to the Internet as well as servers that are only accessible through the internal network. Additionally, all servers need to communicate with each other via specific ports and protocols. The existing on-premises setup utilizes a demilitarized zone (DMZ) for public-facing servers and a Local Area Network (LAN) for private servers. How should you design the networking infrastructure on Google Cloud to meet these requirements?

A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

B. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the

DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

C. 5. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up all traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

D. 2. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to block public ingress traffic for the DMZ.

Question 10: You are working as a software developer in a technology company and have recently built an application on your development laptop that utilizes Google Cloud services. The application leverages Application Default Credentials for authentication and functions smoothly on your laptop. Now, you are tasked with migrating this application to a Compute Engine virtual machine (VM) within the organization, ensuring authentication follows Google-recommended practices and requiring only minor adjustments. What should be your next course of action?

A. Manually generate an API key for each Google service and embed them in your application code.

B. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.

C. Grant access to Google services by adding Compute Engine VM's external IP to the allowed list of API clients.

D. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Question 11: As a team leader in your software development company, you noticed that your developers are excessively using service account keys during projects. To enforce short-lived service account credentials within the organization, you need a fast solution that adheres to these requirements:

• Creation of service accounts needing a key must be centralized in a project called pj-sa. • Service account keys should only be valid for 24 hours.

Considering cost-effectiveness, which Google-recommended solution should you implement for your company?

A. Use Cloud Scheduler to trigger a Cloud Function that rotates service account keys every hour. Allow only WordPress Cronjobs to automatically rotate service account keys in pj-sa.

B. Implement a Cloud Functions job to rotate all service account keys daily in pj-sa. Enforce an org policy denying service account key creation with an exception to pj-sa.

C. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

D. Use a custom App Engine task runner to rotate service account keys every day. Enforce an org policy to allow service account key creation with no exceptions across all projects.

Question 12: You are working as an IT professional at a software company and are tasked with creating a custom IAM role for a GCP service used by your organization. The custom role must be appropriate for production use, and you want to effectively communicate its status to your team. As this is the initial version of the custom role, what steps should be taken?

A. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

B. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to GA while testing the role permissions.

C. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

D. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to PRE-ALPHA while testing the role permissions.

Question 13: You are working as a cloud engineer in a company that uses Google Cloud Platform. Your team has an application deployed in Google Kubernetes Engine (GKE) with cluster autoscaling enabled. The application exposes a TCP endpoint, and there are multiple replicas of it running. There is also a Compute Engine instance in the same region but a different Virtual Private Cloud (VPC), named gce-network, that has no overlapping IP ranges with the first VPC. This instance needs to connect to the application on GKE, and you want to minimize effort. What steps should you take?

A. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Set the service's externalTrafficPolicy to Local. 3. Use the VPC peering method and configure the Compute Engine instance to use the address of the load balancer that has been created.

B. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal 3. Peer the two VPCs together. 4. Configure the Compute Engine instance to use the address of the load balancer that has been created.

C. 1. In GKE, create a Service of type NodePort that uses the application's Pods as backend. 2. Create a Compute Engine instance called proxy with 2 network interfaces, one in each VPC. 3. Use iptables on this instance to forward traffic from gce-network to the GKE nodes. 4. Configure the Compute Engine instance to use the address of proxy in gce-network as endpoint.

D. 1. In GKE, create a Service of type NodePort that uses the application's Pods as backend. 2. Export the GKE cluster's network settings to gce-network. 3. Configure the Compute Engine instance to use the address of the NodePort as the endpoint.

Question 14: As an IT specialist working for a rapidly expanding retail company, you are tasked with migrating an internal application used for managing transactional orders to the cloud. The application, which is used exclusively by employees at the company's headquarters, requires strong consistency, fast queries, and ACID guarantees for multi-table transactional updates. The application was built using PostgreSQL. To ensure seamless integration with minimal code changes, which cloud-based database is the most suitable for the application's requirements?

A. Cloud SQL

B. Memorystore

C. BigQuery Omni

D. Bigtable

Question 15: You are an IT manager at a fast-growing tech company, and currently, you have multiple VPC-native Google Kubernetes Engine clusters running in the same subnet for your operations. However, you notice that the available IP addresses for the nodes have been exhausted, and you need to ensure that the clusters can expand with additional nodes when necessary. What should you do?

A. Create a new region for the GKE clusters.

B. Configure the GKE clusters to use non-VPC-native network mode.

C. Expand the CIDR range of the relevant subnet for the cluster.

D. Create a new VPC, and set up VPC peering with the existing VPC.

Question 16: You have recently joined a global e-commerce company as a software engineer, and you are tasked with creating a custom application that stores customer's relational data. Given that the company has millions of users worldwide and expects rapid growth, you need to develop a database storage solution that can seamlessly scale with this growth while requiring minimal configuration changes. Which storage solution would be optimal for this application?

A. Cloud Spanner

B. Compute Engine

C. Bigtable

D. Cloud Storage

Question 17: You are managing the IT infrastructure of a company that operates across multiple industries. The company requires the establishment of

communication between multiple groups of Compute Engine instances, which are currently running in two separate GCP projects. Each group of Compute Engine instances is hosted in its own VPC. What should you do in order to enable traffic between these groups?

A. Configure Network Load Balancer for each group of instances and update the backend configuration to include instances from both projects.

B. Create a new Shared VPC with all instances from both projects and configure firewall rules to allow traffic between them.

C. Verify that both projects are in a GCP Organization. Create a new VPC and add all instances.

D. Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.

Question 18: As a developer in a software company, you have recently created a Google Cloud Platform project for the team. The project consists of an App Engine application that was configured to be served from the us-central region. However, the company now requires the application to be served from the asia-northeast1 region. What should you do?

A. Use gcloud command-line tool to update the existing App Engine application region to asia-northeast1.

B. Create a Cloud Function in the existing GCP project, specifying asia-northeast1 as the region, and use it to proxy requests to the App Engine application.

C. Update the us-central region settings in the existing App Engine application to enable multi-region support including asia-northeast1.

D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

Question 19: As a data analyst at a digital media company, you're responsible for monitoring the egress network costs of the Apache web server running on a Compute Engine instance that hosts large files. The server is running alongside multiple applications in the project. In order to stay informed, you wish to receive an email when the monthly egress network costs for the server, as measured by Google Cloud, exceed 100 dollars. What should you do to set up this notification?

A. Configure a Google Cloud Monitoring agent on the Apache web server and create a custom dashboard in Monitoring to track egress network costs. Set an hourly reminder to manually review the dashboard and send an email if costs exceed 100 dollars for the current month.

B. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the

Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

C. Deploy a Google Cloud Pub/Sub notification channel to publish a message when egress costs for the Apache web server exceed 100 dollars for the current month, then create a Cloud Function that listens to the channel and sends an email upon receiving the message.

D. Set up a budget alert on the project with an amount of 100 dollars, a threshold of 100%, and notification type of email.

Question 20: As a software engineer in a financial services company, you are tasked with migrating a critical on-premises application that needs 96 vCPUs for optimal performance to Google Cloud Platform (GCP). What is the best approach to ensure the application runs smoothly in a similar GCP environment?

A. Adjust the VM's vCPU configuration after its creation using the GCP Console.

B. Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations.

C. When creating the VM, use machine type n1-standard-96.

D. When creating the VM, use machine type custom with 48 vCPUs and increase the number of VM instances to 2.

Question 21: As a software engineer at a large-scale tech company, you are responsible for managing multiple Google Cloud projects with minimum steps. You want to set up the Google Cloud SDK command line interface (CLI) in such a way that it simplifies handling multiple projects. What is the most efficient method you should follow?

A. 1. Create an individual Google Cloud account for each project and switch between them. 2. Use gcloud init to update the configuration values when you need to work with a non-default project.

B. 1. Create a configuration for each project you need to manage. 2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

C. 1. Use the default configuration for all projects you need to manage. 2. Manually update the project ID within the configuration file each time you need to switch projects.

D. 1. Create a separate installation of Google Cloud SDK for each project you need to manage. 2. Use alias commands to switch between the SDK installations when working with different projects.

Question 22: You are working as a data engineer in a large retail company, and you have just received a massive 5-TB AVRO file stored in a Cloud Storage bucket. It contains crucial information that your analysts, who are proficient

only in SQL, need to access and analyze. You need to find a cost-effective and efficient solution to accommodate their request as soon as possible. What should you do?

A. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

B. Use Google Data Prep to transform the AVRO file into a CSV file and then import it into Cloud SQL.

C. Configure Cloud Dataflow to read the AVRO file and write the data into Cloud Firestore for SQL querying.

D. Load data in Cloud Datastore and run a SQL query against it.

Question 23: As an IT administrator for a software company, you are tasked with setting up a Windows VM on Compute Engine to ensure seamless remote access via RDP for your team. What is the appropriate step to obtain the login credentials for the VM?

A. After the VM has been created, use gcloud compute ssh to retrieve the login credentials for the VM.

B. After the VM has been created, use Google Cloud Console to generate an RDP file and then open it using an RDP client with your Google Account credentials.

C. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

D. When creating the VM, add a firewall rule to allow RDP traffic and use your Google Account credentials to log in.

Question 24: Working as an IT consultant for a company in the finance industry, you have been asked to set up the billing configuration for a new Google Cloud customer. The customer wants to efficiently organize their resources based on common IAM policies. How should you achieve this?

A. Use folders to group resources that share common IAM policies.

B. Use labels to group resources that share common IAM policies.

C. Use VPC peering to connect resources sharing common IAM policies.

D. Set up a proper billing account structure to group IAM policies.

Question 25: As an IT manager at a software development company, you are overseeing a GCP project and need to delegate control to your team members for managing buckets and files in Cloud Storage while adhering to Google-recommended practices. Which IAM roles should you assign to your colleagues?

A. Spanner Admin

B. Storage Admin

C. Storage Object Admin

D. Pub/Sub Admin

Question 26: You are a software engineer at a small tech company and need to deploy an application for a new project. The application is packaged in a container image, exposes an HTTP endpoint, and receives only a few requests per day. Your company wants to minimize costs for this deployment. What should be your preferred choice for deployment?

A. Deploy the container on Cloud Build with Triggers.

B. Deploy the container on Cloud Run.

C. Deploy the container on Dataproc with auto scaling enabled.

D. Deploy the container on Kubernetes Engine with Vertical Pod Autoscaler.

Question 27: As a software engineer at a gaming company, you have built a mobile game that utilizes Google Cloud for deployment. Players use their personal phones to connect to the game via the internet. During multiplayer sessions, the game transmits UDP packets to update the servers with players' actions. Your game backend is designed to scale across multiple virtual machines (VMs), and you need to expose the VMs through a single IP address. What action should be taken?

A. Utilize VPC peering for load balancing between VMs.

B. Configure an External TCP Proxy load balancer in front of the application servers.

C. Configure a Cloud CDN in front of the application servers.

D. Configure an External Network load balancer in front of the application servers.

Question 28: As a software engineer in a tech company, you are tasked with establishing a Compute Engine instance within a new project that has not been created yet. What steps should you take to successfully accomplish this?

A. Enable Kubernetes Engine API in the Cloud Console, and then use the Cloud SDK to create a Compute Engine instance specifying the new project.

B. Enable the Firestore API in the Cloud Console, create a new project, and then use the Cloud SDK to create a Compute Engine instance.

C. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

D. Enable the Compute Engine API in the Cloud Console. Go to the Compute Engine section of the Console to create a new instance, and look for the Create In A New Project option in the creation form.

Question 29: As a software engineer at a fast-growing tech company, you need to deploy additional pods to your existing application running in Google Kubernetes Engine (GKE) which currently consists of multiple pods running on four GKE n1-standard-2 nodes. The additional pods now require n2-highmem-16 nodes. How can you achieve this without any downtime?

A. Use gcloud container clusters resize to add n2-highmem-16 nodes and deploy the new pods.

B. Use gcloud container clusters set-machine-type to change the node type to n2-highmem-16 and deploy the new pods.

C. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

D. Use Kubernetes horizontal pod autoscaling and specify machine type n2-highmem-16 during deployment.

Question 30: You are working as a web developer for an e-commerce company, and your manager has requested that you create a secure website with autoscaling based on the compute instance CPU load. To enhance performance, you need to store static content in Cloud Storage. What resources should you use to distribute user traffic efficiently on this website?

A. An external HTTP load balancer with an SSL proxy pointing to the backend instances to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

B. An internal HTTP(S) load balancer together with Identity-Aware Proxy to allow only HTTPS traffic.

C. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

D. An internal TCP/UDP load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

Question 31: As a DevOps engineer at a software company, you need to deploy a critical application on a Kubernetes cluster. However, you are unsure about the application's resource requirements, as it may vary based on usage patterns, external dependencies, and other factors. To ensure cost-effective recommendations for CPU and memory requirements and maintain consistent performance, you need to follow Google-recommended practices. What should you do?

A. Configure the Vertical Pod Autoscaler recommendations for availability, and configure the Horizontal Pod Autoscaler for suggestions.

B. Configure the Horizontal Pod Autoscaler for cost optimization, and configure the Vertical Pod Autoscaler recommendations for availability.

C. Configure the Horizontal Pod Autoscaler for availability, and configure the cluster autoscaler for suggestions.

D. Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

Question 32: As a software development company working on multiple projects requiring Cassandra databases, you are transitioning from an on-premises environment to Google Cloud. In order to move swiftly and minimize support effort, your development teams need isolated environments for their Cassandra instances. What should be your approach to achieve this on Google Cloud?

A. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

B. 1. Set up a Cloud Dataproc cluster and install Cassandra on it. 2. Configure the cluster for each development team to access their own isolated environment.

C. 1. Set up a managed instance group for each development team with a custom Cassandra image. 2. Configure VPC Network Peering to isolate each team's network traffic.

D. 1. Build a Cassandra Compute Engine instance and take a snapshot of it. 2. Upload the snapshot to Cloud Storage and make it accessible to your developers. 3. Build instructions to create a Compute Engine instance from the snapshot so that developers can do it themselves.

Question 33: You are working as a software engineer in a company that specializes in AI-driven solutions. Your team is developing a new project that relies on Google Cloud Platform (GCP) services such as AutoML. You have a service account with sufficient permissions for AutoML in place. To enable authentication for the API calls from your company's on-premises data center, what should you do?

A. Use gcloud to create a key file for the service account that has appropriate permissions.

B. Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.

C. Create an API key and use it for authentication from your on-premises application

D. Use service account credentials in your on-premises application.

Question 34: As a cloud administrator at a tech company, you have been asked to check when a specific Google Cloud Platform service account was created. How can you achieve this?

A. Filter the Activity log to view the Networking category. Filter the Resource type to Service Account.

B. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

C. Filter the Audit logs to view the Configuration category. Filter the Resource type to Compute Engine.

D. Filter the Activity log to view the Configuration category. Filter the Resource type to BigQuery.

Question 35: As an IT manager in a growing company, you've developed a containerized web application that will serve your internal colleagues during business hours. To minimize costs and prevent any expenses outside of the application's operational hours, you're planning to deploy the app on a new Google Cloud project. What step should you take to ensure this?

A. Create a Cloud Scheduler job to start and stop the Cloud Run (fully managed) service according to the business hours.

B. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

C. Create a cloud monitoring alert to notify you when the application is used outside of business hours, and manually stop it.

D. Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero.

Question 36: As the lead developer at your company, you have been asked to troubleshoot an issue with the company's static website hosted on Cloud Storage. The website provides links to several PDF files. However, when users click these links, the browser prompts them to save the file instead of displaying it directly in the browser. What change should you make to enable users to view the PDFs within the browser without being prompted to save them locally?

A. Enable multi-regional storage class for the bucket containing PDF files.

B. Set Content-Type metadata to application/pdf on the PDF file objects.

C. Use Firebase Hosting instead of Cloud Storage for the static website.

D. Configure the website's caching policy to show application/pdf content.

Question 37: You are an IT specialist at a large manufacturing company, and you have been tasked with deploying a new Enterprise Resource Planning (ERP) system on Google Cloud to streamline operations. The application requires the full database to be held in-memory for rapid data access. Which Google Cloud resource configuration should you select in this scenario to optimize performance?

A. Provision Compute Engine instances with M1 machine type.

B. Deploy the application on Kubernetes Engine with memory optimized nodes.

C. Use a Cloud Spanner instance for in-memory database handling.

D. Use Cloud Datastore with high read/write throughput.

Question 38: As a leading tech company in the software development industry, you have strict requirements to control access to your Google Cloud projects. Your goal is to enable your Site Reliability Engineers (SREs) to approve requests from the Google Cloud support team when an SRE opens a support case while adhering to Google-recommended best practices. How should you proceed?

A. Add your SREs to roles/bigquery.admin role.

B. Add your SREs to a group and then add this group to roles/accessapproval.approver role.

C. Add your SREs to roles/accessapproval.approver role.

D. Add your SREs to a group and then add this group to roles/cloudsql.admin role.

Question 39: As a data engineer at a software company, you need to quickly upload a 32 GB single file to a Nearline Storage bucket from your workplace. The WAN connection at the office is rated at 1 Gbps, and you have exclusive access to the connection. To transfer the file as rapidly as possible, utilizing the rated 1 Gbps speed, what method should you use for uploading the file?

A. Enable parallel composite uploads using gsutil on the file transfer.

B. Use the GCP Console to create a new instance and then transfer the file using gsutil.

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

D. Disable resumable uploads in gsutil.

Question 40: As a cloud engineer at a tech company, you receive an alert stating that the managed instance group has failed to create new instances, causing issues in your organization's infrastructure. How should you resolve the instance creation problem to ensure the smooth functioning of the company's services?

A. Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

B. Verify that the instance template being used by the instance group contains valid syntax. Increase the instance count of the managed instance group.

C. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

D. Check the permissions of the service account being used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

Question 41: You recently joined a software development company as a cloud engineer. Your team leader assigns you a project in Google Cloud Platform that you need to maintain and you decide to perform a security checkup. You want to find out who has been granted the Project Owner role. What should you do?

A. Use the command gcloud projects get-iam-policy to view the current role assignments.

B. Navigate to Identity-Aware Proxy and check the permissions for these resources.

C. Use the command gcloud organizations list to view the organization hierarchy and check the permissions at higher levels.

D. Go to the Firebase Console and check the Authentication section for users who have been granted the Project Owner role.

Question 42: While working on a project at a software development company, you need to update a deployment in Deployment Manager to roll out changes without causing any resource downtime. What command should you use to achieve this task?

A. gcloud deployment-manager resources update –config

B. gcloud deployment-manager deployments update –config

C. gcloud deployment-manager deployments describe –config

D. gcloud deployment-manager deployments list –config

Question 43: You are working for a company in the software development industry with an application running on Compute Engine VM instances in a custom Virtual Private Cloud (VPC). Your company's security policies mandate the use of internal IP addresses on VM instances and prohibit VM instances from connecting to the internet. You need to ensure that the application can access a file hosted in a Cloud Storage bucket within your project while adhering to the security policies. What actions should you take to accomplish this?

A. Configure a custom IAM policy to grant Compute Engine VM instances access to the Cloud Storage bucket.

B. Enable Private Google Access on the subnet within the custom VPC.

C. Configure a Load Balancer to route traffic between the VM instances and the Cloud Storage bucket.

D. Add storage.googleapis.com to the list of restricted services in a VPC Service Controls perimeter and add your project to the list of protected projects.

Question 44: As a software engineer in a leading tech company, you are tasked with developing an App Engine application for a development environment. After successful testing, your team decides to create a new project for the production environment. What is the correct approach to achieve this?

A. Clone the existing project using the GCP Console and use the same deployment settings.

B. Use the GCP Console to create a new project, and then manually copy the source code of the App Engine application.

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

D. Use Cloud Shell to create the new project, and then deploy your application to the new project.

Question 45: You are working as a cloud engineer in a software development company, and you have been assigned a new Google Cloud project linked to a billing account to set up. Your task is to create instances, configure firewalls, and store data in Cloud Storage while adhering to Google's recommended practices. What should be your next step?

A. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

B. Enable only the cloudresourcemanager.googleapis.com API and assume that it will automatically enable Compute Engine and Cloud Storage APIs.

C. Use the gcloud CLI command to create instances, set firewall rules, and store data in Cloud Storage without enabling the necessary APIs.

D. Open the Google Cloud console and run gcloud init –project in a Cloud Shell.

Question 46: As an IT manager at a growing company, you need to establish an efficient and cost-effective solution for archiving data in a Cloud Storage bucket within your organization. The data consists of multiple versions and needs to be archived after 30 days. Additionally, previous versions have to be accessed once a month for reporting purposes and the archive data is occasionally updated at the end of the month. What approach should you take for this task?

A. Add a bucket lifecycle rule that archives data from multi-regional storage after 30 days to Nearline Storage.

B. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Nearline Storage.

C. Add a bucket lifecycle rule that archives data from multi-regional storage after 30 days to Coldline Storage.

D. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

Question 47: You are working as a cloud engineer in a tech company. Your company has an extensive GCP organization with numerous projects and a billing account. As part of a recent acquisition, your company has gained control of another company with its own assortment of projects and billing account. To

streamline GCP costs from both organizations into a single invoice, starting from tomorrow, what action should you take?

A. Enable cost aggregation in the Cloud Console for both billing accounts.

B. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued.

C. Link the acquired company's projects to your company's billing account.

D. Combine the billing account balance of the acquired company and your company's billing account by enabling the joint billing feature.

Question 48: As a developer in a tech company, you are required to refactor the company's database configuration, ensuring that the password is not stored in plain text while adhering to Google-recommended practices. What should you do?

A. Encrypt the database password using Cloud Key Management Service, and store the encrypted string inside a ConfigMap object.

B. Store the database password in a Google Sheet and use Google Sheets API to fetch it during runtime.

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

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

Question 49: As a software developer at a leading tech company, you are tasked with deploying an application in Google Cloud using serverless technology. You also need to test a new version of the application by allocating a small percentage of production traffic. What approach should you take?

A. Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

B. Deploy the application to App Engine. For each new version, create a new service.

C. Deploy the application to Cloud Spanner. Use partitions for traffic splitting.

D. Deploy the application to Compute Engine. Use instance groups for traffic splitting.

Question 50: As a newly hired IT manager at a tech company, you have been tasked with integrating the IT systems of a recently acquired startup. The startup has an active production Google Cloud project in their organization, and you need to transfer this project to your tech company's organization, ensuring that billing is now under your company's account. What method should you employ to complete this task with minimal effort?

A. Create a Private Catalog for the Google Cloud Marketplace, and upload the resources of the startup's production project to the Catalog. Share the Catalog with your organization, and deploy the resources in your company's project.

B. Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

C. Create a Docker container for each resource in the startup's production project, push the containers to Container Registry, and deploy them in a new project within your organization.

D. Create a VPC Network Peering between the startup's Google Cloud project and your organization's project, then configure Billing Export to send billing data from the startup's project to your organization's project.

Practice Exam 2 Solutions

Solution to Question 1: B

The answer should be B: Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role.

Explanation:

Option B follows the Google-recommended practices in terms of granting permissions and managing users within a project. By creating a custom role with delete permissions removed, you are ensuring that users who have this role will not be able to accidentally delete datasets in BigQuery. Adding users to a group, and then adding the group to the custom role, simplifies user management and makes it easier to add or remove users in the future, as you only need to manage group membership.

Reasons why other options will not work:

A. Create a custom role by removing delete permissions, and add users to that role only. While this option seems close to the correct action, it does not adhere to Google-recommended practices since it does not involve the use of groups. Assigning users to individual roles directly can make user management more complicated, as it is harder to keep track of which users have which roles.

C. Create a custom role by adding only read permissions, and add users to that role only. This option doesn't address the issue of using groups for user management, which is a recommended practice. Moreover, creating a custom role by adding only read permissions would restrict users to have only read access without the option to create or modify datasets, which could hinder their ability to perform their tasks.

D. Enable Data Loss Prevention (DLP) on the datasets, instead of modifying user roles. While enabling DLP on the datasets might help in preventing accidental data leaks or data deletion, it does not directly address the problem mentioned in the question. DLP is designed for monitoring and protecting sensitive data; it's not the right tool to manage user permissions. Modifying the user roles by preventing delete permissions according to their business needs is the most efficient method in this scenario.

Solution to Question 2: B

Option B is the correct answer – Change the billing account of your projects to the billing account of your company. This is the most effective way to ensure your company directly handles the billing for Google Cloud expenses. By changing the billing account to your company's account, your personal credit card will no longer be charged and all project-related expenses will be included in the company's monthly invoice.

Option A – Using Google Cloud Pub/Sub to send billing notifications to your finance team will only provide them regular updates on the cloud spendings but

will not address the primary issue of transferring the billing responsibility to the company.

Option C – Enabling Google Cloud Monitoring alerts for billing thresholds will aid the finance team in keeping track of cloud expenses and averting costly surprises, but it does not address the transfer of billing responsibility to the company's account. Your personal credit card would still be charged in this scenario.

Option D – Sharing your credit card details with your financial team and having them add it to a new billing account is not secure, as it increases the risk of unauthorized usage or fraud. Furthermore, this would violate various financial security and privacy policies. The billing responsibility wouldn't be shifted to the company's account, and your personal credit card would remain tied to the billing process.

Solution to Question 3: D

The correct answer is D. Create and deploy a Deployment per microservice.

Explanation:

A Deployment per microservice enables the following:

1. Fine-grained scaling: Separate Deployments allow you to individually scale the instances of each microservice as per their specific requirements, maximizing efficiency.
2. Resource management: Individual Deployments ensure that resources such as CPU, memory, and storage are isolated for each microservice, preventing bottlenecks and maintaining optimal performance.
3. Version control: With separate Deployments, you can update, roll back, and manage versions for each microservice independently. This allows for a more robust and flexible development process.

Why other options will not work:

A. Create and deploy a Function per microservice: Functions are useful for event-driven, serverless use cases. In this scenario, you have an entire application developed with multiple microservices in Docker containers. Moving them into Functions would require a significant rewrite and might not be suitable for the application's architecture.

B. Create and deploy a Firestore Database per microservice: Firestore is a NoSQL document database that is useful for storing and retrieving data. It doesn't have any direct relationship with deploying or scaling microservices in a containerized environment. Therefore, creating a Firestore Database per microservice would not address the requirements.

C. Create and deploy a Docker Compose File: Docker Compose allows you to run multi-container Docker applications by defining multiple containers in a

single file. However, it's mainly designed for local development and testing, not for deploying and scaling applications in a production environment like Google Kubernetes Engine. Therefore, it would not be the best solution in this scenario.

Solution to Question 4: C

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

Explanation:

Option A and D suggest using third-party tools to build automation around scaling the application based on CPU usage monitoring. While this approach can be used, it will require additional effort to set up, maintain, and integrate the tools with Google Cloud Platform, making it less operationally efficient compared to option C, which utilizes native GCP functionality.

Option B suggests using Google Kubernetes Engine (GKE) with horizontal pod autoscaling. While GKE is an excellent option for containerized applications, the requirement in this scenario is to use virtual machines directly, which makes this option inappropriate for this specific use case.

Option C is the best choice because it meets the requirements of automatically scaling the application based on the CPU usage and adhering to the organizational policies of using virtual machines directly. With an instance template and managed instance group, you can create VM instances that are preconfigured with the desired software and settings. Autoscaling will then adjust the number of instances based on the CPU usage, ensuring that scaling is both operationally efficient and completed as quickly as possible. Additionally, this solution uses native Google Cloud Platform functionality, which simplifies management overhead compared to options that involve third-party tools.

Solution to Question 5: B

The correct answer is B because enabling Data Access audit logs for the Cloud Storage API will help you log and record all requests made to access the stored data in the Cloud Storage bucket. This complies with the legal requirements of maintaining a record of requests for accessing sensitive client information. Data Access audit logs give you information about who has accessed the data and what operations they have performed, like creating, modifying, or deleting data. This ensures that you have a comprehensive record for auditing purposes.

Option A is not correct because Cloud Storage Object Lifecycle Management is used to manage the lifecycle of objects within the bucket (like deletion or archival policies), but it doesn't record the requests made to access the data.

Option C is also incorrect because scanning the bucket using the Data Loss Prevention API will not record the requests made to access the data. The Data Loss Prevention API is used to discover, classify, and redact sensitive data, but it doesn't log the requests accessing the data.

Lastly, option D is incorrect because encrypting the bucket data with Cloud KMS (Key Management Service) protects the data at rest by providing encryption keys, but it doesn't record the requests made to access the stored data in the Cloud Storage bucket.

Solution to Question 6: B

The correct answer should be B: Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery. Here's the reasoning behind each part:

1. Migrate from MySQL to Cloud Spanner: Cloud Spanner is a highly scalable, globally distributed database service provided by Google Cloud. It is suitable for the company's primary database, as it can handle high transaction rates, has low latency, and allows for horizontal scaling. MySQL could be moved to Cloud SQL, but Cloud SQL does not provide the same scaling capabilities as Cloud Spanner, making it a less ideal choice for the rapidly growing tech company.
2. Migrate from Apache Kafka to Pub/Sub: Apache Kafka is an event streaming platform, and Google Cloud's Pub/Sub is a natural equivalent. Pub/Sub is a messaging service that allows the company to send, store, and receive messages between independent applications. It has the ability to process large amounts of data in near-real-time and can auto-scale as the company grows. Dataflow, mentioned in option A, is primarily used for ETL (extract, transform, load) jobs and the processing of streaming data, making it unsuitable to replace Kafka.
3. Migrate from Cloud SQL for PostgreSQL to BigQuery: Since the company's PostgreSQL database is for analytical and reporting purposes, migrating to BigQuery is the right choice. BigQuery is a fully-managed, serverless data warehouse that supports fast SQL queries over large datasets. It auto-scales, making it a perfect choice for a rapidly growing tech company. Cloud SQL for PostgreSQL is a managed relational database service, not a data warehouse, and neither Cloud Bigtable nor Firestore (mentioned in options A and D) can serve the purpose of a highly scalable analytical warehouse.

The other options mention solutions that would not perform optimally for the company's requirements as mentioned above. This is why option B is best suited for the migration.

Solution to Question 7: D

The correct answer is D, and here's why:

Option A is incorrect because assigning resource deletion to an external user does not guarantee that all configured services will be shut down promptly. Moreover, this method increases unnecessary risks and management overhead, as opposed to delegating resource deletion to an internal team member or yourself.

Option B is incorrect because pausing billing for the project does not actually shut down all configured services. It may cease additional costs, but the services will remain active until they are explicitly shut down or removed.

Option C is incorrect because, although it is necessary to be assigned the Project Owners IAM role, deleting resources individually would require more steps than the process outlined in Option D. This approach is time-consuming and inefficient, especially if there are a large number of resources to eliminate.

Option D is the correct answer because it allows you to shut down the entire GCP project using the least number of steps, meeting the objective of cutting down on service costs. By verifying that you have the correct IAM role and locating the project in the GCP console, you can easily shut down all configured services at once by clicking "Shut down" and entering the project ID. This streamlined approach ensures an effective and efficient cost-cutting measure for the specific department while adhering to the least number of steps.

Solution to Question 8: A

The correct answer is A: Use GCP Marketplace to launch the Jenkins solution.

Explanation:

A. Choosing the GCP Marketplace to launch the Jenkins solution is the most efficient option: it is a pre-configured, ready-to-deploy solution. This will ensure easy deployment with minimal steps, as Google has already done most of the configuration. You just need to select the Jenkins solution, customize your options, and hit the deploy button. This is not only time-efficient but also requires minimal manual intervention.

B. Creating a Kubernetes cluster on Compute Engine and creating a deployment with the Jenkins Docker image may work, but it is not the most efficient option. This would require several steps like configuring the Kubernetes cluster, creating and deploying Jenkins Docker image, and ensuring all networking and connections are properly set up. This method is more complex than option A and may introduce more room for error.

C. Deploying Jenkins as an API Gateway with an API key is not a suitable option. Jenkins is a Continuous Integration/Continuous Deployment (CI/CD) server, not an API management service. An API Gateway is used for creating, publishing, and securing APIs, which does not apply to the purpose of a Jenkins server.

D. Creating a Jenkins instance using Cloud Functions is not feasible. Cloud Functions is a serverless compute platform designed for event-driven applications, which means it is usually used for lightweight, short-running tasks. Jenkins is a more complex CI/CD server intended for long-running processes and, due to its nature, should not be deployed using Cloud Functions.

Thus, based on these reasons, option A is the most efficient strategy for deploying a Jenkins server with the least number of steps.

Solution to Question 9: A

The correct answer is A: 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Explanation:

Option A is correct because it involves creating a single Virtual Private Cloud (VPC) with separate subnets for the DMZ and LAN. This design allows for the separation of public-facing servers from private servers while still maintaining communication between the two subnets. By setting up specific firewall rules, you can control the flow of traffic between the DMZ and LAN based on the required ports and protocols, ensuring secure communication between the servers. Finally, you'll establish a firewall rule to allow public ingress traffic to only the DMZ, thus providing access to the necessary public-facing servers.

Option B would not be appropriate as it proposes two separate VPCs, one for the DMZ and one for the LAN. This design makes it more complex to manage communication between the two subnets and isn't necessary for maintaining proper separation between public and private servers.

Option C is incorrect because it suggests opening up all traffic between the DMZ and the LAN subnets. This would expose the private servers to unnecessary risks and is generally considered bad practice. Instead, you should limit traffic to only the necessary protocols and ports to maintain the desired security.

Option D is not suitable because it states that you should block public ingress traffic for the DMZ. This would prevent any access to the public-facing servers, which opposes the purpose of having a DMZ in the first place. The DMZ needs to be accessible to the public, while simultaneously ensuring that only necessary communication occurs between the DMZ and the LAN.

Solution to Question 10: D

The correct answer is D. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Here's why D is correct, and the other options will not work:

A. Manually generate an API key for each Google service and embed them in your application code. This is not recommended because it is less secure – anyone with access to the code could potentially misuse the API keys. Moreover, embedding API keys within the code violates the principle of separating the concerns (credentials and code). Google also doesn't recommend using API keys for authentication in GCP applications.

B. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application. This is not the best solution because it introduces unnecessary complexity, and deploying

credentials within a config file increases the risk of exposing sensitive information. Google provides automatic authentication mechanisms like Application Default Credentials, which are already used on the development laptop. It's recommended to stick to this approach, making the transition to the Compute Engine VM easier and secure.

C. Grant access to Google services by adding Compute Engine VM's external IP to the allowed list of API clients. This is not an adequate solution, as it requires making your VM accessible publicly, which introduces potential security risks. Also, this method doesn't provide fine-grained access control for individual application components and users, making it challenging to manage in a production environment.

D. Assign appropriate access for Google services to the service account used by the Compute Engine VM. This is the correct answer because it leverages Google's recommended practices for authentication in GCP applications. By assigning the required permissions to the service account associated with the VM, your application will automatically inherit these permissions and securely access Google services. As the application already utilizes Application Default Credentials, this approach only needs minor adjustments, like verifying the VM's service account has the necessary access. This method is the most secure and the least complex option.

Solution to Question 11: C

The correct answer is C. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

Option C is the best solution because it directly addresses both requirements by setting up organization policy constraints. By enforcing a constraint that allows service account keys to have a maximum lifetime of 24 hours, it ensures that the keys are short-lived. Additionally, it denies service account key creation, except in the centralized project pj-sa, satisfying the centralization requirement.

Option A is not optimal because it involves rotating service account keys every hour using Cloud Scheduler and Cloud Function, which is not cost-effective and doesn't meet the requirement of 24-hour validity. Also, using WordPress Cronjobs is irrelevant and does not address the centralization requirement.

Option B is not the best choice because, although it uses Cloud Functions to rotate service account keys daily in pj-sa, it is not as cost-effective as setting an org policy constraint. Moreover, implementing Cloud Functions requires some additional development effort and maintenance.

Option D is not a good solution because allowing service account key creation with no exceptions across all projects contradicts the centralization requirement. Furthermore, using a custom App Engine task runner for rotation adds unnecessary complexity, development effort, and maintenance costs compared to using org policy constraints.

Solution to Question 12: C

The correct answer is C because it ensures that all permissions used in the custom IAM role are at the 'supported' support level, which is necessary for production use. Additionally, setting the role stage to ALPHA aligns with the initial version of the custom role and effectively communicates its status to the team during testing.

Option A is incorrect because using permissions with the 'testing' support level is not appropriate for a production environment. Moreover, setting the role stage to ALPHA is not sufficient if the role permissions are not properly supported.

Option B is incorrect because it also uses permissions with the 'testing' support level, which is not suitable for production use. Furthermore, setting the role stage to GA (General Availability) implies that the custom role is in a stable and ready state, which contradicts this being the initial version and testing phase of the role.

Option D is not appropriate because using permissions with the 'testing' support level is not fit for a production environment. Additionally, the PRE-ALPHA role stage can create confusion among the team members as it is not a standard term in software development for conveying the status of a custom role or component.

Solution to Question 13: B

The correct answer is B, and here's why:

Option B suggests creating a Service of type LoadBalancer that uses the application's Pods as backend, adding an annotation for an internal load balancer type, peering the two VPCs, and configuring the Compute Engine instance to use the created load balancer address. This is the most efficient and seamless way to achieve the desired connection between the GKE application and the Compute Engine instance on separate VPCs.

Option A is not the best choice because it suggests setting the externalTrafficPolicy to Local. This setting is not required for this scenario, and it would expose the LoadBalancer to external traffic, which is unnecessary here.

Option C is not the optimal solution because it requires creating an additional Compute Engine instance as a proxy with two network interfaces connected to both VPCs, leading to a more complicated setup and potentially more management overhead. Additionally, this approach is less efficient than using VPC peering and an internal load balancer.

Option D is not suitable because it suggests exporting GKE cluster's network settings to the gce-network, which is not advised and might lead to unnecessary complications. Moreover, configuring the Compute Engine instance to use the NodePort's address may not be as efficient as using an internal load balancer for managing connections.

In summary, Option B provides the most efficient and least-effort method to

enable communication between the GKE application and the Compute Engine instance on different VPCs, using an internal load balancer and VPC peering.

Solution to Question 14: A

The most suitable cloud-based database for the application's requirements is A. Cloud SQL. Here's why A is the best option and why the others are not:

A. Cloud SQL: Cloud SQL is a fully managed relational database service offered by Google that allows users to set up, manage, and administer PostgreSQL databases in the cloud. It provides strong consistency, fast query execution, and ACID guarantees for multi-table transactional updates, all of which are essential for the particular application mentioned in your use case. Additionally, this service offers an easy migration process for PostgreSQL applications, which will minimize the code changes required and ensure seamless integration.

B. Memorystore: Memorystore is an in-memory data store service that supports Redis and Memcached, both of which are primarily used for caching and are not suitable for multi-table transactional updates with ACID guarantees offered by relational databases like PostgreSQL. While Memorystore may offer fast query performance, it does not provide the strong consistency and ACID compliance, making it a poor fit for this use case.

C. BigQuery Omni: BigQuery Omni is an extension of Google BigQuery designed to analyze data stored across multiple public clouds. It is a data warehouse solution, not a transactional database management system (DBMS), and is designed for analytical workloads rather than operations with stringent consistency and compliance requirements of the given application. Additionally, it does not provide the necessary ACID guarantees for multi-table transactional updates.

D. Bigtable: Bigtable is a NoSQL database solution designed for large and fast-reading workloads that scales horizontally. However, it lacks support for ACID transactions needed in this scenario due to its NoSQL nature, and it does not provide strong consistency required for the application. While it may offer fast query performance, it does not feature native support for PostgreSQL migration, which would require additional work and code changes for seamless integration.

In conclusion, A. Cloud SQL is the most suitable choice for migrating the PostgreSQL application to the cloud, as it meets all requirements such as strong consistency, ACID guarantees, fast queries, and minimal code changes during migration. The other options lack essential features that make them suitable for the given context.

Solution to Question 15: C

The correct answer is C. Expand the CIDR range of the relevant subnet for the cluster.

Explanation:

A. Creating a new region for the GKE clusters is not the solution since the issue is related to the exhaustion of available IP addresses in the current subnet. Changing the region will not solve the IP address problem and can add unnecessary latency and cost.

B. Configuring the clusters to use non-VPC-native (routes-based) network mode would not resolve the issue. This approach is less efficient compared to using VPC-native mode in terms of resource allocation and network security. Additionally, it would still not address the problem with the exhausted IP addresses.

C. Expanding the CIDR range of the relevant subnet for the cluster is the correct solution. It will increase the number of available IP addresses, allowing the GKE clusters to expand with additional nodes when necessary. This approach maintains the advantages of using VPC-native networking while ensuring the availability of necessary resources.

D. Creating a new VPC and setting up VPC peering with the existing VPC would complicate the network infrastructure without solving the IP exhaustion issue. VPC peering allows networks to communicate, but it doesn't address the problem of limited IP addresses in the current subnet. Instead, it introduces a new set of IP addresses in an entirely separate VPC, which is not the desired solution to the problem.

Solution to Question 16: A

The optimal storage solution for this application is A. Cloud Spanner.

Reasons for choosing Cloud Spanner:

1. Scalability: Cloud Spanner is designed to handle large-scale, global applications and can automatically and seamlessly scale as the number of users grows, making it the perfect match for an e-commerce company with millions of users worldwide.
2. Relational Data: Cloud Spanner is a fully managed relational database, which allows you to store and manage customer relational data efficiently. This is key for an e-commerce application where relationships between customers, orders, and products need to be maintained.
3. Global Consistency: Cloud Spanner offers strong consistency, meaning that the data is always up-to-date across all regions, ensuring an accurate and reliable representation of the customer data.
4. Low Maintenance: Cloud Spanner requires minimal configuration changes as the company scales, allowing you to focus more on application development and less on managing the database.

Reasons for not choosing the other options:

B. Compute Engine: Compute Engine is an Infrastructure-as-a-Service (IaaS) solution that provides virtual machines for running workloads. While it does give you the flexibility to create custom applications, it doesn't offer a specific

storage solution built for handling relational data and scaling seamlessly like Cloud Spanner.

C. Bigtable: Although Bigtable is a scalable NoSQL database that can handle massive amounts of data, it's designed for non-relational data storage and doesn't provide the same level of consistency and support for relational data as Cloud Spanner.

D. Cloud Storage: Cloud Storage is an object storage service mainly used for storing and serving unstructured data such as images, videos, or backups. It is not suitable for storing relational data or handling the complex querying and indexing that an e-commerce application needs.

Solution to Question 17: D

The correct answer is D, and here's the explanation:

D. Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.

In this scenario, enabling communication between multiple groups of Compute Engine instances running in two separate GCP projects requires sharing the VPC from one project and allowing the instances in the other project to use it. This can be achieved using Shared VPC, which allows multiple projects within the same GCP organization to use a common VPC. This facilitates effective communication between instances while keeping the VPC management centralized.

Option A is incorrect because configuring a Network Load Balancer for each group of instances and updating the backend configuration to include instances from both projects would not be sufficient to establish all required connections. Load balancers are used to distribute load among multiple instances, while here, the requirement is to enable communication between distinct groups of instances in different projects.

Option B is incorrect because creating a new Shared VPC with all instances from both projects would recreate the current setup and does not effectively resolve the issue. Migration would involve downtime and would not enable easy communication between Compute Engine instances hosted in their own VPCs within other projects.

Option C is incorrect because merely verifying that both projects are in a GCP Organization and creating a new VPC does not enable traffic between existing groups of Compute Engine instances. The new VPC must be shared across projects, and existing instances should be part of the shared VPC to establish the desired communication channel.

Therefore, the best choice is Option D, where you verify that both projects are in a GCP Organization, share the VPC from one project, and request that the Compute Engine instances in the other project use this shared VPC. This

will enable traffic between the groups of Compute Engine instances in the two separate projects.

Solution to Question 18: D

The answer should be D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

Here's why the other options are incorrect:

A. Use the gcloud command-line tool to update the existing App Engine application region to asia-northeast1. - This option is not feasible because once an App Engine application is created and its region is set, it cannot be changed. Google Cloud Platform documentation explicitly states that "you cannot change an app's region after you set it."

B. Create a Cloud Function in the existing GCP project, specifying asia-northeast1 as the region, and use it to proxy requests to the App Engine application. - While this option would technically place a part of the architecture in the asia-northeast1 region, it would not change the fact that the App Engine application itself is still served from the us-central region. It would only add an intermediary proxy which might increase latency and complexity, rather than directly serving the application from the desired region.

C. Update the us-central region settings in the existing App Engine application to enable multi-region support including asia-northeast1. - This would not work because App Engine does not currently offer multi-region support to automatically serve the application from different regions. App Engine Standard Environment applications must be specifically created in a single region, and that region cannot be changed after creation.

Therefore, the correct choice is D, which ensures that your App Engine application is served directly from the desired region (asia-northeast1) while still complying with the platform's restrictions on region selection. Although creating a new project incurs some overhead, it is the most direct and efficient way to resolve the given issue.

Solution to Question 19: B

The correct answer for setting up a notification when the monthly egress network costs exceed 100 dollars is option B. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

Here's why option B is the correct choice and the other options don't fit the requirement:

Option A: While configuring a Google Cloud Monitoring agent helps in monitoring egress network costs, relying on manual hourly reviews of the dashboard is not as efficient as automating the process. Additionally, there's a possibility of human error in assessing the costs, making this option less effective.

Option B: This option aligns with the desired outcome of receiving an email when the egress costs exceed 100 dollars by automating notifications through Cloud Functions. By using BigQuery, you can accurately track the egress network costs specifically for the Apache web server running on a Compute Engine instance, and Cloud Scheduler allows the Cloud Function to run hourly, thereby actively monitoring costs throughout the month. This method is efficient and precise, making it the best choice.

Option C: Although this option uses Cloud Functions and Pub/Sub for automation, it does not provide a practical method to accurately track egress costs specifically for the Apache web server in a project running multiple applications. It lacks the granularity and accuracy needed for this requirement.

Option D: Setting up a budget alert on the project level will notify about the overall project costs instead of focusing solely on the Apache web server's egress network costs. This option will not isolate the specific egress costs associated with the Apache web server, and therefore will not accurately address the requirement.

Solution to Question 20: C

The best approach to ensure the application runs smoothly in a similar GCP environment is option C: When creating the VM, use machine type n1-standard-96.

Option C is the most suitable solution because n1-standard-96 is a predefined machine type on Google Cloud Platform that comes with 96 vCPUs, which is the exact number required for optimal performance of the critical on-premises application. By using this machine type, you can ensure that the application has the appropriate resources to run smoothly on GCP without additional adjustments.

Option A, adjusting the VM's vCPU configuration after its creation using the GCP Console, can cause unnecessary downtime and potential complications. It requires turning off the VM instance and manually changing its configuration. Also, this doesn't guarantee that the right vCPU settings will be applied, which can lead to suboptimal performance.

Option B, starting the VM using Compute Engine default settings and adjusting as you go based on Rightsizing Recommendations, is not the best approach either. You might need to make multiple adjustments before achieving optimal performance, which can be time-consuming and costly. Furthermore, default settings for the VM might not provide the desired vCPU configuration needed for the application, resulting in ineffective resource allocation.

Option D, using the custom machine type with 48 vCPUs and increasing the number of VM instances to 2, is not as efficient as using n1-standard-96. By dividing the workload between two VM instances, you would add complexity to your setup, increase the risk of performance issues, and add management overhead. There is no reason to do this when n1-standard-96 already provides the exact number of vCPUs needed for optimal performance.

Therefore, the best approach to ensure the application runs smoothly in a similar GCP environment is to choose option C: When creating the VM, use machine type n1-standard-96.

Solution to Question 21: B

The correct answer is B. In this approach, you create a separate configuration for each project you need to manage, and then activate the appropriate configuration when working with each of your assigned Google Cloud projects. This is the most efficient method since it allows you to directly manage multiple projects by only swapping configurations with minimal steps. This can be achieved using the 'gcloud config configurations create' and 'gcloud config configurations activate' commands.

Option A is not efficient since creating multiple Google Cloud accounts for different projects would lead to unnecessary account management overhead and fragmentation of resources. Also, using 'gcloud init' each time you need to switch projects will take longer as you will need to authenticate every time.

Option C is not a good solution as it requires you to continually change the project ID within the configuration file whenever you need to switch projects. This manual approach is error-prone and time-consuming for a software engineer who needs to manage multiple projects.

Option D is even less efficient, as it involves creating separate installations of the Google Cloud SDK for each project. This not only takes up valuable system resources but also requires creating and managing alias commands to switch between projects, resulting in increased overhead and complexity.

Therefore, option B is the recommended approach for managing multiple Google Cloud projects with minimum steps using the Google Cloud SDK CLI.

Solution to Question 22: A

The correct answer is A. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

Explanation for A: BigQuery can seamlessly read external AVRO files stored in a Cloud Storage bucket, which allows you to create tables without importing the data into BigQuery. This approach is cost-effective and efficient as it avoids unnecessary data duplication and transformations. Moreover, BigQuery handles querying large datasets efficiently and is familiar to SQL users.

Reasons why other options are not suitable:

B. Using Google Data Prep to transform the AVRO file into a CSV file and then importing it into Cloud SQL is not efficient and consumes additional resources. Transforming the data adds extra steps and requires more time. Also, Cloud SQL is better suited for transactional workloads rather than analytical queries on large datasets like the 5-TB AVRO file.

C. Configuring Cloud Dataflow to read the AVRO file and write the data into Cloud Firestore for SQL querying adds extra processing time and costs. Cloud Firestore is a NoSQL Firestore, not specifically designed for analysts proficient in SQL. Although it supports SQL-like queries, it is not the best solution for their needs and handling a large dataset may result in performance issues.

D. Loading data into Cloud Datastore and running a SQL query against it is not an ideal solution because Cloud Datastore is a NoSQL database, not specifically built for SQL querying and analytical purposes. Additionally, it might not handle the 5-TB data efficiently, and the performance of SQL-like queries may not be suitable for the analysts' requirements.

Solution to Question 23: C

The correct answer is C, "After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM." The reasoning behind this choice is that the gcloud compute compute reset-windows-password command generates a new Windows Administrator account and a corresponding password, which can be used for future RDP access. This is the appropriate method for obtaining login credentials for Windows VMs on Google Cloud Compute Engine.

Option A is incorrect because gcloud compute ssh is used for SSH access to Linux VMs and does not provide RDP login credentials for Windows VMs.

Option B is incorrect because while you can generate an RDP file using the Google Cloud Console, using your Google Account credentials would not grant access to the Windows VM. RDP requires Windows Administrator username and password, which you can retrieve using Option C.

Option D is incorrect because although adding a firewall rule to allow RDP traffic is an essential step, it doesn't provide the necessary login credentials for remote access. You still need to use the gcloud compute reset-windows-password command to obtain those credentials.

Solution to Question 24: A

The correct answer is A. Use folders to group resources that share common IAM policies.

Explanation: When working as an IT consultant for a company in the finance industry, it is essential to create a well-organized Google Cloud Infrastructure in order to efficiently manage resources and permissions. In this scenario, creating

folders to group resources sharing common IAM policies will help you achieve the customer's desired outcome.

Folders are a powerful tool in the Google Cloud Platform resource hierarchy, as they allow you to logically group resources, apply blanket IAM policies, and enforce organization-wide constraints. By using folders to group resources with common IAM policies, you can create a clean structure to manage access and permissions more effectively.

Options B, C, and D are not the best choices for achieving the desired outcome:

B. Use labels to group resources that share common IAM policies

Labels are meant to be used as metadata to help identify, filter, and organize resources based on various factors such as the environment (e.g. staging or production), teams, or projects. While they can be useful for categorizing resources, they are not designed for grouping resources based on IAM policies and cannot enforce those policies.

C. Use VPC peering to connect resources sharing common IAM policies

VPC peering is a networking connection between two VPCs that enables private communication between resources in those VPCs. VPC peering is typically used to minimize latency, provide redundancy, and improve security. However, it is not a solution for organizing resources based on IAM policies, as its purpose is to facilitate connectivity between VPCs rather than managing access control.

D. Set up a proper billing account structure to group IAM policies

A billing account structure in Google Cloud is used to manage payment information, assign user roles related to billing, and allocate costs to various projects. While setting up an organized billing account structure is important, it is not directly related to organizing resources based on IAM policies. It is more focused on billing management and cost allocation rather than enforcing access control and organizing resources.

Solution to Question 25: B

The correct answer is B. Storage Admin, and here's why:

In the context of a software development company that needs to manage buckets and files in Google Cloud Storage, it's crucial that the appropriate IAM roles are assigned to the team members involved. Following Google-recommended practices, the roles should enable efficient management of the Cloud Storage resources while maintaining strong access controls and security.

B. Storage Admin is the most appropriate choice for the following reasons:

1. It provides a comprehensive set of permissions for managing Cloud Storage resources, including creating, listing, and configuring buckets, as well as managing objects within those buckets.

2. It adheres to Google's principle of least privilege, ensuring that team members are granted just the right amount of access necessary to complete their tasks without risking security breaches.

Let's examine why the other options are not suitable:

A. Spanner Admin: This role is designed for managing Google Cloud Spanner databases and resources. It does not provide the necessary permissions for managing Cloud Storage buckets or objects and is not relevant for the task at hand.

C. Storage Object Admin: Although this role does grant permissions for managing objects within Cloud Storage buckets, it does not include permissions to manage buckets themselves (e.g., creating, updating, or deleting buckets). This limited scope makes it inadequate for providing comprehensive control over the Cloud Storage resources.

D. Pub/Sub Admin: This role is meant for managing Google Cloud Pub/Sub resources, which deal with messaging and event notification services. It's not focused on Cloud Storage and doesn't provide the required permissions for managing buckets and files in Cloud Storage.

In conclusion, the Storage Admin role (Option B) offers the ideal balance of control and security for managing Cloud Storage buckets and objects, making it the best choice for delegating access to your team members according to Google-recommended practices.

Solution to Question 26: B

The correct answer is B: Deploy the container on Cloud Run.

Explanation:

B: Deploy the container on Cloud Run is the best choice for this scenario because Cloud Run allows you to run stateless containers and is designed to automatically scale with the number of requests. It can scale down to zero when there are no requests, which helps in minimizing costs. Additionally, Cloud Run only charges you for the time your code is actually running, making it a more cost-efficient option for a low-usage, stateless application like the one described in this question.

Now, let's analyze why the other options are not suitable for this scenario:

A: Deploy the container on Cloud Build with Triggers is not an ideal choice for deploying an application. Cloud Build is a service primarily used for building and packaging applications into container images. It is not designed to run long-lived applications or to handle request-based scaling.

C: Deploy the container on Dataproc with auto-scaling enabled is not a good fit for this use case because Dataproc is a fully managed service for running Apache Spark and Apache Hadoop clusters. It is designed for big data processing

and is not optimized for running containerized applications that expose HTTP endpoints.

D: Deploy the container on Kubernetes Engine with Vertical Pod Autoscaler might be a viable option, but it can be more expensive than Cloud Run due to the management overhead associated with running a Kubernetes cluster. In addition, the Vertical Pod Autoscaler automatically adjusts the CPU and memory resources allocated to the Pods, which is not necessary for an application with a few requests per day. Cloud Run is more cost-effective and easier to manage for such a low-usage application.

Solution to Question 27: D

The correct answer to this question is D: Configure an External Network load balancer in front of the application servers. The primary reason for choosing this option is that the game uses UDP packets for communication during multiplayer sessions. An External Network load balancer is ideal for situations where a virtual service consists of multiple VMs and requires efficient use of a single IP address.

External Network load balancers support connectionless protocols such as User Datagram Protocol (UDP), making them the best choice in this scenario. They distribute the traffic across multiple VMs, helping to keep the game functioning smoothly even in high-traffic scenarios.

Now, let's analyze why the other options are not suitable:

A. Utilize VPC peering for load balancing between VMs.

VPC peering is used to connect two Virtual Private Clouds (VPCs) and route traffic between them as if they were within the same network. This option is not suitable for this scenario because the primary goal is to distribute traffic across multiple VMs and expose a single IP address, which VPC peering does not provide.

B. Configure an External TCP Proxy load balancer in front of the application servers.

TCP Proxy load balancers handle traffic coming in via the Transmission Control Protocol (TCP) protocol. Since the game utilizes UDP packets, a TCP Proxy load balancer would not be appropriate for this case.

C. Configure a Cloud CDN in front of the application servers.

Cloud CDN (Content Delivery Network) is used to cache static content in edge locations closer to the users, decreasing latency and response time. While this might help the performance of some parts of the game, it does not address the main issue of load balancing UDP traffic across multiple VMs and exposing a single IP address for access.

In conclusion, the best action to take in this situation is D: Configure an External Network load balancer in front of the application servers, as it directly meets

the requirements of handling UDP packets and allows for efficiently exposing a single IP address for multiple VMs.

Solution to Question 28: C

The correct answer is C.

Here's the explanation for the correct answer:

C. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

The reason option C is the correct answer is because it follows the correct sequence of required steps to accomplish the task. First, you need to create the new project using the Cloud SDK, which will provide you with a new project ID to be used for further operations. Then, you must enable the Compute Engine API specifically for this new project. Finally, with the API enabled, you can proceed to create the Compute Engine instance in that project using the Cloud SDK.

Now let's see why the other options are incorrect:

A. Enable Kubernetes Engine API in the Cloud Console, and then use the Cloud SDK to create a Compute Engine instance specifying the new project.

This option is incorrect because Kubernetes Engine API is different from Compute Engine API. Kubernetes Engine is a container orchestration service, while Compute Engine provides virtual machines. Enabling the Kubernetes Engine API will not help you create a Compute Engine instance.

B. Enable the Firestore API in the Cloud Console, create a new project, and then use the Cloud SDK to create a Compute Engine instance.

This option is incorrect because enabling the Firestore API is not related to creating a Compute Engine instance itself. Firestore is a document database service, whereas Compute Engine provides virtual machines. Therefore, enabling Firestore API will not help you create a Compute Engine instance.

D. Enable the Compute Engine API in the Cloud Console. Go to the Compute Engine section of the Console to create a new instance, and look for the Create In A New Project option in the creation form.

This option is incorrect because there isn't an option to create a new instance in a new project directly from the creation form in the Compute Engine section of the Cloud Console. You have to create the project first and then enable the Compute Engine API for that project before creating the instance.

Solution to Question 29: C

The correct answer is C. Here's why:

A. Using `gcloud container clusters resize` to add n2-highmem-16 nodes is incorrect. This command resizes the number of nodes in a particular node pool,

but does not allow you to specify a new machine type. Consequently, you'll still be running the additional pods on n1-standard-2 nodes, instead of the required n2-highmem-16 nodes.

B. Using `gcloud container clusters set-machine-type` to change the node type to n2-highmem-16 is incorrect as well. This method will cause downtime because it updates the existing nodes in the cluster. Besides, you only want to add new pods with the n2-highmem-16 machine type, rather than changing the machine type for the existing nodes and pods.

C. Creating a new Node Pool and specifying machine type n2-highmem-16 is the correct solution. This allows you to maintain your existing application with the current nodes (n1-standard-2) while also adding a new node pool, which runs the additional pods on the more powerful n2-highmem-16 nodes. This method ensures there's no downtime for your application.

D. Using Kubernetes horizontal pod autoscaling with machine type n2-highmem-16 during deployment is incorrect. Horizontal pod autoscaling adjusts the number of pods based on CPU and memory utilization, but it does not allow you to specify a particular machine type for those pods. The n2-highmem-16 node requirement will not be taken into account, leading to insufficient resources for the new pods.

Solution to Question 30: C

The correct answer is C. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

Option C is the best choice because it fulfills all the requirements of a secure website with autoscaling based on compute instance CPU load and enhancing performance by storing static content in Cloud Storage. An external HTTP(S) load balancer provides efficient distribution of user traffic, while a managed SSL certificate ensures secure connections. A URL map is used to target requests for static content to the Cloud Storage backend, which allows for better performance.

Option A is not correct because it only uses an external HTTP load balancer and SSL proxy. While the use of an SSL proxy can provide a secure connection, it lacks the simplicity and usability of a managed SSL certificate. Moreover, it does not specifically mention handling HTTP(S) traffic, which is crucial for ensuring a secure web experience.

Option B is not suitable because it involves using an internal HTTP(S) load balancer and Identity-Aware Proxy. Internal load balancers are not designed for distributing user traffic; they are used for managing internal traffic within a Virtual Private Cloud (VPC) network. Additionally, Identity-Aware Proxy is not required here, as its primary function is to control access to applications based on user identity and context, not handling traffic distribution.

Option D is incorrect because it uses an internal TCP/UDP load balancer, which is designed for load balancing non-HTTP(S) traffic. This load balancer would not be sufficient for a secure website and user traffic distribution. Furthermore, while a managed SSL certificate is mentioned, it is not compatible with internal TCP/UDP load balancers.

In conclusion, the best choice for efficient distribution of user traffic in a secure website with autoscaling based on the compute instance CPU load and enhanced performance through storing static content in Cloud Storage is Option C: An external HTTP(S) load balancer with a managed SSL certificate and a URL map to target the requests for the static content to the Cloud Storage backend.

Solution to Question 31: D

The correct answer is D.

Explanation:

In this situation, the goal is to ensure cost-effective recommendations for CPU and memory requirements while maintaining consistent performance. This can be achieved by following Google-recommended practices to properly configure Horizontal Pod Autoscaler (HPA) and Vertical Pod Autoscaler (VPA).

Option D suggests configuring HPA for availability and VPA for recommendations, which is the ideal approach. HPA can be configured to maintain the desired level of availability by automatically scaling the number of pods replicas based on observed CPU utilization, ensuring consistent performance as the application's resource requirements vary. Meanwhile, VPA can provide recommendations for updating the container's CPU and memory requests and limits, taking into account historical usage patterns and other factors. Together, this approach optimizes the resource utilization while maintaining consistent performance.

Option A is incorrect because it swaps the roles of HPA and VPA. Configuring VPA for availability and HPA for recommendations would not make proper use of their respective features, leading to suboptimal results.

Option B is also incorrect because it misconstrues the primary purpose of HPA and VPA. Configuring the HPA for cost optimization instead of availability can lead to performance issues as the number of pod replicas is not adapted to handle varying resource requirements. Additionally, configuring VPA for availability rather than recommendations also doesn't make the best use of VPA's capabilities.

Option C is incorrect because it leaves out the VPA, which is essential for providing recommendations on CPU and memory requirements. Instead, it suggests configuring the cluster autoscaler for suggestions, which primarily focuses on optimizing the number of nodes in a cluster, not individual containers' resource requirements.

In conclusion, the best choice is option D, which ensures cost-effective recommendations for CPU and memory requirements and maintains consistent performance by properly configuring HPA for availability and VPA for recommendations.

Solution to Question 32: A

The correct approach to achieve isolated environments for Cassandra instances on Google Cloud is A. There are several reasons why other options are not the best choice.

A. The reasons to choose A are: - Cloud Marketplace offers preconfigured and optimized database images, including Cassandra, which will speed up the deployment for development work. - By using Cloud Marketplace, developers can quickly and easily create required isolated environments with Cassandra instances on Google Cloud without additional setup or management overhead.

B. Option B is not ideal because: - Cloud Dataproc is specifically designed for big data processing and analytics using Hadoop and Spark, not for managing databases like Cassandra. - It would require more manual configuration and setup to run Cassandra on a Cloud Dataproc cluster, which increases complexity and may impact agility and developer productivity.

C. Option C is not the best choice due to the following reasons: - Managed instance groups are designed for automatically managing groups of homogeneous instances, not for providing isolated environments for separate development projects. - VPC Network Peering is designed for connecting separate Virtual Private Cloud networks, not for isolating individual development teams' work on database instances.

D. Option D would not be the best approach because: - Taking a snapshot of a Compute Engine instance, uploading it to Cloud Storage, and providing instructions for developers to create instances from the snapshot adds extra complexity and steps, which can slow down the required speed of deployment. - This option may lead to potential consistency issues as every developer creates their own Cassandra instance manually, and keeping snapshots updated can become an additional burden.

Solution to Question 33: A

The correct answer is A. Use gcloud to create a key file for the service account that has appropriate permissions.

Explanation for answer A: Using gcloud to create a key file for the service account with proper permissions is the correct approach because service accounts are used for authenticating applications, not users. With a key file, your on-premises application will be able to authenticate API calls to Google Cloud Platform services, such as AutoML, using the service account's credentials, without having to share or expose the service account itself. This ensures secure and granular access to GCP services.

Why other options will not work:

Option B: Setting up a direct interconnect between your data center and Google Cloud Platform might provide a dedicated and low-latency network connection, but it does not inherently enable or address authentication for your on-premises applications. Authentication is a separate process that requires service account credentials and a key file as explained in option A.

Option C: Creating an API key and using it for authentication from your on-premises application is not recommended because API keys do not provide the same level of security and access control as service accounts. API keys are less secure, cannot be scoped to specific permissions, and can be easily exposed, leading to potential unauthorized access or abuse of your GCP services.

Option D: Using service account credentials directly in your on-premises application is insecure and not recommended. Exposing sensitive service account credentials in your application can lead to unauthorized access, while also making it difficult to manage updates and revocation. It is a better practice to create a key file associated with the service account, as explained in option A, to ensure better security and management of permissions without compromising the service account information.

Solution to Question 34: B

The correct answer is B because it accurately describes the process of finding when a specific Google Cloud Platform service account was created.

To achieve this, you'll need to: 1. Filter the Activity log to view the Configuration category: The Configuration category in the Activity log stores logs for any account- or resource-level changes, such as the creation or deletion of a service account. This allows us to pinpoint the exact time when the service account was created. 2. Filter the Resource type to Service Account: You want information about the service account, so filtering the resource type to service account ensures that the logs displayed only contain information about service accounts.

The other options are incorrect for the following reasons: A. Viewing the Networking category in the Activity log would show logs related to networking resources, not service accounts. It would be irrelevant to this task. C. Filtering the Audit logs for Configuration category is the correct step, but you need to filter by service account, not Compute Engine resource type, as your goal is to find the creation time of a service account. D. Filtering the Resource type to BigQuery would show logs related to BigQuery resources, not service accounts. It would not help you determine when a specific service account was created.

Solution to Question 35: B

The correct answer is option B: Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

By deploying the container on Cloud Run (fully managed) and setting the minimum number of instances to zero, you ensure that no instances are running outside of the application's operational hours as instances will automatically scale to zero when they are not in use. This helps you minimize costs and prevent any expenses outside of the application's operational hours, as you will only pay for the actual usage and execution time of the container instances.

Here is why the other options will not work:

Option A: Creating a Cloud Scheduler job to start and stop the Cloud Run (fully managed) service according to the business hours would not guarantee that there would be no expenses outside of the application's operational hours. Additionally, starting and stopping the service may introduce wait times for users during the start-up/shutdown periods.

Option C: Creating a cloud monitoring alert to notify you when the application is used outside of business hours and manually stopping it still results in costs generated by usage outside of business hours. This approach also adds manual intervention and response time, making it less efficient than an automatic solution.

Option D: Deploying the container on Cloud Run for Anthos and setting the minimum number of instances to zero would run the container on Kubernetes clusters, which will result in additional management overhead, complexity, and costs that are not necessary for your internal web application. Cloud Run (fully managed) is more appropriate for this use case as it provides an automatically scaling, serverless infrastructure.

Solution to Question 36: B

The correct answer is B. Set Content-Type metadata to application/pdf on the PDF file objects.

Option A is incorrect because the multi-regional storage class is mostly used for providing better data redundancy and global access to the files. It does not have a direct impact on how the browser would display or handle the PDF files.

Option B is correct because setting the Content-Type metadata on the PDF file objects to "application/pdf" will tell the browser to display the file using an embedded PDF viewer instead of prompting the user to download and save the file. This is the change needed to achieve the desired behavior.

Option C is incorrect because moving from Cloud Storage to Firebase Hosting is a significant change to your application architecture and will only serve your static website content, not address the specific issue of displaying PDFs in the browser without prompting the users to save them.

Option D is incorrect because configuring the caching policy is related to how often and how long the browser stores a cached version of the website's content. It has no direct effect on how the browser displays the PDF files in the browser.

Solution to Question 37: A

The best choice in this scenario to optimize performance is option A - Provision Compute Engine instances with M1 machine type.

Option A is suitable because the M1 machine type, specifically the "M1 Ultramem" in Google Cloud, is designed for memory-intensive workloads that require vast amounts of memory for rapid data access. The M1 Ultramem offers up to 12 TB of RAM and can host in-memory databases, such as the one required by the ERP system, ensuring high performance and low latency for data processing.

Option B - Deploy the application on Kubernetes Engine with memory-optimized nodes - is not the best choice as Kubernetes Engine is primarily meant for container orchestration and might not provide the desired level of performance for an in-memory database. Moreover, Google Cloud's memory-optimized nodes do provide additional memory compared to other node types, but they might still not offer the same scale and performance as M1 machine types.

Option C - Use a Cloud Spanner instance for in-memory database handling - is not ideal because Cloud Spanner, while providing a highly reliable and scalable database solution, is not specifically designed for in-memory data processing. Additionally, its primary focus is on providing horizontal scalability with transactional consistency, which might not be the main requirement of the ERP system in this scenario.

Option D - Use Cloud Datastore with high read/write throughput - would not be the best choice as Cloud Datastore is a NoSQL database designed for web and mobile applications. While it offers great performance for read/write operations, it is not specifically designed for in-memory data processing, which would mean sacrificing some of the ERP system's performance requirements.

In conclusion, option A - Provision Compute Engine instances with M1 machine type - is the most suitable option for deploying the new ERP system on Google Cloud, as it ensures that the necessary in-memory database requirements are met, optimizing the system's overall performance.

Solution to Question 38: B

The correct answer is B. Add your SREs to a group and then add this group to roles/accessapproval.approver role. This is because the goal is to allow the SREs to approve requests from the Google Cloud support team when they open a support case while adhering to Google-recommended best practices.

By adding the SREs to a group and then assigning the group to the roles/accessapproval.approver role, you are following the best practice of managing permissions through groups rather than granting them directly to individual users. This setup also ensures that your SREs will have the ability to approve access requests from Google Cloud support when needed.

The other options will not work for the following reasons:

A. roles/bigquery.admin role is not relevant to granting access approval permissions. This role focuses on managing BigQuery resources, and it does not allow SREs to approve access requests for support cases.

C. While adding SREs to roles/accessapproval.approver role might also enable the functionality, it is not recommended to grant permissions directly to users. Following the best practice of managing permissions through groups is better for long-term permission management and security.

D. roles/cloudsql.admin role is also not relevant in this scenario. This role focuses on managing Google Cloud SQL resources rather than granting access approval permissions for support cases.

Solution to Question 39: A

The correct answer is A: Enable parallel composite uploads using gsutil on the file transfer.

Explanation for A: Parallel composite uploads using gsutil allow you to upload large files more rapidly by splitting the file into smaller chunks and uploading those chunks concurrently. Given that you have exclusive access to the 1 Gbps WAN connection at the office, enabling parallel composite uploads will allow you to fully utilize the available bandwidth and transfer the 32 GB single file as quickly as possible.

Reasons why other options will not work:

B. Using the GCP Console to create a new instance and then transferring the file using gsutil would not necessarily speed up the transfer. While it's true that you can transfer files using gsutil, creating a new instance would add additional steps and does not directly relate to speeding up the upload process when you already have exclusive access to the office's 1 Gbps WAN connection.

C. Decreasing the TCP window size on the machine initiating the transfer is counterproductive. The TCP window size determines how much data can be sent before receiving an acknowledgment, and reducing it would result in sending less data at once, leading to more acknowledgments and potentially slower transfer speeds. To maximize upload speed, you should maintain or even increase the TCP window size.

D. Disabling resumable uploads in gsutil would not help to transfer the file faster. Resumable uploads are a feature that allows the transfer process to resume from where it left off in case of interruptions, but it does not directly affect the speed of the transfer. In fact, disabling resumable uploads might result in a slower transfer in case of any interruptions, as the entire process would need to start over from the beginning.

Solution to Question 40: C

The correct answer is C. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the

same name as instance names.

Explanation: The issue faced by the managed instance group, which is not able to create new instances, is most likely caused by incompatible naming conventions that prevent instance creation. Persistent disks having the same name as instance names can cause instance creation to fail. To resolve this problem, you must create a new instance template containing valid syntax and ensure there are no persistent disks with the same instance names.

Reasons for eliminating other options:

A. While this option suggests creating an instance template with valid syntax, it does not address the issue of deleting persistent disks that have the same name as instance names. This step is crucial to ensure the problem is resolved.

B. Verifying that the instance template contains valid syntax is important, but increasing the instance count of the managed instance group will not solve the problem of the instance creation failure. The issue of naming conflicts between instance names and persistent disk names is not addressed in this option.

D. Checking the permissions of the service account is not relevant to the instance creation failure in this case. While verifying that the instance name and persistent disk name values are not the same in the template is a good step, it is not sufficient to resolve the problem. Deleting any persistent disks with the same name as instance names is also necessary to ensure a smooth instance creation process.

Solution to Question 41: A

Answer: A. Use the command gcloud projects get-iam-policy to view the current role assignments.

Explanation:

Option A is the correct answer because it directly addresses the requirement of finding out who has been granted the Project Owner role. The gcloud projects get-iam-policy command is used to fetch the IAM policy associated with a given project. The output displays the role assignments for the project, including the Project Owner role. By checking the role assignments listed in the output, you can easily determine who has been granted the Project Owner role in the project.

Option B is not suitable because Identity-Aware Proxy (IAP) is used for controlling access to applications running on Google Cloud Platform based on user identity and group membership, rather than focusing on managing project-level roles like Project Owner.

Option C is not helpful for finding the Project Owner role assignment specifically. The gcloud organizations list command will display the organizational hierarchy and its related information, but you will still need to view the associated IAM policy using a separate command to check the role assignments.

Option D is incorrect because the Firebase Console focuses on managing Firebase projects and their associated authentication methods (e.g., email/password, social logins, etc.). It does not handle the Project Owner role in the context of Google Cloud Platform IAM policies.

Solution to Question 42: B

The correct answer is B: gcloud deployment-manager deployments update –config .

Here's why:

A) gcloud deployment-manager resources update –config

This option is incorrect because the 'resources update' command is used to update individual deployment resources rather than an entire deployment. In this scenario, we need to update the entire deployment to roll out the changes without causing any resource downtime.

B) gcloud deployment-manager deployments update –config

This option is correct because it updates an existing deployment using the specified configuration file. The 'deployments update' command replaces the current running configuration with the new one while preserving the resources, ensuring there's no downtime during the update process. This is what we need to achieve the project task.

C) gcloud deployment-manager deployments describe –config

This option is incorrect because the 'describe' command only provides information about an existing deployment, like its configuration and resource details. It doesn't make any updates to the deployment itself.

D) gcloud deployment-manager deployments list –config

This option is incorrect because the 'list' command is used to display a list of all deployments in the project, but it doesn't modify or update any deployments. Therefore, it isn't suitable for the task described.

Solution to Question 43: B

The correct answer is B: Enable Private Google Access on the subnet within the custom VPC.

Explanation: Enabling Private Google Access allows VM instances with only internal IP addresses to reach Google APIs and services, such as Cloud Storage, using a dedicated private network connection instead of the public internet. This adheres to the company's security policies that mandate using internal IP addresses and prohibits VM instances from connecting to the internet, while still providing access to files hosted in a Cloud Storage bucket.

Reasons why other options will not work:

A: Configuring a custom IAM policy would be required for granting appropriate permission to access the Cloud Storage bucket, but this alone would not fulfill the requirement to prevent VM instances from connecting to the internet or using internal IP addresses only.

C: Configuring a Load Balancer is not necessary in this situation, as the purpose of a Load Balancer is to distribute incoming network traffic across multiple VM instances, while the requirement here focuses on providing non-public access to Cloud Storage. Load Balancers generally do not route traffic or provide access between VM instances and Cloud Storage buckets directly.

D: Adding storage.googleapis.com to the list of restricted services in a VPC Service Controls perimeter and adding your project to the list of protected projects would restrict access to Cloud Storage, but it would not provide a solution for using internal IP addresses to access Cloud Storage without public internet connectivity. Private Google Access would still be needed to meet the security policy requirements.

Solution to Question 44: C

The correct approach is option C: Use gcloud to create the new project, and then deploy your application to the new project.

Option C is the most appropriate choice since using the Google Cloud SDK (gcloud) provides a powerful command-line interface to manage and deploy your Google Cloud Platform (GCP) projects in a more automated, streamlined, and efficient manner. In this case, your team can use gcloud for creating the new project as well as for deploying the App Engine application to the new project. This method will ensure that the production-related configurations are also applied correctly, minimizing the risk of errors or inconsistencies.

Option A (Clone the existing project using the GCP Console and use the same deployment settings) is not suitable, as cloning will carry over all the configurations from the previous project, which may not be relevant or required in the production environment. Moreover, this method can lead to configuration-related issues, creating inconsistencies and potential discrepancies between the development and production environments.

Option B (Use the GCP Console to create a new project, and then manually copy the source code of the App Engine application) is not ideal because manually copying the source code increases the possibility of human errors and can be more time-consuming. Modern continuous integration and deployment methodologies advocate for automation and minimizing manual intervention as much as possible. This approach goes against best practices and is less efficient compared to option C.

Option D (Use Cloud Shell to create the new project, and then deploy your application to the new project) may seem like an acceptable choice; however, it is less favorable than option C. Cloud Shell is a shell environment for GCP and is not specifically focused on creating and managing new projects. Using the

gcloud command-line tool to create and deploy the application will streamline your workflow, allow for scripting, repeatable processes, and provide more control over your deployments. Therefore, option C is the best choice among the given options.

Solution to Question 45: A

The correct answer is A. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

Explanation for answer A: Enabling the necessary APIs for Compute Engine and Cloud Storage separately is accordance with Google's recommended best practices. This step helps ensure you have the required permissions and services for your tasks, such as creating instances, configuring firewalls, and storing data in Cloud Storage. By performing these commands, you are explicitly enabling the required APIs for your project.

Reasons why other options will not work:

B. Enabling only the cloudresourcemanager.googleapis.com API and assuming that it will automatically enable Compute Engine and Cloud Storage APIs is incorrect. The Cloud Resource Manager API is used to manage resources such as projects, folders, and organizations, but it does not automatically enable other APIs. You need to enable the Compute Engine and Cloud Storage APIs separately, as given in option A.

C. Using the gcloud CLI command to create instances, set firewall rules, and store data in Cloud Storage without enabling the necessary APIs is not recommended. If you don't enable the required APIs, you might encounter errors or issues when trying to execute these tasks. By enabling the APIs first, you ensure that your project has the necessary permissions and services for your tasks.

D. Opening the Google Cloud console and running gcloud init –project in a Cloud Shell is incorrect. The gcloud init command is used to initialize, configure, and authorize your gcloud CLI instance, but it doesn't enable specific APIs for your project. You still have to enable the required APIs for Compute Engine and Cloud Storage separately using the gcloud services enable commands, as mentioned in option A.

Solution to Question 46: D

The correct answer is D. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

Explanation:

Option D is the best choice as it allows you to efficiently manage and archive data based on versions. A bucket lifecycle rule for archiving data with newer versions after 30 days to Nearline Storage ensures that you are only archiving the appropriate data after the necessary time frame – 30 days in this case.

Additionally, Nearline Storage is cost-effective for storing infrequently accessed data, which is the case here: previous versions have to be accessed once a month for reporting purposes and occasional updates. Nearline Storage also offers lower storage costs than multi-regional and regional storage classes while still providing the data retrieval capabilities needed for your requirements.

Options A and B are not the best choices because they do not take into account the multiple versions of the data, which is a requirement stated in the question. Simply moving data from multi-regional or regional storage to Nearline Storage without considering the versions could lead to unnecessary data being archived and higher costs.

Option C is not ideal because Coldline Storage is better suited for long-term data storage with very infrequent access. Archiving data from multi-regional storage after 30 days to Coldline Storage would be more expensive, considering the fact that you still need to access the archived data once a month for reporting purposes and perform occasional updates. This contradicts the requirement of finding an efficient and cost-effective solution for archiving the data in this scenario.

Solution to Question 47: C

The correct answer is C: Link the acquired company's projects to your company's billing account.

Explanation: By linking the acquired company's projects to your company's billing account, all costs from both organizations will be consolidated into a single invoice. This makes it easy to manage and track expenses without having to deal with multiple invoices and billing accounts.

Why other options will not work:

A. Enable cost aggregation in the Cloud Console for both billing accounts. While cost aggregation helps in understanding and analyzing expenses, it doesn't merge invoices from different billing accounts. It is a tool to organize costs within a billing account, not a way to combine billing accounts.

B. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued. This option will only alert the finance team when a new invoice is generated but does not consolidate the invoices into one. The team would still have to manage separate invoices for both companies.

D. Combine the billing account balance of the acquired company and your company's billing account by enabling the joint billing feature. There is no "joint billing" feature in GCP that combines billing account balances. Linking projects from both companies to a single billing account is the proper approach to consolidate costs as described in option C.

Solution to Question 48: D

The correct answer is D. Storing the database password inside a Secret object

and modifying the YAML file to populate the DB_PASSWORD environment variable from the Secret is the recommended approach by Google for the following reasons:

1. Secrets are designed specifically for managing sensitive information, such as passwords, API keys, and tokens. They provide better security and control over the data access.
2. Kubernetes handles the lifecycle of Secret objects ensuring that they are only accessible to authorized components and creating mechanisms for fine-grained access control.
3. You can update or configure Secrets independently from other Kubernetes objects and can inject them dynamically into the containers during runtime.
4. Secrets can be encrypted at the storage layer while at rest, which provides additional security compared to plain-text storage.

Other options are not recommended for the following reasons:

A. Encrypting the database password using Google Cloud Key Management Service (KMS) and storing the encrypted string inside a ConfigMap object introduces complexity and does not provide the same level of security as using a Secret object. ConfigMaps are designed to store non-sensitive configuration data, while Secret objects are specifically designed for handling sensitive information.

B. Storing the database password in a Google Sheet and using Google Sheets API to fetch it during runtime is a bad security practice. This approach makes the sensitive data accessible to users who have access to the Google Sheet, creating vulnerabilities. Additionally, using Google Sheets API incurs latency and an external point of failure during runtime.

C. Storing the database password in a file inside a Kubernetes persistent volume and using a persistent volume claim to mount the volume to the container requires manual configuration and management steps. It doesn't provide the security features, lifecycle management, and ease of use that Kubernetes Secret objects offer.

Solution to Question 49: A

The correct answer is A. Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

Explanation for A (correct option): Cloud Run is a serverless platform provided by Google Cloud that enables you to deploy your applications in containers without the need to manage the underlying infrastructure. By using Cloud Run, you can easily create and manage traffic splitting between different revisions of your application. Gradual rollouts enable you to incrementally shift a portion of traffic to the newer version, thus facilitating safe and secure testing of the application before a complete rollout.

Explanation for why other options will not work:

B. Deploy the application to App Engine. For each new version, create a new service. While Google App Engine supports deploying multiple versions of the application, creating a new service for each version is not an appropriate approach for testing a new version with a small percentage of production traffic. Instead, you should be using traffic splitting between different versions within a single service, which allows you to allocate the desired percentage of traffic to the new version without creating separate services.

C. Deploy the application to Cloud Spanner. Use partitions for traffic splitting. Cloud Spanner is a Google Cloud managed database system designed to provide a globally distributed and consistent relational database. It is not a platform designed for deploying applications or handling traffic splitting. Instead, Cloud Spanner is used for storing and managing data. Therefore, this option is not suitable for the given requirements.

D. Deploy the application to Compute Engine. Use instance groups for traffic splitting. Google Compute Engine focuses on providing Infrastructure as a Service (IaaS) rather than serverless execution. While Compute Engine does offer instance groups for managing and scaling instances, using this approach would require manual management of the underlying infrastructure, which is not aligned with the serverless requirement in the question. Additionally, traffic splitting using instance groups does not provide the same ease and granularity as the gradual rollout feature in Cloud Run.

Solution to Question 50: B

The correct answer is B: Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

Explanation for Answer B: Moving the project using the projects.move method is the most efficient and least complex method for transferring the ownership of the startup's Google Cloud project to your tech company's organization. Furthermore, updating the billing account associated with the project will ensure that future bills will be charged to your organization, thus meeting the billing requirement of the task. This action can be done with minimal effort compared to other options.

Reasons why other options won't work:

Option A: Creating a Private Catalog for the Google Cloud Marketplace and uploading the resources of the project requires a lot of manual work and takes more time than moving the project directly. Additionally, this option does not address the requirement of transferring billing to your organization.

Option C: Creating Docker containers for each resource in the startup's production project is unnecessary and time-consuming. Moreover, this method does

not handle the billing account transfer, so it does not meet the task's requirements.

Option D: Establishing a VPC Network Peering between the projects only connects the networks, and does not transfer ownership or resources from the startup's project to your organization's project. Also, configuring Billing Export might help in tracking billing data, but it will not change the billing account associated with the project. Hence, this option does not fulfill the task's requirements.

Practice Exam 3

Question 1: You are working as a software developer at a tech company and have been provided with a developer laptop running Ubuntu and the Cloud SDK installed from the Google Cloud Ubuntu package repository. You need to test your application locally on this laptop, specifically with Cloud Datastore. What should you do?

A. Use the gcloud datastore emulator start command to launch the emulator without installing it.

B. Install the cloud-datastore-emulator component using the gcloud components install command.

C. Install the google-cloud-sdk-app-engine-java component using the apt-get install command.

D. Create a Cloud SQL database and use it as a substitute for Cloud Datastore in your local testing.

Question 2: As a developer at a large tech company, you have recently deployed an application on a managed instance group in Compute Engine within the company's infrastructure. The application accepts Transmission Control Protocol (TCP) traffic on port 389 and necessitates preserving the IP address of the client making a request. To expose the application to the internet using a load balancer, what should be your next course of action?

A. Expose the application by using a TCP Proxy Load Balancer.

B. Expose the application by using an external TCP Network Load Balancer.

C. Expose the application by using an external UDP Network Load Balancer.

D. Expose the application by using Cloud CDN.

Question 3: As a data analyst at a large e-commerce company, you currently work with an on-premises data analytics set of binaries that process data files in memory for approximately 45 minutes every midnight. These data files range between 1 gigabyte and 16 gigabytes in size. You've been tasked with migrating this application to Google Cloud while minimizing effort and cost. What is the best approach to achieve this?

A. Create a container for the set of binaries and use Cloud Scheduler to start the processing on AI Platform every midnight.

B. Upload the set of binaries to BigQuery and use Cloud Scheduler to run a SQL query on the data files every midnight.

C. Deploy the set of binaries on Cloud Storage and use Cloud Scheduler to trigger file processing every midnight.

D. Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

Question 4: As a software engineer at a tech company developing a new web application, you need to integrate it into Google Cloud Platform for deployment. To ensure smooth updates, you are required to test them on a small percentage of actual user traffic while having the majority of users directed to a stable version of the application. What approach should you take to achieve this?

A. Deploy the application on App Engine. For each update, create a new service. Configure traffic splitting to send a small percentage of traffic to the new service.

B. Deploy the application on Cloud Run. For each update, create a new container image and update the service. Configure traffic splitting at the load balancer level to direct a small percentage of traffic to the new container.

C. Deploy the application on Compute Engine. For each update, create a new instance template. Configure traffic splitting between instance groups using a load balancer.

D. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

Question 5: As a network administrator at a software company, you have an application that searches for its licensing server at IP 10.0.3.21. In order to deploy the licensing server on Compute Engine without modifying the application's configuration, and ensuring that the application can still connect to the licensing server, what should you do?

A. Configure the licensing server to listen on all IP addresses in the 10.0.3.0/24 subnet and assign a different static internal IP address to the server.

B. Use the IP 10.0.3.21 as a secondary IP address for the licensing server, and assign it a primary IP address from the same subnet.

C. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

D. Use the IP 10.0.3.21 as a custom ephemeral IP address and assign it to the licensing server.

Question 6: As a data analyst at your company, you need to send all the logs from your Compute Engine instances to a BigQuery dataset named platform-logs to analyze application performance. All instances already have the Cloud Logging agent installed, and you want to minimize cost. What steps should you take to achieve this?

A. 6. Create a BigQuery Transfer Service job to move the logs from Compute Engine instances to the platform-logs dataset in BigQuery daily. 7. Grant BigQuery Data Editor role to the service account used by the Transfer Service job.

B. 1. Create a Dataflow job that reads logs from Compute Engine instances, filter them, and then write the logs to the platform-logs dataset in BigQuery. 2.

Grant BigQuery Data Editor role to the service account used by the Dataflow job.

C. 5. In Cloud Logging, create a logs export with Cloud Storage Bucket as a sink. 6. Use Cloud Functions to read logs from Cloud Storage and insert them into the platform-logs dataset in BigQuery.

D. 1. In Cloud Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the platform-logs dataset as Sink Destination.

Question 7: As an IT specialist at a software development company, your team has developed Docker images for a new application that will be deployed on Google Cloud. The team wants to focus on the application without worrying about managing the infrastructure, while also ensuring that the application can scale automatically as its user base grows. What is the most suitable solution for this requirement?

A. Create an instance template with the container image, and deploy a Managed Instance Group with Autoscaling.

B. Upload Docker images to Artifact Registry, and deploy the application on Google Kubernetes Engine using Standard mode.

C. Create a Dataproc cluster with the Docker image and deploy the application without autoscaling.

D. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Question 8: You are working at a financial company that heavily relies on its Cloud SQL MySQL database for transactional records. In order to comply with industry regulations, you must retain a month-end copy of the database for three years for potential audits. What should you do to achieve this?

A. Configure an on-demand backup for the first of the month. Store the backup file directly within the Cloud SQL MySQL database. Create a snapshot of the first-of-the-month database, and store it in an Archive class Cloud Storage bucket. Set up a scheduled Cloud Scheduler job that will trigger a Cloud Function to extract the month-end database data and store it in a Firestore. Set up a Data Transfer Service to copy the database to Bigtable and retain the month-end copy in an Archive class Cloud Storage bucket. Create a BigQuery scheduled query to transfer a copy of the database into a new dataset on the first of the month and store it in an Archive class Cloud Storage bucket. Configure a serverless export solution using Cloud Run to export the database first-of-the-month to Cloud Spanner, and store in an Archive class Cloud Storage bucket. Configure automated daily export of the entire database, and only store the first of the month copies in a Coldline class Cloud Storage bucket. Create a continuous Dataflow synchronization for the month-end database copy, and store the replicated data into an Archive class Cloud Storage bucket.

B. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

C. Set up an on-demand backup for the first of the month. Write the backup to an Archive class Cloud Storage bucket.

D. Convert the automatic first-of-the-month backup to an export file. Write the export file to a Coldline class Cloud Storage bucket.

Question 9: As a system administrator for your company's cloud infrastructure, you are tasked with ensuring that your team members securely and cost-effectively access the Linux instances hosted on Google Cloud. Which method should you use for this purpose?

A. Create a bastion host with public internet access. Create the SSH tunnel to the instance through the bastion host.

B. Create a GCP load balancer and forward all incoming connections to instances on port 22.

C. Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

D. Use a third party tool to provide remote access to the instances.

Question 10: As an IT manager at a software development company, you are responsible for monitoring the Google Cloud Platform account that includes access to both production and development projects. In order to keep track of compute instances in development and production projects daily, which method should be employed?

A. Create two Service Accounts for each project and use them in a script to access the Google Compute Engine API for listing all compute instances.

B. Go to GCP Console and export this information to Cloud SQL on a daily basis.

C. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

D. Go to Cloud Shell and export this information to Cloud Storage on a daily basis.

Question 11: As a cloud engineer in a rapidly expanding company, you've been tasked with managing employee accounts within the Google Workspace. The number of staff is expected to rise from 100 to 1,000 employees in the next 2 years. In addition to providing access to the company's Google Cloud account, your solution must accommodate 10x growth without compromising performance, adding complexity, or creating security issues. How should you proceed?

A. Import and export all users manually to Google Cloud Storage.

B. Use the built-in GCP Admin Tools to manage accounts as they grow without integration.

C. Connect Google Workspace directly to an on-prem LDAP server for authentication and user management.

D. Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

Question 12: As a network administrator in a software development company, your primary internal IP addresses in a subnet for a custom mode VPC are running low. The subnet currently has an IP range of 10.0.0.0/20, primarily utilized by the virtual machines in your project. You are tasked with providing more IP addresses for these virtual machines. What is the most suitable course of action?

A. Convert the subnet IP range from IPv4 to IPv6.

B. Enable Private Google Access for the virtual machines.

C. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

D. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/17.

Question 13: As a software developer at a multinational financial company, you are tasked with creating a trading application that caters to clients worldwide. The application should utilize a relational data storage structure, ensuring that the data state remains consistent across all clients. To achieve minimal latency for the end users, the application will be deployed in multiple regions. Which data storage option should you choose for this application?

A. Use Cloud Memorystore for data storage.

B. Use Cloud Filestore for data storage.

C. Use Cloud SQL for data storage.

D. Use Cloud Spanner for data storage.

Question 14: As a cloud specialist working for a leading software company, you have been assigned to set up an autoscaling managed instance group for a client's HTTPS web application. Your goal is to ensure that unhealthy VMs are recreated automatically. What is the most effective approach to achieve this?

A. Create a health check on port 443 and use that when creating the Managed Instance Group.

B. Enable Stackdriver Monitoring and Logging for the Managed Instance Group.

C. In the Instance Template, add a startup script that sends a heartbeat to the metadata server.

D. Use the default health check for network load balancing when creating the Managed Instance Group.

Question 15: As a cloud engineer at a major tech company, you've been assigned the task of ensuring all developers have the same permissions, regardless of the Google Cloud project they're working on. Furthermore, the company's security policy limits developer permissions to Compute Engine, Cloud Functions, and Cloud SQL. You are asked to implement this security policy with minimal effort. How can you achieve this task?

A. • Enable API access to Compute Engine, Cloud Functions, and Cloud SQL for all developers, without creating custom roles or assigning Google group permissions.

B. • Create a single custom role consisting of Compute Engine, Cloud Functions, and Cloud SQL permissions for each project and make all developers Project Owners.

C. • Add all developers to a Google group in Cloud Identity. • Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level. • Assign the custom role to the Google group.

D. • Create individual custom roles for Compute Engine, Cloud Functions, and Cloud SQL permissions in each project and assign them to developers.

Question 16: As a DevOps engineer working at a tech company, you are assigned to create a Google Kubernetes Engine (GKE) cluster with a cluster autoscaler feature enabled for the company's infrastructure. The requirement is to ensure that each node of the cluster runs a monitoring pod that sends container metrics to a third-party monitoring solution. What is the appropriate action to take in this situation?

A. Deploy the monitoring pod in a DaemonSet object.

B. Deploy the monitoring pod in a CronJob object.

C. Reference the monitoring pod in a Deployment object.

D. Configure the monitoring pod as a sidecar in all deployments.

Question 17: As a technology consultant firm, you have your clients' infrastructure on-premises, but all machines are running at maximum capacity. The client wishes to burst to Google Cloud while ensuring the workloads on Google Cloud can directly communicate with the on-premises workloads using a private IP range. What solution should you recommend?

A. Use Cloud Interconnect to connect the on-premises infrastructure and Google Cloud without VPN.

B. In Google Cloud, configure the VPC for VPN tunneling using public IP addresses.

C. In Google Cloud, configure the VPC for Private Google Access.

D. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Question 18: In your software development company, the DevOps team requires complete access to Compute Engine resources within the development project but should not be allowed to create or modify other resources in the project. To adhere to Google's recommendations for assigning permissions to the DevOps team, what course of action should you take?

A. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

B. Grant the basic role roles/editor to the DevOps group.

C. Create a custom role at the project level and grant all compute.instance.* permissions to the role. Grant the custom role to the DevOps group.

D. Create an IAM policy and grant all compute.networkAdmin.* permissions to the policy. Attach the policy to the DevOps group.

Question 19: You are working as a data analyst in a telecommunications company that uses BigQuery for data warehousing. Your company is collaborating with a partner company specializing in customer analytics to implement a recommendation engine based on your data. Both companies use Google Cloud to manage resources in separate projects. In order to proceed, you need to provide the partner company access to the BigQuery dataset in your project. What steps should you take to achieve this?

A. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

B. Ask the partner to create a Service Account in their project, and have them give the Service Account access to Cloud Storage in their project.

C. Ask the partner to create a Service Account in their project, and have them give the Service Account access to App Engine in their project.

D. Create a Service Account in your own project, and ask the partner to grant this Service Account access to App Engine in their project.

Question 20: As a data manager in a large media company, you are required to configure a policy for efficiently handling video files stored in a specific Cloud Storage Regional bucket. The policy should ensure that the videos are moved to Coldline storage after 90 days from their creation and eventually deleted after one year. How should you establish this policy?

A. Use Cloud Storage Transfers with SetStorageClass and Delete actions. Set the SetStorageClass action to 90 days and the Delete action to 365 days.

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

C. Use Cloud Storage Object Lifecycle Management using Timestamp conditions with SetStorageClass and Delete actions. Set the SetStorageClass action

to 90 days and the Delete action to 365 days.

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

Question 21: As a cloud architect working on a multitenant product in a tech company, you are utilizing Google Kubernetes Engine (GKE) with a single GKE cluster. Every customer has a dedicated Pod running in the cluster, where they can execute arbitrary code. To ensure maximum isolation between the Pods belonging to different customers, what should be your next step?

A. Enable Google Cloud Private Catalog to manage container images for your customers' Pods.

B. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

C. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

D. Use Cloud Armor to configure security policies for each customer's Pod.

Question 22: As a finance manager at a rapidly growing company, you are responsible for migrating invoice documents stored on-premises to Cloud Storage. The company has specific storage requirements for these documents:

• Documents must be kept for five years. • Up to five revisions of the same invoice document must be stored, to allow for corrections. • Documents older than 365 days should be moved to lower cost storage tiers.

To minimize operational and development costs while following Google-recommended practices, what should you do?

A. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

B. Enable retention policies on the bucket, use Cloud Pub/Sub to trigger a Cloud Run instance to manage document revisions and storage classes.

C. Enable lifecycle rules on the bucket and use Cloud Data Transfer Service to move your documents based on their metadata.

D. Use Google Cloud SQL combined with Cloud Datastore to manage storage requirements and delete old files.

Question 23: In your company, you are tasked with handling the deployment of a third-party application on a Compute Engine instance. Several other Compute Engine instances are already operational with default settings. The application installation files are stored on Cloud Storage, and you need to make sure that only the new instance can access these files, without allowing other virtual machines (VMs) to access them. How should you proceed?

A. Create a new service account and assign this service account to the new instance. Change the storage class of objects on Cloud Storage to Nearline storage.

B. Create a new service account and assign this service account to the new instance. Attach a new Cloud Storage bucket to the instance for the application files only.

C. Create a new service account and assign this service account to the new instance. Use Cloud Identity-Aware Proxy (IAP) to secure access to Cloud Storage objects.

D. Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

Question 24: You are a cloud engineer working at a software development company that uses Google Cloud for deploying its applications. Your team lead has shared a JSON file containing the private key of a Service Account with you, granting access to various resources in the company's Google Cloud project. You have already downloaded and installed the Cloud SDK. Now, you want to authenticate and authorize the gcloud commands using this private key. What step should you follow?

A. Use the command gcloud init and point it to the private key.

B. Use the command gcloud auth activate-service-account and point it to the private key.

C. Use the command gcloud config set account and point it to the private key.

D. Use the command gcloud auth login-service-account and point it to the private key.

Question 25: As an IT manager in a financial services company, you have to select and configure compute resources for a set of nightly batch processing jobs related to client portfolio updates. These jobs take around 2 hours to complete and need to be run every night. You are asked to minimize service costs while ensuring successful job completion. What should you do?

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

B. Select Google Kubernetes Engine. Use a multi-node cluster with large instance types.

C. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types.

D. Select App Engine. Use flexible environment with automatic scaling.

Question 26: You are working as a Cloud consultant for a company that has implemented Cloud Spanner for their database needs. They are experiencing

read latency-related performance issues on one particular table, which is accessed only by their users using a primary key. Given the table schema, how can you effectively resolve this issue?

A. Change the primary key to not have monotonically increasing values.

B. Change the primary key to a composite key consisting of person_id and created_at.

C. Enable interleaved tables to improve read performance.

D. Create a secondary index using the following Data Definition Language (DDL):

Question 27: As a network engineer in a growing tech company, you are tasked with deploying production and test workloads on Compute Engine. The production VMs need to be hosted on a separate subnet than the test VMs, yet all VMs must have the ability to connect with each other using internal IPs without creating additional routes. To accomplish this, how should you configure the VPC and the two subnets?

A. Create a single custom VPC with 3 subnets. Create 2 subnets for production and test in the same region with different CIDR ranges, and the third subnet as the communication link between the two.

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

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

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

Question 28: You are a Cloud Engineer working for a company that develops a web application spanning multiple projects. Your task is to configure service accounts to allow virtual machines (VMs) in the web-applications project to access BigQuery datasets in the crm-databases project, adhering to Google's recommended practices. How should you grant access to the service account in the web-applications project?

A. Grant roles/bigquery.admin role to crm-databases and "project viewer" role to web-applications.

B. Grant "project owner" role to crm-databases and the web-applications project.

C. Grant "project owner" role to crm-databases and roles/bigquery.dataViewer role to web-applications.

D. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

Question 29: You're working as a cloud engineer at a software development company, and last month your projects experienced higher costs than expected. After conducting research, you discovered that a GKE development container generated an excessive amount of logs, leading to the increased expenses. To disable the logs efficiently with the fewest steps possible, what action should you take?

A. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE Cluster Operations resource.

B. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

C. 8. Go to the GKE console, and disable the GKE container temporarily, configure its logging settings to disable Stackdriver Logging, and then restart it.

D. 6. Go to the Monitoring console, and set log-based metrics to zero for the GKE container.

Question 30: As a data engineer working for a retail company, you have to manage a massive amount of unstructured data in various file formats for further analysis. You plan to perform ETL transformations on the data and make it accessible on Google Cloud so that it can be processed by a Dataflow job within your organization. Which approach should you take?

A. Upload the data to Kubernetes Engine using the gcloud container clusters create command.

B. Upload the data to Cloud Storage using the gcloud storage command.

C. Upload the data to BigQuery using the bq command line tool.

D. Upload the data to Firestore using the gcloud firestore command.

Question 31: As a network administrator in a financial services company, you are tasked with setting up an application in a new VPC behind a firewall for your client. The client is particularly concerned about data egress and wants the fewest open egress ports possible. How should you proceed in configuring the firewall to address the client's concern?

A. Configure custom routes to block egress traffic on undesired ports.

B. Use a VPN tunnel to manage egress traffic by allowing only specific ports.

C. Configure a NetworkPeering policy to limit egress traffic to specific subnets.

D. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

Question 32: As a software engineer in a leading tech company, you are tasked with deploying a Dockerfile on Kubernetes Engine for a critical project. What is the appropriate procedure to achieve this?

A. Convert the Dockerfile into a Kubernetes configuration file and use gcloud app deploy .

B. Use kubectl run –image= to deploy the application.

C. Create a docker image from the Dockerfile and upload it to Datastore. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

D. Create a docker image from the Dockerfile and upload it to Container Registry. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

Question 33: As an IT engineer working for a fintech company, you are responsible for maintaining a Google Kubernetes Engine (GKE) cluster named 'dev' that has been deployed on Google Cloud. Your task is to manage the GKE configuration via the command line interface (CLI) after downloading and installing the Cloud SDK. What step would you take to ensure that any future CLI commands by default address this specific cluster?

A. Use the command gcloud config set container/cluster dev.

B. Use the command gcloud container clusters get-credentials dev –region us-central1.

C. Create a file called kubernetes.config in the ~/.gcloud folder that contains the cluster name.

D. Create a file called defaults.json in the ~/.gcloud folder that contains the cluster name.

Question 34: As a software engineer in a tech company, you are managing multiple microservices in a Kubernetes Engine cluster as part of a complex application. The application includes a microservice responsible for image rendering, which demands a high amount of CPU time as compared to memory. The other microservices within the application have workloads optimized for n2-standard machine types. To ensure all workloads in your cluster utilize resources as efficiently as possible, what should your approach be?

A. Use the node pool with compute-optimized machine type nodes for both the image rendering microservice and the other microservices.

B. Use the node pool with general-purpose machine type nodes for the image rendering microservice. Create a separate node pool with preemptible machine type nodes for the other microservices.

C. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

D. Assign the pods of the image rendering microservice a higher pod priority than the other microservices.

Question 35: As a department manager at a tech company, you oversee a team of 10 developers. To encourage innovative thinking, you allow each developer to have their own Google Cloud Project for experimentation purposes. However, you'd like to avoid excessive expenses by receiving notifications if an individual developer's project surpasses a monthly spending limit of $500. What should you do?

A. Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account.

B. Create a single budget for all projects and configure budget alerts on this budget.

C. Set up daily cost quotas for each sandbox project and manually monitor the spending.

D. Create a budget per project and configure budget alerts on all of these budgets.

Question 36: As a cloud administrator at a major tech company, you have been tasked with deploying a critical application on Compute Engine. To avoid any accidental deletions, you need to safeguard the instance from being destroyed due to a wrong click. What action should you take?

A. Enable Preemptibility on the instance.

B. Use the minimal CPU platform for the instance.

C. Enable delete protection on the instance.

D. Disable Automatic restart on the instance.

Question 37: You are working as a cloud engineer in a rapidly growing technology company, and you have been tasked with deploying a critical application to App Engine. The company needs the application to scale based on request rate to accommodate fluctuating user demand. In addition, they require a minimum of 3 unoccupied instances to be available at all times. Which scaling type should you use?

A. Automatic Scaling with min_idle_instances set to 3.

B. Automatic Scaling with max_idle_instances set to 3.

C. Automatic Scaling with target_throughput_utilization set to 3.

D. Basic Scaling with target_cpu_utilization set to 3.

Question 38: You are working as a data engineer in a large tech company, and your team is responsible for managing an App Engine Service that aggregates and visualizes data from BigQuery. The application is deployed with the default App Engine Service account. However, the data you need to visualize is stored in a different project that is managed by another team within the company. You

do not have access to this project, but you want your application to be able to read data from the BigQuery dataset. What action should you take?

A. Request the other team to export their BigQuery dataset to Cloud Storage which your App Engine service can then read and visualize.

B. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

C. Ask the other team to create a Storage Bucket containing their BigQuery dataset and grant you access to read from the bucket.

D. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.

Question 39: As an IT manager at a software development company, you are responsible for a Compute Engine instance hosting a time-tracking application used between 9 AM and 6 PM on weekdays. You need to back up this instance daily for disaster recovery purposes, retain the backups for 30 days, and use the Google-recommended solution with minimal management overhead and the least number of services. What should you do?

A. 5. Update your instances' metadata to add the following value: backup-frequency: daily backup-retention: 30

B. 1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk. 2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM - 2:00 AM - Autodelete snapshots after: 30 days

C. 7. Use Cloud Endpoints to create a snapshot of your instance's disk daily at 1:00 AM and configure the API to delete snapshots older than 30 days.

D. 4. Set up Data Loss Prevention (DLP) on the instance's disk to automatically back up the data daily and delete backups older than 30 days.

Question 40: As a network administrator for a large company hosting an application on bare-metal servers in the company's private data center, you need to provide access to Google Cloud Storage for a critical application. Unfortunately, security policies do not allow the servers to have public IP addresses or access to the internet. To adhere to Google-recommended practices while providing access to Cloud Storage, what steps should be taken?

A. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in Google Cloud. 2. Use Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel. 3. In your on-premises network, configure your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com.

B. 8. Use Cloud NAT to create a managed NAT gateway in a Google Cloud VPC, then configure your on-premises servers to use the NAT gateway to access Cloud Storage without public IP addresses.

C. 4. Use Cloud Pub/Sub to send messages containing your servers' data to Google Cloud, then process these messages with a Cloud Function that stores the data in Cloud Storage.

D. 3. Deploy a Filestore instance in the same VPC as the servers and configure the application to use the Filestore instead of Cloud Storage, while synchronizing the data between Filestore and Cloud Storage manually.

Question 41: You are working as a software engineer in a rapidly growing media company that specializes in video content. Your company is using a video encoding software that needs to be hosted on Compute Engine. The increasing user base requires a highly available and uninterrupted encoding process without CPU limitations. To achieve this and follow Google-recommended practices for automating operations, what is the most appropriate approach?

A. Deploy your solution to an instance group without autoscaling, and manually add instances when CPU utilization is high.

B. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

C. Deploy your solution on multiple standalone Compute Engine instances, and increase the number of existing instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

D. Deploy your solution to an instance group, but use memory utilization as the autoscaling metric instead of CPU utilization.

Question 42: As a company working within the software development industry, you've been asked to produce a list of the enabled Google Cloud Platform APIs for a GCP project using the gcloud command line in the Cloud Shell. The project name is my-project. What should you do?

A. Run gcloud init to set the current project to my-project, and then run gcloud services describe my-project.

B. Run gcloud projects get-iam-policy my-project, and then run gcloud services list –project my-project.

C. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

D. Run gcloud config list to view the project value, and then run gcloud services list –project=my_project.

Question 43: As a data analyst at a large multinational corporation, you are responsible for managing the company's data stored in BigQuery. Recently, the company has accumulated over 1000 datasets across numerous projects from various departments. Your CEO requests that you identify all tables that contain an employee_ssn column while minimizing effort. What method would you choose to accomplish this task?

A. Go to Data Catalog and search for employee_ssn in the search box.

B. Write a script using the Google Cloud SDK to scan through every table in all the projects looking for the employee_ssn column.

C. Manually check each dataset in all the projects for the presence of an employee_ssn column.

D. Configure a custom VPC Service Controls perimeter to restrict access to datasets containing employee_ssn.

Question 44: As a database administrator at a tech company, you have set up an instance of SQL Server 2017 on Compute Engine to evaluate the latest features. To connect to this instance with the least amount of steps, what should you do?

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

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

C. Create a VPN tunnel between your desktop and the GCP environment. Verify that a firewall rule for port 3389 exists. Use your existing RDP client to connect to the SQL Server instance using the internal IP address.

D. Set a Windows username and password in the GCP Console. Verify that a firewall rule for port 5432 exists. Click the RDP button in the GCP Console, and supply the credentials to log in.

Question 45: You are working as a project manager at a technology company, specifically overseeing the Business Intelligence (BI) department. Your company has set up a data pipeline that streams data into BigQuery, and you need to ensure that the BI department can execute custom SQL queries on the most recent data available in BigQuery. What is the best course of action for achieving this objective?

A. Create a service account with BigQuery Data Transfer Service role and share the private key with the BI team to copy data from BigQuery.

B. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

C. Use Cloud Composer to schedule a daily workflow that synchronizes the data in BigQuery with their internal database.

D. Create a Service Account for the BI team and distribute a new private key to each member of the BI team.

Question 46: As a software engineer at a global company, you are managing a project which includes a single Virtual Private Cloud (VPC) and a single subnetwork in the us-central1 region. An application is hosted on a Compute

Engine instance within this subnetwork. You are required to deploy a new instance in the same project in the europe-west1 region, ensuring that the new instance has access to the application while adhering to Google-recommended practices. What steps should you take to achieve this?

A. Create a subnetwork in the same VPC, in europe-west1. Use Cloud Interconnect to connect the two subnetworks. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

B. Deploy the new instance in the us-central1 region and configure its network traffic to route through the existing subnetwork for access to the application.

C. 1. Create a subnetwork in the same VPC, in europe-west1. 2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

D. Create a subnetwork in the same VPC, in europe-west1. Set up an instance group with only the new instance and use the first instance's private address as the backend endpoint.

Question 47: As a cloud engineer at a software development company, you receive an alert from your managed instance group indicating that the recent attempt to create new instances has failed. To ensure your team can handle the anticipated application traffic, you must maintain the specified number of running instances based on the template. What action should you take?

A. Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template.

B. Change the instance group's region and create an instance template that contains valid syntax that will be used by the instance group.

C. Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

D. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

Question 48: As a data engineer at a fast-growing tech company, you have an application that utilizes Cloud Spanner as a database backend for maintaining current user state information. Cloud Bigtable logs all the user-triggered events, while daily backups of Cloud Spanner data are exported to Cloud Storage. One of your data analysts requests you to join data from Cloud Spanner and Cloud Bigtable for certain users. How can you accomplish this ad hoc request as efficiently as possible?

A. Use the Cloud Pub/Sub to create a topic that subscribes to both Cloud Spanner and Cloud Bigtable data events for the specific users in question.

B. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

C. Create a Cloud Datastore database to replicate the data from Cloud Spanner and Cloud Bigtable and run the required queries.

D. Use Google Cloud Data Loss Prevention API to mask the users' sensitive data from Cloud Spanner and Cloud Bigtable before running the data-processing job.

Question 49: As a network engineer in a leading software company, you've been assigned to establish a secure and reliable VPN connection between a new VPC and a remote site belonging to a client. They have emphasized the need for dynamic routing, a shared address space of 10.19.0.1/22, and prevention of overprovisioning of tunnels during a failover event. To ensure high availability of the Cloud VPN and adherence to Google-recommended best practices, what steps should you take?

A. Use a custom mode VPC network, configure static routes, and use active/active routing.

B. Use an automatic mode VPC network, configure static routes, and use active/active routing.

C. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

D. Use a custom mode VPC network, use Cloud Router static routes, and use active/passive routing.

Question 50: As an IT specialist at a fintech company, you are managing a 3-tier solution running on Compute Engine. The current infrastructure configuration has a service account associated with all instances within each tier. Your task is to enable communication on TCP port 8080 between the tiers as follows: * Instances in tier #1 must communicate with tier #2. * Instances in tier #2 must communicate with tier #3. What should you do?

A. 1. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow TCP: 8080 2. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow TCP: 8080

B. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #1 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #3 service account • Protocols: allow TCP: 8080

C. 1. Create an ingress firewall rule with the following settings: • Targets: all

instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP: 8080

D. 1. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow all 2. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow all

Practice Exam 3 Solutions

Solution to Question 1: B

The correct answer is B. Install the cloud-datastore-emulator component using the gcloud components install command.

Explanation:

Option A is incorrect because using the gcloud datastore emulator start command would only start the emulator if it is already installed. In this case, as it is not installed, you would first need to install it using the gcloud components install command.

Option B is correct because installing the cloud-datastore-emulator using the gcloud components install command would ensure that the emulator is installed on your laptop. Once the emulator is installed, you can then run your application locally and test it with Cloud Datastore.

Option C is incorrect because the google-cloud-sdk-app-engine-java component is not the right component for Cloud Datastore. This component is for App Engine Java, and it is not relevant to Cloud Datastore. Therefore, installing this component will not provide you with the ability to test your application with Cloud Datastore locally.

Option D is incorrect because Cloud SQL is a completely different service from Cloud Datastore, and they are not interchangeable. Cloud Datastore is a NoSQL database, while Cloud SQL is a relational database. Thus, moving to Cloud SQL would involve rearchitecting your application in addition to not enabling you to properly test your Cloud Datastore implementation. It is not an appropriate substitute for local testing purposes in this scenario.

Solution to Question 2: B

The correct answer is B. Expose the application by using an external TCP Network Load Balancer.

Here's why option B is the correct choice, and why the other options will not work:

A. Expose the application by using a TCP Proxy Load Balancer. This solution is not suitable because the question specifies the requirement to preserve the IP address of the client making a request. TCP Proxy Load Balancer does not provide the ability to preserve the client IP address as it terminates and establishes new TCP connections between the client and the backend instances.

B. Expose the application by using an external TCP Network Load Balancer. This option is the most appropriate choice for the given scenario as it meets both requirements: the application uses a TCP connection on port 389, and it also preserves the IP address of the client making the request. External TCP

Network Load Balancers can route traffic from clients directly to the backend instances without modifying the source IP address.

C. Expose the application by using an external UDP Network Load Balancer. This solution is not suitable because the question explicitly states that the application accepts TCP traffic on port 389. UDP Network Load Balancers are designed for User Datagram Protocol (UDP) based traffic and are not compatible with a TCP application.

D. Expose the application by using Cloud CDN. This solution is not appropriate since Cloud CDN is a content delivery network mainly used to cache and deliver static and dynamic web content, such as images, video, and API responses. The focus of the question is on exposing the application to the internet using a load balancer, and Cloud CDN is not an appropriate solution for this specific use case. Moreover, Cloud CDN operates at the HTTP/HTTPS layer, not at the TCP layer as needed for this scenario.

In conclusion, the best choice for exposing the application to the internet while preserving the client's IP address is option B, using an external TCP Network Load Balancer.

Solution to Question 3: D

The best approach to achieve the migration while minimizing effort and cost is option D. Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

Option D is the best approach because it requires minimal changes to the existing application, as the on-premises data analytics set of binaries can be directly migrated to a Google Compute Engine virtual machine (VM). This approach ensures that the processing remains in memory, as required, and the instance schedule can be configured to start and stop the VM at midnight as needed. Furthermore, this option is cost-effective, as you'll only be billed for the VM's usage during the processing time.

Options A, B, and C are not suitable for the following reasons:

A. Creating a container for the set of binaries and running it on the AI Platform at midnight is a considerable change from the current on-premises setup, likely requiring more effort than simply migrating to a VM. Additionally, AI Platform may not be the most cost-effective choice for processing data files in memory, as it is designed for machine learning tasks and may have higher resource costs.

B. BigQuery is not the appropriate service for this task, as it is a fully managed, serverless data warehouse for analytics and not designed for processing data files using custom binaries. Instead, it is optimized for running SQL queries over large datasets.

C. Deploying the set of binaries on Cloud Storage is not suitable because Cloud Storage is designed for file storage, not for executing applications in memory.

Connecting it with Cloud Scheduler and handling file processing would require a more complex setup, leading to increased effort and costs.

Solution to Question 4: D

The correct answer is D: Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

This approach is the most suitable because Google App Engine is designed specifically for web applications and allows for easy management of multiple versions of a web application within the same service. Traffic splitting can be easily configured in App Engine to direct a specific percentage of user traffic to different versions of the application, which is useful for testing and rolling out updates. The management of the application and the resources it uses is automatically handled, allowing you to focus on the code and simplifying the integration and deployment process.

Option A is not the best approach because creating a new service for each update would lead to a higher operational overhead and a more complex architecture. Traffic splitting is more effectively done on versions within a single service.

Option B can work, but it is not optimal for a web application. Cloud Run is a serverless solution that focuses on containerized applications and is better suited for individual stateless services or APIs. Configuring traffic splitting at the load balancer level is a more complex process in Cloud Run compared to the setup available in App Engine.

Option C is not suitable because it involves deploying the application on Google Compute Engine, which is an Infrastructure as a Service (IaaS) where you manage the infrastructure yourself. This approach adds extra complexity, and traffic splitting between instance groups using a load balancer is generally not as seamless as handling this on App Engine, which is a Platform as a Service (PaaS) solution tailored for web applications.

Solution to Question 5: C

The correct answer is C, as it instructs to reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server. This ensures that the application, which is configured to search for the licensing server at IP 10.0.3.21, can still connect to it without having to modify its configuration.

Option A will not work because configuring the licensing server to listen on all IP addresses in the 10.0.3.0/24 subnet does not guarantee that the application will connect to the server using the specific IP address 10.0.3.21, which is the requirement.

Option B is not suitable because assigning a secondary IP address will not ensure the application connects to the correct IP (10.0.3.21) as all the IP addresses in the subnet are listened to. Moreover, using a secondary IP address might lead to potential conflicts or issues in managing the network.

Option D is not appropriate because using a custom ephemeral IP address does not provide the necessary stability, as it can change every time the instance is stopped and restarted. The application specifically searches for the licensing server at IP 10.0.3.21, so an IP address change could cause connection issues.

In conclusion, the only viable option is C - reserving the required IP 10.0.3.21 as a static internal IP address using gcloud and assigning it to the licensing server. This ensures that the application can consistently connect to the server without any configuration changes.

Solution to Question 6: D

The correct answer is D, and here is the explanation for why it is the best choice and why the other options will not be effective:

Option A involves using BigQuery Transfer Service to move logs from Compute Engine instances to the dataset named platform-logs in BigQuery. However, the problem with this option is that it does not mention setting up any logging export from Compute Engine instances to BigQuery. Transfer Service is typically used when you want to import data from other sources like SaaS applications or file-based data sources, whereas our goal here is to collect logs from instances.

Option B suggests using a Dataflow job to capture logs from Compute Engine instances and write them to the dataset in BigQuery. Although Dataflow is a powerful tool, it is not the most cost-effective option for this use case since sending logs directly from the Cloud Logging agent to BigQuery through sinks will minimize cost.

Option C involves exporting logs from Cloud Logging to a Cloud Storage Bucket and then using Cloud Functions to read logs from Cloud Storage and insert them into the main dataset in BigQuery. Even though this approach might work, it adds unnecessary complexity, and storing logs in Cloud Storage would incur additional costs.

Option D is the best solution because it focuses on filtering only Compute Engine logs directly from Cloud Logging (Step 1) and creating an export to send these logs to BigQuery (Step 2). By choosing BigQuery as the sink service and specifying the platform-logs dataset as the sink destination (Step 3), it ensures the most direct and cost-effective integration between Cloud Logging and BigQuery for analyzing application performance.

In summary, option D is the most appropriate choice because it minimizes costs and directly exports the data from Cloud Logging to BigQuery without adding unnecessary complexity or intermediate processes.

Solution to Question 7: D

The most suitable solution for this requirement is D - Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Option D is the correct answer because Cloud Run is designed for deploying and

managing serverless containers that can scale automatically according to the user base. By uploading Docker images to Artifact Registry and running them on Cloud Run, the IT specialist team can focus on developing the application without worrying about the infrastructure management.

Option A is not suitable because Managed Instance Groups with Autoscaling require more management as compared to serverless options like Cloud Run. There is some manual work involved, such as creating instance templates and configuring autoscaling settings, which doesn't fulfill the team's requirement to avoid infrastructure concerns.

Option B, deploying the application on Google Kubernetes Engine (GKE) using Standard mode, is not the most suitable option because GKE typically requires more management overhead than Cloud Run. GKE is a fully managed Kubernetes platform, but the team would still need to manage Kubernetes resources, and it could be more complex compared to a fully serverless solution like Cloud Run.

Option C involves creating a Dataproc cluster with the Docker image and deploying the application without autoscaling. The problem with option C is twofold. Firstly, Dataproc is designed for deploying big data processing applications and is not the best fit for general-purpose application deployment. Secondly, the team requires autoscaling, which is not provided in this option.

Solution to Question 8: B

The correct answer is B. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

Here's why option B is the right choice and why the other options will not work:

Option B: An export job can be set up to schedule the creation of a copy of the Cloud SQL MySQL database on the first of each month. Storing the export file in an Archive class Cloud Storage bucket fulfills the 3-year retention requirement for potential audits. Archive class storage provides the benefit of low-cost storage for infrequently accessed data, which is suitable for compliance retention needs.

Option A: Storing the backup file directly within the Cloud SQL MySQL database is not a feasible solution, as backups must be stored externally. Additionally, the question states a month-end copy is required, which an on-demand backup on the first of the month does not satisfy.

Option C: While setting up an on-demand backup for the first of the month may seem appropriate, the use of backups for this purpose is not the best approach. Backups are meant primarily for recovery purposes and exporting data or creating a snapshot is more suitable for long-term storage and compliance needs.

Option D: Although converting a first-of-the-month backup to an export file might work, writing the export file to a Coldline class Cloud Storage bucket may

not be the most cost-effective solution. Archive class storage is generally cheaper than Coldline class storage, making it a better option for storing compliance data that may not be accessed frequently.

The other options provided involve using other Google Cloud services (such as Firestore, Bigtable, BigQuery, Cloud Spanner, and Dataflow) which are not necessary for this specific use case. These services may introduce complexity and additional costs that are not required for the simple task of exporting a month-end copy of a Cloud SQL MySQL database and retaining it for three years. Therefore, they are not suitable solutions for this scenario.

Solution to Question 9: C

The correct answer is C: Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

Here's why this is the optimal choice and why the other options will not work:

A: Creating a bastion host with public internet access and an SSH tunnel through it can provide a secure access point to the Linux instances. However, it is not as cost-effective as using Google's Identity-Aware Proxy (IAP), which provides secure access without the need for an additional bastion host.

B: Using a GCP load balancer to forward incoming connections to instances on port 22 is not secure. Load balancers are designed to distribute traffic among instances, not to provide secure access. This approach could expose the instances to unauthorized access, leaving them vulnerable to security threats.

C: The gcloud compute ssh command with the –tunnel-through-iap flag leverages Google's Identity-Aware Proxy (IAP) to provide secure, authenticated access to the Linux instances without requiring a separate bastion host, making it cost-effective. Allowing ingress traffic from the IP range 35.235.240.0/20 on port 22 ensures that access is provided only to authorized users and devices within the specified IP range, adding an extra layer of security.

D: Using a third-party tool to provide remote access to the instances might work, but it won't be as cost-effective or streamlined as using Google Cloud's native tools and services. Additionally, using a third-party solution might introduce compatibility and integration issues with GCP.

Solution to Question 10: C

The correct answer is C. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

Here's why the other options are not suitable:

Option A: Creating two Service Accounts for each project and using them in a script to access the Google Compute Engine API for listing all compute instances may seem like an appropriate solution. However, it adds unnecessary complexity

to the process. Managing multiple service accounts for different projects can become cumbersome. Using gcloud config with a script simplifies the process of switching between configurations and projects, making it a better choice for the task at hand.

Option B: Going to the GCP Console and exporting the information to Cloud SQL on a daily basis is not an ideal solution. This process would require manual intervention every day when it comes to exporting the data, which is not efficient. An automated solution is needed to extract the information daily, making Option C, which uses a script to switch between configurations, a better choice.

Option D: Going to Cloud Shell and exporting the information to Cloud Storage on a daily basis is also not efficient as it would require manual intervention every day. While Cloud Storage can be used to store and access the exported data, using a script to automate the process is a more efficient solution. Option C, where a script is used in conjunction with gcloud config, is a more automated and efficient method for tracking compute instances in development and production projects on a daily basis.

Solution to Question 11: D

The correct answer is D: Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

Explanation: As the company is expected to grow rapidly from 100 to 1,000 employees, it is essential to have a scalable and secure method to manage employee accounts without adding complexity or compromising performance.

Reasons for choosing D: 1. Scalability: Organizing users in Cloud Identity into groups allows for easier management as the number of employees increases. This method is designed to handle a large number of users without impairing performance. 2. Enhanced Security: Enforcing multi-factor authentication (MFA) in Cloud Identity offers an additional layer of security, preventing unauthorized access and ensuring the company's sensitive data remains protected. 3. Simplified Administration: Using Cloud Identity for group and user management reduces the complexity of administration tasks, while maintaining a centralized place to manage accounts.

Reasons for not choosing other options:

A. Import and export all users manually to Google Cloud Storage: This approach has scalability issues and increased complexity, making it inefficient for managing a rapidly growing number of users. Additionally, manual processes always come with an increased risk of human error and do not provide the same level of security.

B. Use the built-in GCP Admin Tools to manage accounts as they grow without integration: While GCP Admin Tools provide some useful features, they are not built exclusively for handling rapid growth without integrating additional

solutions. This option could lead to inefficiencies and challenges in managing a large number of users and maintaining security.

C. Connect Google Workspace directly to an on-prem LDAP server for authentication and user management: Connecting to an on-prem LDAP server would introduce additional complexity and potential security issues. When dealing with a large number of users, an on-premises server might experience difficulties accommodating the increased load compared to a scalable cloud solution like Cloud Identity.

Solution to Question 12: C

The correct answer is C. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

Explanation: As a network administrator, you can increase the number of available IP addresses in the subnet by reducing the subnet mask, i.e., the CIDR notation value. Changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 will increase the number of usable IP addresses in the range, providing more IP addresses for the virtual machines in your project.

Here's why the other options will not work:

A. Converting the subnet IP range from IPv4 to IPv6 would not solve the problem, as it would require significant changes and compatibility assessment in the entire network infrastructure, including software applications. Additionally, this would not directly increase the number of IP addresses in the current IPv4 range.

B. Enabling Private Google Access for the virtual machines would provide them with a way to access certain Google Cloud services without assigning them external IP addresses. However, this option does not increase the available internal IP addresses within the 10.0.0.0/20 range, which is the primary concern in the question.

D. Changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/17 would indeed provide a larger number of IP addresses, but this is a more drastic change than required. By decreasing the CIDR notation to /18, you get an adequate increase in IP addresses while keeping the network more organized and less prone to potential management and security issues as compared to using a /17 subnet.

Therefore, the most suitable course of action to provide more IP addresses for the virtual machines is to change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 (option C).

Solution to Question 13: D

The answer should be D. Use Cloud Spanner for data storage.

Explanation:

Option A: Cloud Memorystore is an in-memory data store managed by Google Cloud. It provides caching solutions, such as Redis and Memcached, which facilitate high performance by keeping frequently accessed data in memory. Despite its high performance, Cloud Memorystore is not designed to handle relational data storage structures, and it does not natively ensure consistency across multiple regions. Thus, it is not the best choice for a trading application catering to clients worldwide.

Option B: Cloud Filestore is a managed file storage service designed to provide shared storage for applications that run on Compute Engine and Kubernetes Engine. While it offers shared storage for multiple applications, it does not support the relational data storage structure needed for the trading application. Furthermore, it also does not ensure data consistency across multiple regions, making it unsuitable for this scenario.

Option C: Cloud SQL is Google Cloud's managed relational database service that supports MySQL, PostgreSQL, and SQL Server. Although it handles relational data storage well and ensures data consistency, it lacks the ability to natively replicate data across multiple regions. This limitation affects performance and increases latency for clients. Therefore, it is not the most optimal choice for a trading application deployed globally.

Option D: Cloud Spanner is a highly scalable, globally distributed, relational database service designed for mission-critical applications. It supports strong consistency across multiple regions, ensuring the data state remains consistent among all clients. In addition, it provides low latency by choosing the closest regional replica for serving client requests. This makes Cloud Spanner the most suitable choice for the trading application catering to global users with minimal latency.

Solution to Question 14: A

The most effective approach to achieve automatic recreation of unhealthy VMs for a client's HTTPS web application is:

A. Create a health check on port 443 and use that when creating the Managed Instance Group.

Explanation:

Option A is the correct answer because configuring a health check on port 443 specifically targets HTTPS traffic. A health check is a critical component of an autoscaling managed instance group, as it determines and monitors the health of the instances in the group. It ensures that VMs that are not performing optimally are automatically replaced with healthy instances. By configuring a health check on port 443, you ensure that the health check is performed for the secure HTTPS traffic that the web application utilizes, resulting in a more effective approach to maintaining high availability.

Why other options will not work:

B. Enable Stackdriver Monitoring and Logging for the Managed Instance Group: While Stackdriver Monitoring and Logging can help observe the performance and gather diagnostic information for your Managed Instance Group, it does not actively rectify issues, i.e., it does not automatically recreate unhealthy VMs in response to the monitoring data.

C. In the Instance Template, add a startup script that sends a heartbeat to the metadata server: Although this approach could provide some information about the VM's health, it would not be as effective as a health check because it would not take into account the application's specific needs or performance criteria. Additionally, it would require manual monitoring and efforts to respond to instances deemed as unhealthy, defeating the purpose of auto-scaling.

D. Use the default health check for network load balancing when creating the Managed Instance Group: The default health check for network load balancing is designed for the port and protocol that your load balancer uses. In this case, as the application runs on HTTPS, it is more effective to specifically configure the health check for the secure HTTPS traffic on port 443, as it will ensure that the health check is performed specifically for the traffic type the web application is utilizing. Using the default health check would not provide the same level of specificity and reliability as using a health check tailored for the HTTPS traffic.

Solution to Question 15: C

The correct answer is C, and here's why:

Option A is not ideal because it mentions enabling API access without creating custom roles or assigning Google group permissions. This approach does not guarantee that developers will have the same permissions across projects, nor does it ensure compliance with the company's security policy.

Option B is incorrect because it involves creating a custom role for each project and making all developers Project Owners. This could give developers additional permissions beyond Compute Engine, Cloud Functions, and Cloud SQL, violating the security policy.

Option C is the best choice because it follows the security policy and ensures consistent access for developers across all projects. By adding all developers to a Google group in Cloud Identity, you can manage their permissions collectively, simplifying the process. Creating a custom role at the Google Cloud organization level and assigning it to the Google group provides the same level of access to Compute Engine, Cloud Functions, and Cloud SQL for all developers. This method requires minimal effort and ensures compliance with the security policy.

Option D is not suitable because it involves creating individual custom roles for each service within each project. This approach can be time-consuming and does not guarantee that all developers will have the same permissions across projects.

In conclusion, Option C is the most effective way to ensure that all developers

have the same permissions across all Google Cloud projects while adhering to the company's security policy.

Solution to Question 16: A

The correct answer is A: Deploy the monitoring pod in a DaemonSet object.

Explanation: A DaemonSet ensures that all (or some) nodes in the cluster run a copy of the specified pod. As nodes are added to or removed from the cluster, the DaemonSet automatically scales the number of pod instances accordingly. In this case, deploying the monitoring pod in a DaemonSet object is the ideal solution because it ensures that each node in the GKE cluster runs the monitoring pod. This satisfies the requirement that each node should send container metrics to a third-party monitoring solution.

Why other options will not work:

B. Deploy the monitoring pod in a CronJob object: A CronJob object is used to manage time-based jobs that run periodically. It is not a suitable choice for deploying a monitoring pod that should run persistently on each node. A CronJob would only deploy the monitoring pod at specific intervals and not on each node in the cluster.

C. Reference the monitoring pod in a Deployment object: Deploying the monitoring pod as a Deployment object can be useful for creating multiple replicas of the pod. However, a Deployment doesn't ensure that each node in the cluster runs the monitoring pod. Instead, it only ensures that the desired number of replicas is maintained across the cluster.

D. Configure the monitoring pod as a sidecar in all deployments: A sidecar pattern in Kubernetes is used to deploy a secondary, helper container alongside the main container in a single pod. Although this approach could be used to deploy a monitoring pod, it would require adding the monitoring container to all existing and future deployments in the cluster. This adds complexity and maintenance overhead compared to using a DaemonSet, which automatically ensures that the monitoring pod runs on all specified nodes.

Solution to Question 17: D

The correct answer is D: Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Explanation:

The scenario explains that the client is running their infrastructure on-premises, and now they would like to use Google Cloud to handle additional workloads while still being able to communicate between the environments using private IP ranges. To achieve this goal, a secure way of connecting the on-premises infrastructure and the Google Cloud Platform (GCP) environment is required. The most suitable solution, in this case, is setting up Cloud VPN between the on-premises infrastructure and Google Cloud.

Cloud VPN provides a secure, private connection between the client's on-premises infrastructure and their Google Cloud VPC network. The private IP addresses on both sides can communicate with each other over the encrypted VPN tunnel, allowing workloads from on-premises infrastructure to seamlessly interact with those running on Google Cloud.

Here is why other options will not work:

A. Use Cloud Interconnect to connect the on-premises infrastructure and Google Cloud without VPN: While Cloud Interconnect does provide a way to connect the on-premises infrastructure to GCP, it does not offer the secure VPN tunnel that the scenario requires for private IP communication. Cloud Interconnect is also more suited to large-scale organizations or those needing dedicated, high-speed connections to GCP, making it not the best fit for this situation.

B. In Google Cloud, configure the VPC for VPN tunneling using public IP addresses: This option would not provide the necessary private IP range communication that the client requires. Using public IP addresses for VPN tunneling exposes the connection to the public internet, which comes with potential security risks. Moreover, it does not cover communication between the two environments using private IP addresses.

C. In Google Cloud, configure the VPC for Private Google Access: Private Google Access allows VM instances in GCP that do not have external IP addresses to reach the public Google APIs and services. However, it does not provide a direct connection to the on-premises infrastructure or enable communication using private IP ranges as the client requires.

In summary, the best solution for this scenario is to set up Cloud VPN between the infrastructure on-premises and Google Cloud, as it meets the requirements of secure communication and private IP range communication between the two environments.

Solution to Question 18: A

The correct answer is A: Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

Explanation: The given requirement is that the DevOps team needs complete access to the Compute Engine resources within the development project without allowing them to create or modify other resources in the project. According to Google's recommendations for assigning permissions, granting a basic role and a predefined role related to the resource is the best practice.

Option A is correct because it grants the DevOps team basic viewer permissions (roles/viewer) and a predefined role for Compute Engine resource administration (roles/compute.admin), which meets the requirement specified. The DevOps team can access all the Compute Engine resources and manage them, while not being able to modify other resources in the project.

Option B: Granting the basic role roles/editor to the DevOps group is incorrect because it gives the team broader permissions than what's required. The editor role can create, modify, and delete resources in the project, which goes beyond the necessary permissions related to the Compute Engine resources.

Option C: Creating a custom role at the project level may seem like a valid option, but it is not recommended by Google. It can be challenging to maintain and update custom roles, and predefined roles generally satisfy most use cases. Moreover, custom roles can lead to human errors or vulnerabilities if not correctly configured.

Option D: Creating an IAM policy with compute.networkAdmin.* permissions is incorrect because it is too restrictive. It only grants permissions to manage network-related resources within Compute Engine, not providing the DevOps team with the necessary access to manage all aspects of the Compute Engine resources in the project.

Thus, the best course of action to adhere to Google's recommendations for assigning permissions is by choosing option A: Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

Solution to Question 19: A

The correct answer is A - Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

Explanation for why A is the correct answer: When providing access to a BigQuery dataset to another project, the appropriate approach is to use Service Accounts, which allow you to specify access and permissions at a granular level for external entities. By having the partner company create a Service Account in their project, you maintain separation between projects and organizations. Once the Service Account is created, you can grant it access to the specific BigQuery dataset in your project, without exposing other resources.

Reasons why other options would not work:

B. Ask the partner to create a Service Account in their project, and have them give the Service Account access to Cloud Storage in their project. This option is incorrect because granting access to Cloud Storage in the partner's project would not provide access to the BigQuery dataset in your project. Although Cloud Storage can be used to store data, providing access to Cloud Storage alone would not grant access to the specific dataset required for the recommendation engine.

C. Ask the partner to create a Service Account in their project, and have them give the Service Account access to App Engine in their project. Giving access to App Engine in the partner's project does not provide the necessary access to the BigQuery dataset in your project. App Engine is for hosting and running

applications, not for granting access to data stored in an external BigQuery dataset.

D. Create a Service Account in your own project, and ask the partner to grant this Service Account access to App Engine in their project. This option is incorrect because it does not address the primary objective of providing access to the BigQuery dataset in your project to the partner company. Granting access to App Engine in the partner's project would not give them access to the required dataset for the recommendation engine.

In summary, the best option is A - to have the partner create a Service Account in their project and grant the Service Account access to the BigQuery dataset in your project.

Solution to Question 20: D

The correct answer is D. This is because the question specifically asks for a policy to handle video files stored in a Cloud Storage Regional bucket, which requires the use of Cloud Storage Object Lifecycle Management. The Age conditions are the appropriate way to manage these requirements.

Reasons why other options will not work:

Option A: Cloud Storage Transfers service wouldn't be the right approach for this problem, as it mainly focuses on transferring data between buckets, and it is not suited for managing data lifecycle policies like moving videos to Coldline storage or deletion upon aging.

Option B: Using Cloud Storage Object Lifecycle Management with Age conditions is appropriate; however, this option's SetDeleted action is not correct. The SetDeleted action term doesn't exist. Instead, the Delete action should be used and set to 365 days, not 275 days. This ensures the files are deleted after one year, not 90 days short of a year.

Option C: Using Timestamp conditions is not the ideal choice for this scenario. The Timestamp conditions are based on the specific timestamps or dates, while Age conditions fit better when defining policies based on the number of days from object creation. With Age conditions, the policy will automatically adjust itself as new objects are created, making it a better fit for the given requirements.

Solution to Question 21: C

The correct answer is C because creating a GKE node pool with a sandbox type configured to gvisor and adding the parameter runtimeClassName: gvisor to the specification of your customers' Pods will ensure maximum isolation between the Pods belonging to different customers. gVisor is a container runtime that provides a strong security boundary by intercepting and controlling the interactions between containers and the host kernel, thus preventing arbitrary code execution and unwanted access between Pods.

Option A is incorrect because Google Cloud Private Catalog enables you to

manage and share container images within your organization's approved products list. It does not provide isolation between different tenants' Pods in the GKE cluster.

Option B is incorrect because Binary Authorization helps you in enforcing security policies by allowing only approved and verified container images to run in your GKE cluster. While it enhances the security of your cluster, it does not provide isolation between the Pods belonging to different customers, which is the primary requirement in this scenario.

Option D is incorrect because Cloud Armor is a network security solution designed to protect applications and services running on Google Cloud by helping you in managing and implementing security policies, such as allowing or denying traffic based on IP addresses, geographical regions, or user-defined configurations. However, Cloud Armor does not offer the container-to-container isolation necessary for securely running arbitrary code in a multitenant environment like GKE.

Solution to Question 22: A

The correct answer is A. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

Option A meets all company requirements as it allows you to keep documents for five years, store up to five revisions of the same invoice, and move older documents to lower cost storage tiers. By enabling object versioning on the bucket, you maintain the ability to have multiple revisions of an invoice. Lifecycle conditions give you the ability to automatically change the storage class of objects based on their age, allowing cost savings. Moreover, setting the number of versions and deleting old files ensures that you are maintaining efficient storage management, adhering to Google-recommended practices, and minimizing operational and development costs.

Option B is incorrect because enabling retention policies and using Cloud Pub/Sub to trigger a Cloud Run instance creates a more complex solution that requires additional management, development, and operational costs. Retention policies are more suitable for ensuring data immutability, rather than versioning.

Option C is incorrect as Cloud Data Transfer Service doesn't provide mechanisms for managing document revisions or storage classes based on metadata. This approach does not allow for storage class changes or version control based on the company's requirements.

Option D is incorrect because it proposes using Google Cloud SQL and Cloud Datastore for managing storage requirements, which is not the intended use of these services. Such an approach would increase development costs, complicate maintenance, and would not follow the Google-recommended practices for handling these specific storage requirements.

Solution to Question 23: D

The correct answer is D: Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

Explanation: The main goal is to ensure that only the new instance can access the application installation files stored on Cloud Storage, without allowing other VMs to access them. By creating a new service account and assigning it to the new instance, we create a separate and unique identity for this instance. Then, by granting this service account the necessary permissions on Cloud Storage, we ensure that only this instance with the assigned service account will have access to the files.

Reasons why other options will not work:

A. Changing the storage class of objects on Cloud Storage to Nearline storage won't restrict the access to the new instance exclusively. Nearline storage is designed for data that can be stored with lower access latency and higher availability but doesn't provide access controls for different service accounts.

B. Attaching a new Cloud Storage bucket to the instance for the application files only does not ensure that other VMs won't be able to access the files. It just creates a new bucket, but the access control is not appropriately set to restrict other VMs.

C. Cloud Identity-Aware Proxy (IAP) is used to control access to web applications and services running on the Cloud Platform. While it provides secure access control, it is not applicable to Cloud Storage objects and won't limit access to the new instance exclusively.

In conclusion, the correct approach would be to create a new service account, assign it to the new instance, and grant it the required permissions on Cloud Storage (option D). This ensures that only the new instance will have access to the application installation files.

Solution to Question 24: B

The correct answer is B. You should use the command `gcloud auth activate-service-account` and point it to the private key.

Explanation for option B: The `gcloud auth activate-service-account` command is specifically designed to authenticate and authorize gcloud commands when provided with the private key of a Service Account. This command allows you to activate a service account on your local machine and use it for gcloud command-line interactions. It sets up the required environment variables and configuration settings locally so that you can perform authorized operations on your Google Cloud resources.

Why other options don't work:

Option A: `gcloud init` is used to set up a new or reinitialize an existing gcloud environment, and it is primarily used for interactive initialization. Although it can be used to authenticate a user account, it does not have an option to directly point to a service account private key.

Option C: `gcloud config set account` is used to change the default account associated with your gcloud environment. It does not authenticate the Service Account itself or require a private key. Instead, it switches the active user account in the gcloud configuration.

Option D: There is no `gcloud auth login-service-account` command in the gcloud CLI. The correct command to authenticate a Service Account is `gcloud auth activate-service-account` as given in option B.

Hence, the most suitable option for authenticating and authorizing the gcloud commands using the private key of a Service Account is option B: Use the command `gcloud auth activate-service-account` and point it to the private key.

Solution to Question 25: A

The correct answer is A. Select Compute Engine. Use preemptible VM instances of the appropriate standard machine type.

Here's why:

An IT manager's primary objectives for the nighttime batch processing jobs are to reduce costs and ensure successful job completion.

Option A - Compute Engine with preemptible VM instances is the most cost-effective choice as these instances are available at a lower price than regular instances. Preemptible VM instances are well-suited for this purpose since they run on Google's Compute Engine and can be used for tasks that aren't time-critical and can be interrupted. In this case, the nightly batch processing jobs can be repeated in the event of unexpected interruptions or terminations and still be successfully completed before the new day begins.

Option B - Using Google Kubernetes Engine (GKE) with a multi-node cluster with large instance types is not optimal as it's more complex and requires additional setup compared to Compute Engine. Additionally, the cost of running large instance types for the nightly batch processing jobs will be significantly higher when compared to preemptible VM instances without providing a significant gain in efficiency or success rate.

Option C - Using GKE with a three-node cluster with micro instance types is also not suitable as it might not provide the necessary performance to complete the jobs. Micro instance types are often not as powerful or efficient for compute-intensive workloads. Additionally, GKE management and cluster setup costs could be higher compared to Compute Engine preemptible VM instances.

Option D - Selecting App Engine with a flexible environment and automatic

scaling is not ideal. Although App Engine can scale instances automatically, it's designed to manage web applications that need to scale dynamically during the day due to varying user demand. The financial services company's requirement is for batch processing that occurs nightly, meaning the scaling feature in App Engine does not provide any significant cost savings or efficiently manage necessary resources.

Overall, selecting Compute Engine and using preemptible VM instances of the appropriate standard machine type best meets the IT manager's requirements for minimizing costs while ensuring successful completion of nightly batch processing jobs.

Solution to Question 26: A

The correct answer is A. Change the primary key to not have monotonically increasing values.

Explanation for why A is the correct answer:

When using Cloud Spanner, it is essential to avoid designing primary keys with monotonically increasing values, as this can cause read and write hotspots on a single node. By changing the primary key to not have monotonically increasing values, the data will be distributed more evenly across the nodes in the database, which improves read and write performance.

Explanation for why other options will not work:

B. Change the primary key to a composite key consisting of person_id and created_at: While creating composite keys can sometimes help balance workload, simply adding created_at to the primary key might not resolve the issue if both person_id and created_at still have monotonically increasing values. The goal is to avoid such a design for the primary key; therefore, this option is not appropriate for solving the read latency-related performance issue.

C. Enable interleaved tables to improve read performance: Interleaved tables are useful when you want to optimize the performance of queries involving parent-child relationships between tables. However, in this particular case, the issue is related to read latency on a single table and not involving any parent-child relationship between tables. So, enabling interleaved tables would not necessarily resolve the primary key-related performance issue in this case.

D. Create a secondary index using the following Data Definition Language (DDL): Secondary indexes in Cloud Spanner can be useful to optimize query performance, but they do not directly address the primary key-related issue causing read latency in this specific situation. Moreover, the DDL is not specified, so we cannot assess whether the proposed index would be useful in this scenario.

Solution to Question 27: D

The correct answer is D: Create a single custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range.

Here's why the other options will not work:

A. Creating a single custom VPC with 3 subnets is unnecessary and adds complexity to the setup. The third subnet as a communication link between the production and test subnet is not required, since VMs in different subnets of the same VPC can communicate using their internal IPs. This also violates the requirement of having separate subnets for production and test VMs.

B. Creating a single custom VPC with 2 subnets in different regions using the same CIDR range is an incorrect setup. Overlapping CIDR ranges within the same VPC will cause IP address conflicts and routing issues, making it impossible for the VMs to effectively communicate with each other.

C. Creating 2 custom VPCs, each with a single subnet in different regions using the same CIDR range does not fulfill the requirement of allowing all VMs to connect with each other using internal IPs without creating additional routes. Although VMs can communicate across different VPCs using VPC peering, this will require additional configuration and create an unnecessarily complex network setup.

Option D is the best solution because it allows for the desired setup of separate subnets for production and test VMs in a single VPC, following the best practices for resource organization and control. By using different CIDR ranges for the subnets, you avoid IP conflicts, and since they are within the same VPC, VMs can communicate using their internal IPs without additional routing configurations. Furthermore, having each subnet in different regions provides geographical redundancy and supports the company's growth.

Solution to Question 28: D

The correct answer is D. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

Explanation:

To grant access to the service account in the web-applications project according to Google's recommended practices, you should follow the principle of least privilege, which means that you should grant only the required roles and permissions to the service account.

Option A is incorrect because granting the roles/bigquery.admin(role) to the crm-databases project and "project viewer" role to the web-applications project would provide excessive permissions. The service account in the web-applications project does not need administrative access to the crm-databases project.

Option B is incorrect because granting the "project owner" role to both crm-databases and the web-applications project would give the service account ex-

cessive and unnecessary permissions, which goes against the principle of least privilege.

Option C is incorrect because granting the "project owner" role to crm-databases also gives excessive permissions to web-applications. Instead, granting the roles/bigquery.dataViewer role to the web-applications project would allow the service account to access BigQuery datasets in the crm-databases project according to least privilege.

Option D is correct because granting the roles/bigquery.dataViewer role to the crm-databases project appropriately allows read-only access to the datasets within the crm-databases project. Additionally, you should grant the appropriate roles to the web-applications project, which provides the necessary access without giving excessive permissions. This follows the principle of least privilege, making it the best option.

Solution to Question 29: B

The correct answer is B. The reason why this is the most efficient way to disable the logs is that going to the Logs ingestion window in Stackdriver Logging and disabling the log source for the GKE container resource directly addresses the issue with the excessive logs being generated by the GKE development container. Disabling the GKE container resource will efficiently prevent these logs from being produced and will not require any additional steps or modifications.

Option A is incorrect because disabling the log source for the GKE Cluster Operations resource would not affect the logs generated by the GKE container itself. It would only disable logs related to the operations of the GKE cluster, not the logs generated by the specific container causing the excessive logging issue.

Option C is not the most efficient method because it involves several steps, including temporarily disabling the GKE container. This could lead to unnecessary downtime and additional work reconfiguring the logging settings. Additionally, after these steps are completed, you would need to restart the container, which might not be the most efficient way to handle the issue in a production environment.

Option D is also incorrect because setting log-based metrics to zero in the Monitoring console would not actually disable the logs. Log-based metrics are useful for gaining insights and understanding the performance of various resources, but adjusting their values will not stop the logs from being generated and contributing to the higher costs experienced by your projects.

In conclusion, the best option for disabling the GKE development container logs efficiently with the fewest steps is Option B - going to the Logs ingestion window in Stackdriver Logging and disabling the log source for the GKE container resource. This direct approach effectively addresses the issue without causing unnecessary downtime or altering unrelated settings.

Solution to Question 30: B

The correct answer is B. Upload the data to Cloud Storage using the gcloud storage command.

Explanation:

As a data engineer managing massive amounts of unstructured data, you need a scalable and efficient storage solution to handle the data in various file formats. Google Cloud Storage (GCS) is designed explicitly for this purpose, offering robust, highly available, and cost-effective storage that can cope with huge amounts of unstructured data.

Uploading the data to Cloud Storage using the gcloud storage command provides an excellent platform for performing ETL transformations and processing the data. Moreover, GCS seamlessly integrates with Google Dataflow, allowing you to efficiently process the data within your organization.

Why the other options will not work:

A. Kubernetes Engine, while an excellent platform for deploying containerized applications, is not well-suited for large-scale storage and processing of unstructured data. It is not designed for ETL scenarios but for orchestrating and managing containerized apps.

C. BigQuery is a robust and highly efficient data warehousing solution. However, it is specifically designed for structured data and not ideal for handling unstructured data in various file formats. Uploading the unstructured data to BigQuery without proper transformations would not fulfill the required purpose.

D. Firestore is a scalable NoSQL database offered by Google Cloud, well-suited for storing and synchronizing small documents. However, when dealing with large amounts of unstructured data in various formats, Firestore is not the optimal choice for ETL transformations and integration with Dataflow.

In conclusion, uploading the data to Cloud Storage using the gcloud storage command (Option B) is the best approach for managing unstructured data and performing ETL transformations within the given scenario, mainly due to its compatibility with Google Dataflow and its ability to handle massive amounts of data in different file formats.

Solution to Question 31: D

The correct answer is D. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

The reason why option D is the best choice is that it directly addresses the client's concern about data egress security by ensuring that only the necessary ports are open. By setting up a low-priority rule that blocks all egress traffic and a high-priority rule that allows only the essential ports, the firewall will ensure that egress traffic is tightly controlled and minimized according to the client's requirements.

The other options are not as effective in addressing the client's concerns or they deal with other aspects of network security:

Option A - Configure custom routes to block egress traffic on undesired ports: While this may help block traffic on certain ports, custom routes are not the same as firewall rules and are not primarily designed for controlling traffic in and out of the network. In addition, this method could become difficult to manage if there are many ports to block.

Option B - Use a VPN tunnel to manage egress traffic by allowing only specific ports: Although a VPN tunnel can increase the network's overall security, it will not directly address the issue of limiting egress ports. A VPN tunnel can encrypt and redirect traffic, but it doesn't control which ports are opened or closed.

Option C - Configure a NetworkPeering policy to limit egress traffic to specific subnets: Network Peering is used for connecting two VPCs and enabling traffic flow between them. This does not directly address the issue of limiting egress ports for an application. It serves a different purpose.

In conclusion, option D is the most efficient and effective solution for meeting the client's requirement of minimizing the number of open egress ports. By setting up a high-priority rule that allows only the necessary ports and a low-priority rule that blocks all other egress traffic, the network administrator can ensure a secure environment in line with the client's needs.

Solution to Question 32: D

The correct answer is D because it outlines the appropriate procedure for deploying a Dockerfile on Kubernetes Engine. In this option, we create a Docker image from the Dockerfile and upload it to Google Container Registry, which is a private registry for Docker images. Then, we create a Kubernetes Deployment YAML file that references the uploaded Docker image. Finally, the kubectl command is used to create the deployment based on the YAML file.

Option A is incorrect as it suggests converting the Dockerfile into a Kubernetes configuration file, which is not the correct approach. A Dockerfile serves as a set of instructions for building a Docker container image, whereas a Kubernetes configuration file (YAML) is used to define the desired state of a Kubernetes cluster.

Option B is incorrect because it attempts to deploy the Dockerfile directly by using the kubectl run command with the Dockerfile's name as the image reference. However, the actual requirement is to deploy the Docker image created from the Dockerfile and not the Dockerfile itself.

Option C is incorrect because it recommends uploading the Docker image to Datastore, which is a NoSQL database provided by Google Cloud Platform. Datastore is not designed to store and manage Docker images; it is used for

structured data storage. The correct place to store Docker images for use with Kubernetes Engine is Google Container Registry, as stated in option D.

Solution to Question 33: A

Option A: Use the command gcloud config set container/cluster dev.

This is the correct answer because it sets the default cluster property within the gcloud configuration. By running `gcloud config set container/cluster dev`, the specific 'dev' cluster will be addressed as the default for any future gcloud CLI commands performed with the Cloud SDK. As a result, the IT engineer can easily manage the GKE configuration for that specific cluster.

Option B: Use the command gcloud container clusters get-credentials dev –region us-central1.

This option is incorrect because it only fetches the access credentials for the 'dev' cluster and configures kubectl to use them. It does not set the cluster as the default in the gcloud configuration. While kubectl might be set to the correct cluster, any gcloud CLI commands would not implicitly target the 'dev' cluster by default.

Option C: Create a file called kubernetes.config in the ~/.gcloud folder that contains the cluster name.

This is incorrect because the ~/.gcloud folder does not store configurations like cluster names. Creating a file named kubernetes.config does not have any influence on the gcloud CLI commands or the default cluster setting.

Option D: Create a file called defaults.json in the ~/.gcloud folder that contains the cluster name.

This option is incorrect because, similar to option C, the ~/.gcloud folder does not store default configurations for the container or cluster. Creating a file named defaults.json would not impact the behavior of gcloud CLI commands and would not set the default cluster to the 'dev' cluster.

Solution to Question 34: C

The correct answer is C. Here's why:

A. Using the compute-optimized machine type nodes for both the image rendering microservice and the other microservices will waste resources, as not all microservices require high CPU time. Instead, it would be better to use these resources only for the necessary microservices, in this case, the image rendering microservice.

B. Using a node pool with general-purpose machine type nodes for the image rendering microservice may cause insufficient resources for it, leading to slower processing and performance. Also, while preemptible machine type nodes are cost-effective, they aren't guaranteed to be available all the time; they can be terminated unexpectedly, which isn't suitable for critical microservices.

C. Creating a node pool with compute-optimized machine type nodes for the image rendering microservice addresses the high CPU requirements, while using the node pool with general-purpose machine type nodes for the other microservices ensures that they have the necessary resources to function efficiently without over-allocating resources. This approach maximizes resources' utilization and performance.

D. Assigning higher pod priority to the image rendering microservice doesn't address the underlying resource requirements issue. While it may improve the scheduling of the microservice, it still wouldn't allocate the proper resources for that microservice to function at its best. The resource allocation problem would persist, leading to potential performance issues.

In conclusion, the only viable solution is option C, as it tailors the resources of the Kubernetes Engine cluster to meet the needs of the different microservices, ensuring efficiency and optimized performance.

Solution to Question 35: D

The correct answer is D because creating a budget per project and configuring budget alerts on all of these budgets allows a department manager to receive notifications if an individual developer's project surpasses the monthly spending limit of $500. By creating individual budgets, specific to each project, the manager can track and receive notifications for each developer's expenses separately, ensuring that no project's costs are overlooked or masked by others.

Option A is not ideal because setting up a separate billing account per sandbox project and creating a Data Studio dashboard would only visualize the spending but not provide automatic notifications when a specific project surpasses the spending limit. This requires manual monitoring, which is less efficient and effective.

Option B is not suitable because creating a single budget for all projects does not enable the department manager to track individual project expenses separately. If one project surpassed the $500 limit, the manager would not receive a dedicated alert or easily pinpoint which project is causing excessive spending.

Option C is also not the best choice as setting up daily cost quotas and manually monitoring spending can be a time-consuming task and lacks the automatic notification capabilities. This method may also not be as accurate or efficient as configuring budget alerts for individual project budgets.

Solution to Question 36: C

The correct answer is C, enable delete protection on the instance. This is because enabling delete protection will prevent the accidental deletion of a Compute Engine instance by ensuring that the instance cannot be deleted unless the delete protection is explicitly removed.

Here's why the other options will not work:

A. Enable Preemptibility on the instance: Preemptibility is a feature that allows Google Cloud to preempt (shut down) a Compute Engine instance if resources are needed elsewhere or in case of pricing constraints. This option would not protect the instance from accidental deletion and may even lead to the instance being shutdown more frequently.

B. Use the minimal CPU platform for the instance: The CPU platform is an attribute that determines the type of processors available to a Compute Engine instance. Choosing the minimal CPU platform will have minimal impact on the performance and cost, but it will not have any effect on safeguarding an instance from accidental deletion.

D. Disable Automatic restart on the instance: Automatic restart is an option that configures the instance to automatically reboot when it experiences an unplanned outage or maintenance event. Disabling automatic restart does not protect the instance from deletion but instead may lead to the instance remaining unavailable in case of an outage or maintenance event.

Therefore, the best choice to safeguard the instance from accidental deletion is option C, enabling delete protection on the instance.

Solution to Question 37: A

The correct answer is A. Automatic Scaling with min_idle_instances set to 3.

Here's why:

A. Automatic Scaling with min_idle_instances set to 3 - This is the correct choice because App Engine's Automatic Scaling scales instances based on incoming request rates. By setting the min_idle_instances parameter to 3, it ensures that there will always be at least three unoccupied instances available to handle fluctuations in user demand.

B. Automatic Scaling with max_idle_instances set to 3 - This option is not suitable as it sets an upper limit of three unoccupied instances, thereby potentially limiting the ability to handle unexpected spikes in user demand. The company needs the application to scale based on request rate, and limiting the number of idle instances is not the best way to achieve this.

C. Automatic Scaling with target_throughput_utilization set to 3 - This is also not suitable because target_throughput_utilization is a floating-point number between 0 and 1 that represents the desired utilization of each instance. A value of 3 is invalid and will not be accepted by the system. Moreover, it does not guarantee a minimum of three unoccupied instances as required.

D. Basic Scaling with target_cpu_utilization set to 3 - This option is not adequate because Basic Scaling does not scale based on request rate, which is a crucial requirement for the company. Basic Scaling is more appropriate for workloads with predictable, steady user demand, and not for applications that need to handle rapid fluctuations in user traffic. Setting target_cpu_utilization to 3 is also invalid as it should be a floating-point number between 0 and 1.

In conclusion, Option A, Automatic Scaling with min_idle_instances set to 3, is the best choice for deploying the application with the scalability and minimum unoccupied instances required by the company.

Solution to Question 38: B

The correct answer is B. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

Explanation: The BigQuery Job User role (roles/bigquery.jobUser), when granted to your default App Engine Service account, will allow your application to read data from the BigQuery dataset in the other team's project. This role enables your App Engine Service account to run BigQuery jobs, which includes querying the required data for visualization purposes. This is the most straightforward and secure way to share access to BigQuery between projects.

Here's why the other options will not work:

A. Request the other team to export their BigQuery dataset to Cloud Storage which your App Engine service can then read and visualize: This approach provides an indirect way to access data and adds unnecessary complexity to the process. It would require the other team to continually export updated data to Cloud Storage, increasing the chances of your application working with outdated data and creating synchronization issues.

C. Ask the other team to create a Storage Bucket containing their BigQuery dataset and grant you access to read from the bucket: Similar to Option A, this is an indirect approach and has the same drawbacks. It requires exporting the data to a bucket and may lead to synchronization issues, plus an increased risk in data readability and latency during visualization.

D. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer: Granting the BigQuery Data Viewer role (roles/bigquery.dataViewer) to your service account in your own project will not help access data in the other team's project. You need the other team to grant your service account the required role (BigQuery Job User) in their project to access their BigQuery dataset.

Solution to Question 39: B

The answer should be B because it uses the Google-recommended solution for backing up Compute Engine instance disks with minimal management overhead. This approach involves creating a snapshot schedule directly from the Cloud Console for the instance's disk. This method ensures that backups are created daily during the specified time, keeping the snapshots aligned with the application work-hours, and automatically deleting snapshots older than 30 days. This process reduces management overhead while providing an effective backup and retention strategy.

Option A is incorrect because updating the instances' metadata with backup-frequency and backup-retention values does not automatically create backups

or manage retention. Metadata values are used to provide information about instances, but they do not implement the desired actions.

Option C is not suitable because using Cloud Endpoints to create snapshots and manage retention would require additional work to create and maintain APIs, which is contrary to the requirement of minimal management overhead and the least number of services.

Option D is invalid because Data Loss Prevention (DLP) is a service primarily meant for discovering and managing sensitive data. It does not provide native support for creating daily backups of Compute Engine instance disks or automatically deleting backups older than a specified number of days.

Solution to Question 40: A

The correct answer is A, and here's why:

Option A follows Google-recommended practices to provide access to Cloud Storage for servers without public IP addresses or internet access. By creating a tunnel to a VPC in Google Cloud using Cloud VPN or Interconnect, the connection between the on-premises network and Google Cloud is secure and private. Cloud Router is then utilized to create a custom route advertisement and announce the network to the on-premises network through the VPN tunnel. Finally, configuring the on-premises DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com ensures that access is limited to only the required services, keeping the security policies in place. This setup adheres to both the company's security policies and Google-recommended practices.

Option B does not work because using Cloud NAT creates a managed NAT gateway within the Google Cloud VPC; however, this option does not provide a secure and private connection to Google Cloud Storage for the on-premises network lacking public IP addresses.

Option C is not a suitable solution because Cloud Pub/Sub introduces unnecessary complexity to the system. The communication process would have to go through additional steps of processing, message sending, and Cloud Function triggering, rather than directly accessing Google Cloud Storage securely.

Option D is not a suitable choice because replacing Cloud Storage with Filestore requires significant changes to the application and manual synchronization. Additionally, this setup doesn't make use of the best practices laid out by Google and doesn't provide direct access to Cloud Storage, which is the ultimate goal for the application's needs.

Solution to Question 41: B

The most appropriate approach to meet the requirements and follow Google-recommended practices is Option B: Deploy your solution to an instance group and set the autoscaling based on CPU utilization.

Here's why Option B is the correct choice and why the other options will not work:

Option A: Deploy your solution to an instance group without autoscaling, and manually add instances when CPU utilization is high.

This option does not follow Google's recommended practices for automating operations. Manually adding instances when CPU usage is high may lead to delays and is inefficient. It may also cause disruptions in the high availability and uninterrupted encoding process due to a lack of timely resource scaling.

Option B: Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

As mentioned, this is the most appropriate option. Autoscaling allows the instance group to automatically add or remove instances based on the CPU utilization, which ensures high availability and uninterrupted encoding during peak usage. This approach follows Google's best practices for automating operations and provides improved resource management without interruptions.

Option C: Deploy your solution on multiple standalone Compute Engine instances, and increase the number of existing instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

This option is not as efficient as Option B since using multiple standalone instances lacks the benefits of autoscaling within an instance group. Maintaining multiple standalone instances also requires more manual intervention, which doesn't follow Google's automation best practices.

Option D: Deploy your solution to an instance group, but use memory utilization as the autoscaling metric instead of CPU utilization.

This option is not suitable for the given scenario because the requirement specifically states that the encoding process should function without CPU limitations. Memory utilization is not directly related to CPU performance, and using it as an autoscaling metric may not guarantee uninterrupted encoding during increased user activity. This might lead to underutilization of resources and a suboptimal deployment.

In summary, Option B best meets the requirements of a highly available, uninterrupted encoding process without CPU limitations. With autoscaling based on CPU utilization in an instance group, the company benefits from improved resource management, high availability, and adherence to Google-recommended practices for automating operations.

Solution to Question 42: C

The correct answer is C: Run gcloud projects list to get the project ID, and then run gcloud services list –project .

Here's why the answer is C and the other options will not work:

A. Run gcloud init to set the current project to my-project, and then run gcloud services describe my-project.

This option is incorrect because 'gcloud services describe' is not a valid gcloud command. Instead, you should use 'gcloud services list' to list the enabled APIs for a specific project.

B. Run gcloud projects get-iam-policy my-project, and then run gcloud services list –project my-project.

This option is incorrect because the command 'gcloud projects get-iam-policy' retrieves the IAM policy for a project, but it does not provide a list of enabled APIs. Then, using 'gcloud services list' requires the project ID, not the project name.

C. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

This option is correct because first, you list GCP projects to get the specific project ID assigned to 'my-project'. Then, you use 'gcloud services list' and the '–project' flag to list the enabled APIs for the corresponding project ID.

D. Run gcloud config list to view the project value, and then run gcloud services list –project=my_project.

This option is incorrect because 'gcloud config list' will display the configuration parameters, but it does not provide the project ID, which is required for the 'gcloud services list –project' command to work. Additionally, the project name is used in this command instead of the project ID, making it invalid.

Solution to Question 43: A

The correct answer is A. Go to Data Catalog and search for employee_ssn in the search box.

Here's why the other options will not work as effectively:

Option B. Write a script using the Google Cloud SDK to scan through every table in all the projects looking for the employee_ssn column. Writing a script would require more time and effort compared to conducting a quick search using the Data Catalog. Although this method could potentially work, it does not minimize effort as requested by the CEO.

Option C. Manually check each dataset in all the projects for the presence of an employee_ssn column. This method would take a significant amount of time and effort to accomplish, especially with over 1000 datasets to check. Manually checking the datasets does not meet the requirement of minimizing effort.

Option D. Configure a custom VPC Service Controls perimeter to restrict access to datasets containing employee_ssn. This option focuses on restricting access to datasets, not identifying tables containing a specific column. Additionally,

this method would still require locating the datasets with an employee_ssn column in the first place.

In conclusion, utilizing the Data Catalog's search feature (option A) is the most efficient and effective method for identifying all tables containing an employee_ssn column while minimizing effort.

Solution to Question 44: B

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

Option B is the best choice because it requires the least amount of steps to connect to the SQL Server 2017 instance on Compute Engine. Installing an RDP client on your desktop allows you to connect directly to the instance through Remote Desktop Protocol (RDP). This method involves setting a Windows username and password in the GCP Console to secure the connection, and then using these credentials to access the instance. With these steps, the connection can be established efficiently.

Option A is not the best choice because it mentions port 22, which is actually used for SSH connections, not Remote Desktop Protocol (RDP). RDP uses port 3389 by default, so verifying a firewall rule for port 22 is unrelated to connecting to the SQL Server instance via RDP.

Option C involves creating a VPN tunnel between your desktop and the GCP environment, which adds unnecessary complexity to the process of connecting to the SQL Server instance. Additionally, establishing a VPN tunnel between your desktop and GCP might not be possible due to corporate policies or other constraints.

Option D is incorrect because it refers to port 5432, which is typically used for PostgreSQL servers, not SQL Server instances. Like Option A, this choice is focused on the wrong port for establishing an RDP connection. RDP requires port 3389 for proper functionality, not port 5432.

Solution to Question 45: B

The best course of action for achieving the objective of allowing the BI department to execute custom SQL queries on the most recent data available in BigQuery is option B: Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

Option B is the most appropriate choice because it adheres to the principle of least privilege by giving the required permissions to the BI team without granting unnecessary additional permissions. By adding the BI team members to a Google Group and assigning the IAM role of BigQuery User, team members can execute their SQL queries directly on BigQuery's most recent data without having to copy data or involve external tools. The BigQuery User role comes

with the "bigquery.jobs.create" permission, enabling the execution of custom SQL queries.

Option A is not suitable because creating a service account with the BigQuery Data Transfer Service role would merely enable the BI team to copy the data from BigQuery instead of directly querying the latest data in BigQuery. Sharing private keys is also a security risk and against best practices.

Option C is not appropriate because using Cloud Composer to schedule a daily workflow would add operational complexity and additional delay between the data ingestion in BigQuery and when it becomes available to the BI team for querying. The BI team would not be working with the most recent data in real-time.

Option D is also not a good choice because creating a service account and distributing a new private key to each BI team member poses the risk of service accounts being used improperly or keys being compromised. Moreover, it does not specify the attached permissions and roles that would enable the custom SQL queries on the most recent data in BigQuery. The focus should be on using IAM roles to manage permissions instead of sharing keys.

Solution to Question 46: C

The correct answer is C, and here's why:

Creating a subnetwork in the same VPC, in europe-west1 ensures that both instances are within the same network infrastructure and will be able to communicate with each other securely and efficiently. This also adheres to Google's recommended practices. Using the first instance's private address as the endpoint ensures a direct and secure connection between the two instances.

Option A is not the best choice because Cloud Interconnect is unnecessary in this scenario. Cloud Interconnect is used to connect on-premises infrastructure with Google Cloud resources, but in this case, both instances are already within the same VPC. Therefore, it is an unnecessary additional step.

Option B is incorrect because deploying the new instance in the us-central1 region would not allow the application to be accessed from the europe-west1 region. Additionally, routing the network traffic through the existing subnetwork might lead to congestion and reduced performance.

Option D is also incorrect because creating an instance group with only one instance is not following Google's best practices for horizontal scaling. An instance group is designed to manage multiple instances, so using it for a single instance is not optimal. Furthermore, using the first instance's private address as the backend endpoint might result in reduced performance of the application.

Solution to Question 47: D

The correct answer is D. "Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the

same name as instance names." Here's an explanation of why this is the best choice, and the reasons why other options are incorrect:

A: While this option correctly asks you to verify the instance template and delete any persistent disks with the same name as instance names, it also suggests to set the disks.autoDelete property to true in the template. Setting disks.autoDelete to true will automatically delete the disks when deleting an instance, which may not be necessary to solve the issue of instance creation failure. It might also lead to accidental data loss.

B: Changing the instance group's region is unnecessary to resolve the issue. The main objective is to maintain the specified number of running instances, not to change the region they are in. Additionally, this option could cause data transfer and latency issues if the new region is not near existing resources.

C: This option suggests to create an instance template with valid syntax and ensure the instance names and persistent disk names do not match in the template. However, it does not mention deleting any existing persistent disks with the same name as instance names. Without this step, new instances may still fail to create due to conflicts with existing disks.

D: This is the correct answer. Creating an instance template with valid syntax will help ensure that new instances can be created with the correct configuration. Additionally, deleting any persistent disks with the same name as instance names will also resolve any naming conflicts that could prevent successful instance creation, thus maintaining the desired number of running instances.

Solution to Question 48: B

The correct answer is B: Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

An explanation for why B is the most efficient way to accomplish the ad hoc request:

1. BigQuery is built for handling large-scale data analytics quickly and efficiently, which aligns with the requirements of an ad hoc request.
2. In this case, we can use BigQuery's federated querying capabilities on Cloud Spanner backups stored in Cloud Storage, along with creating an external table on Cloud Bigtable, which allows for real-time data querying.
3. By creating two separate external tables and joining them through user fields, we can efficiently run analytics on the combined datasets without the need for additional data-preprocessing or replication.

Reasons why other options will not work as efficiently:

A. Cloud Pub/Sub is a messaging service used for real-time data streaming and communication between various services. It does not support direct data analytics or aggregation for joining data. This means additional processing and

storage would be required to achieve the desired result, making this option less efficient.

C. Cloud Datastore is a NoSQL database designed for web and mobile applications, rather than analytical workloads. It also requires replication of the data from Cloud Spanner and Cloud Bigtable. Querying and processing large volumes of replicated data would be less efficient compared to directly querying data in BigQuery, as suggested in option B.

D. Google Cloud Data Loss Prevention API focuses on discovering, classifying, and de-identifying sensitive information in text and images. It is not designed for joining or analyzing data across multiple sources. Although it can be used to protect sensitive user data, it would not help achieve the desired outcome of efficiently joining data from Cloud Spanner and Cloud Bigtable.

Solution to Question 49: C

The correct answer is C: Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

Here's why:

First, using a custom mode VPC network is necessary to meet the client's requirement of a shared address space of 10.19.0.1/22. Custom mode VPC networks allow you to control the IP address ranges of your subnetworks, unlike automatic mode VPC networks, which assign predetermined IP ranges. This eliminates option B.

Second, dynamic routing is essential to establish a secure and reliable VPN connection as per the client's specifications. Dynamic routing can be achieved by using Cloud Router border gateway protocol (BGP) routes. BGP is a widely used routing protocol that exchanges routing information between autonomous systems, which helps maintain the VPN's high availability and reliability. This eliminates options A and D, which propose using static routes.

Finally, the active/passive routing configuration is appropriate for preventing overprovisioning of tunnels during a failover event. In active/passive routing, one tunnel is active for data transfer, while the other is a backup that becomes active in case the primary tunnel fails. This setup ensures efficient use of resources and meets the client's requirement of failover protection. Active/active routing, on the other hand, would involve both tunnels transferring data simultaneously, increasing the risk of overprovisioning. This eliminates option A.

In summary, the most suitable approach to address the client's requirements is to use a custom mode VPC network, implement Cloud Router BGP routes, and use active/passive routing (option C). This configuration will provide a secure, highly available VPN connection with dynamic routing and efficient resource allocation during failover scenarios.

Solution to Question 50: C

The correct answer is C because it specifically allows communication between the required tiers by creating ingress firewall rules that target instances based on their associated service accounts. This method ensures that only the desired communication between the specified tiers occurs on the required TCP port 8080.

Option A is incorrect because it suggests creating egress firewall rules with IP ranges. This will not achieve the intended communication between the tiers, as egress rules regulate the outgoing traffic from instances, not incoming traffic.

Option B is incorrect because it swaps the targets and source filter, meaning that the instances with tier #1 service account are targeted to receive traffic from instances with tier #2 service account, which is not the objective here. The objective is for instances in tier #1 to communicate with tier #2, and instances in tier #2 to communicate with tier #3.

Option D is incorrect because it creates an ingress firewall rule with IP ranges that allows all protocols. This not only exposes the instances to potential security risks but also does not guarantee the intended communication between the tiers. Additionally, the IP ranges do not accurately reflect the communication desired between specific tier instances, which may mistakenly allow traffic from unspecified tiers or instances.

Practice Exam 4

Question 1: You are working as a network administrator for a company with two subnets (subnet-a and subnet-b) in their default VPC. The company's database servers are located in subnet-a, while the application servers and web servers operate in subnet-b. Your task is to configure a firewall rule that permits database traffic exclusively from the application servers to the database servers. What steps should be taken to accomplish this?

A. • Create service accounts sa-app and sa-db. • Associate service account sa-app with the application servers and the service account sa-db with the database servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

B. Create network tags db-server and app-server. • Add the db-server tag to the application servers and the app-server tag to the database servers. • Create an egress firewall rule to allow network traffic from source network tag db-server to target network tag app-server.

C. Create a service account sa-app and a network tag db-server. • Associate the service account sa-app with the database servers and the network tag db-server with the application servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target network tag db-server.

D. Create a service account sa-app and a network tag app-server. • Add the service account sa-app to the application servers and the network tag app-server to the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-b IP addresses.

Question 2: As a data engineer for a company in the retail industry, you are required to configure service accounts for an application that spans across multiple projects. Virtual machines (VMs) within the web-applications project need access to BigQuery datasets in the crm-databases-proj. Following Google-recommended practices, how should you grant access to the service account in the web-applications project?

A. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

B. Disable BigQuery API in web-applications project and enable it in crm-databases-proj with bigquery.dataViewer role.

C. Create a new service account in crm-databases-proj and give it a bigquery.dataViewer role in web-applications project.

D. Create a new project and link crm-databases-proj and web-applications, then give bigquery.dataViewer role to the linked project.

Question 3: As an IT engineer at a tech company, you are managing a Linux VM that needs to connect to Cloud SQL. You've created a service account with appropriate access rights, but now you need to ensure that the Linux VM

uses this service account instead of the default Compute Engine service account. What steps should be taken to achieve this?

A. Configure an environment variable to override the default Compute Engine service account on the VM.

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

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

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

Question 4: As a database administrator in a growing tech company, you've been tasked with selecting and configuring a cost-effective solution for relational data on Google Cloud Platform. You'll be dealing with a small set of operational data in one geographic location, and you need to support point-in-time recovery for data protection. What should you do?

A. Select Cloud Datastore. Set up your instance with 2 nodes.

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

C. Select Firestore (Datastore Mode). Set up your instance as single regional.

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

Question 5: You are working as a software engineer at a tech company and are tasked with hosting an application on a Compute Engine instance in a project shared across different teams within the company. To avoid any accidental downtime on the application caused by other teams, which feature should you use?

A. Use a Managed Instance Group

B. Restrict SSH access to the instance

C. Enable deletion protection on the instance.

D. Configure a firewall rule for the instance

Question 6: You are working as a software developer in a company that uses the App Engine environment for hosting its applications. You have been asked to build a new version of an application and test it with 1% of users before fully transitioning to the new version. What is the best approach to achieve this task?

A. Use Cloud Load Balancing to distribute traffic between the current version and the new version of your application.

B. Create a new network in VPC and deploy the new version of your application in App Engine, then use GCP Console to split traffic.

C. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

D. Deploy a new version of your application in Cloud Functions and then use GCP Console to split traffic.

Question 7: You are working as a cloud security manager for a company that requires an external auditor to evaluate your cloud infrastructure. The auditor must have access to review the company's Google Cloud Platform (GCP) Audit Logs and Data Access logs. Which action should you take to grant them the necessary permissions?

A. Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage.

B. Assign the auditor's IAM user to a custom role with the permission monitoring.logsWriter. Perform the export of logs to Cloud Storage.

C. Assign the auditor the IAM role roles/logging.privateLogViewer and roles/pubsub.editor. Perform the export of logs to Cloud Storage.

D. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

Question 8: As a software engineer in the telecommunications industry, your team has recently designed a complex application comprised of various microservices. To accommodate constant growth, you have decided to deploy this application to Google Kubernetes Engine (GKE) with minimal manual intervention when adding new microservices in the future. What approach should you take to achieve this?

A. Deploy the application on GKE, and create a CronJob to scale the deployment periodically.

B. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

C. Deploy the application on multiple VM instances in Compute Engine with an instance group and configure autoscaling.

D. Deploy the application on GKE and add both a HorizontalPodAutoscaler and VerticalPodAutoscaler to cover all scaling possibilities.

Question 9: As a cloud systems administrator in a large IT company, you are responsible for ensuring the optimal performance of Compute Engine instances running in multiple zones. To configure autohealing for network load balancing and re-create VMs if they become unresponsive after 3 attempts of 10 seconds each, what should you do?

A. Create a network load balancer and configure the backend health check to healthy (HTTP)

B. Create a managed instance group. Set the Autohealing health check to healthy (HTTP)

C. Create a managed instance group and verify that autoscaling and autohealing settings are off

D. Configure Cloud NAT for the instances and set the Autohealing health check to healthy (HTTP)

Question 10: As a system administrator at a software company, you're responsible for maintaining a Compute Engine instance that hosts a critical application. Your manager requires you to set up a notification system using Google services that sends an email if the instance consumes over 90% of its CPU resources for more than 15 minutes. What should you do?

A. 1. Create a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it. 2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

B. 1. In Cloud Logging, create a logs-based metric to extract the CPU usage by using this regular expression: CPU Usage: ([0-9] {1,3})% 2. In Cloud Monitoring, create an Alerting Policy based on this metric. 3. Configure your email address in the notification channel.

C. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Write a script that monitors the CPU usage and sends it as a custom metric to Cloud Monitoring. 3. Create an uptime check for the instance in Cloud Monitoring.

D. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Set up a Cloud Function to monitor the instance's CPU usage. 3. Trigger an email notification using Cloud Pub/Sub when the CPU usage exceeds the threshold.

2. Use Stackdriver Debugger to monitor the instance's CPU usage. 3. Set up an email notification channel to receive alerts when the CPU usage exceeds the threshold.

3. Configure a Cloud Scheduler job to monitor the instance's CPU usage. 2. If the CPU usage exceeds the threshold, set up a Cloud Task to send an email notification.

4. Use the Google Cloud Console to manually monitor the instance's CPU usage. 2. Set up a Google Groups mailing list to receive email notifications when the CPU usage exceeds the threshold.

5. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Monitor the CPU usage using a built-in Cloud Monitoring

agent. 3. Enable Google Workspace email notifications and configure alerts to be sent when the CPU usage exceeds the threshold.

6. Use a Cloud Run instance to monitor the CPU usage of the Compute Engine instance. 2. Set up a Cloud Storage bucket to store the results. 3. Configure email notifications for high CPU usage using Cloud Pub/Sub.

7. Use Google Kubernetes Engine to monitor the Compute Engine instance's CPU usage. 2. If the CPU usage exceeds the threshold, create a log entry in Google Cloud Logging. 3. Configure Cloud Logging to send email notifications for high CPU usage events.

8. Set up a Cloud Identity-Aware Proxy to monitor the CPU usage of the Compute Engine instance. 2. Configure the Identity-Aware Proxy to send email notifications after the CPU usage remains above the threshold for more than 15 minutes.

Question 11: As a cloud engineer at a rapidly growing e-commerce company, you need to create a copy of a custom Compute Engine virtual machine (VM) to handle the increased application traffic due to a recent business acquisition. What should you do?

A. Create a custom Compute Engine image from a snapshot. Create your instances from that image.

B. Create a Compute Engine managed instance group from your base VM. Create your instances from that instance group.

C. Create a custom Compute Engine image from your base VM. Create your instances from that image.

D. Export your base VM as a Cloud Storage object. Create your instances from that object.

Question 12: You are working as an IT specialist for a radiology company that stores its medical images in an on-premises data room. The company wants to utilize Cloud Storage for the archival storage of these images and seeks an automated process to upload any new medical images to Cloud Storage. How should you design and implement the solution?

A. Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

B. Configure a Cloud Storage Transfer Service to sync the on-premises storage with Cloud Storage daily, without using a cron job or script.

C. Create a Pub/Sub topic, and create a Cloud Function connected to the topic that writes data to Cloud Storage. Create an application that sends all medical images to the Pub/Sub topic.

D. Create a Cloud SQL instance and develop a script to import the image files into the database. Schedule the script as a cron job.

Question 13: You are working as a Cloud Administrator in a software company that uses Google Cloud Spanner. You have been tasked to allow three of your colleagues access to view and edit table data on your company's Cloud Spanner instance. What is the appropriate action to take?

A. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

B. Run gcloud projects add-iam-policy-binding my-project –member group:group@example.com –role roles/spanner.databaseUser.

C. Run gcloud iam roles describe roles/spanner.viewer –project my-project. Add the users to a new group. Add the group to the role.

D. Run gcloud projects add-iam-policy-binding my-project –member user:email@example.com –role roles/spanner.databaseUser.

Question 14: You are working as a web developer for a reputable company that has a live web application deployed as a managed instance group. The company needs a gradual deployment of a new version of the web application without causing any decrease in available capacity. As part of the process, what should be your ideal approach?

A. Create a new instance template with the new application version. Update the instances within the managed instance group one by one manually, without setting maxSurge or maxUnavailable values.

B. Create and deploy the new application version in a Cloud Run container without using a managed instance group.

C. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

D. Create a new managed instance group with an updated instance 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.

Question 15: While working at an IT company, you create a Deployment with 2 replicas in a Google Kubernetes Engine cluster with a single preemptible node pool for a new project management application. After a few minutes, you use kubectl to examine the status of your Pod and notice that one of them is still in Pending status. What could be the most likely cause for this issue?

A. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

B. Google Cloud Load Balancer failed to register the pending Pod's backend service, causing the Pod to remain in Pending status.

C. A firewall rule is blocking communication between the control plane and the node, preventing the Pod from being scheduled.

D. The GKE autoscaler is not set up correctly, causing the cluster to not scale out.

Question 16: As a cloud storage expert working in a fast-paced data-driven company, you are responsible for implementing Object Lifecycle Management for data stored in storage buckets. The data is created once and accessed frequently for the first 30 days. After that, it is rarely accessed unless required for specific purposes. The company wants to retain the data for three years while keeping costs to a minimum. What policy should you set up?

A. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

B. Set up a policy that uses Nearline storage for 30 days, then moves to Coldline for two years, and then moves to Archive storage for one year.

C. Set up a policy that uses Coldline storage for 30 days and then moves to Archive storage for three years.

D. Set up a policy that uses Nearline storage for 30 days and then moves to Coldline storage for three years.

Question 17: As the lead developer of a tech company, you need to create a new billing account and link it with an existing Google Cloud Platform project for one of your clients. What steps should you follow?

A. Verify that you are Billing Account Administrator for the billing account. Create a new GCP project and link the new project to the existing billing account.

B. Verify that you are Billing Administrator for the GCP project. Create a new billing account and update the existing project to link it to the new billing account.

C. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

D. Verify that you are Project Billing Manager for the GCP project. Create a new GCP project and link the new project to the existing billing account.

Question 18: As an IT specialist working in a tech company, you have just set up a new project in Google Cloud via the gcloud command line interface (CLI) and connected it to a billing account. Now, you need to establish a new Compute Engine instance using the CLI. To ensure all necessary steps are properly carried out, what prerequisite task should you complete?

A. Create a BigQuery dataset in the project.

B. Create a VPC network in the project.

C. Enable the compute.googleapis.com API.

D. Create a Cloud Run service in the project.

Question 19: As a member of the IT department in a fast-paced tech company, you are responsible for maintaining the infrastructure. As part of a recent collaboration, you identify some necessary changes to the current infrastructure. To effectively communicate your proposed changes with your colleagues and adhere to Google's recommended best practices, what approach should you take?

A. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

B. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Pub/Sub. Create a Shared VPC in the organization and apply the proposed changes for team review. Store the Deployment Manager templates describing the proposed changes in Firestore. Discuss the proposed changes in a Google Meet session. Use Cloud Logging to share the proposed changes with the rest of the team. Migrate the existing infrastructure to Anthos and then share the proposed changes using Anthos Config Management. Use Cloud Functions to automatically apply the proposed changes for team review. Create a diagram of the proposed changes and share it through Google Drive or Google Docs.

C. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

D. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.

Question 20: You work as a software engineer for a company in the IT industry. Recently, you deployed an application on a single Compute Engine instance within the company's infrastructure. This application writes logs to disk. However, your colleagues from different departments have started reporting errors with the application. In order to diagnose the issue, what should you do?

A. Deploy a new version of the application using Cloud Functions.

B. Navigate to Cloud Logging and view the application logs.

C. Use Stackdriver Monitoring to view the application logs.

D. Install and configure the Ops agent and view the logs from Cloud Logging.

Question 21: As a financial analyst at a tech company that extensively uses Google Cloud, you are in charge of managing costs across various projects linked to different billing accounts. To accurately forecast future expenses and present a single, up-to-date visual report of all costs incurred, what action should you take?

A. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

B. Visit the Cost Table page to get a CSV export and visualize it using Data Studio.

C. Export the billing data of each project to Cloud Storage in CSV format and use Data Studio to visualize the costs.

D. Use Cloud Billing Budget & Thresholds to create a single budget for all projects and visualize it in Data Studio.

Question 22: As an IT manager at a rapidly growing tech company, you're responsible for providing secure access to your operational team to manage numerous instances on Compute Engine. All employees have Google accounts, and each team member requires only administrative access to the servers. Your security team has requested an operationally efficient deployment of credentials and the ability to determine who accessed any given instance. How should you proceed?

A. Create a shared Gmail account for the team and use its Google account to generate an SSH key pair. Add the public key to each member's Google account and grant 'compute.osAdminLogin' role to the shared Gmail account.

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

C. Ask each member of the team to generate a new SSH key pair and add the public key to a shared Google Sheet. Use a configuration management tool to deploy those keys on each instance and grant 'compute.osAdminLogin' role to the Google group corresponding to this team.

D. Generate a new SSH key pair. Give the private key to each member of your team. Restrict the access using firewall rules and grant 'compute.osAdminLogin' role to the Google group corresponding to this team.

Question 23: As an IT manager at a large software development company, you are handling an application deployed on a general-purpose Compute Engine instance, which is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk. The application primarily reads large files from disk, and the disk size is currently 350 GB. Your goal is to provide the maximum amount of throughput while minimizing costs. What should you do?

A. Migrate to use a Local SSD on the instance.

B. Optimize the Operating System for disk reads.

C. Migrate to use a Regional SSD on the instance.

D. Increase the size of the disk to 750 GB.

Question 24: You are working as a developer in a software company and you have successfully created a development environment for an application using Compute Engine and Cloud SQL. Now, your team needs to create a production environment for the same application. The security team at your company has prohibited any network routes between these two environments and has asked

you to adhere to Google-recommended practices. What steps should you take to achieve this?

A. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

B. Create two new Cloud SQL instances in the existing project, one for the development environment and one for the production environment, and restrict traffic between them using firewall rules.

C. Create a new separate VPC for the production environment within the existing project and connect the two environments using VPC peering.

D. Enable Private Google Access and Private Service Access in the existing project to restrict traffic between the Compute Engine and Cloud SQL instances for both environments.

Question 25: You recently joined a tech company and were provided with a new corporate laptop. As part of your role, you need to access and manage the existing instances of your company on Google Cloud. Before running the gcloud compute instances list command, what are the two essential steps you must follow?

A. Run gcloud compute instances create to create a new instance before listing existing instances.

B. Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI.

C. Create a .boto configuration file and store it in your home folder.

D. Run gcloud config set compute/zone $my_zone to set the default zone for gcloud CLI.

Question 26: You are working as a web developer for a company that has its website hosted on App Engine standard environment. The company wants to test a new version of the website on 1% of the users while keeping the complexity at a minimum. What should be your approach for this task?

A. Deploy the new version using the same application and enable traffic splitting in App Engine by assigning 1% traffic to the new version using the Console.

B. Create a new Cloud Storage bucket and deploy the new version in the same project. Use the App Engine library to proxy 1% of the requests to the new version.

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

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

Question 27: As a project manager working at a software development company, you have recently created a new solution using various Google Cloud products. Your supervisor has requested an estimate of the monthly total cost for utilizing these services. How should you proceed to provide the most accurate cost estimate?

A. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

B. Visit pricing forums or community groups and ask other users to estimate the cost of your solution without using the pricing calculator.

C. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Create a Google Sheet that summarizes the expected monthly costs for each product.

D. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Navigate to the Billing Report page in the Cloud Console. Multiply the 1 week cost to determine the monthly costs.

Question 28: As an employee at a prominent financial company, you are responsible for storing audit log files for a duration of 3 years across hundreds of Google Cloud projects. In order to achieve this in a cost-effective manner, what approach should you implement?

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

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

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

D. Export logs to Cloud Pub/Sub and utilize Cloud Dataflow pipeline to store logs in Cloud Bigtable.

Question 29: As a software engineer at a tech company developing an application that will operate on Google Kubernetes Engine, you need to utilize a managed MongoDB system with a support SLA for your app's database requirements. What action should you take?

A. Download a MongoDB installation package, and run it on Compute Engine instances.

B. Deploy MongoDB on Cloud Run and configure it as a stateful service.

C. Deploy a MongoDB container on Cloud Functions and trigger it with an event.

D. Deploy MongoDB Atlas from the Google Cloud Marketplace.

Question 30: You are working as a cloud engineer in a software development company and recently deployed an App Engine application using gcloud app deploy. However, the application did not deploy to the intended project. To determine why this occurred and where the application was deployed, what should you do?

A. Review logs in the App Engine dashboard in Google Cloud Console to check any deployment issues.

B. Verify IAM permissions for the App Engine Admin API in the intended project.

C. Run gcloud projects list to verify the proper project ID for the intended project.

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

Question 31: As an IT manager in a growing software company, you have deployed multiple Linux instances on Compute Engine for your development team. The company plans to expand, and you anticipate adding more instances in the coming weeks. Your goal is to enable the team to access all instances through an SSH client over the internet without configuring specific access on the existing and new instances. However, you don't want the Compute Engine instances to have a public IP. What solution should you implement?

A. Configure Cloud Identity-Aware Proxy for HTTPS resources.

B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

C. Use Cloud Load Balancer with the TCP Proxy protocol for the instances.

D. Create an SSH keypair and store the private key as a project-wide SSH Key.

Question 32: You are working as a system administrator in a company that relies on user identities stored in Active Directory. The management intends to centralize the user identities in Active Directory for all Google services, including Google Cloud Platform (GCP) organization. They also want to ensure the company has full control over the Google accounts used by employees. What approach should you take?

A. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

B. Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console.

C. Use Google Cloud SQL to store users' data and connect it to Cloud Identity.

D. Use the GCP Console to migrate users from Active Directory to Cloud Identity.

Question 33: You are working as a network administrator at a tech company and have recently deployed an LDAP server on Compute Engine. The server is reachable via TLS through port 636 using UDP, and you need to ensure that clients can access it over that specific port. What action should you take to confirm its reachability?

A. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag.

B. Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

C. Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server.

D. Create a VPC peering connection to allow access to the LDAP server on port 636 using UDP. Enable the 'Allow Secure LDAP access over the Internet' option in the Compute Engine settings. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow ingress on TCP port 636 for that network tag. Create a Cloud VPN tunnel and configure the LDAP server to be reachable only through the VPN. Create a firewall rule to allow ingress on UDP port 636 without specifying any specific network tags. Set the VM instance to use a shared VPC and enable ingress on UDP port 636 in the Shared VPC settings. Deploy an Identity-Aware Proxy for the LDAP server and allow access on UDP port 636 only for authorized users. Create a Cloud NAT gateway and configure it to allow access to the LDAP server on port 636 using UDP.

Question 34: As a network administrator in a tech company, you are assigned to manage an instance group for load balancing a public web application over HTTPS while ensuring client SSL session termination. In this scenario, following Google-recommended practices, what type of load balancer should you configure?

A. Configure a global external forwarding rule.

B. Configure an HTTP(S) load balancer.

C. Configure an internal HTTPS load balancer.

D. Configure a regional external forwarding rule.

Question 35: As a backend developer for an international retail company, you have been assigned the task of developing a backend service that can handle a large volume of global transactions coming from various mobile and web clients. The business team wants to be able to run SQL queries for data analysis purposes. In order to achieve a highly available and scalable data store for the platform, what should be your top choice of action?

A. Create a multi-region BigQuery dataset with optimized tables.

B. Use a multi-region Pub/Sub for streaming transaction data and analyze it using Dataflow.

C. Create a multi-region Cloud SQL for MySQL database with no read replicas.

D. Create a multi-region Cloud Spanner instance with an optimized schema.

Question 36: You are working in an IoT-enabled manufacturing company that uses Google Cloud to manage a large repository of data from various streamlining sensors across different plants. As a cloud architect, you've been asked to create a highly available and resilient architecture based on Google-recommended practices for the data lake of your IoT application. What approach should you take?

A. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

B. Stream data to Cloud Pub/Sub, and use Dataflow to send data to Cloud SQL.

C. Stream data to IoT Core, and use Cloud Functions to send data to Cloud Storage.

D. Stream data to Pub/Sub, and use Dataflow to send data to Firestore.

Question 37: You are the system administrator for a tech company that extensively uses Google Cloud Platform for various projects. You have been asked to add a new auditor to one of the projects, granting them read-only access to all project items without allowing them to modify anything. How should you set up the auditor's permissions in this situation?

A. Select the built-in IAM project Viewer role. Add the user's account to this role.

B. Create a custom role with view-only service permissions. Add the user's account to the custom role.

C. Assign the user to the IAM BigQuery Data Viewer role with project-wide permissions. Add the user's account to this role.

D. Add the user to the IAM Billing Account Viewer role with project-wide permissions. Add the user's account to this role.

Question 38: You are working as a cloud administrator in a technology company and have been tasked to provide an external member of your team with list access to compute images and disks within one of your company's projects. Following Google-recommended practices, how should you grant the required permissions to this user?

A. Grant only the Compute Image User role without including the compute.disks.list permission at the project level.

B. Grant the Compute Storage Admin role and the Compute Image Admin role at the organization level.

C. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

D. Grant the Compute Image User role and the Compute Disk Viewer role at the project level.

Question 39: As a software engineer in a financial organization, you have been tasked with setting up a Google Kubernetes Engine cluster. Ensuring verifiable node identity and integrity is critical for your company, and nodes should not be accessible from the internet. You are also expected to minimize operational costs and follow Google-recommended practices. What should you do?

A. Deploy a public App Engine cluster and enable shielded nodes.

B. Deploy a public Cloud SQL instance with shielded nodes enabled.

C. Deploy a public autopilot cluster.

D. Deploy a private autopilot cluster.

Question 40: As a software developer at a tech company, you've installed the Google Cloud CLI on your office workstation and configured the proxy settings. To maintain security, you want to avoid having your proxy credentials recorded in the gcloud CLI logs. How can you make sure your proxy credentials aren't logged?

A. Store your proxy credentials in a JSON file and use the gcloud auth activate-service-account command to enable them in the gcloud CLI.

B. Provide values for CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD in the gcloud CLI tool configuration file.

C. Encrypt your proxy credentials using asymmetric encryption and set them in the gcloud CLI by using gcloud config set proxy/username and gcloud config set proxy/password commands.

D. Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

Question 41: As a software engineer at a fast-growing tech company, you're responsible for maintaining an application that utilizes Cloud Spanner as its backend database. Due to the nature of your industry, the application experiences highly predictable traffic patterns. Your goal is to automatically scale the number of Spanner nodes up or down, depending on traffic. What method should you implement to achieve this?

A. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

B. Create a cron job that runs on a scheduled basis to review Cloud Monitoring metrics, and then resize the Spanner instance accordingly.

C. Create a Cloud Monitoring alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly.

D. Create a Cloud Monitoring alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.

Question 42: As a data analyst in a media company, you need to extract text from audio files using the Speech-to-Text API for further analysis. The audio files are uploaded to a Cloud Storage bucket, and it's crucial to implement an authenticated, fully managed, serverless compute solution according to Google-recommended practices. To streamline the process, you want to automate the API call by submitting each file to the API as soon as the audio file arrives in the bucket. How should you proceed?

A. Run a Kubernetes job to scan the bucket regularly for incoming files, and call the Speech-to-Text API for each unprocessed file.

B. Create a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

C. Create a Dataflow job triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

D. Implement a Cloud Scheduler job to regularly scan the bucket and call the Speech-to-Text API for each unprocessed file.

Question 43: As a leading financial services company, our organization needs a storage solution on the Google Cloud Platform that adheres to compliance requirements for data from a specific geographic location. This data has to be archived after 30 days and accessed only once a year. What would be the ideal course of action?

A. Select Regional Storage. Add a bucket lifecycle rule that moves data to Bigtable after 30 days.

B. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

C. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Cloud Storage Archive.

D. Select Regional Storage. Add a bucket lifecycle rule that archives data after 60 days to Coldline Storage.

Question 44: You are an IT engineer working at a software company that is looking to migrate a critical application from your local data center to Google Cloud. To ensure high availability and immediate data access in case of a zonal failure, what approach should you take?

A. Store the application data in a Firestore database and create VM instances in two zones with read access to the Firestore data.

B. Use Cloud Datastore to store the application data and configure inter-zone replication for high availability.

C. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

D. Store the application data on a Cloud Filestore instance with multiple zones as NFS mounts.

Question 45: You are working as a developer in a game development company, and your team is responsible for building a multi-player gaming application. The application will store game information in a database, and as the game's popularity skyrockets, there are concerns about maintaining consistent performance. Your task is to ensure optimal gaming experiences for users worldwide without adding management complexity. What approach should you take?

A. Use Cloud Datastore in native mode with regional indexes for better query performance for game statistics.

B. Use Cloud SQL with read replicas in each region to store game statistics and serve global users.

C. Use Cloud Spanner to store game statistics with manual sharding to achieve optimal performance.

D. Use Cloud Spanner to store user data mapped to the game statistics.

Question 46: You're working as a security specialist in a financial technology company dealing with customer transactions. A team member was recently terminated, but their access to Google Cloud was not revoked until 2 weeks after the termination. Your task is to determine if this former employee accessed any sensitive customer data post-termination. What should you do?

A. View Data Access audit logs in Cloud Logging. Search for the service account associated with the user.

B. View VPC Flow Logs in Cloud Logging. Search for the IP address associated with the user.

C. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

D. View Admin Activity logs in Cloud Auditing. Search for the IP address associated with the user.

Question 47: As a security analyst in a financial services company, you are responsible for monitoring a Bigtable instance with three nodes that store sensitive personally identifiable information (PII) data. You need to ensure that all read and write operations, including any metadata or configuration reads, are

logged in the company's Security Information and Event Management (SIEM) system. What should be your course of action?

A. • Install the Ops Agent on the Bigtable instance during configuration. • Create a service account with read permissions for the Bigtable instance. • Create a custom Dataflow job with this service account to export logs to the company's SIEM system.

B. Create a serverless app with Cloud Run to pull logs from the Bigtable instance and forward them to your SIEM system.

C. • Navigate to the Audit Logs page in the Google Cloud console, and enable Admin Write logs for the Bigtable instance. • Create a Cloud Functions instance to export logs from Cloud Logging to your SIEM.

D. • Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.

Question 48: As an IT manager in a large manufacturing company, you oversee a nightly batch workload that uses numerous virtual machines (VMs) and can tolerate some VMs being terminated. However, the current cost of the VMs is becoming a concern. How should you proceed to reduce costs while maintaining reliability?

A. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

B. Run a test using a managed instance group. If the test is successful, use N2 Standard VMs in the managed instance group when running future jobs.

C. Run a test using N1 standard VMs instead of N2. If the test is successful, use N1 Standard VMs when running future jobs.

D. Run a test using Cloud Functions with the same workload. If the test is successful, migrate the workload to Cloud Functions.

Question 49: As a cloud security analyst in a financial services firm, you have been tasked to conduct a periodic security assessment of your firm's Google Cloud environment. In order to determine who has access to view data stored in your company's Google Cloud Project, what action should you take?

A. Review the instance metadata for any suspicious API calls.

B. Create and apply a VPC Service Controls perimeter.<

C. Create a Data Loss Prevention job.

D. Review the IAM permissions for any role that allows for data access.

Question 50: As an IT manager in a tech company, you oversee a team of data scientists who occasionally need access to a Google Kubernetes Engine (GKE)

cluster with GPUs for their long-running, non-restartable projects. Your goal is to minimize the cost for the company. What is the most appropriate strategy for managing this resource?

A. Create a node pool with regular VMs and GPUs attached to those VMs.

B. Manually add and remove GPU-enabled instances to the GKE cluster as needed.

C. Enable node auto-provisioning on the GKE cluster.

D. Enable Cluster Autoscaler on the existing GKE cluster without adding GPU-enabled VMs.

Practice Exam 4 Solutions

Solution to Question 1: A

The correct answer is A. Here's why:

A: This option correctly configures a firewall rule that exclusively permits traffic from application servers to database servers. By creating separate service accounts (sa-app and sa-db) and associating them with the appropriate servers, you can create a specific ingress firewall rule allowing traffic from the source service account (sa-app) to the target service account (sa-db). This configuration ensures that only traffic from the application servers in subnet-b can access the database servers in subnet-a.

B: This option is incorrect because it creates an egress firewall rule, which controls outbound traffic instead of inbound traffic. The desired configuration is to control inbound traffic to the database servers. Also, the network tags are reversed in this option, which would not accomplish the goal of allowing traffic from application servers to access database servers exclusively.

C: This option is incorrect because it mixes service accounts and network tags in the firewall rule, making the rule ineffective. By using a service account for database servers and a network tag for application servers, the firewall rule would not properly filter the allowed traffic. Additionally, an ingress rule must define the source and target using the same type of identifier (either both service accounts or both network tags).

D: This option is incorrect because the ingress firewall rule focuses on VPC IP addresses and subnet-b IP addresses, rather than the service accounts or network tags associated with the servers. This configuration would not accurately control traffic between the application and database servers, and may also allow unwanted inbound traffic to the database servers.

Solution to Question 2: A

The correct answer is A: Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

Explanation:

In this scenario, we need to grant access to the service account in the web-applications project so that VMs within that project can access BigQuery datasets in the crm-databases-proj. Following Google-recommended practices, providing the least amount of privilege is crucial.

Option A is the best solution because it enables granular control over the access to specific resources. By granting the bigquery.dataViewer role to the crm-databases-proj and appropriate roles to the web-applications, we ensure that the VMs in the web-applications project can access the BigQuery datasets they need without giving them more permissions than necessary.

Option B would not work because disabling the BigQuery API in the web-applications project restricts the VMs in that project from accessing the dataset. Enabling the API in the crm-databases-proj with the bigquery.dataViewer role without providing proper access to the web-applications project's VMs would not be sufficient for the required data access.

Option C is not preferred mainly because it creates additional complexity and overhead. A new service account would not be necessary in this case, and granting the bigquery.dataViewer role to the new service account in the web-applications project still leaves us with the task of allowing the VMs access through that new service account. Option A is much more efficient and follows the principle of least privilege.

Option D is not suitable as it creates unnecessary complications by introducing a new project, and this may not provide an optimal security framework. The mere linking of the projects does not guarantee the appropriate roles and permissions required for the VMs to access the BigQuery datasets.

In conclusion, option A provides the most effective, efficient, and secure solution by giving the bigquery.dataViewer role to the crm-databases-proj and appropriate roles to the web-applications project.

Solution to Question 3: C

The correct answer is C, "When creating the VM via the web console, specify the service account under the 'Identity and API Access' section." This is because, during the VM creation process, you have the option to set a custom service account with the required permissions, which the VM will use for all API access.

Option A is incorrect because environment variables are not used to override the default Compute Engine service account for a VM. They can be used to configure the signing credentials for certain services, but this does not affect the service account used by the VM itself.

Option B is incorrect because, while downloading a JSON Private Key for the service account may be necessary for authentication, saving the JSON file under ~/.gcloud/compute-engine-service-account.json will not change the service account used by the VM. This method is helpful for accessing Google API resources from outside the VM using the service account's credentials, but it does not affect the VM's service account.

Option D is incorrect because adding the JSON Private Key to the Project Metadata does not modify the service account associated with individual VM instances. As a matter of fact, storing private keys in project metadata can expose them to potential security risks.

Therefore, the correct approach is to specify the desired service account during the VM creation process, as described in option C. This ensures that the VM uses the appropriate service account with the necessary access rights to connect to Cloud SQL.

Solution to Question 4: D

The correct answer should be D, "Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected." Here's why:

A. Cloud Datastore is not the appropriate solution because it is a NoSQL database, whereas the requirement is for a relational database.

B. Cloud Spanner is not a cost-effective solution for the scenario given because it is designed for large-scale databases and heavy workloads that span across multiple regions. Since the requirement is for a small dataset that is utilized in one geographic location, Cloud Spanner would be excessive and not cost-effective.

C. Firestore (Datastore Mode) is also not the right choice because it is designed for scalable, serverless NoSQL databases, and the requirement is for a relational data solution.

D. Cloud SQL (MySQL) is the ideal choice for this situation because it is designed to handle relational databases on the Google Cloud Platform. It is also more cost-effective since the dataset is small and pertains to a single geographic location. In addition, enabling the binary logging option will allow the support of point-in-time recovery for data protection, which is one of the essential requirements for the task. This solution best addresses the needs of the database administrator while maintaining cost-efficiency.

Solution to Question 5: C

The correct answer is C. Enable deletion protection on the instance.

Explanation:

A. Use a Managed Instance Group - While Managed Instance Groups can provide high availability and automatic scaling for applications, they do not specifically protect against accidental downtime caused by other teams within the company.

B. Restrict SSH access to the instance - Restricting SSH access can prevent unauthorized access, but it does not ensure protection from accidental deletions or other actions that may cause downtime on the Compute Engine instance by team members with authorized access or access to the Google Cloud Console.

C. Enable deletion protection on the instance - This is the correct answer because enabling deletion protection prevents an instance from being accidentally deleted, effectively protecting the application from being taken down mistakenly by other teams within the company. This feature is specifically meant to provide protection against accidental deletions of critical instances.

D. Configure a firewall rule for the instance - While configuring firewall rules is important for security purposes and controlling network traffic, it does not address accidental deletion or actions taken by other teams within the company that could cause downtime on the instance.

Solution to Question 6: C

The correct answer is C. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

Explanation:

Option A is not suitable because Cloud Load Balancing is used to distribute traffic across multiple Compute Engine instances rather than between App Engine versions. Therefore, it would not help with the specific scenario of testing the new version of your application within the App Engine environment.

Option B is incorrect because creating a new network in VPC is not necessary for this task, given that App Engine automatically manages the infrastructure, including network configurations. Additionally, deploying the application in a new network in VPC would not inherently provide traffic splitting capabilities required for this scenario.

Option C is the best choice because it allows you to test the new version of your application within the App Engine environment by deploying a new version and then configuring the traffic split between the current version and the newly deployed version. This approach lets you control the percentage of users who will be directed to the new version, ensuring that you can test it with the required 1% of users before full adoption.

Option D is inappropriate because, in the given context, you are working with App Engine applications rather than Cloud Functions. Deploying a new version of your application in Cloud Functions would not fit the constraints of the problem, and you would not be able to test the new version among App Engine users correctly.

Solution to Question 7: D

The correct answer is D. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy. The reason being that this option provides the auditor with the necessary permissions to view and review the company's Google Cloud Platform (GCP) Audit Logs and Data Access logs, which are crucial for the evaluation of the cloud infrastructure.

Option A is not suitable since the roles/logging.privateLogViewer role allows the auditor to view logs, but it does not automatically export logs to Cloud Storage for further review. The export of logs to Cloud Storage should be done through the log export process, which is achieved with an additional role, such as roles/logging.viewer, if required.

Option B is incorrect because the monitoring.logsWriter does not allow the auditor to view the logs, but rather only allows them to write logs. The permission is not suitable for review purposes, and assigning a custom role might also re-

sult in granting unnecessary permissions. Furthermore, exporting logs to Cloud Storage is not mentioned in the provided options.

Option C is incorrect as well. Although it grants the auditor permissions to view private logs with roles/logging.privateLogViewer role, the additional roles/pubsub.editor role is unnecessary in this scenario. The roles/pubsub.editor role is used to grant access to manage Pub/Sub resources, which is not required for the purpose of reviewing GCP Audit Logs and Data Access logs.

Therefore, option D is the appropriate choice, as it assigns the auditor the required permissions to view the private logs and also suggests reviewing logs for changes to Cloud IAM policy. This helps ensure that the auditor has a comprehensive view of the company's cloud security and compliance status.

Solution to Question 8: B

The correct answer is B. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

Explanation: The goal here is to deploy a complex application with various microservices in the telecommunications industry, with minimal manual intervention when adding new microservices in the future. Google Kubernetes Engine (GKE) is an ideal choice for deploying containerized applications, as it can manage, scale, and update your applications easily.

Option B addresses this requirement by suggesting the creation of a GKE cluster with autoscaling enabled on the node pool. Autoscaling helps in adding or removing nodes in the cluster based on the overall resource usage and demand. This way, you need minimal manual intervention to accommodate constant growth, and additional resources can be allocated when needed.

The other options are not optimal for this scenario:

Option A - Deploy the application on GKE and create a CronJob to scale the deployment periodically. This option involves manual configuration and constant updating of the scaling using a CronJob. It does not dynamically adapt to the demand and, therefore, potentially leads to over-provisioning or under-provisioning of resources.

Option C - Deploy the application on multiple VM instances in Compute Engine with an instance group and configure autoscaling. Although this option includes autoscaling, it uses Compute Engine VM instances instead of GKE, which lacks the benefits of Kubernetes, such as container orchestration, easier updates, and the abstraction of the underlying infrastructure.

Option D - Deploy the application on GKE and add both a HorizontalPodAutoscaler and VerticalPodAutoscaler to cover all scaling possibilities. While using both HorizontalPodAutoscaler (HPA) and VerticalPodAutoscaler (VPA) could be of benefit in some scenarios, deploying them together is not recommended since HPA scales the number of pods, while VPA adjusts the resources allocated

to each pod. These autoscaling systems might conflict when used together, leading to unstable behavior of the application.

Therefore, the best approach to deploy the application with minimal manual intervention when adding new microservices in the future is option B: Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

Solution to Question 9: B

The correct answer is B: Create a managed instance group. Set the Autohealing health check to healthy (HTTP).

Option B is correct because Managed Instance Groups (MIGs) provide autohealing capabilities, ensuring that VM instances remain healthy and available for serving requests. By configuring an autohealing health check for a MIG, you can set up a mechanism to regularly evaluate the health of each instance. In this case, you would need to set a health check with a healthy threshold of three attempts and a health check interval of 10 seconds, which ensures that VM instances will be recreated if they become unresponsive after three consecutive attempts.

Option A is not correct because it only configures a network load balancer without implementing autohealing. Moreover, the network load balancer, in this case, serves more to distribute the incoming traffic among instances to better balance their load rather than monitoring VM instances' health.

Option C is not correct as it suggests creating a managed instance group without enabling autohealing settings. This will not provide the desired autohealing functionality that can keep the instances in optimal performance.

Option D is not correct because Cloud NAT is primarily used to configure instances without external IP addresses to connect to the internet. Enabling Cloud NAT by itself does not ensure autohealing for network load balancing or recreate unresponsive VMs, so it does not serve the purpose of the given scenario.

Solution to Question 10: A

The correct answer is A because it directly utilizes Google Cloud Monitoring for tracking the CPU usage of the Compute Engine instance and setting up a notification system based on given conditions. By creating a Workspace and associating the GCP project with it, you maintain the CPU resource usage; if the instance's CPU consumption is over 90% for more than 15 minutes, the Alerting Policy with the specified condition triggers an email notification.

Other options are incorrect for the following reasons:

Option B: This method uses Cloud Logging and a logs-based metric, which is not optimal for monitoring real-time CPU usage efficiently. Cloud Monitoring excels in this task without requiring log-based metrics.

Option C: This method lacks email notification components and uses an unnecessary uptime check, making it unsuitable for the problem.

Option D: Although this solution also utilizes a Cloud Monitoring Workspace, the use of Cloud Function and Cloud Pub/Sub for email notifications would require additional development and maintenance time and increase complexity.

Option 2: Stackdriver Debugger is not designed for monitoring CPU usage or triggering email notifications. It is best for debugging applications in real-time.

Option 3: Using Cloud Scheduler and Cloud Task adds unnecessary complexity and overhead, considering Cloud Monitoring provides a built-in solution for the problem.

Option 4: Manual monitoring is not a viable, scalable solution for monitoring CPU usage, and using Google Groups is not a direct integration with Google Cloud monitoring.

Option 5: Although this option includes creating a Cloud Monitoring Workspace, it suggests using Google Workspace email notifications without a clear way to associate them with monitoring alerts.

Option 6: Cloud Run is not designed for monitoring Compute Engine instances, and utilizing Cloud Storage for results introduces complexity and storage overhead.

Option 7: Google Kubernetes Engine is designed for container management, not for monitoring CPU usage in Compute Engine instances. Cloud Logging is not the optimal choice for this use case.

Option 8: Cloud Identity-Aware Proxy is used for securing applications and resources, not for monitoring CPU usage or triggering notifications.

Solution to Question 11: A

The correct answer is A: Create a custom Compute Engine image from a snapshot. Create your instances from that image.

Explanation:

When you need to create a copy of a custom Compute Engine virtual machine (VM) to handle increased application traffic, it's crucial to capture the entire VM state and use that as a starting point in creating new instances. Creating a custom Compute Engine image from a snapshot of the original VM provides an identical configuration, ensuring that the newly created instances will have the same environment and setup as the original.

By choosing the other options, you will not achieve the desired results:

B: Creating a Compute Engine managed instance group from your base VM creates instances from an instance template, which might not capture all the customization and environment variables set in the original VM. This can lead

to inconsistencies between the original VM and the new instances, potentially causing issues.

C: Creating a custom Compute Engine image from your base VM directly is not possible. Google's platform requires creating a snapshot first, and then creating the image from that snapshot to ensure data consistency. Skipping the snapshot step can lead to image corruption, failed instances, or data inconsistencies.

D: Exporting your base VM as a Cloud Storage object is more for backup purposes and transferring VMs between clouds or on-premises environments. This option doesn't ensure an efficient deployment of new instances in the Google Cloud Platform, and would require additional steps to convert the object into a usable VM image. This approach is unnecessarily complex and time-consuming compared to the recommended snapshot and image method.

Solution to Question 12: A

The correct answer is A: Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

Here's why the other options are not suitable:

Option B: Configure a Cloud Storage Transfer Service to sync the on-premises storage with Cloud Storage daily, without using a cron job or script. - This option seems attractive since it's a managed service by Google Cloud Platform. However, Cloud Storage Transfer Service does not support transferring data from on-premises data storage to Cloud Storage. It is primarily used for transferring data between different cloud storage buckets or from other cloud providers such as Amazon S3.

Option C: Create a Pub/Sub topic, and create a Cloud Function connected to the topic that writes data to Cloud Storage. Create an application that sends all medical images to the Pub/Sub topic. - Although this option uses a message-based architecture by using Pub/Sub and serverless processing with Cloud Functions, it is not the most optimized solution for transferring large medical images. This approach would incur additional operational overhead and costs due to developing and maintaining custom applications for sending messages and managing serverless components. Moreover, Pub/Sub is designed for messaging, not for bulk data transfer.

Option D: Create a Cloud SQL instance and develop a script to import the image files into the database. Schedule the script as a cron job. - This option is inappropriate for storing large medical images, as Cloud SQL is a database service and not suitable for storing binary data such as images. Storing images in a database can lead to performance degradation, increased costs, and reduced system scalability. Additionally, this approach will waste resources by unnecessarily replicating the data into another storage service.

In conclusion, option A is the most suitable solution for the given scenario. It

involves creating a script that uses the gcloud storage command to synchronize on-premises storage with Cloud Storage for archival purposes and is scheduled as a cron job to run automatically. This approach leverages existing infrastructure and tools, such as cron, to set up an automated process. It also directly uploads the images to Cloud Storage, which is suitable for storing large binary data, and is optimally designed for archiving such files.

Solution to Question 13: A

The correct answer is A because it outlines all the necessary steps to provide viewing and editing privileges for your colleagues in Google Cloud Spanner.

Answer A involves running the "gcloud iam roles describe roles/spanner.databaseUser" command, which retrieves the necessary information about the role that allows users to view and edit table data in Cloud Spanner instances. Then, it instructs you to add the users to a new group and assign the group to the role (roles/spanner.databaseUser). This role will permit the users within the group to have the required access to Cloud Spanner, simplifying access management.

Let's discuss why other options are incorrect:

Option B: The role assignment in this option does not include a step to group the users, making access management more difficult. Grouping the users as proposed in Answer A is a best practice for managing access for multiple users.

Option C: This option runs the "gcloud iam roles describe roles/spanner.viewer" command, which retrieves information about the role that allows users to view Cloud Spanner instances but not edit table data. Since the requirement is to provide privileges for viewing and editing table data, this role is insufficient.

Option D: Similar to Option B, this answer does not provide a proper way to manage access for multiple users. Assigning the role directly to a user instead of adding them to a group creates an administrative overhead, especially when the task is to grant access to multiple users. Grouping users and granting access to the group, as described in Answer A, is a more efficient approach.

Solution to Question 14: C

Option C is the correct answer because performing a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0 enables a gradual deployment of the new version with no loss of capacity. This approach ensures that only one additional instance is created and running in parallel with the old instances until the new version rollout is complete, and ensures no decrease in available capacity as every replaced instance is appropriately updated before a new one is created. This allows for a smoothly controlled and gradual deployment process.

Option A is not ideal because updating instances within the managed instance group one by one manually is time-consuming and prone to errors. Additionally, not setting the maxSurge or maxUnavailable values could lead to a temporary

decrease in available capacity during the update process, which the company specifically wants to avoid.

Option B is not suitable because deploying the new application version in a Cloud Run container does not use managed instance groups, which the company is already using to manage and scale its web application. Such a drastic change in deployment architecture could introduce unanticipated complications and jeopardize the resources already in the managed instance group.

Option D is incorrect because creating an entirely new managed instance group and adding it to the backend service for the load balancer can result in a more complicated deployment process and increased management overhead. Additionally, deleting the old managed instance group only after all instances in the new group are healthy might cause temporary over-provisioning, thus increasing costs unnecessarily. Choosing option C addresses the outlined needs more efficiently and effectively.

Solution to Question 15: A

The most likely cause for this issue is Option A: Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

Explanation for Option A: Google Kubernetes Engine is designed to manage and schedule resources efficiently, but there may be cases when resources are completely consumed by the existing Pods. When this occurs, scheduling for new Pods gets blocked due to insufficient resources, which can lead to the Pending status observed. In this case, the single preemptible node pool might have its resources fully consumed by other Pods, leaving no room for the pending Pod to be scheduled.

Why other options will not work:

Option B: Google Cloud Load Balancer is responsible for routing traffic to the Pods, not for the scheduling of Pods. The Load Balancer failure would not prevent a Pod from getting scheduled.

Option C: A firewall rule might block communication, but it would generally lead to a failure in the control plane's ability to manage the cluster, rather than only a specific Pod being in Pending status.

Option D: GKE autoscaler is designed to automatically adjust the cluster size based on the actual load. However, if it were not set up correctly, it wouldn't directly cause the Pending status for a Pod. Additionally, incorrect autoscaler setup would affect the entire cluster, not just a specific Pod.

Hence, the answer should be A as it is the most likely cause of the issue in this scenario.

Solution to Question 16: A

The correct answer is A. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years. Here is an explanation of why:

During the first 30 days, the data is accessed frequently, requiring a storage class with low latency and high throughput. Standard storage meets these requirements, providing low-cost storage with high performance for frequently used data.

After the first 30 days, the data is rarely accessed. This makes Archive storage the ideal solution for the remaining three years. Archive storage is designed for long-term storage of infrequently accessed data and offers the lowest storage costs.

The other options are incorrect, and here's why:

B. In this policy, the Nearline storage for the first 30 days might not provide the necessary performance for frequently accessed data. Additionally, transitioning between three storage classes would lead to higher costs due to data retrieval and movement.

C. Coldline storage for the initial 30 days is not suitable for frequently accessed data, as it has higher retrieval costs and latency compared to Standard storage. These costs and latencies can have a significant impact on performance and user experience.

D. Nearline storage for the first 30 days might not provide the necessary performance for frequently accessed data. Moreover, moving to Coldline storage for three years instead of Archive storage would result in higher costs since Archive storage has lower costs than Coldline storage, making it more economical for long-term, infrequently accessed data storage.

Solution to Question 17: C

The correct answer is C: Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

Option C is the correct answer because it follows the requirements stated in the question. As the lead developer, you need to create a new billing account and link it with an existing GCP project. To do this, you must have Project Billing Manager permissions on the existing GCP project, as this role will allow you to create and associate billing accounts with that project. Once verified, you can proceed with creating a new billing account and linking it to the existing GCP project accordingly.

Option A is incorrect because it involves creating a new GCP project instead of linking the new billing account to the existing project. While it does mention verifying the Billing Account Administrator role, it doesn't accurately address the given requirements of linking the new billing account to an existing project.

Option B is incorrect because it refers to the Billing Administrator role for the GCP project, which is not a valid role in GCP. The correct role is Project Billing Manager. Additionally, after creating a new billing account, the steps do not indicate whether you should link the new billing account to the existing project, which does not fulfill the requirements.

Option D is incorrect because it requires you to create a new GCP project instead of linking the new billing account to the existing project. As a result, this option does not align with the question's requirements.

Solution to Question 18: C

The correct answer is C. Enable the compute.googleapis.com API.

Explanation:

Creating a Compute Engine instance using the gcloud CLI requires the necessary API to be enabled for the project. This API is called compute.googleapis.com. Enabling this API allows the project to access all the features and services related to Compute Engine. Thus, before establishing a Compute Engine instance, it's important to enable this API to ensure smooth communication with all the required services.

As for the other options:

A. Creating a BigQuery dataset in the project would be helpful if the purpose is to analyze data, but it is not necessary when dealing with Compute Engine instances. BigQuery is unrelated to Compute Engine, so this task is not a prerequisite for setting up a new instance.

B. Creating a VPC network in the project might be a required task for networking purposes, but this is not a prerequisite for establishing the Compute Engine instance itself. The instance can be created first, and then connected to the VPC network later. So it's not a mandatory step before creating a Compute Engine instance.

D. Creating a Cloud Run service in the project is useful for deploying and managing containers, but it isn't a prerequisite for creating a Compute Engine instance. While both Compute Engine and Cloud Run are designed for running applications, they serve different purposes and are therefore independent of each other. Cloud Run focuses on serverless deployment, whereas Compute Engine involves provisioning VMs. Therefore, this option is not required before setting up a new Compute Engine instance.

Solution to Question 19: C

The answer should be C: "Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories."

Explanation:

Option C is the most suitable approach as it adheres to Google's recommended best practices for collaborating on infrastructure changes. Deployment Manager templates provide a way to describe and manage infrastructure as code, making it easy to review, collaborate on, and maintain the proposed changes. By storing the Deployment templates in Cloud Source Repositories, you can ensure that the team has a single source of truth and can collaborate using a version-controlled system.

Why other options will not work:

Option A: While applying changes in a development environment is a good practice, saving the gcloud compute instances list output in Cloud Source Repositories is not an ideal way to discuss and collaborate on proposed changes. It does not provide a clear representation of the changes or enable easy collaboration and version control like Deployment Manager templates stored in Cloud Source Repositories.

Option B: This option lists several unrelated components and services which are not applicable for the desired purpose (e.g., storing Deployment Manager templates in Cloud Pub/Sub, using Firestore, and using Cloud Logging). Moreover, this option seems to be an arbitrary mixture of different approaches without providing a clear and coherent method for effectively communicating and collaborating on the proposed changes.

Option D: Applying the changes in a development environment is appropriate, but saving gcloud compute instances list output in a shared Storage bucket is not ideal for effective collaboration. This approach does not provide a clear, organized, and easily maintainable way of describing and managing the proposed infrastructure changes like the Deployment Manager templates in Cloud Source Repositories.

Therefore, option C is the most suitable approach for communicating and collaborating on proposed infrastructure changes while adhering to Google's best practices.

Solution to Question 20: D

The correct answer is D. Install and configure the Ops agent and view the logs from Cloud Logging.

Explanation:

When an application is deployed on a Compute Engine instance, it writes logs to the disk. To diagnose the reported errors, you need to access the logs written by the application to understand what is causing the issues.

Option A is incorrect because deploying a new version of the application using Cloud Functions does not help with diagnosing the current issue. While Cloud Functions might simplify deployment in the future, it does not provide insights into the errors occurring with the current application instance.

Option B is incorrect because navigating to Cloud Logging will not automatically show the application logs. Since the application is deployed on a Compute Engine instance, you first need to configure a monitoring agent (Ops agent) to collect and forward the logs to Cloud Logging before you can view them there.

Option C is incorrect because Stackdriver Monitoring has been rebranded as Cloud Monitoring, and its primary purpose is to monitor application performance and health, not directly accessing application logs. In order to view logs, you'll need to utilize Cloud Logging, which works in conjunction with the Ops agent on the Compute Engine instance.

Therefore, the correct answer is to install and configure the Ops agent (Option D) on the Compute Engine instance. By doing this, the agent will collect the logs written by the application and forward them to Cloud Logging. From there, you can view and analyze the logs, which would help diagnose the reported application errors.

Solution to Question 21: A

The correct answer is A: Configure Billing Data Export to BigQuery and visualize the data in Data Studio. The reason this option is the most suitable one is that it allows for a streamlined, automated process to export and consolidate cost data across multiple projects and billing accounts. By using BigQuery, you can effectively analyze large datasets and create comprehensive reports. Integrating Data Studio further enables you to create interactive, real-time visualizations that make it easier to forecast and manage costs.

The other options are not as suitable for the following reasons:

B. Visit the Cost Table page to get a CSV export and visualize it using Data Studio: This option is a manual process that does not work well with multiple billing accounts. It would require manual effort to consolidate data from different projects and accounts, making the forecasting and reporting tasks more prone to errors and inconsistencies.

C. Export the billing data of each project to Cloud Storage in CSV format and use Data Studio to visualize the costs: Although this option can export data from individual projects, it does not provide a comprehensive solution for consolidating the data in an organized manner. It would still require manual work to merge the multiple CSV files and could potentially lead to inconsistencies in reporting.

D. Use Cloud Billing Budget & Thresholds to create a single budget for all projects and visualize it in Data Studio: This option does not enable an accurate forecast of future expenses as it focuses on setting budget thresholds rather than analyzing cost data in detail. It also does not serve the purpose of presenting a single, up-to-date visual report of all costs incurred, which is the main objective of the question.

By choosing option A, you can easily achieve the goal of managing costs across

various projects linked to different billing accounts while presenting a unified, real-time visualization of the data.

Solution to Question 22: B

The correct answer is option B. Here's why the other options are not suitable:

Option A: Creating a shared Gmail account and using its Google account to generate an SSH key pair is not a secure solution. Sharing a single account among the team members prevents you from having a proper audit trail and accountability, as you cannot track who accessed any given instance. Additionally, it does not comply with the security best practices of not sharing credentials.

Option B: This option is the most appropriate choice because it entails that each team member generates their own SSH key pair, and adds the public key to their Google account. This allows for proper tracking and auditing of access to the instances in Compute Engine. By granting the 'compute.osAdminLogin' role to the Google group associated with the team, you ensure that team members have the required permissions to manage the instances securely and efficiently.

Option C: Although you have individual SSH keys for each team member in this option, storing the keys in a shared Google Sheet poses a security risk. Using a configuration management tool to deploy keys adds unnecessary complexity and potential points of failure. Additionally, it does not allow you to effectively track and audit who accessed each instance, as the process does not integrate seamlessly with Compute Engine access management.

Option D: Generating a new SSH key pair and distributing the private key to each team member is not a secure practice, as private keys should never be shared. This approach makes it challenging to track individual accesses and maintain accountability. Moreover, relying only on firewall rules for access restriction is not sufficient, as it does not integrate seamlessly with Compute Engine access management.

In summary, option B is most suitable because it allows for secure and efficient management of credentials, integrates seamlessly with Google Cloud Platform's access management, and enables tracking and auditing of user access to the instances.

Solution to Question 23: A

The correct answer is A. Migrate to use a Local SSD on the instance.

Reasoning for choosing A:

Local SSDs offer high performance and low latency, making them an ideal choice for applications that require large amounts of throughput. In this case, migrating to use a Local SSD would provide the needed performance for an application that primarily reads large files from disk. Additionally, Local SSDs can be more cost-effective due to their pricing per GB compared to SSD Persistent Disks.

Reasoning for not choosing the other options:

B. Optimize the Operating System for disk reads. While optimizing the operating system can lead to some improvements in performance, it is unlikely to provide the maximum amount of throughput required in this case. The main issue is the current disk type (Zonal SSD Persistent Disk), which is not optimized for high-throughput applications.

C. Migrate to use a Regional SSD on the instance. Regional SSD Persistent Disks provide higher availability and durability as the data is replicated across multiple zones. However, this option does not necessarily improve the disk performance, which is the main concern in this scenario. Additionally, this option can also lead to higher costs compared to Local SSDs.

D. Increase the size of the disk to 750 GB. Increasing the size of the Zonal SSD Persistent Disk to 750 GB would increase the performance linearly, but it would not provide the maximum throughput needed for an application that primarily reads large files. This option also leads to increased costs due to the larger disk size without necessarily solving the performance problem.

Solution to Question 24: A

The correct answer should be A, and here's why:

A. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment. This option ensures that there are no network routes between the development and production environments, as each environment will reside in its separate project. Additionally, it aligns with Google-recommended practices to isolate environments using separate projects, providing a clear boundary and ensuring the security team's guidelines are followed.

B. Create two new Cloud SQL instances in the existing project, one for the development environment and one for the production environment, and restrict traffic between them using firewall rules. This option doesn't comply with the security team's prohibition of any network routes between the environments. Although firewall rules may restrict traffic, the environments are still within the same project and network, making it less secure compared to Option A.

C. Create a new separate VPC for the production environment within the existing project and connect the two environments using VPC peering. This option does not adhere to security guidelines provided by the team since they require no network routes between the two environments. VPC peering creates a network route between the environments, making it less secure and not suitable for the given requirements.

D. Enable Private Google Access and Private Service Access in the existing project to restrict traffic between the Compute Engine and Cloud SQL instances for both environments. These features help private communication within an environment, but they don't isolate the environments from each other. Both environments would still reside in the same project, violating the security team's guidelines of no network routes between the environments.

Solution to Question 25: B

The correct answer is B - Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI.

To access and manage the existing instances on Google Cloud, you must be authenticated and authorized to use the Google Cloud Platform (GCP) resources. Option B is the essential step here, as the "gcloud auth login" command initializes your account for the Google Cloud SDK and opens a dialog window for you to enter your login credentials. Then, you will receive an authorization token to paste in your gcloud CLI, granting you the necessary access to manage the instances.

Now, let's discuss why the other options will not work:

Option A: Running "gcloud compute instances create" is unnecessary here, as you need to access and manage existing instances, not create a new one. This command will only add an additional instance and not help in listing the existing instances.

Option C: Creating a .boto configuration file and storing it in your home folder might be useful for configuring authentication, but this file is primarily used for accessing Google Cloud Storage using the gsutil command, not for general gcloud CLI authentication. gcloud uses its own configuration files.

Option D: Running "gcloud config set compute/zone $my_zone" sets the default zone for gcloud CLI, which can streamline future interaction by limiting API calls to a specific zone. However, this command is not essential for listing the instances, and you can still access and manage them without specifying a default zone.

Solution to Question 26: D

The correct answer is D. Deploy the new version in the same application and use the –splits option to give a weight of 99 to the current version and a weight of 1 to the new version.

Explanation:

Option D is the most appropriate choice in this scenario because it allows you to easily manage the traffic distribution between the old and new versions of the website within App Engine, and you only need to update the –splits option to change the traffic allocation. This approach is straightforward and minimizes complexity, which is what the company wants.

Option A is not the correct solution for this scenario because although it does involve traffic splitting in App Engine, it requires using the Console, which would not be as simple and straightforward as using the –splits option to adjust the traffic split.

Option B is not the correct choice because creating a new Cloud Storage bucket is not required for this task, and it increases complexity. Additionally, using the

App Engine library to proxy 1% of the requests to the new version would not be as efficient as using traffic splitting.

Option C is not the correct choice because creating a new App Engine application within the same project will increase the management complexity. Moreover, configuring a network load balancer to send 1% of the traffic to the new application is not as easy to manage as simply using the –splits option in the deployment command.

Therefore, the best approach for this task is to deploy the new version in the same application and use the –splits option to give a weight of 99 to the current version and a weight of 1 to the new version (Option D). This ensures that 1% of the users will be directed to the new version while keeping the complexity at a minimum.

Solution to Question 27: A

Option A is the best approach to provide the most accurate cost estimate for utilizing various Google Cloud products in the project. By reviewing the pricing details on each product's pricing page, you ensure that you are using the most up-to-date and correct information directly from Google. Moreover, using the Google Cloud pricing calculator makes it easy to input the necessary parameters, usage, and resources for each product. The calculator automatically computes the total monthly costs, factoring in any potential discounts or promotions.

Option B is not reliable as it relies on unofficial sources where the information might not be accurate or up-to-date. You could receive misleading estimations and expose your company to unpredictable costs.

Option C might seem promising, but manually creating a Google Sheet to summarize the expected costs leaves room for human error. Plus, it could be more time-consuming compared to using the pricing calculator, which derives those values automatically.

Option D is not appropriate because it can lead to inaccurate cost estimates. Leaving the solution provisioned for only 1 week will not give you an accurate estimate of the monthly total cost, as costs could vary week by week due to fluctuations in usage or other factors. Furthermore, this method could generate unnecessary expenditures, especially if the solution isn't optimized or fully utilized during that week.

Solution to Question 28: C

The correct approach to store audit log files for a duration of 3 years across hundreds of Google Cloud projects in a cost-effective manner is Option C: Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket.

Reasoning for Option C: Coldline Storage buckets offer cost-effective, long-term storage for infrequently accessed data, making it an ideal solution for storing audit log files. By creating an export to the sink, you can directly save logs

from Cloud Audit to a Coldline Storage bucket, which simplifies the process and reduces the overall costs.

Reasoning against other options: A. Writing a custom script that uses the logging API to copy logs from Stackdriver logs to BigQuery would require constant maintenance and the potential for errors. Moreover, BigQuery is designed for real-time analytics and is not the most cost-effective solution for long-term storage of audit logs.

B. Exporting logs to Cloud Pub/Sub and writing a Cloud Dataflow pipeline to store logs in Cloud SQL is not a recommended solution for this use case. Cloud SQL is mainly used for relational databases with a high number of transactions, not for long-term storage of log files. Additionally, implementing a Cloud Dataflow pipeline would introduce unnecessary complexity and additional costs for this task.

D. Exporting logs to Cloud Pub/Sub and utilizing a Cloud Dataflow pipeline to store logs in Cloud Bigtable is not ideal for long-term storage purposes. Cloud Bigtable is designed for fast, random access to large amounts of data, making it particularly useful for analytical and operational workloads, but not cost-effective for long-term storage of infrequently accessed data like audit logs.

In conclusion, Option C provides the most cost-effective and efficient solution for storing audit log files for an extended period across multiple Google Cloud projects.

Solution to Question 29: D

The correct option is D: Deploy MongoDB Atlas from the Google Cloud Marketplace. This is because MongoDB Atlas is a managed MongoDB service that offers support SLA and is directly available on the Google Cloud Platform Marketplace. It provides an efficient and scalable solution for your application's database requirements on Google Kubernetes Engine (GKE).

Here is the explanation for the other options:

Option A: Download a MongoDB installation package and run it on Compute Engine instances. This option is not ideal because it would require manual management of the MongoDB instances, which would make it more difficult to scale and maintain. Additionally, you would not have the benefit of a support SLA from MongoDB, as you would be handling the management of the instances yourself.

Option B: Deploy MongoDB on Cloud Run and configure it as a stateful service. Cloud Run is designed to run stateless containers, and configuring MongoDB to work as a stateful service on Cloud Run would be both challenging and unsupported. Moreover, you wouldn't have a support SLA from MongoDB in this case, as you would be deploying the MongoDB container on your own.

Option C: Deploy a MongoDB container on Cloud Functions and trigger it with an event. This option is not feasible since Cloud Functions is a serverless plat-

form meant for running single-purpose stateless functions in response to events. It is not designed to host stateful applications like MongoDB, and running a MongoDB instance on Cloud Functions would be highly impractical and unsupported. In addition, you would not have a support SLA from MongoDB.

In conclusion, considering the aspects of a managed MongoDB system with a support SLA for an application that operates on Google Kubernetes Engine, option D: Deploy MongoDB Atlas from the Google Cloud Marketplace is the most appropriate choice.

Solution to Question 30: D

The correct answer is D. Go to Cloud Shell and run gcloud config list to review the Google Cloud configuration used for deployment.

Explanation:

When you deploy an App Engine application using gcloud app deploy, the deployment is performed based on the active project and configuration settings in your Cloud SDK gcloud CLI. The command gcloud config list allows you to review your current Google Cloud configuration, including the active project and any other settings that may influence the deployment of your application. By running this command, you can verify if the project setting is indeed set to your intended project, or if it's set to a different one. In case the active project is incorrect, you can correct it using the gcloud config set project command.

Why other options will not work:

A. Review logs in the App Engine dashboard in Google Cloud Console to check any deployment issues - While reviewing logs is useful for identifying runtime and deployment issues, it does not help determine which project the application was deployed to if the wrong project was selected during deployment.

B. Verify IAM permissions for the App Engine Admin API in the intended project - IAM permissions determine who can deploy and manage App Engine applications but do not address why the application was deployed to an unintended project in the first place. The issue in this scenario is related to the configuration settings of gcloud CLI, not permissions.

C. Run gcloud projects list to verify the proper project ID for the intended project - This command will give you a list of accessible projects with their associated project IDs but will not reveal the currently active project in your gcloud CLI configuration that was used for deployment. The focus should be on finding the active project during the deployment rather than verifying project IDs.

Solution to Question 31: B

The correct answer is B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

Explanation: Since your goal is to enable the development team to access all instances through an SSH client over the internet without configuring specific access on the existing and new instances, configuring Cloud Identity-Aware Proxy (IAP) for SSH and TCP resources is the best solution. IAP helps manage access to SSH and TCP services running on your instances without using a public IP. This way, developers can access the instances securely, and no additional configuration is needed for each new instance.

Here's why other options will not work:

A. Configure Cloud Identity-Aware Proxy for HTTPS resources: This won't work as the requirement is to enable access for the SSH client, not HTTPS resources. IAP for HTTPS resources is used for web applications and services over HTTPS, but not suited for SSH access management.

C. Use Cloud Load Balancer with the TCP Proxy protocol for the instances: Cloud Load Balancer with TCP Proxy protocol is designed for load balancing of TCP traffic, not for managing access to instances over SSH. While it might allow routing traffic to instances, it doesn't provide access control and security features needed for the given requirement.

D. Create an SSH keypair and store the private key as a project-wide SSH Key: While this solution might give your team SSH access, it doesn't adhere to the requirement of not having a public IP. Additionally, this approach is not scalable, as it becomes challenging to manage access keys with the growing number of instances and team members. It is also less secure than using Cloud Identity-Aware Proxy, as it does not provide any access control features.

Solution to Question 32: A

The correct answer is A. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity. The reason is that GCDS enables you to synchronize the user identities in your company's Active Directory with Cloud Identity, which serves as a centralized repository for all Google services, including GCP organization. By using GCDS, the management can provide seamless and unified access to Google services while maintaining full control over the Google accounts used by employees.

The other options will not work for the following reasons:

B. Exporting users from Active Directory as a CSV and importing them to Cloud Identity via the Admin Console is not the best solution because it would require manual effort to keep both systems up-to-date. Additionally, it does not provide real-time synchronization of user accounts between Active Directory and Cloud Identity. This would be highly inefficient and more error-prone.

C. Using Google Cloud SQL to store users' data and connecting it to Cloud Identity is not suitable because it does not directly integrate with Active Directory. This option adds an unnecessary step and could result in data inconsistencies

between the two systems. GCDS provides a more streamlined solution for synchronizing user identities between Active Directory and Cloud Identity.

D. Using the GCP Console to migrate users from Active Directory to Cloud Identity is not a viable option because it does not provide a direct method for syncing user identities between Active Directory and Cloud Identity. It would require manual effort to keep both systems up-to-date and would not be as efficient as using GCDS, which is specifically designed for this purpose.

Solution to Question 33: B

The correct answer is B, and here's why:

Option A: In this scenario, you should create a firewall rule to allow ingress, not egress. Egress refers to traffic leaving the network, while ingress refers to traffic entering the network. Additionally, since we are only concerned about allowing clients to access the LDAP server over a specific port, creating a firewall rule for egress on UDP port 636 is not suitable for this situation.

Option B: This is the correct action to take because adding a network tag to the instance and creating a firewall rule to allow ingress on UDP port 636 for that network tag ensures that clients can access the LDAP server over the required port. The ingress rule allows traffic to enter the network, which is necessary for clients to connect to the server.

Option C: Creating a route is unnecessary in this situation, as you want to ensure that clients can access the LDAP server over a specific port, not control the path that the traffic takes in the network. Additionally, routes are designed to direct traffic to instances based on the destination IP address range, rather than a specific port.

Option D: Establishing a VPC peering connection, enabling the 'Allow Secure LDAP access over the Internet' option, creating a Cloud VPN tunnel, or configuring a Cloud NAT gateway are not necessary in this scenario. Cloud VPN and Cloud NAT are used to establish secure connections between multiple networks or provide internet access to private instances, respectively. In this case, the main concern is to allow clients to access the LDAP server over a specific port, and these options do not directly address that requirement.

Options E to J: These options are irrelevant and excessive for the given situation since the main requirement is to allow clients to access the LDAP server over UDP port 636. These options involve creating additional components or adjusting other settings, whereas the most straightforward and effective solution is B: adding a network tag to the instance and creating a firewall rule to allow ingress on UDP port 636.

Solution to Question 34: B

The correct answer is B. Configure an HTTP(S) load balancer.

An HTTP(S) load balancer is the appropriate choice in this scenario, as it is

designed to provide global load balancing for HTTP and HTTPS traffic. This means it can manage the distribution of incoming traffic across instance groups, ensuring proper load balancing for a public web application. Moreover, it supports client SSL session termination, which meets the specific requirement mentioned in the question.

Here is why the other options will not work:

A. Configure a global external forwarding rule: A global external forwarding rule alone is not sufficient to provide the load balancing and SSL termination features required in this scenario. It is used to match incoming traffic and route it to a target proxy, but the actual load balancing and SSL termination are handled by the target proxies, such as in the case of HTTP(S) load balancers.

C. Configure an internal HTTPS load balancer: An internal HTTPS load balancer is designed for load balancing traffic within a Virtual Private Cloud (VPC) and between backends within the same region. It cannot be used for balancing a public web application, as it is not exposed to the internet and does not support client SSL termination.

D. Configure a regional external forwarding rule: Similar to option A, a regional external forwarding rule alone is not sufficient to provide the required load balancing and SSL termination features. It is used to match incoming traffic and route it to a target uniquely within a region, but the actual load balancing and SSL termination are handled by different target proxies. Furthermore, it lacks the global load balancing capabilities offered by the HTTP(S) load balancer.

In conclusion, in order to manage an instance group for load balancing a public web application over HTTPS while ensuring client SSL session termination, following Google-recommended practices, you should configure an HTTP(S) load balancer.

Solution to Question 35: D

The correct answer should be D. Create a multi-region Cloud Spanner instance with an optimized schema, and here's why:

A. Creating a multi-region BigQuery dataset with optimized tables would work well for large-scale data analytics and running SQL queries. However, BigQuery is more suited for data warehousing and batch processing, rather than handling real-time transactions of a retail company. Therefore, it is not the best choice for this scenario.

B. Using a multi-region Pub/Sub for streaming transaction data and analyzing it using Dataflow might be good for ingesting and processing real-time data. Still, it does not function as an appropriate data store for the transactional data that the backend service needs to handle.

C. Creating a multi-region Cloud SQL for MySQL database with no read replicas would provide some degree of high availability by being present in multiple regions. However, it lacks the ability to scale horizontally for handling large

volumes of global transactions efficiently. The absence of read replicas also limits the capabilities of running SQL queries for data analysis purposes without affecting the transaction processing performance.

D. Creating a multi-region Cloud Spanner instance with an optimized schema is the best choice for this scenario. Cloud Spanner is a fully managed, scalable, and highly available database service designed to handle large volumes of global transactions. It provides strong consistency across regions and automatic sharding for horizontal scalability. This solution meets the business team's requirement of running SQL queries for data analysis purposes and can cope with the large volume of transactions coming from various mobile and web clients.

Solution to Question 36: A

The correct answer is A. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

Explanation for choosing A:

By implementing option A, you are using the best Google Cloud services which are specifically designed for their focus: Pub/Sub for reliable message streaming, Dataflow for data processing and Cloud Storage for scalable data storage.

Cloud Pub/Sub provides at-least-once delivery of messages, which ensures no data loss, and is scalable to handle high-throughput data streams due to its global nature. Dataflow is capable of processing both real-time and batch data from ingested data streams, and by merging data to Cloud Storage, it creates a highly available, resilient and distributed storage.

Explanation for not choosing B, C, and D:

B. Streaming data to Cloud Pub/Sub and using Dataflow to send data to Cloud SQL is not ideal because Cloud SQL has some limitations and is not primarily designed as a data lake; it's more suitable for structured relational data. This choice lacks the scalability and cost-effectiveness that options like Cloud Storage provide for storing massive amounts of data.

C. Streaming data to IoT Core is not recommended because it is a device management service meant to manage and authenticate IoT devices. Cloud Functions can have a high cost in terms of execution time, which can contribute to longer latencies, and Cloud Storage by itself is not optimal for handling real-time streaming data directly.

D. Stream data to Pub/Sub and use Dataflow to send data to Firestore: Firestore is not ideal for use as a data lake. It's better suited to mobile and web applications for real-time data access. Firestore has limitations on data storage when compared to Cloud Storage, which is more suited to handling large volumes of data and is more cost-effective for storing data in a data lake scenario.

Solution to Question 37: A

The correct answer is A. Select the built-in IAM project Viewer role. Add the user's account to this role.

Explanation for A:

The built-in IAM project Viewer role provides read-only access to all project items without allowing any modifications, which matches the requirement for the auditor in this situation. It is a pre-defined role that efficiently provides the needed permissions without any additional configuration. By adding the user's account to this role, they'll have the necessary access without risking any unwanted changes to the project.

Explanation for why other options will not work:

B. Creating a custom role with view-only service permissions might seem like a viable solution, but it is unnecessary when there is already a built-in role (Viewer) that meets the criteria. Custom roles should be used when there's a need for more unique or granular control over permissions, but in this case, the Viewer role is sufficient.

C. Assigning the user to the IAM BigQuery Data Viewer role with project-wide permissions specifically focuses on providing read-only access to data within BigQuery, not the entire project. As the auditor needs access to all project items, this option is too limited for their requirements.

D. Adding the user to the IAM Billing Account Viewer role with project-wide permissions gives read-only access to the billing account and its cost-related information but not to the other project resources. The auditor needs access to all project items, not just billing information, thus making this choice inappropriate for their role.

Solution to Question 38: C

The correct answer is C. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

Explanation:

Option A: Granting only the Compute Image User role without the compute.disks.list permission at the project level will not provide the desired access. This is because Compute Image User role does not include the ability to list compute disks, which is necessary for the requirements of the given task.

Option B: Granting the Compute Storage Admin role and the Compute Image Admin role at the organization level is not recommended because it violates the principle of least privilege. The external team member would be granted broader and more permissions than required for their task, which goes against Google-recommended practices.

Option C: Creating a custom role and adding the required compute.disks.list and compute.images.list permissions meets the necessary requirements without

granting excessive permissions. By granting the custom role to the user at the project level, we ensure that the external team member has sufficient access to complete their task while adhering to Google's recommended practices for security and access management.

Option D: Granting the Compute Image User role and the Compute Disk Viewer role at the project level would provide the necessary permissions related to compute images and disks; however, the Compute Disk Viewer role has excessive permissions that are not required for the given task, making it a less ideal solution than a custom role tailored to the specific requirements (Option C).

Solution to Question 39: D

The correct answer is D as it recommends deploying a private autopilot cluster. Here is the explanation:

A private autopilot cluster provides all the necessary security features required in a financial organization. The nodes are not accessible from the internet, which ensures that the cluster's security is maintained. By making it an autopilot cluster, Google automatically takes care of the cluster management, which helps minimize operational costs. Plus, private clusters in GKE follow Google-recommended practices, ensuring the project's reliability.

Option A is incorrect because it suggests deploying a public App Engine cluster, which would expose the nodes to the internet. This is a security risk for a financial organization. Although the option mentions enabling shielded nodes, it does not solve accessibility concerns.

Option B is incorrect because it suggests deploying a public Cloud SQL instance, making it accessible from the internet, and consequently, increasing security risks. Shielded nodes do provide some additional security, but it still does not address the vulnerability of being a public instance.

Option C is incorrect because it suggests deploying a public autopilot cluster, which would make the nodes accessible from the internet. This exposes the financial organization's data to security threats and goes against providing verifiable node identity and integrity.

In conclusion, the best choice is to deploy a private autopilot cluster (Option D) to meet all the requirements stated while ensuring high levels of security, minimizing operational costs, and adhering to Google-recommended practices.

Solution to Question 40: D

The correct answer is D, "Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool."

This is because using environment variables ensures that the sensitive proxy credentials are not permanently stored, reducing the risk of exposure in logs or configuration files. This method is preferred because it helps adhere to best

practices for handling secure data, and the credentials are available only during a specific session.

Option A is incorrect because using a JSON file to store proxy credentials poses a risk by having them saved in an external file that could be accidentally exposed or logged, which may lead to security breaches.

Option B is incorrect because providing values in the gcloud CLI tool configuration file represents a security risk, as the credentials could be exposed when sharing or syncing configurations. It's better to use a temporary way to store credentials, like environment variables, as mentioned in option D.

Option C is incorrect, as asymmetric encryption doesn't provide the required protection for the proxy credentials. While encryption may offer some degree of enhanced security, storing encrypted credentials in the gcloud CLI can still lead to exposure if the decryption keys are compromised. In comparison, option D provides a better approach by using temporary storage for the sensitive data.

Solution to Question 41: A

The correct answer is A: Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

Here's why:

A: With this option, you automate the process of scaling Cloud Spanner nodes up or down, based on traffic patterns. By using a Cloud Monitoring alerting policy, you can set a CPU usage threshold that, once exceeded, will trigger an alert. The webhook will send this alert to a Cloud Function, which is designed to listen for HTTP requests and take appropriate action to resize Spanner resources in response.

B: Using a cron job may indeed review Cloud Monitoring metrics periodically, but its fixed schedule could potentially miss rapid changes in traffic patterns, resulting in inefficient resource allocation. Furthermore, this approach lacks the real-time responsiveness needed to handle dynamic scaling requirements, which may eventually impact application performance.

C: While sending an alert to the SRE's email when the CPU load exceeds the threshold engages a proactive approach, it still requires human intervention. This method could result in delays or inconsistencies in scaling, as SREs may not always be available to act immediately. Moreover, it is not an automated solution and can contribute to resource wastage and higher operating costs.

D: Relying on Google Cloud Support to handle the scaling process based on alert emails lacks efficiency and proactivity. This method is subject to the response time of the support team and manual intervention, which can lead to resource underutilization or overload, negatively impacting the application's performance.

Hence, Option A is the best solution, as it automates the scaling process and responds to changes in traffic patterns more efficiently, ensuring optimal resource allocation for the Cloud Spanner database.

Solution to Question 42: B

The correct answer is option B, which involves creating a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API. This approach is ideal because it aligns with the requirements for an authenticated, fully managed, serverless compute solution following Google-recommended practices. Furthermore, it automates the process by immediately sending each file to the API as soon as the audio file is uploaded to the Cloud Storage bucket.

Option A is not suitable because it entails using a Kubernetes job to regularly scan the bucket for incoming files. While Kubernetes is a powerful container orchestration tool, it is not a serverless solution and requires more management compared to a Cloud Function.

Option C is not the best choice because it involves creating a Dataflow job triggered by Cloud Storage bucket events. Dataflow is designed for large-scale data processing tasks and might be overkill for the given scenario. It isn't as straightforward or cost-effective as Cloud Functions for addressing the specific requirement described.

Option D is not appropriate because implementing a Cloud Scheduler job to scan the bucket regularly would not offer real-time processing as desired. It would only check for new files at the scheduled interval, leading to delays in processing audio files when compared to a Cloud Function triggered by bucket events. This also might incur unnecessary costs due to repetitive scanning.

Solution to Question 43: B

The ideal course of action for this scenario is Option B: Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

Here's why Option B is the correct answer and why the other options will not work:

Option A: Select Regional Storage. Add a bucket lifecycle rule that moves data to Bigtable after 30 days. - Bigtable is not a suitable solution for this scenario. It is a highly available and scalable NoSQL database designed for real-time analytics and operational workloads, not for archiving data that is accessed rarely.

Option B (Correct answer): Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage. - Regional Storage ensures that data is stored within a specific geographic location, which adheres to the compliance requirements. - Coldline Storage is designed for data archiving, which requires infrequent access (e.g., once a year, as stated in the question). -

The bucket lifecycle rule correctly moves data to Coldline Storage after 30 days to align with the organization's archiving needs.

Option C: Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Cloud Storage Archive. - This option seems plausible but is ambiguous. Cloud Storage Archive likely refers to the "Archive Storage" class in Google Cloud Storage. However, Archive Storage has higher data retrieval costs and longer data retrieval times compared to Coldline Storage. Since the data will be accessed once a year, Coldline Storage is a more cost-effective and appropriate choice.

Option D: Select Regional Storage. Add a bucket lifecycle rule that archives data after 60 days to Coldline Storage. - Although this option suggests archiving data to Coldline Storage, it does not meet the organization's 30-day archiving requirement as it specifies a 60-day archiving period instead of 30 days.

In conclusion, the ideal solution for this scenario is Option B. It caters to the organization's needs by storing data in a specific geographic location (Regional Storage) while adhering to the 30-day archiving requirement, and using Coldline Storage for cost-effective long-term storage with infrequent access.

Solution to Question 44: C

The correct answer is C, which involves storing the application data on a regional persistent disk. If an outage occurs, you can create an instance in another zone with this disk attached. This approach guarantees high availability and immediate data access in case of a zonal failure. Regional persistent disks automatically replicate data between two zones within the same region, ensuring that your data remains available even if one zone goes down.

Option A is not ideal because Firestore databases are used for managing collections of documents and not application data. Although replicating VM instances in two zones provides redundancy, it does not directly address high availability and immediate data access during zonal failures, as the mentioned storage solution is not ideal for this use case.

Option B does not offer the required high availability, as Cloud Datastore has been deprecated in favor of Firestore, which does not handle replication across zones for this type of application. Furthermore, Cloud Datastore does not provide an inter-zone replication feature for high availability.

Option D is not the best solution, as Cloud Filestore instances are designed for file-serving purposes and not optimized for application data storage. Additionally, using multiple zones as NFS mounts for the Cloud Filestore instance could lead to potential latency issues during data recovery if any zonal failure were to occur.

Solution to Question 45: D

The correct answer is D. Use Cloud Spanner to store user data mapped to the game statistics. The reasons for choosing this option and why the other options

are not suitable are as follows:

Option D - Cloud Spanner is a fully managed, scalable, and globally consistent database service that is designed to handle high-concurrency read and write operations. Using Cloud Spanner to store user data mapped to game statistics ensures that the gaming experience remains consistent, regardless of the number of users or their location, without adding management complexity.

Option A - Though using Cloud Datastore in native mode with regional indexes might improve query performance for game statistics, it doesn't fulfill the requirements for a multi-player gaming application which demands global consistency, high-concurrency, and low-latency. Furthermore, it might increase the risk of eventual consistency issues, which can harm the gaming experience.

Option B - Using Cloud SQL with read replicas in each region might help serve global users, but it introduces operational complexity by managing replicas independently in different regions. Additionally, Cloud SQL's replication process might add latency to the system, resulting in a slower gaming experience.

Option C - While Cloud Spanner is the right choice, using manual sharding is unnecessary, since one of the main benefits of Cloud Spanner is its automatic horizontal scaling. Manual sharding could complicate data management, and you may not achieve the optimal performance required for a seamless gaming experience.

In conclusion, using Cloud Spanner to store user data mapped to game statistics (Option D) is the most suitable approach, as it ensures optimal gaming experiences for users worldwide without adding management complexity.

Solution to Question 46: C

The correct answer is C: View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

Explanation: To determine if the former employee accessed any sensitive customer data post-termination, it's crucial to look into the Data Access audit logs. These logs store records of Google Cloud API calls that result in data being read or modified. By searching for the user's email as the principal, you can effectively trace any unauthorized access to sensitive customer information under the terminated employee's account. This process specifically targets the necessary data and the relevant timeframe.

Why other options will not work:

A. View Data Access audit logs in Cloud Logging. Search for the service account associated with the user. - This option would not work effectively in tracking the unauthorized access as service accounts are usually tied with server and application resources, rather than human users. It is important to focus on the personal account of the terminated employee to analyze their actions.

B. View VPC Flow Logs in Cloud Logging. Search for the IP address associated

with the user. - VPC Flow Logs record the network flows in a Virtual Private Cloud (VPC) network. While this helps monitor network traffic, it does not target the specific data access events at the application level. This would make it difficult to determine if the terminated employee accessed any sensitive customer information.

D. View Admin Activity logs in Cloud Auditing. Search for the IP address associated with the user. - Admin Activity logs record the actions done by admins, focusing primarily on configuration changes and modifications. This approach might not provide detailed information about data access events necessary to identify sensitive customer data access. Searching by the user's IP address is not effective as it can change and does not provide a definitive way to trace the user.

Solution to Question 47: D

The correct answer is D because it ensures that all read, write, metadata, and configuration operations in the Bigtable instance are logged and forwarded to the company's SIEM system. Let's break down each option and explain why it's the best choice:

Option A: Installing the Ops Agent is not the appropriate solution for logging read and write operations in a Bigtable instance. Moreover, creating a custom Dataflow job is an unnecessary complexity when attempting to export logs to the company's SIEM system, as Pub/Sub and Cloud Logging sinks can be used for this purpose.

Option B: Cloud Run is designed to run serverless applications on a fully managed environment, not for monitoring or logging Bigtable instances. Additionally, this method does not mention logging metadata or configuration operations, which are required for the question's scenario.

Option C: The issue with this option is that it only enables Admin Write logs. By doing so, only write operations will be logged in the Bigtable instance while the question's requirement is to log all read and write operations, including metadata and configuration reads.

Option D: This is the correct course of action because it fulfills all the requirements stated in the question. By navigating to the Audit Logs page in Google Cloud Console and enabling Data Read, Data Write, and Admin Read logs for the Bigtable instance, you ensure that all necessary events are being logged. Creating a Pub/Sub topic as a sink destination in Cloud Logging and adding your SIEM as a subscriber to the topic ensures the logs are forwarded to your company's SIEM system. This method meets the requirements for monitoring and logging in the given scenario.

Solution to Question 48: A

The correct answer is A: Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

Here's why each option is either a suitable or not suitable solution:

A) Running a test using simulated maintenance events can help you determine if your nightly batch workload can successfully tolerate VMs being terminated. By using Spot N2 Standard VMs when running future jobs, you can benefit from significantly discounted prices compared to regular VMs. Spot VM instances are also built to withstand terminations, as they are designed for workloads that can tolerate some disruption. This will enable you to maintain reliability while reducing costs.

B) Running a test using a managed instance group might provide some scalability and fault tolerance, but it does not inherently address the concern of the high cost of the VMs being used. N2 Standard VMs in a managed instance group could still be expensive, which would not provide the desired cost reduction.

C) N1 Standard VMs might be less expensive than N2, but they could also provide less performance. It may lead to longer processing times or resource constraints for your nightly batch workload. Moreover, if your load can tolerate some terminations, you still miss the opportunity to capitalize on the lower-cost Spot instances.

D) Cloud Functions are not an ideal solution for this workload, as they are better suited for lightweight tasks or single-function applications. Running a nightly batch workload that utilizes numerous VMs might require more processing capability than what can be offered by Cloud Functions. Additionally, the pay-per-invocation nature of Cloud Functions could result in a cost increase compared to appropriately sized VM instances.

In summary, Option A provides an optimal balance between cost savings and maintaining the reliability of the nightly batch workload. It takes advantage of the lower-cost Spot N2 Standard VMs, which are specifically designed for workloads that can accommodate VM terminations, addressing both the cost and reliability concerns.

Solution to Question 49: D

The correct answer is D. Review the IAM permissions for any role that allows for data access.

Explanation:

As a cloud security analyst, your main focus is on determining who has access to view data stored in your company's Google Cloud Project. IAM (Identity and Access Management) is the primary tool in Google Cloud for controlling access to resources. By reviewing the IAM permissions associated with various roles, you can gain insight into who has permissions to access data.

Option A is incorrect because instance metadata is a way for virtual machine (VM) instances to access information about themselves, such as instance-specific metadata or project-wide metadata. Reviewing instance metadata for suspicious

API calls would not provide you with information about who has access to view data stored in your company's Google Cloud Project.

Option B is incorrect because VPC Service Controls is a feature that allows you to define a security perimeter around your Google Cloud resources. While it can help prevent data exfiltration, it does not directly provide information about who has access to view data stored in your company's Google Cloud Project.

Option C is incorrect because Data Loss Prevention (DLP) focuses on discovering, classifying, and protecting sensitive data. Creating a DLP job can help you find and redact sensitive data in your storage systems but does not give you information on who has access to view data within your Google Cloud Project.

In conclusion, the best action to take in order to determine who has access to view data stored in your company's Google Cloud Project is to review the IAM permissions for any role that allows for data access (Option D).

Solution to Question 50: C

The most appropriate strategy for managing this resource is Option C: Enable node auto-provisioning on the GKE cluster.

Explanation: As an IT manager, your goal is to minimize cost while still providing the necessary resources to your team of data scientists. Your team occasionally needs access to Google Kubernetes Engine (GKE) cluster with GPUs, and their projects are long-running and non-restartable. Here's why Option C is the best choice and why other options will not work efficiently:

Option A: Creating a node pool with regular VMs and GPUs attached to those VMs can be more expensive and less flexible in comparison to node auto-provisioning. In this case, you would need to have GPU-enabled VMs running continuously to support the occasional demand from your data scientists, which increases the overall cost.

Option B: Manually adding and removing GPU-enabled instances can be time-consuming, error-prone, and less efficient. It requires constant monitoring and intervention from your side to ensure the resources are allocated and deallocated properly when required. This can lead to increased management overhead and potential delays in resource provisioning.

Option C (Correct Answer): Enabling node auto-provisioning in GKE allows the system to dynamically allocate and deallocate resources based on the actual workload requirements. This includes GPU-enabled nodes. By using this approach, you can ensure that your team gets the GPU resources they need when they need them, without wasting resources or incurring unnecessary costs. This approach aligns with the goal of cost minimization and efficient resource management.

Option D: Enabling Cluster Autoscaler on the existing GKE cluster without adding GPU-enabled VMs will not be sufficient because it does not fulfill the

requirement of providing GPU-enabled resources when needed. Cluster Autoscaler is useful for adjusting the number of nodes based on demand but it does not handle provisioning GPU-enabled nodes specifically.

Practice Exam 5

Question 1: As a software engineer managing a CI/CD pipeline for your company's application, you've encountered an issue where your CI/CD server can't execute Google Cloud actions in a specific project due to permission issues. In order to verify if the used service account has the appropriate roles in the specific project, what step should you take?

A. Check if the needed API is enabled for the specific project in the Google Cloud console.

B. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

C. Check the firewall settings in the VPC network configuration to ensure proper access.

D. Open the Google Cloud console, and run a query of the audit logs to find permission denied errors for this service account.

Question 2: As an IT professional working for a company in the finance industry, you are tasked with setting up IAM access audit logging in BigQuery to allow external auditors to access the necessary data while adhering to Google's recommended practices. How should you proceed?

A. Add the auditors group to the 'bigQuery.viewer' and 'logging.writer' predefined IAM roles.

B. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

C. Add the auditor user accounts to two new custom IAM roles.

D. Add the auditor user accounts to the 'bigQuery.user' and 'logging.writer' predefined IAM roles.

Question 3: As an IT administrator working for a multinational company, you have downloaded and installed the gcloud command line interface (CLI) and authenticated with your Google Account. The majority of your company's Compute Engine instances in your project run in the europe-west1-d zone. To efficiently manage these instances without specifying the zone with each CLI command, what should you do?

A. Create an environment variable named DEFAULT_ZONE with the value europe-west1-d.

B. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

C. Modify the gcloud CLI source code to include europe-west1-d as the default zone.

D. Create a text file named default_zone.txt containing europe-west1-d and place it in the .config folder of your user directory.

Question 4: As an IT specialist at a large pharmaceutical company, you manage their Google Cloud Platform project, which relies on BigQuery for data warehousing. The data science team at your company changes regularly and has a limited number of members. Your task is to enable the team members to conduct queries while adhering to Google's recommended practices. What actions should you take?

A. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery machineLearningAdmin user role to the group.

B. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery admin user role to the group.

C. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery jobUser role to the group.

D. 1. Create an IAM entry for each data scientist's user account. 2. Assign the BigQuery editor role to the group.

Question 5: You are an IT administrator at a growing company that relies on virtual machines for its business operations. You are tasked with finding a dynamic way to provision VMs on Google Compute Engine, ensuring that the exact specifications are outlined in a dedicated configuration file while adhering to Google's best practices. Which method should you employ?

A. Cloud Dataproc

B. Cloud SQL

C. Deployment Manager

D. Cloud Spanner

Question 6: During your tenure as a security manager at a leading tech company, you noticed several users with email addresses not associated with your company's domain in your Google Cloud resources. To ensure the security of your company's data, you want to remove these mismatched users and avoid auditing your resources repeatedly to identify such users. What approach should you take to achieve this?

A. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

B. Implement a Google Cloud Function that monitors projects for mismatched users and automatically removes them.

C. Configure a Pub/Sub topic to monitor resource sharing and notify you if a mismatched user is detected.

D. Enable Identity-Aware Proxy to limit access to your resources by domain.

Question 7: As a network administrator in a tech company, you are managing multiple virtual machines within a managed instance group with autoscaling enabled. The autoscaling policy is set to add more instances when the CPU utilization exceeds 80% and stops after reaching the maximum limit of five VMs or when the CPU utilization goes back to 80%. The initial delay for HTTP health checks is 30 seconds, and it takes around three minutes for the VM instances to be available for users. You notice that the instance group adds more instances than needed to handle the user traffic during autoscaling. What should you do to properly maintain instance group sizes while autoscaling?

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

B. Set the maximum number of instances to 1.

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

D. Increase the instance group's maximum limit to 10.

Question 8: As a Billing Administrator in a multinational e-commerce company, you are assigned the task to manage billing for new marketing initiatives across three existing Google Cloud projects. How can you ensure only the Marketing department is billed for their Google Cloud services?

A. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud account. 2. Create a budget for the Marketing department, but don't create a separate project or billing account.

B. 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account. 2. Create a billing report only for Marketing department's resources usage and send it to the accounting team.

C. 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account. 2. Create a new Google Cloud Project for the Marketing department. 3. Set the default key-value project labels to department:marketing for all services in this project.

D. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud Project for the Marketing department. 2. Link the new project to a Marketing Billing Account.

Question 9: As a software engineer working in a company that relies heavily on cloud infrastructure, you recently deployed an application on a single Compute Engine instance within the company's project. The application is designed to write logs to disk. However, users have now started reporting errors with the application and you need to diagnose the problem. What should be your next course of action?

A. Enable Stackdriver Trace to trace and analyze application logs.

B. Set up a load balancer and point it to the affected instance, then monitor the application logs.

C. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

D. Create a Google Cloud Function to process and analyze the application logs.

Question 10: As a Data Engineer in a tech company, you have a Dataproc cluster running in a single Virtual Private Cloud (VPC) network in a single subnet with range 172.16.20.128/25. However, there are no private IP addresses available in the VPC network. Your task is to add new VMs to communicate with your cluster using the minimum number of steps. How should you proceed?

A. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

B. Create a new GCP project with an additional VPC network and set up Shared VPC for the Dataproc cluster.

C. Use a Cloud Interconnect between the existing VPC network and a new VPC network for the VMs.

D. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

Question 11: You are working as a software developer at a startup company in the tech industry and are developing a new application for the company. The team requires a Jenkins installation for building and deploying the source code, and the goal is to automate the installation process as quickly and easily as possible. What is the most effective solution to achieve this?

A. Create an instance template with the Jenkins executable. Create a managed instance group with this template.

B. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application.

C. Deploy Jenkins through the Google Cloud Marketplace.

D. Use Cloud Build to create an instance of Jenkins and deploy the application.

Question 12: You are working as a network engineer at a global company that has an application receiving SSL-encrypted TCP traffic on port 443. The clients for this application are spread across the world, and your goal is to minimize latency for these clients. Which load balancing option would be most suitable in this scenario?

A. Backend Services Load Balancer

B. SSL Proxy Load Balancer

C. Cloud VPN Load Balancer

D. Network Load Balancer

Question 13: As a data engineer at a Boston-based company, you are tasked with configuring the optimal data storage solution for files stored in Cloud Storage for minimal cost, without compromising a mission-critical analytics pipeline that is used continuously. The users are all located in Boston, MA (United States). How should you proceed?

A. Configure regional storage for the region closest to the users. Configure a Nearline storage class.

B. Configure regional storage for the region closest to the users. Configure a Standard storage class.

C. Configure dual-regional storage for the region furthest from the users. Configure an Archive storage class.

D. Configure regional storage for a region furthest from the users. Configure a Standard storage class.

Question 14: You are working as a cloud engineer at a software development company. You've recently deployed an application on a Compute Engine instance for an ongoing project. A Linux expert, who is an external consultant, needs access to the Linux-based instance to perform some critical tasks. The consultant is connected to your company's corporate network through a VPN connection but does not have a Google account. What should you do to grant the consultant access?

A. Grant the external consultant Compute Engine Viewer role and have them use Google Cloud Console's SSH feature to access the instance.

B. Enable Cloud Identity-Aware Proxy for Compute Engine instances and provide the consultant with a client certificate.

C. Instruct the external consultant to generate an SSH key pair, and request the public key from the consultant. Add the public key to the instance yourself, and have the consultant access the instance through SSH with their private key.

D. Provide the consultant with your Google account credentials and have them access the instance using your account.

Question 15: You are a software engineer in a tech company, and your team is working with multiple microservices in a Kubernetes Engine cluster. One such microservice handles image rendering and demands a relatively high amount of CPU time with low memory requirement compared to others. The other microservices are designed to work best with n1-standard machine types. In order to optimize the cluster resources for maximum efficiency, what action should you take?

A. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

B. Increase the number of replicas for the image rendering microservice without changing machine types.

C. Enable autoscaling only for the image rendering microservice and keep the other microservices with static resource allocations.

D. Use preemptible VMs for the image rendering microservice and regular VMs for the other microservices.

Question 16: You are working in a software development company and have recently deployed a new version of your application on App Engine. After deployment, you discover a critical bug in the release and need to immediately revert to the prior version. What is the best course of action to achieve this?

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

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

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

D. Stop the current version on the App Engine page, then restart the previous version. Use gcloud app migrations command to revert to the previous version. On the App Engine Services page of the GCP Console, delete the faulty version and select the prior version to be live. Use gcloud app versions command to switch to the previous version of the application.

Question 17: Working at a software company, you need to securely share a Cloud Storage bucket object containing sensitive data with a client for collaboration. The client's company doesn't have a Google account, and you want to make sure their access expires after four hours. What is the most secure method with the fewest steps to achieve this?

A. Set object access to 'public', enable the temporary hold feature, and share the URL with the company. After four hours, release the temporary hold and delete the object.

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

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

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

passed.

Question 18: As an IT manager at a software development company, you are tasked with handling multiple applications running on different Compute Engine instances in the same project. Your goal is to have finer control over the service account each instance uses when calling Google Cloud APIs. How should you proceed?

A. When creating the instances, specify a Service Account for each instance.

B. Create a Shared VPC and connect each instance to it, then assign a Service Account to the Shared VPC.

C. When creating the instances, assign the name of each Service Account as instance metadata.

D. After starting the instances, use gcloud compute instances update to specify a Service Account for each instance.

Question 19: As a software engineer at a prominent tech company, you oversee a monthly batch process on an on-premises server, which takes approximately 30 hours to complete. This task can be performed offline, and must be restarted if interrupted. Your goal is to migrate this workload to the cloud while keeping costs to a minimum. What is the most suitable course of action?

A. Create an Instance Template with Preemptible VMs On. Create a Managed Instance Group from the template and adjust Target CPU Utilization. Migrate the workload.

B. Migrate the workload to Cloud SQL for batch processing.

C. Use App Engine standard environment to run the workload.

D. Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

Question 20: You are working at a media production company and have been tasked with migrating your on-premises data to Google Cloud. Your current data includes:

• 200 TB of video files in SAN storage • Data warehouse data stored on Amazon Redshift • 20 GB of PNG files stored on an S3 bucket

Your goal is to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud Storage bucket. The company wants you to follow Google-recommended practices and avoid writing any code for the migration. What course of action should you take?

A. Use Storage Transfer Service for the video files, Dataproc for the data warehouse data, and Storage Transfer Service for the PNG files.

B. Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

C. Use Dataproc for the video files, BigQuery Data Transfer Service for the data warehouse data, and Cloud Pub/Sub for the PNG files.

D. Use Cloud Data Fusion for the video files, Dataflow for the data warehouse data, and Storage Transfer Service for the PNG files.

Question 21: As a financial analyst at a tech company, you are tasked with analyzing Google Cloud Platform service costs from three separate projects within the firm. Your goal is to create service cost estimates by service type, daily and monthly, for the next six months using standard query syntax. How should you proceed?

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

B. Export your bill to a Compute Engine instance and analyze using a custom Python script.

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

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

Question 22: As an IT administrator at your company, you currently have all of your virtual machines operating in a subnet with a subnet mask of 255.255.255.240. The current subnet has reached its limit for IP addresses, but the company is expanding and now needs an extra 10 IP addresses for new VMs. It's crucial that the existing and new VMs can communicate without any additional routes. What is the most appropriate solution to address this issue?

A. Split the current subnet into two smaller subnets and distribute the VMs accordingly.

B. Create a new VPC network with a wider subnet range and migrate the VMs to the new network.

C. Use gcloud to expand the IP range of the current subnet.

D. Create a new subnet with the same starting IP but a wider range to overwrite the current subnet.

Question 23: As a software development company in the United States, you have multiple development teams each with their own Google Cloud project. You want to ensure that the teams can only create cloud resources within the US. How can you accomplish this?

A. Configure Cloud Monitoring to alert the organization if resources are created outside of the US. Set up manual deletion for those resources.

B. Use Cloud Functions to implement a custom IAM policy that checks and restricts resources to only the US regions for all dev projects.

C. Create a folder to contain all the dev projects and use an IAM policy to restrict the resources to US regions.

D. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations. Most Voted

Question 24: As a software developer in a tech company, you are using Container Registry to manage and store your organization's container images in a separate project. You need to create a Google Kubernetes Engine (GKE) cluster in a different project and ensure that Kubernetes can access and download images from the Container Registry. What would be the best action to take in this scenario?

A. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

B. Use Workload Identity Federation to provide access to the images stored in the Container Registry.

C. Enable Container Registry VPC Service Controls and create a perimeter around the project where the GKE cluster is being created.

D. Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account.

Question 25: As a project manager in a software development company, how would you grant access to an external auditor to view, but not modify, resources in a project where Domain Restricted Sharing is enabled?

A. Ask the auditor for their Google account, and give them the Viewer role on the project.

B. Create a temporary account for the auditor in Cloud Identity, and give that account the Editor role on the project.

C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

D. Ask the auditor for their Google account and give them the Security Admin role on the project.

Question 26: As an IT manager at a software development company, you oversee nightly batch workloads utilizing a substantial number of virtual machines (VMs). The workloads are fault-tolerant, and can withstand termination of some VMs. However, the current cost of VMs is becoming a concern. What should you do to reduce the cost while maintaining the efficiency of the workloads?

A. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

B. Run a test using Google Kubernetes Engine (GKE). If the test is successful, use Node Pools with N1 Standard VMs when running future jobs.

C. Run a test using Dataflow. If the test is successful, use N1 Standard VMs in the Dataflow pipeline when running future jobs.

D. Run a test using simulated maintenance events. If the test is successful, use N1 Standard VMs when running future jobs.

Question 27: As a data analyst working at a tech company, you are responsible for keeping track of sensitive information stored in three Cloud Storage buckets with data access logging enabled. You need to examine the activities of a specific user, verify the addition of metadata labels, and identify the files they viewed from those buckets using the fewest possible steps. How should you go about this task?

A. Create custom Google Cloud Functions to monitor the activities in real-time.

B. Using the GCP Console, filter the Activity log to view the information.

C. Create a trace in Stackdriver to view the information.

D. Enable and configure Google Cloud Armor to view the logs.

Question 28: You are working as a Cloud Engineer in a company that uses Google Cloud Platform. Your application is hosted in a managed instance group (MIG) on Google Cloud, and you have discovered errors in Cloud Logging for one VM, indicating that one of the processes is unresponsive. You want to quickly replace this problematic VM within the MIG. What action should you take?

A. Enable autoscaling for the MIG based on CPU utilization.

B. Use the gcloud compute instance-groups managed resize command to resize the MIG.

C. Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

D. Create a new instance template based on the current instance and migrate the MIG to use the new template.

Question 29: You are working as a data engineer in a finance company, and your latest project involves building a pipeline to manage and analyze time-series data for stock market transactions. Which combination of Google Cloud Platform services would be the most suitable to implement in your pipeline for processing and analyzing the data at different stages (boxes 1, 2, 3, and 4)?

A. Cloud Pub/Sub, Cloud Dataflow, Cloud Datastore, BigQuery

B. Cloud Pub/Sub, Cloud Dataflow, Cloud Spanner, Cloud Storage

C. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery

D. Cloud Pub/Sub, Cloud Dataflow, Firebase Realtime Database, Firestore

Question 30: You are working as a Cloud Storage Manager at a Software Development Company. Your company's application stores files on Cloud Storage utilizing the Standard Storage class, and it only requires access to files created within the last 30 days. In order to efficiently reduce costs on files that are no longer accessed by the application, what should you do?

A. Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

B. Create a BigQuery table to identify files older than 30 days and delete them using a scheduled query.

C. Use gsutil to set the lifecycle configuration on the bucket to delete files older than 30 days.

D. Set the storage class of the bucket to Nearline Storage and specify a 30-day minimum storage duration.

Question 31: As a cybersecurity specialist for a major financial institution, you are required to comply with the company's security vulnerability management policy. This policy mandates that a member of the security team has visibility into vulnerabilities and other OS metadata for a specific Compute Engine instance hosting a mission-critical application in your Google Cloud project. To effectively implement this policy, what should you do?

A. Enable the VPC Service Controls for the Google Cloud project.

B. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Create a log sink to BigQuery dataset. • Provide the security team member with access to this dataset.

C. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.vulnerabilityReportViewer permission.

D. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.inventoryViewer permission.

Question 32: As a leading construction equipment rental company in the industry, we equip all our rental machinery with multiple sensors that send event information every few seconds, such as engine status, distance traveled, and fuel level. Clients are billed according to the consumption data collected from these sensors. With a high expected throughput, reaching thousands of events per hour for each device, we need to ensure that we can retrieve consistent data based on the event's timing. Storing and retrieving individual signals must be atomic. What approach should our company take to efficiently handle this task?

A. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

B. Create a file in Google Sheets per device and append new data in it.

C. Store the sensor data in separate tables in BigQuery for each device.

D. Ingest the data into Datastore. Store data in an entity group based on the device.

Question 33: You are working as a DevOps engineer at a software company and you need to review the configured Kubernetes Engine cluster of an inactive configuration in your gcloud setup while using multiple configurations. To achieve this with the fewest possible steps, what should you do?

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

B. Use kubectl config get-contexts to review the output.

C. Use gcloud config configurations describe to review the output.

D. Use kubectl get nodes to review the output.

Question 34: As a network administrator in a global corporation, you are required to manage workloads running on both Compute Engine and on-premises systems. Your company's WAN is connected to the Google Cloud Virtual Private Cloud (VPC) via a Virtual Private Network (VPN). To deploy a new Compute Engine instance without allowing any public internet traffic to reach it, what action should you take?

A. Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

B. Create the instance with Private Google Access enabled.

C. Restrict the instance to only allow traffic from on-premises WAN IP addresses.

D. Create the instance without a public IP address.

Question 35: As a cloud engineer at a tech company, you have been assigned the task of monitoring resources distributed across multiple projects in the Google Cloud Platform. The goal is to consolidate reporting under a single Stackdriver Monitoring dashboard. What approach should you take?

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

B. Use a single Stackdriver account but create separate dashboards for each project and then merge the dashboards.

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

D. Configure Stackdriver in one project and use Google Cloud Functions to export monitoring data to the main project.

Question 36: You are a network administrator for a company that has adopted a hybrid cloud approach, with some applications deployed on Google Cloud and others on your on-premises network. To enable secure communication between these two environments, you have established a Virtual Private Network (VPN) tunnel between your Google Cloud Virtual Private Cloud (VPC) and your on-premises network. Several applications in the Google Cloud require access to a database server located on your on-premises network. You wish to avoid altering IP configurations in all applications whenever the database server's IP changes. What should you do?

A. Configure the IP of the database as custom metadata for each instance, and query the metadata server.

B. Utilize Google Cloud Endpoints to create an API proxy for your database and avoid changing the IP configuration in the applications.

C. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

D. Create an external Cloud DNS zone to ensure all applications can resolve the database's IP address.

Question 37: You work at a fast-growing tech company that utilizes Google Cloud for various projects. Your company has hired a dedicated person to create and manage all service accounts for these projects. To ensure they have the minimum required role, which one should you assign them?

A. Add the user to roles/iam.serviceAccountAdmin role.

B. Add the user to roles/iam.serviceAccountOperator role.

C. Add the user to roles/iam.serviceAccountAuditor role.

D. Add the user to roles/iam.serviceAccountUser role.

Question 38: As a cloud security specialist working in a reputable tech company, you have been entrusted with the responsibility of implementing an effective authentication method using your organization's single sign-on (SSO) identity provider that supports Security Assertion Markup Language (SAML) integration with service providers. The company has users in Cloud Identity. What should you do to enable users to authenticate through your company's SSO provider?

A. In Cloud Identity, set up SSO with Google as an identity provider to access GCP Native services.

B. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

C. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications.

D. Configure Cloud Identity-Aware Proxy to use your company's SSO provider for authentication.

Question 39: As a network engineer working for a company specializing in creating latency-sensitive websites, you've been tasked with setting up a single caching HTTP reverse proxy on Google Cloud Platform (GCP) for an upcoming project. The proxy requires minimal CPU usage, needs a 30-GB in-memory cache, and an additional 2 GB of memory for other processes. Your goal is to minimize costs while implementing this solution. How should you run this reverse proxy?

A. Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

B. Run it on Compute Engine with a custom instance type having 2 vCPUs and 40 GB of memory.

C. Deploy the reverse proxy on a Compute Engine instance with the instance type e2-highmem-16.

D. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

Question 40: You are working in a tech company as the organization and billing administrator. Your engineering team, who holds the Project Creator role in the organization, should not have the ability to link projects to the billing account. The finance team, however, should be able to link a project to a billing account without having the authority to make other changes to projects. What measure should you take to ensure this?

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

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

C. Give the finance team only the Compute Network User role on the organization.

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

Question 41: As a software engineer at a tech company, you are tasked with permanently deleting a Pub/Sub topic managed by Config Connector in your Google Cloud project. What is the appropriate action to take?

A. Use kubectl to delete the topic resource.

B. Use kubectl to rename the topic resource.

C. Use gcloud CLI to delete the topic.

D. Use Firebase CLI to delete the topic resource.

Question 42: As a software engineer at a tech company, you have been tasked with enabling your development team to deploy new features to an existing Cloud Run service in production. Your goal is to minimize the risk associated with a new revision and reduce the number of customers potentially affected by an outage, without introducing any development or operational costs to your customers. You've been advised to follow Google-recommended practices for managing revisions to a service. What strategy should you implement?

A. Enable Cloud Scheduler to perform periodic health checks on the new revision and reroute traffic to the old revision if issues are detected.

B. Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

C. Create a separate Cloud Run service with the new revision and manually manage the traffic between old and new services.

D. Deploy your application to a second Cloud Run service, and ask your customers to use the second Cloud Run service.

Question 43: You are working as a software developer for a company in the media industry, and you have created a code snippet to process the metadata of any new media files that are uploaded to the Cloud Storage bucket. To deploy this code snippet and ensure that it is automatically triggered for every new file, what should you do?

A. Use Cloud Dataproc and configure an ephemeral cluster to read the bucket's contents.

B. Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub.

C. Use Cloud IAP and create a notification channel to trigger the application.

D. Use Cloud Functions and configure the bucket as a trigger resource.

Question 44: As an IT professional responsible for cloud security at a rapidly growing tech firm, you've been tasked with gaining better insight into the company's Google Cloud environment following a recent security breach. Specifically, you need to monitor unexpected firewall changes and instance creation, while adhering to the company's preference for simple solutions. What approach should you take?

A. Deploy a custom intrusion detection system (IDS) on a compute instance and configure it to monitor changes in firewall rules and instances using Cloud Pub/Sub to communicate the events.

B. Create custom monitoring dashboards using Grafana and integrate them with Google Cloud Monitor to visualize the changes in firewall and instance actions.

C. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

D. Create a log sink to forward Cloud Audit Logs filtered for firewalls and compute instances to Cloud Storage. Use BigQuery to periodically analyze log events in the storage bucket.

Question 45: As a project manager in the tech industry, you've noticed that several team members have been using their personal credit cards to pay for Cloud Platform projects, which are then reimbursed by the company. To increase efficiency and centralize all project expenses, the company plans to create a single billing account for these projects. What is the appropriate course of action to achieve this?

A. In the Google Cloud Platform Console, go to Billing and merge all individual employee accounts into a single corporate account.

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

C. Create a Google Group for your company, and invite all employees to join. Use this group to combine all billing accounts.

D. Ask each employee to create their own billing account with the company credit card and link their projects to that account.

Question 46: As an IT manager at a software development company, you oversee multiple teams working on distinct projects, all of which utilize numerous Google Cloud services centralized within a single project. The DevOps team specifically requires access to all production services to execute their tasks effectively. To avoid potential security risks from future alterations in Google Cloud products and adhere to Google-recommended practices, what strategy should you implement?

A. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

B. Create a custom role with Compute Admin permissions and grant all members of the DevOps team the custom role on the production project.

C. Create a custom role that combines the required permissions, but grant the DevOps team the Project Viewer role on the production project.

D. Grant the DevOps team the role of Project Editor on the test and development projects.

Question 47: As a data recovery specialist working for a leading tech company, you have been tasked with storing application backup files for disaster recovery purposes using Google Cloud Storage. To adhere to Google's recommended practices, which storage option should you choose?

A. Coldline Storage

B. Uniform Bucket-Level Access

C. Archive Storage

D. Firebase Realtime Database

Question 48: As a project manager in a software development company, you have been assigned to estimate the total cost of cloud infrastructure for running a three-tier web application on Google Cloud instances and Cloud SQL. The application will be hosted on virtual machines using a MySQL database. How can you accurately calculate the required costs?

A. Create a Google spreadsheet with multiple Google Cloud resource combinations. On a separate sheet, import the current Google Cloud prices and use these prices for the calculations within formulas.

B. Contact Google Cloud Support to get an estimate without providing any details about your web application or infrastructure requirements.

C. Use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource you expect to use. Use similar size instances for the web server, and use your current on-premises machines as a comparison for Cloud SQL.

D. Look for a pre-existing pricing structure of a similar 3-tier web application on Google Cloud Platform Forums, and adapt this structure to your own use case.

Question 49: You are working as a data analyst at a tech company and are using Looker Studio to visualize a table from your data warehouse built on top of BigQuery. During the day, data is appended to the data warehouse, and at night, the daily summary is recalculated by overwriting the table. Recently, you have discovered that the charts in Looker Studio are broken, and you need to analyze the issue. What steps should you take to resolve the problem?

A. Contact the Looker Studio support team for assistance in resolving the issue.

B. Verify Cloud Dataflow pipeline for any data ingesting issues in the Google Cloud platform.

C. In Cloud Logging, create a filter for your Looker Studio report.

D. Use the BigQuery interface to review the nightly job and look for any errors.

Question 50: As a network engineer at a growing tech company, you are asked to design a custom VPC with a single subnet for the organization. To accommodate future expansion, the subnet range must be as large as possible. Which range should you choose for the subnet?

A. 10.0.0.0/8

B. 169.254.0.0/16

C. 192.168.1.0/24

D. 192.168.0.0/16

Practice Exam 5 Solutions

Solution to Question 1: B

The correct answer is B. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

Explanation:

The issue in the question is related to permissions, specifically the roles assigned to the service account being used in your CI/CD pipeline. To resolve this, you should check the IAM roles for the service account in question, ensuring that it has the necessary permissions to execute the required Google Cloud actions.

Option A is incorrect because it suggests checking if the required API is enabled for the specific project. While enabled APIs are important for the functioning of the application, it is not directly related to the permissions of the service account, which is the core issue in this scenario.

Option C is incorrect because it suggests checking the firewall settings in the VPC network configuration. Although firewall settings can impact network connectivity and access, they are not directly related to the permissions issue specified in this scenario. The problem is with the roles assigned to the service account, not network access.

Option D is incorrect because it suggests running a query on the audit logs to find permission denied errors for the service account. While audit logs can provide valuable information about the activities and errors generated by service accounts, it is not the most efficient method to check for IAM roles assigned to the service account. The direct approach is to check the IAM roles in the Google Cloud console, as specified in option B.

Solution to Question 2: B

The correct answer is B. You should add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

Here's why the other options will not work:

Option A: Adding them to the 'bigQuery.viewer' and 'logging.writer' predefined IAM roles wouldn't be appropriate because the 'logging.writer' role will give them permission to write logging data, which is not required for an auditor. It's important to follow the principle of least privilege, in which you should only grant the minimum set of permissions necessary to perform their job.

Option C: Creating two new custom IAM roles might sound like a personalized solution, but it isn't recommended best practice. Using predefined IAM roles ensures that you are granting the required and standardized permissions for specific tasks. Custom roles might lead to an overly complex and difficult-to-manage access system that can increase the risk of misconfigurations and

unauthorized access.

Option D: Adding the auditor user accounts to the 'bigQuery.user' and 'logging.writer' predefined IAM roles would again give unnecessary permissions to the auditors. As mentioned earlier, the 'logging.writer' role would grant write permissions, and the 'bigQuery.user' role would allow them to run jobs and manage their own data. This doesn't adhere to the principle of least privilege as it grants more permissions than needed for an auditor.

In conclusion, Option B is the best solution, as it ensures that auditors have enough access to view log data and BigQuery datasets without giving them excessive permissions that could compromise security and compliance with Google's recommended practices.

Solution to Question 3: B

The correct answer is B: Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

Explanation: The gcloud CLI allows you to set configuration properties that persist across sessions, making it easier to manage resources and settings. By setting the default zone using the gcloud config subcommand, you ensure that the CLI automatically targets the europe-west1-d zone for any command that requires a zone, allowing you to manage instances in that zone efficiently. You can do this by running:

```
gcloud config set compute/zone europe-west1-d
```

Why other options will not work:

A. Creating an environment variable named DEFAULT_ZONE with the value europe-west1-d would not work because the gcloud CLI does not look for environment variables with this name. It relies on its own internal configuration settings.

C. Modifying the gcloud CLI source code to include europe-west1-d as the default zone is not recommended. It would make it difficult to manage software updates and maintain support from Google. Additionally, it would not persist across devices or users and could lead to inconsistencies in your team's workflow.

D. Creating a text file named default_zone.txt containing europe-west1-d and placing it in the .config folder of your user directory would not work, as the gcloud CLI does not look for or parse such a file for configuration. It uses its own internal configuration management through the gcloud config subcommand.

Solution to Question 4: C

The correct answer is C. Here's why:

Option A: Assigning the BigQuery machineLearningAdmin user role to the group is not the best choice. This role is specifically designed for managing

Machine Learning models and resources within BigQuery, rather than conducting general queries. Since the task is to enable the data science team to conduct queries, this is not the appropriate role.

Option B: Assigning the BigQuery admin user role is not recommended because it grants extensive permissions, including the ability to create, delete, and update datasets, tables, and views. This can be risky, as a small error by one team member may lead to the loss of critical data. Google's recommended practices suggest granting the minimum necessary level of access.

Option C: This option is the best choice because it adheres to Google's recommended practices. By creating a dedicated Google group in Cloud Identity and adding each data scientist's user account to the group, you make it easy to manage access for a constantly changing team. Assigning the BigQuery jobUser role gives them the ability to run queries (and only that) – fulfilling the task requirements and adhering to the principle of least privilege.

Option D: This option is not ideal because it suggests creating an IAM entry for each data scientist's user account instead of using a Google group. This can make it difficult to manage access when the team changes regularly. Furthermore, it suggests assigning the BigQuery editor role, which gives more extensive permissions than necessary for simply conducting queries, consequently going against the principle of least privilege.

Solution to Question 5: C

The correct answer is C. Deployment Manager.

Explanation:

Option A: Cloud Dataproc is not the right answer because it is a managed Apache Hadoop and Apache Spark service. It is used for big data processing and does not cater to the provisioning of virtual machines on Google Compute Engine.

Option B: Cloud SQL is also not the right choice because it is a fully-managed relational database service that offers various SQL databases like MySQL, PostgreSQL, etc. It does not handle provisioning of VMs in Google Compute Engine.

Option C: Deployment Manager is the best choice for this requirement. Deployment Manager is an Infrastructure as Code (IaC) tool provided by Google Cloud Platform. It allows you to automate the provisioning of VMs on Google Compute Engine and create dedicated configuration files that adhere to Google's best practices. It enables you to manage your infrastructure with version control, templating, and modularity, providing a dynamic way to create, manage, and maintain virtual machines in Google Compute Engine.

Option D: Cloud Spanner is not the correct answer because it is a fully managed, horizontally scalable, multi-versioned, and globally distributed relational database service. It is not designed for provisioning or managing VMs on Google Compute Engine.

So, the answer should be C. Deployment Manager, as it helps you to dynamically provision and manage VMs on Google Compute Engine with the exact specifications outlined in dedicated configuration files while adhering to Google's best practices.

Solution to Question 6: A

The correct approach would be option A: Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users. This option will help you enforce a domain-based identity constraint at the organizational level, making sure that only users with your company's domain email addresses can access the resources. Moreover, it will help you avoid auditing the resources repeatedly for mismatched users. Once the policy has been set, you can then remove any existing mismatched users from your resources.

Option B: Implementing a Google Cloud Function that monitors projects for mismatched users and automatically removes them is not the best solution because it requires additional maintenance and complexity. It would help if you also periodically checked and updated these functions to make sure they align with any changes in the role management.

Option C: Configuring a Pub/Sub topic to monitor resource sharing and notify you if a mismatched user is detected only provides you with a notification but does not prevent mismatched users from accessing your resources by default. This approach would still require manual efforts to remove the mismatched users and is not proactive in preventing unauthorized access.

Option D: Enabling Identity-Aware Proxy (IAP) helps you limit access to your application but does not inherently prevent mismatched users from being granted access to your Google Cloud resources. It focuses more on app-level access control and user authentication, which is not the primary goal in this scenario.

Solution to Question 7: C

The correct answer is C. Increase the initial delay of the HTTP health check to 200 seconds.

Explanation:

C. Increasing the initial delay of the HTTP health check to 200 seconds allows more time for the VM instances to become available. Since it takes around three minutes for the VM instances to be available for users, the 30-second initial delay is not enough time. By increasing the delay, it will prevent the autoscaling policy from assuming that the instances are unhealthy and create unnecessary additional instances. This way, the instance group properly maintains its size while autoscaling.

A. Using a TCP health check instead of an HTTP health check will not address the issue of autoscaling creating too many instances. Health checks are necessary

for determining the health of the instances, but changing the type of health check does not impact the time it takes for the instances to become available.

B. Setting the maximum number of instances to 1 would limit the ability of the autoscaling policy to properly scale the instances according to the actual demand. This would undermine the purpose of autoscaling; possibly leading to insufficient resources to handle the user traffic.

D. Increasing the instance group's maximum limit to 10 does not solve the problem of having more instances than needed, but instead, it increases potential excess VMs. The issue is with the time it takes for instances to become available, not the maximum limit. Increasing the limit might put additional unnecessary resources and cost to the company.

Solution to Question 8: D

The correct answer is D, and here's why:

Option D ensures that the Marketing department is billed separately for their Google Cloud services by exclusively linking their project to an individual Marketing Billing Account. As a Billing Administrator, you can manage and monitor costs effectively, allowing transparency and chargeback mechanisms for the Marketing department.

Option A is incorrect because simply creating a budget does not actually change the underlying billing relationship or allocation for the Marketing department. It does not facilitate transparency and proper cost allocation since there is no separate project or billing account maintained for the Marketing department.

Option B does not address the main task of managing billing, as it only provides reports on resource usage. It does not ensure that the Marketing department is being billed separately. Additionally, being assigned the Organization Administrator IAM role is not enough for managing billing, as it doesn't provide the necessary permissions to work with billing accounts.

Option C is incorrect because, while it does create a new project for the Marketing department, it does not address the crucial step of linking the project to a separate billing account. The default key-value project labels can help organize resources, but this is not enough to segregate costs or to ensure only the Marketing department is billed for their Google Cloud services.

In conclusion, the best way to ensure that only the Marketing department is billed for their Google Cloud services is to appropriately link their project to a dedicated Marketing Billing Account, as described in option D.

Solution to Question 9: C

The correct answer is C. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

Explanation: The application is designed to write logs to disk, and users are reporting errors. To diagnose the problem, you need to have access to these

logs. Cloud Logging Agent will help to collect and stream the logs to Google Cloud's Operations suite (formerly Stackdriver Logging) so that you can view and analyze them. By doing this, you can quickly identify the issues affecting the application and resolve them.

Here's why other options won't work:

A. Enable Stackdriver Trace to trace and analyze application logs. Stackdriver Trace is more suitable for tracing and analyzing latency data in distributed applications, not for analyzing application logs. It wouldn't be helpful in this scenario where you need to check the logs stored on the disk.

B. Set up a load balancer and point it to the affected instance, then monitor the application logs. Setting up a load balancer would help you distribute the incoming traffic among multiple instances. However, it doesn't directly solve the problem of accessing and analyzing the application logs. It might not even be necessary if the issues are specific to the application's code or configuration.

D. Create a Google Cloud Function to process and analyze the application logs. Google Cloud Functions are used for serverless computing, allowing you to run standalone functions in response to events without having to manage any underlying infrastructure. While you could potentially create a Cloud Function to process and analyze the logs, it would be a more complex and less efficient solution compared to using Cloud Logging to collect and analyze the logs directly. Cloud Logging is designed specifically for managing and analyzing logs, making it the most suitable tool in this scenario.

Solution to Question 10: D

The correct answer is D, and here's why:

D. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

This is the correct approach because creating a new VPC network for the VMs provides them with separate private IP address space, ensuring they can be provisioned. Enabling VPC Peering allows both networks to communicate efficiently without any additional steps, ensuring direct network connectivity while minimizing latency.

Now, let's discuss why the other options are incorrect:

A. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

While this option does create a new VPC network for VMs and enables VPC Peering, configuring a custom Route exchange is an unnecessary step when VPC Peering already provides direct network connectivity. So, this option requires more steps than D.

B. Create a new GCP project with an additional VPC network and set up Shared VPC for the Dataproc cluster.

Creating a new GCP project is not necessary when creating a new VPC network and enabling VPC Peering (option D) would provide the solution required. Shared VPC is a more complicated option that requires multiple steps, making this option less efficient than D.

C. Use a Cloud Interconnect between the existing VPC network and a new VPC network for the VMs.

Cloud Interconnect is mainly used for connecting on-premises networks to Google Cloud VPC networks, requiring more steps and complexity that is not needed for this scenario. VPC Peering (option D) is a more direct and efficient way of connecting two VPC networks, reducing latency and resource usage.

Solution to Question 11: C

The most effective solution to achieve the automation of Jenkins installation for building and deploying the source code is option C: Deploy Jenkins through the Google Cloud Marketplace.

Explanation:

Option C: Deploying Jenkins through the Google Cloud Marketplace allows you to quickly and easily set up Jenkins in your environment with a few clicks. It provides you with an automated and pre-configured installation with support for deploying on Google Cloud infrastructure. The Google Cloud Marketplace ensures you have the latest version of Jenkins and automatically handles the required dependencies and configurations. This method is both efficient and time-saving for your team since it leverages Google Cloud Platform's automation capabilities.

Option A: Creating an instance template with the Jenkins executable and a managed instance group is not the most effective solution. Although it can automate the deployment of Jenkins for a group of instances, it adds extra steps to configure, manage and maintain the managed instance groups and instance templates. This approach may also require manual updates and modifications when new versions of Jenkins are released.

Option B: Using a Cloud Storage bucket for storing the Jenkins executable and deploying the application is not an efficient method. This option requires you to manually manage and configure the Jenkins installation, set up the necessary dependencies, and keep the Jenkins version up-to-date. Additionally, deploying the actual application may require further scripting and setup that are not automatically taken care of in this option.

Option D: Cloud Build is a service mainly used for building and testing applications in various languages and platforms, not particularly tailored for Jenkins installation. While it is possible to configure Cloud Build for setting up a Jenkins

instance, this option can be time-consuming and involve more manual configuration compared to deploying Jenkins through the Google Cloud Marketplace.

In conclusion, deploying Jenkins through the Google Cloud Marketplace (Option C) is the most effective way to automate the installation process as quickly and easily as possible in a software development environment.

Solution to Question 12: B

The correct answer is B. SSL Proxy Load Balancer, and here's the explanation for why it's the most suitable option for this scenario and why other options will not work:

B. SSL Proxy Load Balancer: The SSL Proxy Load Balancer is designed to handle SSL traffic, which means it can efficiently decrypt and process incoming traffic on port 443. It employs the use of SSL termination to manage SSL connections, which reduces the latency for clients connecting globally. This makes it the ideal choice for a global company with an application receiving SSL-encrypted TCP traffic on port 443, and clients spread across the world.

A. Backend Services Load Balancer: Backend Services Load Balancer is a regional-based load balancing option that distributes traffic between backend instances within a particular region. While it can support SSL-encrypted TCP traffic, it is not the best choice for a global company with clients across the world because it lacks the global edge network required to minimize latency for distributed clients.

C. Cloud VPN Load Balancer: Cloud VPN Load Balancer is not a suitable option in this scenario because it is designed for site-to-site VPN connections. It's intended to be used for secure communication between two virtual private networks and does not focus on SSL-encrypted TCP traffic or reducing latency for global clients accessing an application.

D. Network Load Balancer: Network Load Balancer is a regional-based load balancer designed to handle large volumes of TCP and UDP traffic. Although it can handle high volumes of traffic, it does not provide SSL termination or the global edge network needed to minimize latency for clients distributed across the world. It would require additional setup to handle SSL-encrypted traffic, which could potentially increase latency. Therefore, it is not the best option for this scenario.

In conclusion, SSL Proxy Load Balancer is the most suitable load balancing option for a global company with an application receiving SSL-encrypted TCP traffic on port 443 and clients spread across the world. It is specifically designed to handle SSL traffic, reduce latency and provide a global edge network to enhance user experience.

Solution to Question 13: B

The correct answer is B: Configure regional storage for the region closest to the users. Configure a Standard storage class.

Here's why answer B is the best choice:

1. Regional storage location: Since all users are located in Boston, MA (United States), it makes sense to choose the closest regional storage available. This will ensure lower latency and faster access to the data when it is needed for their mission-critical analytics pipeline, which cannot afford to be compromised.
2. Standard storage class: Standard storage class provides a balance between storage price and features suitable for active workloads like a mission-critical analytics pipeline. It offers low-latency access and high performance, ensuring that users can access the data quickly and continuously without any delay.

Why other options will not work:

A: Configure regional storage for the region closest to the users. Configure a Nearline storage class.

This option would provide a regional storage location close to the users but using the Nearline storage class might not be suitable for the mission-critical analytics pipeline as it is designed for infrequently accessed data. Low-latency access and high performance may not be guaranteed, which can compromise the analytics pipeline.

C: Configure dual-regional storage for the region furthest from the users. Configure an Archive storage class.

This option would configure a dual-regional storage location far away from the users, resulting in higher latency and slower access to the data. Additionally, the Archive storage class is meant for long-term storage of data that is rarely accessed, which is not suitable for mission-critical analytics pipeline, leading to an unacceptable performance impact.

D: Configure regional storage for a region furthest from the users. Configure a Standard storage class.

This option would configure a regional storage location far away from the users, resulting in higher latency and slower access to the data. Although the Standard storage class provides adequate performance, the increased latency due to the regional storage location can compromise the mission-critical analytics pipeline.

Solution to Question 14: C

The correct answer is C. Here's why:

A. Grant the external consultant Compute Engine Viewer role and have them use Google Cloud Console's SSH feature to access the instance.

This option is not suitable because the external consultant does not have a Google account. Granting the Compute Engine Viewer role would require a Google account, and even if the consultant had an account, the viewer role only

provides read-only access, not the necessary access to perform critical tasks on the instance.

B. Enable Cloud Identity-Aware Proxy for Compute Engine instances and provide the consultant with a client certificate.

This option is not appropriate because Cloud Identity-Aware Proxy is designed for controlling access to web-based applications, not SSH access to Compute Engine instances. Additionally, this method would still require a Google account for the consultant.

C. Instruct the external consultant to generate an SSH key pair, and request the public key from the consultant. Add the public key to the instance yourself, and have the consultant access the instance through SSH with their private key.

This is the correct approach because it allows you to grant the consultant access to the Compute Engine instance without requiring a Google account. The consultant generates an SSH key pair, shares the public key with you, and you add it to the instance. The consultant can then use their private key to securely connect to the instance through SSH.

D. Provide the consultant with your Google account credentials and have them access the instance using your account.

This option is highly insecure and against best practices, as it would give the consultant full access to your Google account and all your projects. Sharing credentials is never recommended and could lead to security breaches and unauthorized access to your company's sensitive data.

Solution to Question 15: A

The correct answer is A. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Explanation for why Option A is the correct answer: The image rendering microservice demands a high amount of CPU time with a low memory requirement. Compute-optimized machine types are designed for such workloads, as they offer superior performance per core while keeping the memory usage to a minimum. By creating a separate node pool for this microservice with compute-optimized machine type nodes, the resource allocation is better suited to handle its needs, thus leading to maximum efficiency in operation. By keeping the rest of the microservices in node pools with general-purpose machine type nodes, their resource requirements are also optimally addressed.

Reasons why other options are not correct:

Option B: Increasing the number of replicas for the image rendering microservice without any changes to the machine types will not optimize the cluster resources. Scaling out may distribute the workload but does not address the

specific requirements of a microservice that demands high CPU time and low memory.

Option C: Enabling autoscaling only for the image rendering microservice can cause unnecessary scaling activities without a proper resource allocation system in place. Without addressing the different hardware requirements of each microservice, autoscaling alone does not achieve maximum efficiency within the cluster.

Option D: Using preemptible VMs for the image rendering microservice may marginally lower costs but does not optimize the cluster resources for maximum efficiency. Preemptible VMs can be terminated at any time by the provider. The microservices with different resource requirements must be assigned to different machine types to ensure the efficient allocation of resources within the cluster, without compromising the computation speed and reliability.

Solution to Question 16: B

The best course of action in this scenario is option B, which involves going to the App Engine Versions page in the Google Cloud Platform (GCP) Console and routing 100% of the traffic to the previous version. This approach allows for immediate reversion to the prior version without any downtime for users, and it caters to a swift and seamless rollback from the buggy release.

Option A is not advisable because deploying the original version as a separate application introduces unnecessary complexity and could increase costs. Additionally, splitting traffic between applications may not fully address the issue, as traffic routing between applications is not the same as rolling back a version within the same application.

Option C is incorrect because there is no "Revert" button or option on the App Engine page of the GCP Console.

Option D is not optimal, as stopping and restarting versions may lead to potential downtime for users, defeating the purpose of a seamless reversal.

Using the gcloud app migrations command or gcloud app versions command is not the correct solution, as these commands are not designed for reverting versions of an application. The "migrations" command is used for migrating traffic, and the "versions" command is used for managing application deployments. Neither will provide the desired rollback function.

Finally, deleting the faulty version on the App Engine Services page and selecting the prior version to be live is not a good solution, as this will result in a complete loss of the buggy version. It is often useful to have that version accessible for analysis, debugging, and understanding its shortcomings.

In summary, the best course of action is to use option B – routing 100% of the traffic to the previous version through the App Engine Versions page – as this allows for a seamless, immediate reversion to the prior version of the application without downtime or additional costs.

Solution to Question 17: C

The correct answer is C, creating a signed URL with a four-hour expiration and sharing the URL with the company.

A signed URL is the best method because it offers a secure, temporary link to the object in the Cloud Storage bucket that can be accessed without needing a Google account. By setting a four-hour expiration, access to the object will be automatically revoked after the designated time, ensuring security and eliminating extra steps for manual handling.

Option A is not secure because setting object access to 'public' would expose the file to anyone with the URL, and there is a chance of unauthorized access during the four hours it holds. Furthermore, the temporary hold feature is used to protect objects from accidental deletion rather than controlling access.

Option B is also incorrect because setting object access to 'public' poses a risk of unauthorized access. Additionally, using object lifecycle management to remove the object after four hours doesn't immediately revoke access once the four-hour threshold has passed. The object could still be accessed until the lifecycle action takes effect, which may not be exactly after four hours.

Option D is not the best option, as creating an entirely new Cloud Storage bucket and copying the object increases complexity and raises the cost in terms of both storage and egress fees. Additionally, deleting the entire bucket after four hours is not the most efficient way to revoke access to the sensitive data.

Solution to Question 18: A

The answer should be A: When creating the instances, specify a Service Account for each instance.

Explanation: In Google Cloud Platform, Compute Engine instances use service accounts to authenticate API requests. By assigning a specific service account to each instance when creating it, you can ensure appropriate permissions and finer control over which API resources are accessed by each instance.

Reasons why other options will not work:

B.Option B: Create a Shared VPC and connect each instance to it, then assign a Service Account to the Shared VPC. This option is incorrect because a Shared VPC allows you to share network resources across multiple projects, but doesn't provide fine-grained control over service accounts used by Compute Engine instances. Service accounts need to be assigned on a per-instance basis to achieve the desired control.

C.Option C: When creating the instances, assign the name of each Service Account as instance metadata. This option is incorrect because simply assigning the service account name as metadata will not create a valid association between the instance and the service account. It is important to explicitly specify the desired service account during the instance creation process.

D.Option D: After starting the instances, use gcloud compute instances update to specify a Service Account for each instance. This option is incorrect because you cannot change the service account of a running Compute Engine instance. You need to specify the service account during the instance creation process. If you need to change the service account after the instance has been created, you would need to recreate the instance with the desired service account.

Solution to Question 19: D

The most suitable course of action in this case is option D, which involves migrating the workload to a Compute Engine VM and starting and stopping the instance as needed. This approach provides a few key benefits that make it the best choice:

1. Cost Efficiency: By starting and stopping the VM instance when needed, you can optimize costs and only pay for compute resources when the batch process is running. This is especially important when dealing with a lengthy process like the one in question, which takes about 30 hours to complete.
2. Robustness: Compute Engine VM instances are known for their reliability and performance, making them a suitable choice for a 30-hour long workload. This ensures that the process continues uninterrupted and can be restarted if needed.
3. Control and Flexibility: With a Compute Engine VM, you have full control over the software, hardware, and network configurations, providing the flexibility to effectively accommodate the workload's requirements. This allows you to optimize the environment for the batch process.

Now, let's discuss why the other options are not ideal:

A. Preemptible VMs have a maximum lifetime of 24 hours, which is insufficient for the 30-hour batch process. If the process is interrupted, it must be restarted, which would lead to increased processing times and potential data inconsistencies.

B. Cloud SQL is generally used for online transaction processing (OLTP), not batch processing. It is optimized for intensive short-lived tasks and is not suitable for this type of workload.

C. App Engine standard environment is designed for web applications that have rapid scaling requirements. It does not provide the level of control and customization that would be needed for this kind of long-running batch process, nor does it guarantee the flexibility to handle the workload without interruptions.

Solution to Question 20: B

The correct answer is B. Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for

the PNG files. Here's why:

A. Using Storage Transfer Service for the video files is not ideal because it is designed for transferring data from external sources like Amazon S3, HTTP/HTTPS, or another Google Cloud Storage bucket. Since the video files are in SAN storage, Transfer Appliance is better suited for large on-premises data transfers. Dataproc is intended for distributed big data processing, which is not relevant for the data migration tasks described.

B. This answer follows Google-recommended practices and requires no code writing. Transfer Appliance is designed for bulk data migration from on-premises data centers to Google Cloud Storage. BigQuery Data Transfer Service is specifically intended to transfer data from external data warehouses, like Amazon Redshift, into BigQuery. Storage Transfer Service is the correct choice for transferring PNG files from an Amazon S3 bucket to Google Cloud Storage.

C. Dataproc is not suitable for transferring video files, as it is meant for distributed data processing, not migration. Cloud Pub/Sub is inappropriate for the PNG files, as it is designed for messaging and event streams, not data storage or file transfer.

D. Cloud Data Fusion is an ETL (Extract, Transform, Load) service, and Dataflow is a data processing service, both of which are unnecessary for the migration tasks described. These services would introduce complexity and require code writing, which was a criterion to avoid.

Therefore, option B is the correct choice, as it follows Google-recommended practices, leverages the appropriate services, and does not require writing any code.

Solution to Question 21: A

The correct answer should be A, which is to "Export your bill to a BigQuery dataset, and then write time window-based SQL queries for analysis."

The reason for this is that BigQuery is a fully-managed, serverless data warehouse solution by Google Cloud Platform, specifically designed for large scale data analytics. Its powerful SQL querying capabilities enable you to analyze huge amounts of data efficiently and quickly, which is essential for a financial analyst's job. By exporting the billing information to a BigQuery dataset, you can take advantage of these features and write time window-based SQL queries to compute daily and monthly service cost estimates by service type for the next six months.

Option B, "Export your bill to a Compute Engine instance and analyze using a custom Python script," this is less ideal compared to using BigQuery. Compute Engine instance is more suited for running virtual machines and custom applications, not specifically designed for data analysis tasks. Moreover, writing a custom python script might consume valuable time and resources when compared to utilizing BigQuery's querying capabilities. While it is possible to

analyze and make projections using this approach, it's not the most effective or efficient way.

Option C, "Export your bill to a Cloud Storage bucket, and then import into Cloud Bigtable for analysis," will not be suitable for this use case. Cloud Bigtable is a NoSQL database designed for low-latency, high-throughput read and write operations. Although it's great for large-scale operational data, it is not an appropriate choice for analytical tasks like computing cost estimates. Moreover, its querying capabilities are primarily suited for key-value lookups and not complex analytical queries that you would require for this task.

Option D, "Export your bill to a Cloud Storage bucket, and then import into Google Sheets for analysis," this approach may work for small-scale data analysis tasks, but it's not the most suitable choice for large-scale data analytics and creating complex, time-based projections. Google Sheets has certain limitations in terms of the maximum number of rows per sheet, real-time collaboration, and the complexity of the formulae that can be used. It is more suitable for less complex and smaller datasets than the multiple projects data you would be dealing with in this scenario.

In conclusion, option A is the most effective way for a financial analyst at a tech company to analyze Google Cloud Platform service costs and create service cost estimates by service type, daily and monthly, for the next six months using standard query syntax.

Solution to Question 22: C

The most appropriate solution to address this issue is option C: Use gcloud to expand the IP range of the current subnet.

Explanation: Option C allows you to increase the available IP addresses within the existing subnet without impacting your current VMs' connectivity or requiring additional routes. This is because expanding the IP range of the current subnet will enable the existing and new VMs to communicate seamlessly within the same network.

Option A: Splitting the current subnet into two smaller subnets and distributing the VMs accordingly is not an ideal solution because it increases network complexity and may require additional routing configuration to allow VMs across the subnets to communicate with each other.

Option B: Creating a new VPC network with a wider subnet range and migrating the VMs to the new network is an unnecessary approach since it involves moving the VMs to a different VPC network and incurring their downtime. Moreover, this process might require re-configuring firewall rules, network settings, and communication paths.

Option D: Creating a new subnet with the same starting IP but a wider range to overwrite the current subnet is not a feasible solution. Overwriting the existing subnet can cause a brief outage to the VMs as they lose their network

connectivity, and it could lead to incorrect IP assignments or misconfiguration, affecting the entire system.

Therefore, option C is the most appropriate solution because it allows expanding the IP range without any impact on the existing VMs' connectivity, ensuring seamless communication and meeting the company's requirements.

Solution to Question 23: D

The correct answer is D because it achieves the goal of ensuring that development teams can only create cloud resources within the US by utilizing an organization policy with location restriction.

Option D allows you to create a folder to group all the development projects, which simplifies management, and apply an organization policy to limit resources in US locations. With an organization policy, you can enforce a location policy for all projects within the folder, ensuring that resources are created only in the desired locations. This approach effectively restricts the creation of cloud resources to the US locations compliantly and at scale.

Option A is inadequate because it only takes action after resources have already been created in non-US locations. The goal is to prevent the creation of resources outside of the US, whereas this option merely alerts and requires manual deletion. This method is reactive, time-consuming, and may lead to errors due to its manual nature.

Option B is not a suitable solution because Cloud Functions are not meant to implement custom IAM policies. Cloud Functions is a service that automatically runs code in response to events, whereas IAM policies manage access to resources. This proposal does not fulfill the goal of preventing resources from being created outside the US locations.

Option C can group all the dev projects in a folder but fails to effectively restrict the resources to US regions. Applying an IAM policy is not the right approach for resource location restriction, as IAM policies are used for access control and permissions. Organization policies, not IAM policies, should be used for location restrictions.

In summary, option D is the best solution because it employs organization policy with location restriction to meet the requirements of creating resources only in US locations at an organizational level, ensuring that the development projects abide by the desired limitations.

Solution to Question 24: A

The best action to take in this scenario would be option A, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes. This is because the Storage Object Viewer role allows access to read and download objects stored in the Container Registry. By granting this role, you ensure that your GKE cluster in the different project can access and download the required container images.

Option B, using Workload Identity Federation, is not the most suitable solution in this case. Workload Identity Federation is primarily for external applications and services to obtain short-lived credentials to access Google Cloud resources. Since this scenario involves two projects within the same organization, granting the necessary IAM role directly to the service account is a simpler and more appropriate solution.

Option C, enabling Container Registry VPC Service Controls and creating a perimeter around the project where the GKE cluster being created, is not appropriate for this scenario. VPC Service Controls restrict how services within a project can connect with other services. It's mainly used to prevent exfiltration and limit access to resources. However, it does not grant direct access for the GKE cluster to download images from the Container Registry.

Option D, configuring the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account, is not an effective solution. Although ACLs could be used to provide access, managing permissions on each image individually is cumbersome and time-consuming. Granting the Storage Object Viewer IAM role to the service account would provide the necessary access in a simpler and more manageable way.

Solution to Question 25: C

The correct answer is C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

Here's why other options will not work:

A. Ask the auditor for their Google account, and give them the Viewer role on the project. This option is not suitable because Domain Restricted Sharing is enabled. With Domain Restricted Sharing, only users within specific domains, such as the domain of the software development company, are allowed access. Therefore, granting access to an external auditor's Google account would not work.

B. Create a temporary account for the auditor in Cloud Identity and give that account the Editor role on the project. This option is incorrect because it would grant the auditor the ability to not only view but also modify resources within the project. As the question specifies that the auditor should only be able to view resources without modification capabilities, the Editor role is not appropriate in this scenario.

D. Ask the auditor for their Google account and give them the Security Admin role on the project. This option is not suitable for two reasons. First, granting the Security Admin role would provide the auditor with more permissions than necessary, including managing security policies and configurations. Secondly, Domain Restricted Sharing is enabled, so the auditor's Google account from a different domain would not be allowed access.

In conclusion, creating a temporary account for the auditor in Cloud Identity,

and giving that account the Viewer role on the project (Option C) is the best choice. This ensures that the auditor has access to view, but not modify, resources in the project under the Domain Restricted Sharing policy.

Solution to Question 26: A

The correct answer is A. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

The reason behind choosing option A is that preemptible VMs are available at a significantly lower cost compared to regular VMs, while still providing the same level of performance. This makes them a suitable choice for fault-tolerant and flexible workloads, such as nightly batch workloads. Since the workload in question can withstand termination of some VMs, using preemptible VMs is a cost-effective solution. Additionally, running a test using simulated maintenance events can help confirm that the workloads can handle the interruptions caused by termination of some VMs.

Option B is not the best choice because Google Kubernetes Engine (GKE) is primarily used for managing containerized applications and not directly focused on reducing VM costs. Although GKE can be used to run workloads, it might not provide the same cost benefits as preemptible VMs in this specific scenario.

Option C is not suitable because Dataflow is designed for executing batch and stream data processing pipelines, and not specifically for reducing VM costs. Dataflow is a higher-level service that abstracts away infrastructure management, and using N1 Standard VMs in the Dataflow pipeline might not have a significant impact on cost reduction.

Option D is not the most effective choice because it suggests using regular N1 Standard VMs instead of preemptible ones. While running a test using simulated maintenance events is a good practice, using the regular N1 Standard VMs will not lead to cost reduction, as opposed to the preemptible VMs that offer a lower cost.

Solution to Question 27: B

The correct answer is B: Using the GCP Console, filter the Activity log to view the information.

Explanation for why B is the correct answer:

As a data analyst with the responsibility of tracking sensitive information and user activities, using the GCP Console to filter the Activity log is the most direct and efficient way to achieve your goal. Since data access logging is already enabled for the Cloud Storage buckets, the necessary logs are available and can be filtered to review a specific user's actions, metadata additions, and accessed files. This can be done in a few simple steps through the GCP Console, without requiring any additional setup, making it the most efficient option.

Why the other options are not suitable:

A. Create custom Google Cloud Functions to monitor the activities in real-time.

This option might offer real-time monitoring capabilities, but it requires additional setup and development of custom functions. Moreover, Google Cloud Functions may not be the ideal tool for reviewing historical logs and verifying specific metadata labels and accesses. This option is more complex and time-consuming compared to filtering Activity logs in the GCP Console.

C. Create a trace in Stackdriver to view the information.

Stackdriver (now called Google Cloud Monitoring) is primarily designed to monitor the performance of applications and services in real time. While it does provide logs, creating a trace is not the most efficient way to access specific information about user activities, metadata labels, and accessed files. This option is not tailored to the specific task at hand.

D. Enable and configure Google Cloud Armor to view the logs.

Google Cloud Armor is a security service that provides Distributed Denial of Service (DDoS) protection and Web Application Firewall (WAF) capabilities. It is not designed to monitor and log user activities within Cloud Storage buckets. This option would not provide the necessary information and is not an appropriate solution for the task.

Solution to Question 28: C

The correct answer should be C: Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

When facing a problematic VM within a managed instance group (MIG), the best action to take is to replace the problematic VM with a new one, while retaining the same configuration. Option C offers this solution by utilizing the gcloud compute instance-groups managed recreate-instances command. This command serves to replace a particular VM in a MIG with a new one without changing other instances.

Option A suggests enabling autoscaling for the MIG based on CPU utilization. This is not a valid solution, as autoscaling is primarily used to scale the number of VM instances in a group according to the workload, not to replace a problematic VM.

Option B proposes to resize the MIG using the gcloud compute instance-groups managed resize command. This is also not effective, as resizing a MIG involves adding or removing instances from the group to adjust to the target size, but it does not address the specific problematic VM issue within the group.

Lastly, option D involves creating a new instance template and migrating the MIG to that new template. While this could potentially resolve the issue, it is a longer process and may not reveal the root cause of the problem. Moreover, it could potentially affect the entire MIG rather than focusing on the specific problematic VM. Therefore, it is not an ideal solution in this scenario.

In summary, the most appropriate action to quickly replace a problematic VM within a MIG is to use the gcloud compute instance-groups managed recreate-instances command, making option C the correct choice.

Solution to Question 29: C

The most suitable combination of Google Cloud Platform services for this pipeline is option C: Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, and BigQuery. Let us discuss why this combination is preferred and why the other options will not work.

Option C: 1. Cloud Pub/Sub: This is a reliable and scalable messaging service that can be used to ingest data from various sources like stock market transactions, ensuring efficient data ingestion in real-time. 2. Cloud Dataflow: It is a fully managed service for processing and transforming vast volumes of data. Suitable for handling time-series data processing tasks, it can integrate with other GCP services like Bigtable and BigQuery, making it an ideal choice. 3. Cloud Bigtable: Designed for handling large-scale, low-latency workloads such as time-series data, Cloud Bigtable provides high availability and strong consistency. This makes it a perfect fit for managing and analyzing the stock market data. 4. BigQuery: A fully managed, serverless data warehouse, BigQuery enables super-fast SQL queries across petabytes of data. Stock market transactions can be aggregated and analyzed with ease, allowing for advanced analytics and insights.

Now let's examine why other options will not work:

Option A: 1. Cloud Datastore: Although it is a NoSQL database, Cloud Datastore provides better support for traditional web applications rather than time-series data management. It lacks efficient querying abilities optimized for time-series data, making it less suitable than Cloud Bigtable.

Option B: 1. Cloud Spanner: A relational database, Cloud Spanner, provides horizontal scaling and global consistency. However, it is not optimized for time-series data management and analysis. Cloud Bigtable is a better alternative. 2. Cloud Storage: A durable, scalable object storage service, it is not optimized for time-series data analysis and cannot compete with BigQuery's analytical capabilities.

Option D: 1. Firebase Realtime Database: This NoSQL cloud database focuses primarily on assisting app developers with their real-time data needs. It lacks the level of scale, consistency, and analytics needed for managing large-scale time-series data. 2. Firestore: A NoSQL database ideal for mobile and web app development, Firestore is not tailored for large-scale time-series data and analytics, again proving less suitable than Cloud Bigtable and BigQuery.

In conclusion, option C, which includes Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, and BigQuery, is the most suitable combination for implementing a pipeline to manage and analyze time-series data for stock market transactions.

Solution to Question 30: A

The correct answer is A: Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

This is because an object lifecycle management policy allows you to automatically transition objects between storage classes as they age. In this specific situation, objects with an age over 30 days will be transitioned to the Archive Storage class. The Archive Storage class is a cost-effective solution for files that are no longer accessed by the application, as it is Google Cloud Storage's lowest-cost storage class designed for long-term retention and backup.

Here is why other options will not work:

B: Creating a BigQuery table to identify files older than 30 days and delete them using a scheduled query is an inefficient solution, as it will permanently delete the files, which might not be the desired outcome, and it is more complex than simply changing the storage class.

C: Using gsutil to set the lifecycle configuration on the bucket to delete files older than 30 days is also not the most efficient solution. While gsutil can be used to apply lifecycle configurations to a bucket, it's again opting to delete the files rather than transitioning them to a more cost-effective storage class. This could potentially result in data loss on files, which might still be required beyond 30 days.

D: Setting the storage class of the bucket to Nearline Storage and specifying a 30-day minimum storage duration is not as cost-effective as using Archive Storage because Nearline Storage costs will be higher. Moreover, changing the entire bucket's storage class would affect all the files in the bucket, not just those that are older than 30 days.

Solution to Question 31: C

The correct answer is C, and here's why:

Option A is incorrect because VPC Service Controls is designed to protect Google Cloud resources from unauthorized access and data exfiltration. It does not provide visibility into vulnerabilities and OS metadata.

Option B is incorrect because it involves creating a log sink to a BigQuery dataset, which can result in storing logs in BigQuery. However, this does not provide visibility into vulnerabilities and OS metadata effectively. It would require manual analysis of logs, which may not be up-to-date or complete.

Option C is correct because it ensures that the OS Config agent is installed on the Compute Engine instance. OS Config is explicitly designed to provide visibility into vulnerabilities and OS metadata. By providing a security team member the roles/osconfig.vulnerabilityReportViewer permission, they can access vulnerability reports for the specific Compute Engine instance.

Option D is incorrect because the Ops Agent is not designed to provide visibility into vulnerabilities and OS metadata. It is mainly focused on collecting logs and metrics from Compute Engine instances. Additionally, roles/osconfig.inventoryViewer permission will not provide the access needed to view vulnerability reports.

So, to effectively implement the security vulnerability management policy, option C should be chosen: ensure the OS Config agent is installed on the Compute Engine instance and provide the security team member with roles/osconfig.vulnerabilityReportViewer permission.

Solution to Question 32: A

The correct answer is A: Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

The reason for this choice is that Cloud Bigtable is specifically designed to handle massive workloads, such as millions of simultaneous read/write operations and terabytes of data storage. It is capable of offering high throughput, scalability, and low-latency access, which is better suited for the given scenario.

By creating a row key based on the event timestamp, it ensures the atomic operation of storing and retrieving consistent data based on event timings, as each event's storage will be handled separately based on unique key values associated with the time of event generation.

Now, let's discuss why other options are not suitable for this task:

B. Creating a file in Google Sheets per device and appending new data to it would not be efficient or scalable in this situation. Google Sheets is not designed for handling such high-throughput data requirements, and it may not provide the performance and consistency needed for this application.

C. Storing the sensor data in separate tables in BigQuery for each device is not the best approach because BigQuery is designed for data warehousing and analytics, and not for real-time data ingestion and retrieval. While BigQuery provides excellent query performance for large datasets, it may not guarantee the atomicity and real-time consistency required for this task.

D. Ingesting the data into Datastore and storing data in an entity group based on the device might not be as efficient as using Cloud Bigtable. While Datastore can handle large amounts of structured data, Cloud Bigtable delivers better performance in terms of low-latency access and support for high-frequency read/write operations. Additionally, Datastore's entity groups have a write limitation (about 1 transaction per second), which may not be suitable for the given scenario as it could lead to operation throttling.

So, considering the specific requirements of high expected throughput and atomic operations for storing and retrieving event data, the best solution for the company would be to use Cloud Bigtable and create a row key based on the event timestamp.

Solution to Question 33: A

The correct answer is A, using kubectl config use-context and kubectl config view to review the output.

Reasons why A is the correct answer:

- First, use the kubectl config use-context command to set the current context for the Kubernetes Engine cluster of the inactive configuration. This allows you to switch to the desired configuration with ease.
- Next, use kubectl config view to display the details of the configured Kubernetes Engine cluster for the selected context. By doing so, you can review the configuration with the fewest steps, fulfilling your requirement.

Reasons why other options do not work:

- Option B: kubectl config get-contexts does provide the output of all contexts available, but it only gives an overview of the contexts and not the configured Kubernetes Engine cluster's details for an inactive configuration.
- Option C: gcloud config configurations describe is a gcloud command exclusively used for managing and viewing gcloud configurations, not kubectl contexts or Kubernetes Engine clusters. Therefore, it will not provide the required output.
- Option D: kubectl get nodes is used for displaying the list of worker nodes in a Kubernetes cluster. It does not provide any information related to the configured Kubernetes Engine cluster of an inactive configuration. Connecting to the desired context and displaying the cluster's details are both not achieved using this option.

Solution to Question 34: D

The correct answer is D. Create the instance without a public IP address.

Explanation:

A. Create a route on the VPC to route all traffic to the instance over the VPN tunnel - This option is incorrect because creating a route will not prevent public internet traffic from accessing the Compute Engine instance. Routing traffic does not act as a security control.

B. Create the instance with Private Google Access enabled - Private Google Access allows a Compute Engine instance to reach Google APIs without traversing the public internet. However, enabling it does not prevent public internet traffic from accessing the instance. It only ensures the instance's communication with Google services stays within Google's network.

C. Restrict the instance to only allow traffic from on-premises WAN IP addresses - While restricting the instance to specific IP addresses can limit the exposure to public internet traffic, it does not entirely prevent it. There will still be a

potential attack vector through the allowed IP addresses, making this option less secure than option D.

D. Create the instance without a public IP address - By creating a Compute Engine instance without a public IP address, you ensure that the instance is only accessible through the VPC and VPN tunnel. This configuration eliminates the possibility of public internet traffic reaching the instance, providing the desired security level.

Solution to Question 35: C

The correct answer is C: Configure a single Stackdriver account, and link all projects to the same account.

Explanation: Stackdriver, now part of Google Cloud's Operations Suite, is a comprehensive monitoring solution that allows easy tracking and reporting of resources, especially in the Google Cloud Platform. By configuring a single Stackdriver account and linking all projects to the same account, you will be able to consolidate reporting from multiple projects under a single dashboard. This centralized approach makes it easier to view performance metrics, track resources, and monitor overall health across various projects.

Reasons why other options will not work:

A. Configure a single Stackdriver account for one of the projects. In Stackdriver, create a Group and add the other project names as criteria for that Group. - Creating a group is not sufficient to consolidate monitoring across multiple projects. To achieve the desired goal, you need to link all projects to the same Stackdriver account.

B. Use a single Stackdriver account but create separate dashboards for each project and then merge the dashboards. - While merging dashboards might seem like a logical solution, it could cause confusion and disorganization. Linking all projects to the same account allows a more efficient and organized monitoring of resources across projects.

D. Configure Stackdriver in one project and use Google Cloud Functions to export monitoring data to the main project. - This approach adds unnecessary complexity and latency to the monitoring process, especially when trying to export data between projects. Linking all projects to a single Stackdriver account is a more efficient and streamlined approach for consolidating reporting.

Solution to Question 36: C

The correct answer is C: Create a private zone on Cloud DNS, and configure the applications with the DNS name.

Explanation: Creating a private zone on Cloud DNS allows you to manage your company's DNS records within the VPC environment in Google Cloud. This private zone does not allow public internet access. By using a DNS name for the database server instead of its IP address, you can simplify IP management,

so if the database server's IP changes, your applications will not need any configuration changes.

Option A is incorrect because using custom metadata for each instance would still require updates in the applications if the IP of the database changes. Also, querying the metadata for the server might become a bottleneck, especially when dealing with large distributed systems.

Option B is incorrect because Google Cloud Endpoints is designed to develop, deploy, protect, and monitor APIs. While you can create an API proxy for the database, this will add an additional layer of complexity to your architecture. Additionally, it does not address the primary issue of handling IP configuration changes for the database server.

Option D is incorrect because an external Cloud DNS zone is designed for public-facing resources. This means that it enables DNS resolution for resources available on the internet. Since your goal is to securely communicate between your on-premises network and your Google Cloud VPC through a VPN tunnel, using an external Cloud DNS zone would not be appropriate.

Solution to Question 37: A

The correct answer is A, which is to add the user to the roles/iam.serviceAccountAdmin role. Let's analyze each role and explain why other options will not work.

A. roles/iam.serviceAccountAdmin: This role is the correct one because a service account administrator requires the ability to create, manage and delete service accounts. The Service Account Admin role permits a user to perform these essential tasks, ensuring that the user will have the necessary permissions to efficiently handle service accounts.

B. roles/iam.serviceAccountOperator: This role is not sufficient for the user's job because it only allows the user to perform actions as a service account, but not manage the service accounts themselves. It lacks the permissions to create, update or delete service accounts, which are crucial responsibilities for someone tasked with service account management.

C. roles/iam.serviceAccountAuditor: This role only grants the user read-only access to view the service accounts and their keys. The user would not be able to create, manage, or delete service accounts, which is necessary in their role as the service account manager.

D. roles/iam.serviceAccountUser: This role allows a user to impersonate, or act as, a service account. However, it does not grant permissions to create, update, or delete service accounts. It would not be sufficient for a user responsible for managing service accounts across projects.

In conclusion, only option A, the roles/iam.serviceAccountAdmin role, will provide the minimum required permissions for the dedicated person to manage service accounts efficiently. The other roles do not grant the necessary permis-

sions to create, manage, or delete service accounts as required by the individual's job responsibilities.

Solution to Question 38: B

The correct answer is B: In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

This is the best option because it matches the requirement of implementing an effective authentication method using the organization's single sign-on (SSO) identity provider and supports SAML integration with service providers. By setting up SSO with a third-party identity provider and configuring Google as a service provider, you will enable users in Cloud Identity to authenticate through the company's SSO provider.

Let's discuss why other options will not work:

A. In Cloud Identity, set up SSO with Google as an identity provider to access GCP Native services. This option is incorrect because it does not fulfill the requirement of using the organization's single sign-on (SSO) identity provider. Instead, it suggests using Google as the identity provider, which is not the desired outcome.

C. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications. This option focuses on OAuth 2.0, which is an authorization framework rather than an authentication method. It does not mention SSO or SAML integration, so it does not satisfy the requirements outlined in the question.

D. Configure Cloud Identity-Aware Proxy to use your company's SSO provider for authentication. Although this option includes using the company's SSO provider, Cloud Identity-Aware Proxy is used for controlling access to applications running on Google Cloud Platform, not for configuring SSO between identity providers and service providers. SAML integration is not mentioned, making it an inappropriate solution for the given scenario.

In conclusion, the best approach for enabling users in Cloud Identity to authenticate through the company's SSO provider is to set up SSO with a third-party identity provider and configure Google as a service provider (Option B).

Solution to Question 39: D

The correct answer is D, and here's why:

The given scenario involves setting up a caching HTTP reverse proxy which requires minimal CPU usage with a focus on latency-sensitive websites. This makes Cloud Memorystore for Redis (Option D) the most suitable option.

Google Cloud Memorystore for Redis is a fully managed in-memory datastore where you can build latency-sensitive applications. It provides an in-memory cache that makes it perfect for caching HTTP reverse proxies. In this case,

setting up a Memorystore instance with a 32-GB capacity would suffice for the 30-GB in-memory cache requirement and the 2 GB needed for other processes.

Here's why the other options don't work as well:

A. Running the reverse proxy on Compute Engine with the instance type n1-standard-1 and adding a 32-GB SSD persistent disk would not meet the requirement of a 30-GB in-memory cache. Additionally, this instance type provides only 3.75 GB of memory, which is insufficient for the given requirement of 2 GB of memory for other processes.

B. Running the reverse proxy on Compute Engine with a custom instance type having 2 vCPUs and 40 GB of memory seems like it could work. However, it would involve additional costs for vCPUs, which are not necessary in this case as the requirements specified minimal CPU usage. Therefore, this option wouldn't be the most cost-effective choice for the task.

C. Deploying the reverse proxy on a Compute Engine instance with the instance type e2-highmem-16 is not optimal, as this instance provides a significant amount of vCPU and memory resources, leading to higher costs. As the requirement is for minimal CPU usage and a focus on in-memory cache, this option is not cost-efficient for this specific task.

To minimize costs while fulfilling the requirements, the best choice is Option D - creating a Cloud Memorystore for Redis instance with a 32-GB capacity.

Solution to Question 40: D

The correct answer is D. The reason behind this is that the finance team should only have the authority to link a project to a billing account without making any other changes to the projects. This can be ensured by assigning them two specific roles: the Billing Account User role on the billing account and the Project Billing Manager role on the organization.

Option A is incorrect because assigning the engineering team the Project Owner role would give them more authority than required, as they would have the ability to link projects to the billing account. In addition, the Billing Account User role would not limit their capabilities in handling the billing accounts.

Option B is incorrect because the engineering team should not have the ability to link projects to the billing accounts. The Billing Account User role gives them authority over billing accounts and linking projects, which goes against the requirements.

Option C is incorrect because the Compute Network User role is unrelated to the finance team's responsibilities. This role only grants permissions to use networking-related resources, but it does not allow the finance team to link a project to a billing account.

Thus, the best measure to ensure the engineering team does not have the ability to link projects to billing accounts while allowing the finance team to do so with

specified limitations is option D.

Solution to Question 41: A

The correct answer is A: Use kubectl to delete the topic resource.

Explanation: As a software engineer at a tech company working with a Pub/Sub topic managed by Config Connector in your Google Cloud project, you should be familiar with the Kubernetes ecosystem. Config Connector is a Kubernetes add-on that allows you to manage Google Cloud resources through Kubernetes configuration files, and kubectl is a command-line tool to interact with the Kubernetes API. To permanently delete a Pub/Sub topic, you should use kubectl to delete the topic resource from your Kubernetes cluster. With the appropriate Kubernetes configuration file, use the command `kubectl delete -f your-config-file.yaml`, which will in turn remove the connected Google Cloud Pub/Sub topic.

The other options will not work as explained below:

B: Use kubectl to rename the topic resource. Renaming the topic resource by editing its metadata using kubectl may change the resource's name in your Kubernetes cluster, but this will not delete the Pub/Sub topic on Google Cloud. Furthermore, Config Connector may not recognize the renamed resource, resulting in a failed operation.

C: Use gcloud CLI to delete the topic. Although gcloud is a command-line tool for managing Google Cloud resources, it does not interact with Config Connector directly. Therefore, removing the Pub/Sub topic using gcloud does not remove the corresponding Config Connector Kubernetes resources and relationships, leading to inconsistencies in the configuration.

D: Use Firebase CLI to delete the topic resource. Firebase is a different platform that is used to develop web and mobile applications quickly. Firebase CLI is the command-line interface for managing Firebase projects, and it has no role in managing resources for a Google Cloud project with Config Connector. Hence, attempting to delete the topic resource using Firebase CLI will not work in this situation.

Solution to Question 42: B

The correct answer should be B: Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

Explanation for B: By gradually rolling out the new revision and splitting customer traffic between the old and new revisions, you are minimizing the risk associated with a new deployment. This is because the traffic will be distributed, allowing customers to test the new features while still retaining access to the old features in case of an issue. Moreover, this approach aligns with Google's recommended practices for managing revisions to a Cloud Run service. It also provides the flexibility to rollback if any issues occur, reducing the number of customers that might be affected by an outage.

Why other options will not work:

A: While using Cloud Scheduler to perform periodic health checks might help detect issues in the new revision, it adds complexity to the system and does not minimize the risk associated with a new deployment. Rerouting the traffic based on health checks may lead to a less stable experience for customers, as the system may switch between the old and new revision frequently.

C: Creating a separate Cloud Run service with the new revision and manually managing the traffic between the old and new services would increase operational complexity and make it challenging to roll back in case of an issue. Additionally, it wouldn't follow Google's recommended practices for managing revisions to a service, which limits the risk associated with the deployment of a new revision.

D: Deploying the application to a second Cloud Run service and asking customers to use the second service would impose an unnecessary burden on customers to switch services. Customers would need to change the way they access the application and keep track of the new service, and it would add operational overhead to manage multiple services instead of using a single one with proper management of revisions. This strategy also does not align with Google's recommended practices for managing revisions to a Cloud Run service.

Solution to Question 43: D

The correct answer is D: Use Cloud Functions and configure the bucket as a trigger resource.

Here's why the other options will not work:

Option A: Use Cloud Dataproc and configure an ephemeral cluster to read the bucket's contents. - Cloud Dataproc is primarily used for running big data analytics tasks and is not the most suitable option for the requirements of the question. Creating a cluster for reading metadata of each new media file will be a resource-intensive and inefficient process, and it won't automatically trigger the code snippet upon new file uploads.

Option B: Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub. - App Engine is used for building scalable applications and not specifically designed for reacting to events. Cloud Scheduler is used to schedule tasks; however, this setup requires periodic polling instead of automatically triggering on new file uploads. This approach may result in higher latency and increased complexity in implementation without effectively fulfilling the real-time triggering requirement.

Option C: Use Cloud IAP and create a notification channel to trigger the application. - Cloud IAP (Identity-Aware Proxy) is used for controlling access to your applications running on Cloud Platform. It does not directly support event-driven processing, nor is it related to media file processing. Using Cloud IAP would not address the need for automatic triggering for every new media file uploaded to the Cloud Storage bucket.

Option D: Use Cloud Functions and configure the bucket as a trigger resource. - Cloud Functions are designed to react to specific events from various Google Cloud resources and are perfectly suited for this use-case. Configuring the Cloud Storage bucket as a trigger resource will automatically invoke a serverless function whenever a new media file is uploaded, allowing the code snippet to process the metadata without additional setup or latency. This option meets the requirement to automatically trigger the code for every new file.

Solution to Question 44: C

The correct answer is C. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

Explanation:

Option A is incorrect because deploying a custom intrusion detection system (IDS) on a compute instance adds unnecessary complexity for the given requirement. The company prefers simple solutions, and setting up an IDS along with Cloud Pub/Sub for communication is not the most straightforward approach when native tools like Cloud Logging are available.

Option B is wrong because creating custom dashboards using Grafana is not the simplest way to gain insight into the company's Google Cloud environment. The main focus in the requirement is to monitor firewall changes and instance creations, not to visualize them. Moreover, integrating Grafana with Google Cloud Monitor adds an unnecessary level of complexity when straightforward monitoring with alerts can be done using the Google Cloud environment's Cloud Logging features.

Option C is correct because Cloud Logging filters are a simple and effective way to create log-based metrics for firewall and instance actions directly in the Google Cloud environment. These filters can be used to monitor changes, and setting up alerts ensures that you are proactively notified of any unexpected events or actions. This meets all the requirements given without adding unnecessary complexity.

Option D is incorrect because creating a log sink to forward Cloud Audit Logs to Cloud Storage and using BigQuery for analysis is a more complex solution than needed. The company prefers simple solutions, and the process described in this option requires multiple services. In addition, it doesn't provide real-time monitoring or alerts compared to Cloud Logging filters which can provide real-time insights and solution simplicity.

Solution to Question 45: B

The most appropriate course of action to achieve the centralization of all project expenses is option B: In the Google Cloud Platform Console, create a new billing account and set up a payment method.

Option B works because by creating a new billing account and setting up a company payment method, all Cloud Platform project expenses can be managed efficiently in a single place. This helps keep track of the company's expenses, minimizes the chance of unauthorized charges, and ensures the seamless management of budgets and resources.

Option A is not suitable because merging all individual employee accounts into a single corporate account in Google Cloud Platform is not possible. Google Cloud Platform doesn't offer such functionality, making this option unfeasible.

Option C misses the point as creating a Google Group doesn't help centralize and maintain an organized billing system. Google Groups primarily serve as a platform for communication and collaboration, not handling financial or billing-related matters.

Option D does not address the issue of centralizing and streamlining project expenses. Instead, it continues the practice of having multiple billing accounts, still utilizing individual employee accounts and inserting the company credit card into each of them. This complicates the billing process and undermines the goal of maintaining a centralized billing account for the company.

Therefore, the best course of action is option B, as it directly addresses the challenge of centralizing project expenses into a single billing account and simplifying the overall billing management process for the company.

Solution to Question 46: A

The correct answer is A: Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

The reason behind this is that it provides the necessary permissions to the DevOps team to access and manage the production services without compromising the security aspects. Customizing the roles enables you to adhere to the principle of least privilege by granting only the required permissions for the team to perform their tasks. This approach aligns with Google-recommended practices and minimizes the security risks that may arise from future alterations in Google Cloud products.

On the other hand, the other options may not be suitable for the following reasons:

Option B: Creating a custom role with only Compute Admin permissions may restrict the DevOps team from accessing other necessary Google Cloud services, which is not effective for their tasks in a centralized production project. This could hinder the team's productivity and project success.

Option C: Creating a custom role that combines the required permissions but only granting the DevOps team the Project Viewer role on the production project essentially limits their capabilities to viewing and not managing the necessary services. This would obstruct the team from effectively executing their tasks, affecting their performance and the overall project's success.

Option D: Granting the DevOps team the role of Project Editor on the test and development projects does not address their need for access to production services. While it may provide the necessary permissions for non-production environments, the team would still be unable to manage and monitor the production services as required by their tasks. This could lead to delays, increased costs, and unsatisfactory project outcomes.

Solution to Question 47: A

The correct answer is A. Coldline Storage. As a data recovery specialist, you need to store the application backup files securely and cost-effectively while prioritizing retrieval times for disaster recovery purposes. Coldline Storage is specifically designed for long-term data storage, such as application backups, with infrequent access.

Here's why the other options will not work:

B. Uniform Bucket-Level Access: This is not a storage class but an access control mechanism within Google Cloud Storage. It simplifies managing access to Cloud Storage buckets by disabling object-level ACLs (Access Control Lists) and only using bucket-level IAM (Identity and Access Management) policies. While it is recommended for administration purposes, it does not address the storage needs for backups and disaster recovery.

C. Archive Storage: While Archive Storage is also meant for long-term storage with very low storage costs, it comes with a 90-day minimum storage period and much slower data retrieval times compared to Coldline Storage. This makes it less ideal for disaster recovery purposes where faster retrieval times may be crucial.

D. Firebase Realtime Database: This is a cloud-hosted NoSQL database used by mobile and web developers to store and sync application data in real time. It isn't designed for storing application backup files for disaster recovery purposes and is more suitable for use in real-time, responsive applications.

In conclusion, Coldline Storage is the best option for storing application backup files for disaster recovery purposes in Google Cloud Storage, as it provides a balance between cost-effectiveness and retrieval times while adhering to Google's recommended best practices.

Solution to Question 48: C

The ideal answer should be C. Use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource you expect to use. Use similar size instances for the web server and use your current on-premises machines as a comparison for the Cloud SQL.

This option is the best because the Google Cloud Pricing Calculator is a customizable tool that allows you to choose the specific resources you need for your application (such as the type of compute instances, storage, databases, and their sizes) and accurately determine its cost. It also offers you the flexibility

to compare between different components and pricing models to find the most cost-effective solution tailored for your project.

Option A is not as accurate because creating a spreadsheet with various resource combinations will likely consume more time and effort than using the Pricing Calculator, which is explicitly designed for cost estimation. Additionally, manual data import and formula creation make this option prone to errors, which can lead to inaccurate estimations.

Option B is not a good choice because simply contacting Google Cloud Support to get an estimate without providing any details about your web application or infrastructure requirements will not yield accurate results. Support personnel cannot provide a meaningful cost estimate without specific information about your project's needs and infrastructure.

Option D is not recommended because relying on pre-existing pricing structures from Google Cloud Platform Forums may not be applicable to your particular use case. Every application has unique requirements and resource needs, which may not be the same as any other project. Adopting someone else's pricing structure would likely result in inaccurate cost estimations and potential issues with scaling or performance.

Solution to Question 49: D

The correct answer is D. Use the BigQuery interface to review the nightly job and look for any errors.

Explanation: As the issue is observed with the charts in Looker Studio, it is essential to primarily focus on the data source, which is the data warehouse built on top of BigQuery. Since the daily summary is recalculated at night by overwriting the table, it is crucial to analyze if there are any errors in the nightly job responsible for the overwrite. The BigQuery interface provides all the necessary information about jobs and can help you identify any abnormalities in the nightly job, which can cause issues downstream in Looker Studio visualizations.

A. Contacting the Looker Studio support team would not be the first step, as the issue might most likely be originating from BigQuery, the data source. It is always better to verify the data source first to rule out any data issues before reaching out to Looker Studio support.

B. Verifying the Cloud Dataflow pipeline for data ingestion issues on Google Cloud Platform is not directly related to the problem at hand. While it is crucial to maintain data quality in the data warehouse, the data pipeline does not resolve the issue with the nightly job in BigQuery, which is responsible for updating the table and causing Looker Studio chart anomalies.

C. Creating a filter for your Looker Studio report in Cloud Logging would not address the problem of broken charts. Cloud Logging is used for managing logs, not fixing visualization or data issues in Looker Studio. The primary task is to check the BigQuery nightly job to ensure that the correct data is being

brought into the table before focusing on other aspects such as log filtering and visualization adjustment.

Solution to Question 50: A

Answer A (10.0.0.0/8) should be chosen for the subnet range, and here's why:

Option A (10.0.0.0/8) provides the largest address space among the given choices as it has a prefix length of 8 bits. This means there are 24 bits left for the host portion of the addresses, giving a total of 2^24 (approximately 16.7 million) available IP addresses. With such a large address space, the organization will be able to accommodate future expansion without running into issues with insufficient IP addresses.

Options B, C, and D are not the best choices, and here's why:

Option B (169.254.0.0/16) is a link-local address range as defined by RFC 3927. These IP addresses are used for communication only within a local network segment and are not routable on the internet. Choosing this range will not allow the organization to correctly implement the VPC.

Option C (192.168.1.0/24) is a private IP range, but it has a prefix length of 24 bits. This means there are only 8 bits left for the host portion of IP addresses, giving a total of 2^8 (256) available IP addresses. This address space is significantly smaller than what Option A offers and may not be sufficient for accommodating future expansion.

Option D (192.168.0.0/16) is also a private IP range, with a prefix length of 16 bits. This leaves 16 bits for the host portion of IP addresses, giving a total of 2^16 (65,536) available IP addresses. While this is a more substantial pool of addresses than Option C, it is still significantly smaller than the range offered by Option A (10.0.0.0/8), which provides ample room for future growth.

Therefore, considering the goal of having the largest possible subnet range to accommodate future expansion, the best choice would be Option A (10.0.0.0/8).

Practice Exam 6

Question 1: As an IT manager in a large software company, you need to set up a new Compute Engine instance for two different Google Cloud Platform accounts—one in the default region and zone and another in a non-default region and zone. You want to achieve this using the command line interface. What should you do?

A. Use gcloud compute instances create [INSTANCE_NAME] with –account flag to specify the correct GCP account.

B. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud configurations list to start the Compute Engine instances.

C. Create two configurations using gcloud config configurations create [NAME]. Run gcloud configurations list to start the Compute Engine instances.

D. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

Question 2: You are working as a Senior IT Administrator for a large tech company that recently acquired a smaller startup which utilizes Google Cloud. Your task is to ensure that your team of Site Reliability Engineers (SREs) have the same project permissions in the newly acquired startup's Google Cloud organization as they have in your own company's organization. What approach should you take to accomplish this?

A. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

B. In the Google Cloud Console for your organization, invite the startup company's users as members, and grant them the same access levels as your SREs.

C. Use the gcloud iam org-policies set-policy command and enforce the same role policies for the startup company's organization as your organization.

D. Use the gcloud iam roles copy command, and provide the project IDs of all projects in the startup company's organization as the destination.

Question 3: As a database administrator at a fast-growing tech company, you need to manage a Cloud Spanner instance for optimal query performance. The production instance runs in a single Google Cloud region, and you need to enhance its performance in minimal time while adhering to Google's best practices for service configuration. What would be the most appropriate course of action?

A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

B. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 45%. If you exceed this threshold, add nodes to your instance.

C. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 55%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

D. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 75%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

Question 4: You are working as an IT specialist in a company that relies on Compute Engine virtual machines (VMs) in us-central1-a for hosting their applications. To ensure continued operation in case of a single Compute Engine zone failure and to eliminate downtime while keeping costs to a minimum, what strategy should you implement?

A. Use Cloud Pub/Sub with a regional endpoint to balance the load between VMs in us-central1-a and us-central1-b.

B. Configure VMs in us-central1-a to run as serverless instances using Google App Engine standard environment, and distribute traffic between the two zones using App Engine Traffic Splitting.

C. Create a Cloud Datastore instance in us-central1-b and set up replication between the two instances.

D. Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

Question 5: As a network administrator in a technology company, you are managing a Dataproc cluster that runs in a single Virtual Private Cloud (VPC) network within a single subnetwork with a range of 172.16.20.128/25. The subnetwork has no private IP addresses available, but you need to add additional VMs to communicate with your cluster in the fewest number of steps. What is the most efficient solution?

A. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

B. Create a new VPC network for the VMs with a subnet of 172.16.20.64/26. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

C. Modify the existing subnet range to 172.16.20.0/24.

D. Configure a VPN between the existing VPC network and a new VPC network for the VMs. Create a new subnetwork in the new VPC network and configure

the VMs to use that subnetwork.

Question 6: As a cloud engineer at a software development company, you are tasked with setting up an autoscaling managed instance group for a secure web application (HTTPS) and ensuring that unhealthy VMs are automatically recreated. What steps should you take to achieve this?

A. Create a health check on port 443 and use that when creating the Managed Instance Group.

B. In the Managed Instance Group configuration, set the target utilization to 100%.

C. Select Multi-Zone instead of Single-Zone when creating the Managed Instance Group.

D. Use the default health check for network load balancing when creating the Managed Instance Group.

Question 7: You are working as a data analyst for a technology company and you need to run an important query in BigQuery for a large dataset. Being on an on-demand pricing model, you want to estimate the cost of running this query before executing it. How can you determine the cost accurately?

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

B. Run the query in multiple parts and pay for each part separately.

C. Apply Data Studio to visualize and estimate the cost of the query.

D. Use the BigQuery UI to estimate the cost without actually running the query.

Question 8: As a data analyst at a multinational corporation, you are tasked with handling a massive amount of unstructured data in various file formats. Your goal is to perform ETL transformations on this data and make it available on Google Cloud for processing by a Dataflow job. What is the most appropriate action you should take?

A. Upload the data to Cloud Storage using the gcloud storage command.

B. Upload the data to Bigtable using the gcloud bigtable command.

C. Upload the data to Datastore using the gcloud datastore command.

D. Upload the data to Cloud Functions using the gcloud functions deploy command.

Question 9: You are working at a tech company that specializes in IoT solutions, and you have been tasked with creating a data lake on Google Cloud for their IoT application. The application receives continuous input from millions of connected sensors, each sending structured and unstructured data. To ensure that this data lake is both highly available and resilient, following Google-

recommended practices is crucial. What is the best approach to accomplish this?

A. Stream data to IoT Core, and use Cloud Functions to send data to Bigtable.

B. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

C. Stream data to Dataflow, and use Dataprep by Trifacta to send data to Bigtable.

D. Stream data to Dataflow, and use Dataprep by Trifacta to send data to Cloud Storage.

Question 10: You are working as a Data Security Specialist for a company in the financial industry, and your team is storing sensitive information in a Cloud Storage bucket. Due to industry regulations and legal obligations, you must record all requests that access any of the stored data. How can you ensure compliance with these requirements in this scenario?

A. Enable the Identity Aware Proxy API on the project.

B. Activate VPC Service Controls around the bucket.

C. Enable Data Access audit logs for the Cloud Storage API.

D. Enable the Security Command Center service.

Question 11: You are working in a company that heavily relies on data analytics, and your organization is utilizing Google BigQuery for data warehousing purposes. Recently, your company decided to collaborate with another company that offers a recommendation engine for enhancing your services, and they operate their application on Google Cloud. They need access to your BigQuery dataset to effectively integrate their recommendation engine with your existing system. What should be your approach to provide them access to the required dataset in your BigQuery project?

A. Create a Service Account in your own project, and ask the partner to grant this Service Account access to App Engine in their project.

B. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

C. Create a Service Account in your own project, and grant this Service Account access to Compute Engine in your project.

D. Ask the partner to create a Service Account in their project, and have them give the Service Account access to BigQuery in their project.

Question 12: As an IT administrator at a growing company, you have several VMs running in a subnet with a subnet mask of 255.255.255.240. The current subnet has run out of free IP addresses, and you need to accommodate 10 additional IP addresses for new VMs. To ensure the existing and new VMs can communicate with each other without additional routes, what should you do?

A. Change the subnet mask of the existing subnet to 255.255.255.224.

B. Upgrade the VMs to larger machine types to increase the number of available IP addresses.

C. Use gcloud to expand the IP range of the current subnet.

D. Create a new subnet with the same IP range but a different region and use VPC Network Peering.

Question 13: You work for a tech company that utilizes G Suite for all internal communication and collaboration. Your team is currently working on a project using Google Cloud Platform, and you need to provide access to specific G Suite users within your organization. What is the appropriate method to grant them access to the project?

A. Create an IAM role and assign it to a Google Group, then manually add each G Suite user's email address to the group.

B. Use the Cloud SDK to create a new user role and assign it to each G Suite user's email address.

C. Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.

D. Grant them the required IAM roles using their G Suite email address.

Question 14: You are working as a system administrator for a large manufacturing company and have been tasked with deploying a new Enterprise Resource Planning (ERP) system on Google Cloud. The application is designed to hold the full database in-memory for fast data access. What is the most appropriate resource configuration on Google Cloud for this application?

A. Provision Compute Engine instances with T2 machine type.

B. Use a Cloud Spanner instance for in-memory database handling.

C. Use Cloud Functions with high memory configurations.

D. Provision Compute Engine instances with M1 machine type.

Question 15: As a software developer in a tech company, you have developed an application that is packaged into a Docker image, and you are tasked with deploying this Docker image as a workload on Google Kubernetes Engine. What is the appropriate course of action to accomplish this?

A. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

B. Upload the image to Container Registry and create a Kubernetes StatefulSet referencing the image.

C. Upload the image to Firestore and create a Kubernetes Service referencing the image.

D. Upload the image to Compute Engine and create a Kubernetes Deployment referencing the image.

Question 16: In your company that operates in the tech industry, you have established a sophisticated organizational structure on Google Cloud, consisting of hundreds of folders and projects. To grant limited access to the hierarchy for selected team members while adhering to Google's best practices, which action should you take?

A. Add the users to a group, and add this group to roles/iam.roleViewer role.

B. Create a custom IAM role with limited resource access and assign it to the users.

C. Add the users to roles/cloudtrace.agent role.

D. Add the users to a group, and add this group to roles/browser.

Question 17: You're working as a Cloud Engineer at a tech company, and your task is to set up permissions for a group of Compute Engine instances. These instances need to have the ability to write data into a specific Cloud Storage bucket while adhering to Google's recommended practices. How should you proceed?

A. Create a service account and add it to the IAM role 'serviceAccount-tokenCreator' for that bucket.

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

C. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/compute.read'

D. Create a service account and add it to the IAM role 'compute.admin' for that bucket.

Question 18: As a project manager at a leading software company, you are tasked with creating a cost estimation report for a solution you have designed using multiple Google Cloud products. The report should outline the monthly total costs for the entire solution. How should you proceed?

A. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

B. Calculate your costs by manually reviewing the Pricing page for each Google Cloud product and using intuition rather than the pricing calculator.

C. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Use Cloud Monitoring to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

D. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Navigate to the Billing Report page in the Cloud Console. Multiply the 1 week cost to determine the monthly costs.

Question 19: As a software engineer working in a gaming company, you've been tasked with optimizing a popular multiplayer mobile game running on the Google Cloud platform. Players use their personal smartphones to connect via the Internet, and the game sends UDP packets to update servers about in-game actions. The game's backend can scale across multiple virtual machines (VMs), and you need to find a way to expose these VMs through a single IP address. What would be the best solution to implement?

A. Configure an SSL Proxy load balancer in front of the application servers.

B. Utilize VPC peering for load balancing between VMs.

C. Configure an External HTTP(s) load balancer in front of the application servers.

D. Configure an External Network load balancer in front of the application servers.

Question 20: You are working for a software development company and have recently deployed an application on a single Compute Engine instance in the cloud. The application writes logs to disk. After receiving reports from users about errors with the application, you need to diagnose the problem. What is the recommended course of action in this situation?

A. Install and configure the Ops agent and view the logs from Cloud Logging.

B. Set up a VPN connection between the instance and your local workstation to access the logs.

C. Create a new Google Kubernetes Engine cluster and migrate the application there.

D. Use Cloud Pub/Sub to push error logs from the application to a subscriber.

Question 21: As a Cloud Engineer in a media company that relies on a Compute Engine instance to host an Apache web server for distributing large files, you have multiple applications running within the project. To manage expenses better, you need to configure an alert to send you an email when the egress network costs related to the Apache web server exceed 100 dollars in the current month, as measured by Google Cloud. How should you achieve this goal?

A. Set up a budget alert on the Compute Engine instances with an amount of 100 dollars, a threshold of 100%, and notification type of email.

B. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

C. Deploy a Google Cloud Pub/Sub notification channel to publish a message when egress costs for the Apache web server exceed 100 dollars for the current month, then create a Cloud Function that listens to the channel and sends an email upon receiving the message.

D. Set up a budget alert on the billing account with an amount of 100 dollars, a threshold of 100%, and notification type of email.

Question 22: In your company's e-commerce department, you are responsible for developing an internal application to manage transactional orders across various warehouses. The application is intended for exclusive use by your company's staff, who are located in a single headquarters. It is essential that the application offers robust consistency, swift query processing, and adheres to ACID principles for multi-table transaction updates. Your team has developed the initial version of the application using PostgreSQL, and you now seek to migrate it to the cloud with minimal code modifications. Which cloud-based database solution is most suitable for this scenario?

A. Cloud SQL

B. Cloud Datastore

C. BigQuery

D. Datastream

Question 23: As a project manager in a software development company, you need to grant an external team member the required permissions to access compute images and disks in one of your projects, following Google's recommended practices. How should you proceed?

A. Create a custom role based on the Compute Storage Admin role. Exclude unnecessary permissions from the custom role. Grant the custom role to the user at the project level.

B. Create a custom role based on the Compute Storage Admin role, but do not exclude any permissions. Grant the custom role to the user at the project level.

C. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

D. Create a custom role based on the Compute Image User role. Add the compute.disks.list to the includedPermissions field. Grant the custom role to the user at the project level.

Question 24: As a Cloud Engineer at a tech company, you receive a notification that your managed instance group has raised an alert, stating that new instance creation has failed. To resolve this issue, what action should you take?

A. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance

names.

B. Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template.

C. Create an instance template that contains valid syntax. Delete any firewall rules blocking instance creation in the instance group.

D. Create an instance template that contains valid syntax and add it to an existing instance group. Increase the instance count to generate new instances.

Question 25: You are working as a data engineer in a tech company, and you need to upload a 32 GB single data file to a Nearline Storage bucket for the company's project. The dedicated WAN connection you have access to has a rated speed of 1 Gbps and you are the sole user of this connection. Your goal is to maximize the usage of the available 1 Gbps speed to transfer the file as quickly as possible. What method should you employ to upload the file?

A. Increase the latency on the machine initiating the transfer.

B. Disable resumable uploads in gsutil.

C. Enable parallel composite uploads using gsutil on the file transfer.

D. Run multiple instances of gsutil in parallel without using composite uploads.

Question 26: You work as a project manager for a tech company and oversee a team of 10 developers. You've assigned each developer their own Google Cloud Project for experimentation and personal growth. Your primary objective is to ensure that no developer spends over $500 per month on resources in their respective sandbox environment. How do you monitor and receive notifications about this expenditure?

A. Configure Google Cloud billing notification with a spending threshold of $500 per month on the Organization level.

B. Enable VPC Flow Logs to monitor resource consumption in sandbox projects and set up alerting based on the spending.

C. Create a budget per project and configure budget alerts on all of these budgets.

D. Create a single budget for all projects and configure budget alerts on this budget.

Question 27: As a data analyst working in a company that relies heavily on cloud-based services, you have an application that uses Cloud Spanner as a database backend to maintain up-to-date information on users, and Cloud Bigtable to log all user-triggered events. Daily backups of Cloud Spanner data are exported to Cloud Storage. One of your colleagues requires you to merge data from Cloud Spanner and Cloud Bigtable for specific users in the most

efficient way possible for an ad hoc request. What should you do to accomplish this task?

A. Use Cloud Data Fusion to create a pipeline that reads data from Cloud Spanner and Cloud Bigtable, applies necessary transformations, and outputs the result to Cloud Storage.

B. Create a Cloud Dataproc cluster that runs a Spark job to extract data from Cloud Spanner and Cloud Bigtable for specific users.

C. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

D. Create a dataflow job that copies data from Cloud Bigtable and Cloud Storage for specific users.

Question 28: As a data analyst working at a tech company, you are tasked with granting your colleagues access to query datasets in BigQuery without giving them the ability to accidentally delete the datasets. You want to follow Google's recommended practices. What is the appropriate course of action?

A. Create a custom role by removing delete permissions. Add users to the group, and then.add the group to the custom role.

B. Enable Data Loss Prevention (DLP) on the datasets, instead of modifying user roles.

C. Add users to roles/bigquery dataEditor role only, instead of roles/bigquery dataOwner.

D. Add users to roles/storage.objectViewer role, instead of roles/bigquery dataOwner.

Question 29: As a Linux system administrator working in a multinational corporation, your team is responsible for managing Linux workloads on Compute Engine instances. The corporation has decided to collaborate with an external operations partner that does not utilize Google Accounts. In order to provide them access to maintain the installed tooling on these instances, what action should you take?

A. Configure a Google Cloud Pub/Sub topic that allows the operations partner to send and receive messages related to instance maintenance.

B. Implement a dedicated Shared VPC and provide the operations partner with access to the subnets of the instances.

C. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

D. Enable Cloud NAT and grant the operations partner access to the Cloud NAT gateway to allow traffic redirection.

Question 30: You are working as a network administrator at a large technology company. The current project you are managing has a single Virtual Private Cloud (VPC) and a single subnetwork in the us-central1 region, with a Compute Engine instance hosting an application in that subnetwork. Your task is to deploy a new instance in the same project, but in the europe-west1 region, ensuring it has access to the application. Following Google-recommended practices, what steps should you take?

A. Create a subnetwork in the same VPC, in europe-west1. Set up an instance group with only the new instance and use the first instance's private address as the backend endpoint.

B. 1. Create a subnetwork in the same VPC, in europe-west1. 2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

C. Create a subnetwork in the same VPC, in europe-west1. Enable global routing in the VPC and create the new instance in the new subnetwork, using the first instance's private address as the endpoint.

D. 1. Create a VPC and a subnetwork in europe-west1. 2. Peer the 2 VPCs. 3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

Question 31: As a software developer in a multinational corporation, you are required to develop a custom IAM role for a GCP service that your company intends to deploy. The role needs to have permissions suitable for production and should enable clear communication of the custom role version status within the organization. For the initial version of the custom role, what is the recommended course of action?

A. Use permissions in your role that use the 'preview' support level for role permissions. Set the role stage to BETA while testing the role permissions.

B. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to BETA while testing the role permissions.

C. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

D. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to GA while testing the role permissions.

Question 32: As the lead engineer for a cloud services company, you are tasked with implementing a dynamic way of provisioning VMs on Compute Engine. The exact specifications will be included in a dedicated configuration file and should follow Google's recommended practices. Which method should you use?

A. Bigtable

B. Managed Instance Group

C. Cloud Composer

D. Deployment Manager

Question 33: You are working as a data storage expert for a company that accumulates a large amount of data. They require an Object Lifecycle Management configuration for their storage buckets. The company's data storage pattern involves writing objects once and accessing them frequently for 30 days. After this period, the objects are typically not read again unless a specific need arises. They want to retain these objects for three years while minimizing storage costs. How should you set up the Object Lifecycle Management policy for this requirement?

A. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

B. Set up a policy that uses Nearline storage for 30 days and then moves to Coldline storage for three years.

C. Set up a policy that uses Coldline storage for 30 days and then moves to Archive storage for three years.

D. Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years.

Question 34: As a software developer working in a company that utilizes Google Cloud platform, you encounter an issue where your continuous integration and delivery (CI/CD) server cannot execute Google Cloud actions in a specific project due to permission issues. To verify if the service account being used has the appropriate roles in this particular project, what should you do?

A. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

B. Use gcloud CLI to list the permissions assigned to the organization and compare with the required project permissions.

C. Visit the CI/CD server logs and look for any configuration errors.

D. Review the resource and service account quotas.

Question 35: As a software engineer in a data-driven company, you need to configure service accounts for an application that spans multiple projects. You need to provide Virtual machines (VMs) running in the web-applications project access to BigQuery datasets in the crm-databases project while following Google-recommended practices. How should you grant access to the service account in the web-applications project?

A. Grant "project owner" role to crm-databases and the web-applications project.

B. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

C. Grant "project owner" role to crm-databases and roles/bigquery.dataViewer role to web-applications.

D. Grant "project owner" role to both crm-databases and web-applications projects.

Question 36: As a DevOps Engineer at a successful software company, you've been tasked with configuring an SSH connection to a single Compute Engine instance for users in the dev1 group. This instance is the only resource in this particular Google Cloud Platform project that the dev1 users should be able to connect to. How should you proceed?

A. Enable block project wide keys for the instance. Generate an SSH key for each user in the dev1 group. Associate the keys with that instance and direct them to use Cloud SDK to connect.

B. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

C. Create a Cloud Storage bucket and grant the dev1 group the storage.objectAdmin role. Direct them to use the Cloud Shell to ssh to that instance.

D. Set metadata to enable-oslogin=true for the instance. Set the service account to no service account for that instance. Direct them to use the Cloud Shell to ssh to that instance.

Question 37: As a software engineer at a tech company, you have developed an application on your personal laptop that leverages Google Cloud services. The app uses Application Default Credentials for authentication and functions well on your laptop. Now, you are tasked with transferring the app to a Compute Engine virtual machine (VM) and implementing authentication following Google's best practices, while making minimal changes. What approach should you take?

A. Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application.

B. Create a new Google account with appropriate access for Google services and use its credentials in a Compute Engine VM.

C. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

D. Manually generate an API key for each Google service and embed them in your application code.

Question 38: You're working as a data engineer in a tech company, and your current project utilizes a Dataproc cluster running in a single VPC network with a single subnet range of 172.16.20.128/25. Unfortunately, there are no private IP addresses available in the VPC network. You've been assigned the task of adding new VMs to communicate with your cluster using the minimum number of steps. What should you do?

A. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

B. Create a VPN tunnel between the existing VPC network and a new VPC network for the VMs.

C. Create a new Secondary IP Range in the VPC and configure the VMs to use that range.

D. Add VMs with public IP addresses in the existing VPC network and configure firewall rules to allow communication between VMs and rest of the VPC.

Question 39: You are working as a software engineer at a tech company that uses Google Kubernetes Engine with autoscaling enabled to deploy a new application. Your task is to ensure that this application is accessible to the public via HTTPS on a public IP address. What steps should you take to achieve this?

A. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

B. Create a Kubernetes Service of type ClusterIP for your application. Configure the public DNS name of your application using the IP of this Service.

C. Configure a Google Compute Engine instance with Nginx as a reverse proxy, and expose the application on HTTPS. Connect this instance to your GKE cluster.

D. Deploy your application on Google Cloud Functions and use API Gateway to expose the HTTPS endpoint.

Question 40: You are working as a cloud engineer in a software development company that extensively utilizes the Google Cloud Platform. You recently developed an App Engine application within a GCP project, initially setting it up to be served from the us-central region. Now, your manager wants to serve the application from the asia-northeast1 region. What should be your course of action?

A. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

B. Create a Cloud Function in the existing GCP project, specifying asia-northeast1 as the region, and use it to proxy requests to the App Engine application.

C. Create a Datastore instance in the existing GCP project specifying asia-northeast1 as the region, then migrate the App Engine application to it.

D. Change the region property setting in the existing App Engine application from us-central to asia-northeast1.

Question 41: As a project manager in a growing software company, you need to set up Google Cloud resources for the marketing team's project named Marketing Data Digest. These resources must be organized independently of the resources for the existing sales team project called Sales Data Digest with the ID acme-data-digest. What should you do?

A. Create a new marketing folder under acme-data-digest project and grant the Marketing team folder editor access.

B. Utilize Cloud Composer to build a pipeline that transfers data from acme-data-digest to the Marketing team's resources.

C. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

D. Create a separate organization for the Marketing team and migrate the acme-data-digest project there.

Question 42: As an IT specialist in a software development company, you are tasked with setting up a Windows VM on Compute Engine to ensure seamless remote access via RDP for your team members. What step should you take to retrieve the login credentials for the VM?

A. After the VM has been created, use gcloud compute instances describe to find the user name and then log in to the VM with it.

B. When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value.

C. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

D. After the VM has been created, use your Google Account credentials to log in into the VM.

Question 43: You are working as a Cloud Architect at a technology company and have been tasked with creating a new billing account, then linking it to an existing Google Cloud Platform project. What should you do?

A. Verify that you are Project Billing Manager for the GCP project. Create a new GCP project and link the new project to the existing billing account.

B. Verify that you are Billing Administrator for the billing account. Create a new project and link the new project to the existing billing account.

C. Verify that you are Billing Administrator for the billing account. Update the existing project to link it to the existing billing account.

D. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

Question 44: You are working as a cloud architect in a tech company that relies on a production-critical on-premises application requiring 96 vCPUs to function optimally. Your task is to migrate this application to GCP and ensure it runs in a similar environment. What is the most appropriate action to take?

A. Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs.

B. When creating the VM, use machine type n1-standard-96.

C. Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations.

D. When creating the VM, use machine type n1-highmem-32.

Question 45: As a cloud service manager of a large corporation, you've been assigned the task of reducing GCP service costs for one of the company's divisions. You need to shut down all configured services in the division's existing GCP project in the fewest possible steps. What should you do?

A. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID.

B. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Switch to the project in the GCP console, locate the resources and delete them.

C. 1. Verify that you are assigned the Organizational Administrator IAM role for this project. 2. Locate the project in the GCP console, enter the project ID and then click Shut down.

D. 1. Verify that you are assigned the Storage Administrator IAM role for this project. 2. Switch to the project in the GCP console, locate the storage buckets, and delete them.

Question 46: As a security analyst in a major corporation, you need to give an external auditor access to your company's Google Cloud Platform (GCP) Audit Logs and Data Access logs. What is the appropriate action for you to take?

A. Assign the auditor the IAM role roles/logging.privateLogViewer and roles/pubsub.editor. Perform the export of logs to Cloud Storage.

B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

C. Assign the auditor's IAM user to a custom role that has logging.logEntries.list permission and roles/storage.objectViewer. Perform the export of logs to Cloud Storage.

D. Assign the auditor the IAM role roles/logging.privateLogViewer and roles/storage.admin. Perform the export of logs to Cloud Storage.

Question 47: As a database administrator at a multinational company, you've been assigned to develop a globally distributed application utilizing Cloud Spanner for data storage. Before initiating the process of creating a Cloud Spanner instance, what is the first step you should take?

A. Create a new Google Cloud Firestore instance for global data storage.

B. Create a new Cloud SQL instance with global infrastructure.

C. Enable the Cloud Spanner API.

D. Grant yourself the IAM role of Cloud Spanner Admin.

Question 48: You are working as a cloud engineer at a company that uses Compute Engine VM instances in a custom Virtual Private Cloud (VPC) to run their applications. The company's security policies are strict and only allow the use of internal IP addresses on VM instances, disallowing connections to the internet. You have a task to ensure that the application can access a file hosted in a Cloud Storage bucket within the same project. What action should you take?

A. Enable Private Google Access on the subnet within the custom VPC.

B. Enable Private Service Access on the Cloud Storage Bucket.

C. Configure a Load Balancer to route traffic between the VM instances and the Cloud Storage bucket.

D. Configure a custom IAM policy to grant Compute Engine VM instances access to the Cloud Storage bucket.

Question 49: You are the lead developer at a fintech company that has recently developed a financial application to be deployed on Google Kubernetes Engine. Some parts of the application are non-critical, allowing for occasional downtime, while other components are crucial and must be available at all times. In order to optimize costs while configuring the Google Kubernetes Engine cluster, what should you do?

A. Create a cluster with both a Spot VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Spot VM node pool.

B. Create a cluster with both a Custom VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Custom VM node pool.

C. Create a cluster with a single node-pool by using standard VMs. Label the fault-tolerant Deployments as spot_true.

D. Create a cluster with a single node-pool by using Balanced Persistent Disks. Label the critical Deployments as disk_balanced_false.

Question 50: You are working as a Cloud Architect in a company, and the company hosts an application from Compute Engine virtual machines (VMs) in the us-central1-a region. Your manager has asked you to modify the existing design to ensure that it can support the failure of a single Compute Engine zone, eliminate downtime, and minimize additional costs. What steps should you take?

A. Create a global Cloud Spanner instance and configure the VMs in us-central1-a and us-central1-b to share the same Spanner database.

B. Create an HTTP(S) Load Balancer. Create one or more global forwarding rules to direct traffic to your VMs.

C. Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

D. Create a Kubernetes cluster in us-central1-a and us-central1-b, and use Kubernetes services to balance the load between VMs in both zones.

Practice Exam 6 Solutions

Solution to Question 1: D

The correct answer is D because it allows you to properly manage multiple Google Cloud Platform accounts and their respective Compute Engine instances using the command line interface by creating separate configurations and activating them as needed.

Option A is incorrect because using the –account flag with the gcloud compute instances create [INSTANCE_NAME] command only specifies the GCP account but does not provide a way to manage regions and zones for each account.

Option B is incorrect because although it suggests activating two configurations, it does not specify creating them in the first place. Additionally, running gcloud configurations list will only list the available configurations, and it does not start the Compute Engine instances.

Option C is incorrect because it suggests creating two configurations, but the command to run the configurations list will again only display the available configurations, and it does not start the Compute Engine instances. Also, there is no mention of activating the configurations to switch between accounts as needed.

In summary, option D is best suited to address the requirements of managing two different GCP accounts with separate region and zone settings as it involves creating configurations for each account and activating them while running commands to start the Compute Engine instances. This ensures a seamless workflow and allows the IT manager to efficiently manage the separate Compute Engine instances for each GCP account.

Solution to Question 2: A

The correct answer is A. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

Option A is the most efficient and appropriate way to ensure that your SREs have the same project permissions in the newly acquired startup's Google Cloud organization. By using the gcloud iam roles copy command, you can directly copy the roles and permissions from your organization to the startup company's organization, ensuring a consistent level of access for your SREs.

Option B is not correct because inviting the startup company's users as members to your organization and granting them the same access levels as your SREs will not help you in ensuring your SREs have the same access in the startup company's organization.

Option C is not the best solution because the gcloud iam org-policies set-policy command is used for managing organization policies, not for copying roles and permissions between organizations.

Option D is not correct because by providing the project IDs of all projects in the startup company's organization as the destination, you will only be copying the roles and permissions to the specific projects rather than the whole organization. This method is inefficient and may not effectively provide the desired level of access for your SREs across the startup company's entire Google Cloud organization.

Solution to Question 3: A

The most appropriate course of action would be Option A. There are several reasons why this option is the best choice, while the other options would not be as suitable.

Option A: Creating an alert in Cloud Monitoring when the percentage of high priority CPU utilization reaches 65% allows you to proactively detect and address performance issues before they become critical. By adding nodes to your instance in response to exceeding this threshold, you can quickly expand your Cloud Spanner's capacity, ensuring better query performance and adhering to Google's best practices for service configuration.

Option B: Creating an alert when the percentage of high priority CPU utilization reaches 45% may be too conservative. Adding nodes at such a low threshold could lead to unnecessary costs and could involve additional management overhead. It's more optimal to allow CPU usage to reach a higher percentage before taking action, as long as it's within Google's recommended best practices.

Option C: While alerting when CPU utilization reaches 55% and then optimizing queries is a valid approach to improve query performance, it might not be enough in the context of a fast-growing tech company. Relying solely on query optimization can be a time-consuming process, and it might not always provide an immediate solution to performance issues. On the other hand, increasing instance capacity by adding nodes can provide a faster and more reliable approach to improving overall performance.

Option D: Creating an alert when the percentage of high priority CPU utilization reaches 75% might be too late to prevent negative impact on query performance in a production environment. While optimizing queries is important, having an alert at such a high threshold can lead to possible performance degradation and service disruptions. Google recommends taking action before CPU utilization reaches 65% to maintain optimal performance.

In conclusion, Option A is the most appropriate course of action since it strikes a balance between proactive monitoring, scalability, and adherence to Google's best practices for service configuration. By monitoring CPU utilization and adding nodes when necessary, you keep optimal performance for your Cloud Spanner instance while ensuring the database grows in line with the tech company's needs.

Solution to Question 4: D

The correct answer is D, and here's why:

Creating Compute Engine resources in us-central1-b and balancing the load across both us-central1-a and us-central1-b zones ensures availability and redundancy in the event of a single zone failure. This strategy allows you to maintain operations without downtime, and it is cost-effective compared to the other options.

Option A - Using Cloud Pub/Sub with a regional endpoint for balancing the load between VMs in different zones does not help achieve the goal. Cloud Pub/Sub is a messaging service, not a load balancer meant for managing the availability of VMs.

Option B - Configuring VMs to run as serverless instances using Google App Engine standard environment and distributing traffic between the two zones with App Engine Traffic Splitting does not help in this scenario. The main concern here is maintaining Compute Engine VMs, not converting them to serverless instances. Moreover, changing the infrastructure to Google App Engine might add unnecessary redevelopment costs.

Option C - Creating a Cloud Datastore instance in us-central1-b and setting up replication between two instances focuses on datastore redundancy instead of maintaining operations during a Compute Engine zone failure. Although data replication is crucial, this option does not address the main concern, which is ensuring the availability of Compute Engine VMs.

Thus, option D is the best strategy for ensuring continued operation in case of a single Compute Engine zone failure while keeping costs to a minimum.

Solution to Question 5: C

The correct answer is C, to modify the existing subnet range to 172.16.20.0/24. Here's the explanation of why this is the most efficient solution and why the other options will not work as efficiently:

A. Creating a new VPC network with a subnet of 172.32.0.0/16 and enabling VPC network peering, as well as configuring a custom route exchange, will create connectivity between the two networks. However, this option requires more steps - creating a new VPC, setting up peering, and configuring route exchange - than simply modifying the existing subnet range.

B. Creating a new VPC network with a subnet of 172.16.20.64/26 and enabling VPC network peering, as well as configuring a custom route exchange, will also create connectivity between the two networks. However, this option still involves more steps than modifying the existing subnet range. Additionally, choosing a subnet with this range may cause IP address overlaps and conflicts since the current subnet range 172.16.20.128/25 is already part of 172.16.20.0/24.

C. Modifying the existing subnet range to 172.16.20.0/24 allows the addition of VMs within the existing VPC network with less complexity. By widening the

subnet range, more private IP addresses become available for use without creating a new VPC network or establishing additional configurations like peering or route exchanges. This option is the most efficient because it requires only one step: modifying the existing subnet range.

D. Configuring a VPN between the existing VPC network and a new VPC network involves creating a new VPC, setting up a VPN, and configuring a new subnetwork for the VMs. This option involves more steps and complexity as compared to option C, which only requires modifying the existing subnet range.

Given these explanations, the most efficient solution is option C, to modify the existing subnet range to 172.16.20.0/24, as it allows the addition of new VMs with the fewest number of steps.

Solution to Question 6: A

The correct answer is A: Create a health check on port 443 and use that when creating the Managed Instance Group.

Explanation for why A is the correct answer: As a cloud engineer, your goal is to set up an autoscaling managed instance group for a secure web application that uses HTTPS and ensure that unhealthy VMs are automatically recreated. HTTPS uses port 443, so creating a health check specifically for port 443 is essential to monitor the health of the VMs in the group. Using this custom health check when creating the Managed Instance Group will allow the system to detect and replace unhealthy VMs automatically.

Explanation for why other options do not work:

B. In the Managed Instance Group configuration, set the target utilization to 100%: Setting the target utilization to 100% is not a good option. Target utilization is the percentage of CPU, memory, or other resources that your instances must maintain for scaling up or down automatically. Setting this value too high will result in slow scaling and can cause performance issues. It does not address the problem of unhealthy VMs.

C. Select Multi-Zone instead of Single-Zone when creating the Managed Instance Group: While choosing Multi-Zone can improve availability and fault tolerance, it does not directly address the problem of detecting and replacing unhealthy VMs. Multi-Zone can be a good choice for redundancy and high availability, but it does not solve the question's requirements.

D. Use the default health check for network load balancing when creating the Managed Instance Group: The default health check for network load balancing will not be sufficient for the requirements as it does not monitor the specific port required (443) for the secure web application (HTTPS). Using this default health check will not accurately detect unhealthy VMs, leading to potential issues.

So, the best option is A: Create a health check on port 443 and use that when creating the Managed Instance Group. This custom health check will ensure that

unhealthy VMs running the secure web application are automatically recreated based on the health check at port 443 for HTTPS traffic.

Solution to Question 7: A

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

The reason for choosing option A is that it allows you to get an accurate estimate of the cost without actually running the query. With a dry run query, you can understand the number of bytes read by the query, which is the main factor affecting the cost in an on-demand pricing model. After obtaining the bytes estimate, using the Pricing Calculator helps to convert that information into a monetary value, giving you the total expense of running the said query.

Option B is not the right choice because running the query in multiple parts does not provide any information about estimating the cost of the query upfront. Besides, breaking a query into smaller parts may lead to inefficiencies, and this approach does not guarantee any cost savings.

Option C is incorrect because Data Studio is used for data visualization and reporting purposes, and does not provide features to estimate the cost of running a query in BigQuery.

Lastly, option D is wrong because the BigQuery UI does not have a built-in function to estimate the cost without running the query. While you can use the UI to view previous query costs and history, it cannot accurately estimate the cost of a new query without executing it. Dry run with the command line is the most accurate way to estimate query cost without running it.

Solution to Question 8: A

The most appropriate action that should be taken is option A: Upload the data to Cloud Storage using the gcloud storage command.

Explanation for choosing option A: Cloud Storage is designed for managing unstructured data and supporting various file formats. It is the ideal choice for storing large volumes of data as it provides a scalable and cost-effective solution. Additionally, Dataflow, which is the tool you intend to use for processing, directly integrates with Cloud Storage. This makes it easy to access data stored in Cloud Storage and perform ETL transformations using Dataflow jobs, matching the requirements of the given task.

Reasons why other options will not work:

Option B: Uploading the data to Bigtable using the gcloud bigtable command. Bigtable is a managed NoSQL database service designed for large analytical and operational workloads. It might not be the best choice for handling unstructured data, as it requires a predefined schema and may not be as flexible as Cloud

Storage in terms of scalability and cost. Moreover, Bigtable is not built for easy integration with Dataflow, which is the desired processing tool for this task.

Option C: Uploading the data to Datastore using the gcloud datastore command. Datastore is another managed NoSQL database service, specifically designed for web and mobile applications. Just like Bigtable, Datastore requires the data to have a schema, which is not suitable for unstructured data. Furthermore, it is not designed for handling massive amounts of data and large-scale ETL transformations needed for this task. Datastore is not directly integrated with Dataflow, making it less suitable for this scenario than Cloud Storage.

Option D: Uploading the data to Cloud Functions using the gcloud functions deploy command. Cloud Functions is a serverless execution environment for running event-driven code in the cloud. It is not a data storage service, and therefore, it is not appropriate for the task of storing and handling unstructured data. Additionally, Cloud Functions cannot directly process data using Dataflow jobs since it is primarily designed to execute specific functions triggered by events, rather than handling large-scale data processing tasks.

Solution to Question 9: B

The correct answer to this question is B - stream data to Pub/Sub and use Dataflow to send data to Cloud Storage. Here's why:

A. Streaming data to IoT Core and using Cloud Functions to send data to Bigtable would not be the best approach, as Bigtable is designed for high throughput and low-latency storage. While it works well for real-time data, a data lake solution should consist of cost-effective and scalable storage, which is not the primary focus of Bigtable. Additionally, Cloud Functions might not be a diverse enough tool for complex and large-scale data processing required in IoT applications.

B. Streaming data to Pub/Sub and using Dataflow to send data to Cloud Storage is the best approach because it checks all the necessary requirements for an IoT data lake solution. Pub/Sub ensures reliable, real-time, and high-volume data ingestion from connected IoT devices. Dataflow simplifies data processing by providing an extensible and auto-scalable solution that can handle structured and unstructured data. Finally, Cloud Storage provides cost-effective, scalable, and resilient storage for various data types, making it an ideal choice for a data lake solution.

C. Streaming data to Dataflow and using Dataprep by Trifacta to send data to Bigtable is not the preferred approach, as Dataprep by Trifacta is mainly used for data preparation, transformation, and cleaning. While it can work with Dataflow, it introduces unnecessary complexity in the process, and as mentioned earlier, Bigtable is not the best choice for a data lake storage solution.

D. Streaming data to Dataflow and using Dataprep by Trifacta to send data to Cloud Storage may work, but it is not as efficient as using Pub/Sub and Dataflow. As mentioned earlier, Dataprep by Trifacta is an additional tool that

might not be needed for large-scale, real-time data ingestion and processing. Pub/Sub is a better solution for streaming data due to its high reliability and scalability.

Solution to Question 10: C

The correct answer is C. Enable Data Access audit logs for the Cloud Storage API.

Explanation:

Data Access audit logs are designed to capture all API calls that access the stored data in your Cloud Storage bucket and record them. By enabling these logs for the Cloud Storage API, you will be able to keep track of all requests that access the sensitive information in the bucket, ensuring compliance with the industry regulations and legal obligations.

Incorrect options:

A. Enabling the Identity Aware Proxy (IAP) API on the project is not the right solution in this scenario. IAP is mainly used to control access to your applications and resources running on the Google Cloud Platform, but it does not provide the required data access logging functionality for compliance purposes.

B. Activating VPC Service Controls around the bucket is useful for protecting the data from unauthorized access and for creating a perimeter around the sensitive data in your Cloud Storage bucket. This option tightens the security to protect the resources but does not record data access requests, which is necessary for compliance in this case.

D. Enabling the Security Command Center (SCC) service helps your organization to monitor, detect, and respond to security threats. While it provides insights into the security posture of your Google Cloud assets, it does not specifically record all requests accessing the stored data in the Cloud Storage bucket as required for compliance with industry regulations and legal obligations in this scenario.

Solution to Question 11: B

The correct answer is B. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

Reasoning:

Option A is incorrect because creating a Service Account in your project and asking the partner to grant access to App Engine wouldn't fulfill the requirement of providing access to your BigQuery dataset. App Engine is a separate service and irrelevant to the data warehousing objective in this scenario.

Option B is the correct approach as it allows the partner to create a Service Account in their project, and you can then grant their Service Account access

to the specific BigQuery dataset in your project. This approach follows the principle of least privilege, ensuring that the partner only gets access to the required resources without exposing other information in your project.

Option C is incorrect because creating a Service Account in your project and granting access to Compute Engine is not related to providing access to your BigQuery dataset. Compute Engine is a service for running virtual machines and does not constitute data access to BigQuery.

Option D is incorrect because asking the partner to create a Service Account in their project and giving their Service Account access to BigQuery in their project would not facilitate access to your BigQuery dataset in your project. The partner needs access to your dataset, not their own, to integrate their recommendation engine with your existing system.

Solution to Question 12: C

The correct answer is C. Use gcloud to expand the IP range of the current subnet.

Here's why the other options will not work:

A. Changing the subnet mask of the existing subnet to 255.255.255.224 will increase the number of available IP addresses in the subnet, but it would not necessarily accommodate the 10 additional IP addresses without readdressing some of the existing VMs, which can lead to potential downtime and additional complexity.

B. Upgrading the VMs to larger machine types will not increase the number of available IP addresses in the subnet. This option is related to the performance and resources allocated to individual VMs rather than the IP address space of the subnet.

D. Creating a new subnet with the same IP range but in a different region, and using VPC Network Peering will allow the new VMs to communicate with the existing VMs in the original subnet, but this solution is more complex and less efficient than simply expanding the IP range in the current subnet. Furthermore, using the same IP range in two different subnets, even in different regions, is not a best practice and can lead to potential routing issues.

Thus, the best solution is to use gcloud to expand the IP range of the current subnet, which would accommodate the 10 additional IP addresses required for new VMs and ensure they can communicate with the existing VMs without any additional routing complexity.

Solution to Question 13: D

The correct answer is D: Grant them the required IAM roles using their G Suite email address.

Explanation: Identity and Access Management (IAM) is Google Cloud Platform's way of managing access to resources and services. IAM allows you to

manage access control by defining roles and assigning them to users or groups. In this case, you have G Suite users that need access to your project. The appropriate method to grant them access is by assigning the required IAM roles using their G Suite email address. This allows the users to access the necessary resources through their existing G Suite accounts.

Reasons why other options will not work:

A. Create an IAM role and assign it to a Google Group, then manually add each G Suite user's email address to the group.

This option is incorrect because it adds unnecessary overhead in managing permissions. Creating a Google Group for this purpose might be useful in certain scenarios when managing access for multiple users across various projects. However, it is not the most efficient solution in this case, as you can directly assign IAM roles to G Suite users without creating a Google Group.

B. Use the Cloud SDK to create a new user role and assign it to each G Suite user's email address.

This option is unnecessary as there is no need to create a new role. IAM already offers pre-defined roles that can be assigned to users, such as Viewer, Editor, or Owner roles. Instead of creating a new role, it's better to use these existing roles to grant access. Additionally, this option does not mention that role assignment takes place within IAM, and the Cloud SDK's purpose is for administrating and managing cloud resources rather than user roles directly.

C. Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.

This option is incorrect because it involves creating separate Google Cloud Platform accounts for the G Suite users, which is unnecessary. They can access resources using their existing G Suite accounts by assigning them IAM roles. Using a CSV sheet and the gcloud command line tool to create new accounts results in extra, undesired steps and account management complications.

Solution to Question 14: D

The correct answer is D. Provision Compute Engine instances with M1 machine type.

Here's why:

A. Provision Compute Engine instances with T2 machine type will not work because T2 machine types are designed for general-purpose workloads and do not provide the high memory capacity required for an in-memory database. These instances typically offer a cost-effective solution for variable workloads but are not optimized for high data access scenarios such as those demanded by an ERP system.

B. Using a Cloud Spanner instance for in-memory database handling is not appropriate because Cloud Spanner is a fully managed, globally scalable relational

database service, which does not inherently offer in-memory database capabilities. While it is designed for high availability, strong consistency, and low latency, it is not optimized for holding an entire database in-memory.

C. Using Cloud Functions with high memory configurations is not suitable because Cloud Functions are designed for event-based, serverless workloads and are not meant for holding in-memory databases. They are triggered by events and have short execution times, so they are not ideal for a resource-intensive application like an ERP system that requires sustained performance and high memory capacity.

D. Provisioning Compute Engine instances with M1 machine type is the most appropriate resource configuration for this application because M1 machine types are specifically designed for memory-intensive workloads, such as holding large databases in-memory, offering higher memory capacity and better performance, which is a requirement for an ERP system. Additionally, M1 instances can be scaled up or down depending on the demand, providing both computational power and flexibility necessary for a large manufacturing company's ERP deployment.

Solution to Question 15: A

The correct answer is A: Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Explanation for why the answer is A:

Uploading the Docker image to the Container Registry allows it to be stored, managed, and securely accessed in a centralized place. Google Kubernetes Engine (GKE) natively integrates with the Container Registry, which helps in seamlessly deploying the container images. Creating a Kubernetes Deployment allows for easy management and scaling of the application based on the Docker image. It defines the desired state of the application and automates deploying and managing the containers. Therefore, option A is the most appropriate course of action to deploy the Docker image as a workload on GKE.

Why other options will not work:

B: Uploading the image to Container Registry is correct, but creating a StatefulSet is not the appropriate action in most scenarios. StatefulSets are meant for applications requiring stable network identifiers and persistent storage. However, the question does not indicate that these specific requirements are necessary for the given application. A regular Deployment scales better and caters to non-persistent scenarios, making it more suited in a general scenario.

C: Uploading the image to Firestore is not the right choice, as Firestore is a NoSQL database, not a container registry. In addition, creating a Kubernetes Service is not enough for deploying the container images as you also need to define the desired state of the application using a Deployment or StatefulSet.

D: Uploading the image to Compute Engine is incorrect, as Compute Engine is an Infrastructure as a Service (IaaS) offering, not a container registry. It is primarily used for running virtual machines and not meant for handling Docker images. Therefore, uploading the image to Compute Engine and then creating a Kubernetes Deployment would not work for deploying the Docker image on GKE.

Solution to Question 16: D

The correct answer is D. Add the users to a group, and add this group to roles/browser.

Explanation:

A. This option is incorrect because adding the users to a group with the roles/iam.roleViewer role will grant the users access to view roles in the IAM system, but it does not provide limited access specifically to the hierarchy of your Google Cloud organization's folders and projects.

B. While creating a custom IAM role might be a feasible option, it is not the recommended best practice in this case as it can lead to complex and time-consuming management processes. The predefined roles, like roles/browser, are designed to provide fine-grained access controls suitable for most use cases.

C. This option is incorrect because adding the users to roles/cloudtrace.agent role will grant the users access to write trace data for applications but does not provide limited access to the hierarchy of your Google Cloud organization's folders and projects.

D. This is the correct answer because it adheres to Google's best practice of using groups for managing access to resources. By adding the users to a group and adding this group to roles/browser role, you are granting the users the ability to list and browse the resources in your Google Cloud organization (e.g., folders and projects) in a limited manner. This approach ensures that selected team members have the required visibility with appropriate access control, without granting unnecessary permissions.

Solution to Question 17: B

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

Explanation: In this scenario, you need to ensure that the Compute Engine instances have the ability to write data into a specific Cloud Storage bucket while following Google's recommended practices.

Option A is incorrect because the 'serviceAccount-tokenCreator' role is used for creating OAuth2 access tokens on behalf of a user. This role does not provide write access to the Cloud Storage bucket.

Option B is correct because the 'storage.objectCreator' role is the recommended practice for allowing the service account to write data into the Cloud Storage

bucket. This role grants the minimal permissions needed for the task, adhering to the principle of least privilege.

Option C is incorrect because the access scope 'https://www.googleapis.com/auth/compute.read' would only provide read access to Compute Engine resources. This does not provide the required write access to the Cloud Storage bucket.

Option D is incorrect because the 'compute.admin' role grants full administrative access to Compute Engine resources, which is not necessary for the task. The instances only need the ability to write data to a specific Cloud Storage bucket, so this role would provide excessive permissions, violating the principle of least privilege.

In conclusion, the best approach for this task is to create a service account and add it to the IAM role 'storage.objectCreator' for that bucket, following Option B.

Solution to Question 18: A

The correct answer is A, as it is the most accurate, systematic, and reliable method for estimating monthly total costs for a solution using multiple Google Cloud products.

A: By reviewing the pricing details on each product's pricing page and using the pricing calculator, you are ensuring that you have the most up-to-date and accurate information regarding the Google Cloud services included in your solution. This helps to provide a precise estimate of monthly costs, which is essential for a cost estimation report. The pricing calculator takes into consideration various parameters like resource usage, location, and other factors to provide a comprehensive view of the estimated costs.

B: Relying on manual calculations and intuition, rather than using the dedicated pricing calculator, introduces a high risk of error into the estimation process. Due to the complex nature of cloud services and the different factors that can affect costs, manually reviewing the pricing page will not provide a detailed, accurate estimate. This may lead to inconsistencies, misjudgements, and potential budgeting issues for the company.

C: Although provisioning the solution on Google Cloud for a week and using Cloud Monitoring to determine used resource amounts sounds like a practical idea, it is not the most efficient method for generating a cost estimation report. You might end up spending additional resources and time to set up the solution on Google Cloud. Moreover, one week may not be long enough to cover the different usage patterns and fluctuations that occur throughout a month, which might lead to inaccurate monthly cost estimations.

D: Similar to option C, provisioning the solution on Google Cloud for a week and using the Billing Report page in the Cloud Console to determine the monthly cost may seem like a good approach. However, it is not efficient, as it requires additional resources and time for setup. Furthermore, basing the entire monthly

costs on just one week's cost might not fully capture variations in usage or service consumption throughout the month, resulting in inaccurate estimations.

To summarize, option A is the best approach for creating a cost estimation report for a solution using multiple Google Cloud products, as it provides the most accurate, systematic, and comprehensive estimate of the monthly total costs. The other options may result in errors, inefficiencies, or inaccurate estimations that could negatively impact the project and the company's budget.

Solution to Question 19: D

The best solution to implement in this scenario would be option D: Configure an External Network load balancer in front of the application servers.

An External Network load balancer is the most suitable solution because it works at the transport layer (Layer 4) of the OSI model and delivers UDP traffic, which is the type of traffic that the multiplayer mobile game generates. Having a single IP address for the VMs allows the gaming backend to scale horizontally and handle a higher load while providing smooth gameplay experience to the users. An External Network load balancer distributes traffic evenly across the VMs, reducing the latency and ensuring that the application servers remain available during high-traffic times.

Option A: Configure an SSL Proxy load balancer in front of the application servers is not the most suitable solution because SSL Proxy load balancers work with SSL/TLS traffic and focus on HTTPS applications. Our scenario involves a mobile game with UDP traffic, and hence, SSL Proxy load balancer wouldn't be effective.

Option B: Utilize VPC peering for load balancing between VMs is not a suitable solution because VPC peering is a way to connect two Virtual Private Cloud (VPC) networks for sharing resources and routing traffic directly between them using their internal IP addresses. It is not a load balancing solution, and therefore, it doesn't address the requirements of exposing multiple VMs using a single IP address for the gaming backend.

Option C: Configure an External HTTP(s) load balancer in front of the application servers is not a suitable solution because an HTTP(s) load balancer is designed to balance traffic for HTTP and HTTPS services, operating at the application layer (Layer 7) of the OSI model. Since the multiplayer mobile game is sending UDP packets, an HTTP(s) load balancer would not be effective in distributing the traffic.

In conclusion, option D is the best solution for ensuring an optimized multiplayer mobile game on the Google Cloud platform, as it effectively exposes the VMs through a single IP address and effectively manages the delivery of UDP traffic generated by the game.

Solution to Question 20: A

The recommended course of action in this situation is Option A: Install and configure the Ops agent and view the logs from Cloud Logging.

Option A is the correct choice for the following reasons:

1. The Ops agent is designed specifically for monitoring, logging, and troubleshooting applications running on Google Cloud Platform. It consolidates logs and metrics, making it easier to identify and diagnose problems.
2. The Cloud Logging service is integrated with Compute Engine and provides centralized log management, allowing you to view, search, and analyze the logs from the application along with other cloud resources across your project.
3. Installing and configuring the Ops agent is a relatively simple process that does not require significant infrastructure changes or costs.

The other options are not appropriate for the following reasons:

Option B: Setting up a VPN connection between the instance and your local workstation to access the logs is not ideal because it requires additional setup and maintenance work, and it is less secure than using a cloud-native logging solution. Moreover, this approach does not provide centralized log management or the ability to analyze logs alongside other cloud resources.

Option C: Creating a new Google Kubernetes Engine cluster and migrating the application there is not an efficient solution to troubleshoot the error reports from users. This option would involve significant time, effort, and costs, and there is no guarantee that the problem would be resolved by moving the application to a new environment.

Option D: Using Cloud Pub/Sub to push error logs from the application to a subscriber is not the most appropriate solution for diagnosing the problem. While Cloud Pub/Sub is well-suited for real-time message processing and data streaming, it is not designed specifically for centralized log management, monitoring, or troubleshooting. Cloud Logging provides better tools for handling and analyzing logs in this context.

Solution to Question 21: B

The correct answer is B. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

Option B is the best solution because it allows you to query the billing data with a high level of granularity and isolate the egress network costs specifically related to the Apache web server. By exporting the billing data to BigQuery, you can write a query to sum the egress network costs for the current month and compare them to the desired threshold of 100 dollars. A Cloud Function can be created to run this query and send an email if the threshold is exceeded. Using Cloud

Scheduler to run the Cloud Function hourly ensures that you are constantly monitoring the egress costs and are alerted promptly when the threshold is met.

Option A, setting up a budget alert on the Compute Engine instances, would only work if you wanted to track costs associated with all usage types within the Compute Engine instances, not specifically the egress network costs.

Option C, using Google Cloud Pub/Sub to create a notification channel for egress costs, is not a suitable solution because there is no direct built-in way to monitor egress costs and trigger a Pub/Sub message when the costs exceed a certain amount. This method would require manual intervention or an additional monitoring mechanism, defeating the purpose of automated alerts.

Option D, setting up a budget alert on the billing account, would encompass all costs associated with the entire billing account, including costs from other services within the project. This would not allow for a specific focus on the egress network costs related to the Apache web server.

Solution to Question 22: A

The most suitable cloud-based database solution for this scenario is option A: Cloud SQL. The reasons for choosing Cloud SQL and not the other options are as follows:

A. Cloud SQL: Cloud SQL is a fully managed relational database service for MySQL, PostgreSQL, and SQL Server that provides robust consistency, swift query processing, and adheres to ACID principles. Since the application was initially developed using PostgreSQL, migrating to Cloud SQL requires minimal code modifications. Additionally, it offers excellent support for multi-table transaction updates and is suitable for internal applications, making it the ideal choice for your company's e-commerce department.

B. Cloud Datastore: Cloud Datastore is a NoSQL database designed for scalability and flexibility. While it can handle large amounts of data and is suited for applications with high read and write workloads, it does not inherently support the same level of consistency, ACID compliance, and relational data management as PostgreSQL or Cloud SQL. Migrating the application to Cloud Datastore would require significant code changes and may not provide the desired consistency and transaction management features.

C. BigQuery: BigQuery is a data warehousing and analytics solution optimized for handling large quantities of data and performing complex queries on them. However, it is not a relational database and does not adhere to ACID principles nor supports multi-table transactions. BigQuery is primarily intended for analytical purposes, not for managing transactional orders across warehouses as required in this scenario.

D. Datastream: Datastream is a serverless, real-time data change capture and replication service that allows you to synchronize and transfer data between

databases, storage systems, and applications. It is not a standalone database solution but rather a tool to help with data integration and migration tasks. Migrating the application to Datastream would not meet the consistency, transaction management, and relational data requirements.

In conclusion, Cloud SQL is the most suitable option for your needs due to its compatibility with PostgreSQL, ACID compliance, robust consistency, swift query processing, and support for multi-table transaction updates.

Solution to Question 23: C

The correct answer is C because it provides the most precise way to grant the necessary permissions to the external team member following Google's best practices. By creating a custom role and including only the required permissions (compute.disks.list and compute.images.list) as includedPermissions, you are granting the least amount of privilege needed for the team member to perform their task without compromising security or violating the principle of least privilege.

Option A, creating a custom role based on the Compute Storage Admin role and excluding unnecessary permissions, will not be the best choice because the Compute Storage Admin role contains many unnecessary permissions beyond just listing compute images and disks. This could result in a complex custom role and increase the risk of granting unnecessary access.

Option B, creating a custom role based on the Compute Storage Admin role without excluding any permissions, is clearly not the best practice. This action would grant the user more permissions than necessary, violating the principle of least privilege and potentially compromising project security.

Option D, creating a custom role based on the Compute Image User role and adding the compute.disks.list permission is also not the best approach because the Compute Image User role doesn't inherently provide the compute.disks.list permission. Although adding the permission manually would grant the necessary access, it is better to create a custom role from scratch (as in option C) to ensure only the required permissions are granted, maintaining adherence to Google's recommended practices.

Solution to Question 24: A

The correct answer is A: Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

Explanation: When there is a failure in creating new instances, it is crucial to ensure that the instance template being used is correct, and any conflicts with resources like persistent disks are resolved. Option A suggests starting by creating an instance template with valid syntax, and then deleting any persistent disks with the same name as instance names to avoid conflicts. This approach tackles both the possible issues with the instance template and persistent disks.

Option B is incorrect because, although it does involve verifying the instance template syntax and deleting persistent disks with the same name as instance names, it also suggests setting the disks.autoDelete property to true. This action is unrelated to the issue in question and is unnecessary in resolving the instance creation failure.

Option C is incorrect because it only suggests creating an instance template and deleting any firewall rules that might be responsible for instance creation issues. While creating a valid instance template is correct, deleting firewall rules isn't the appropriate action, as firewall rules don't have any direct impact on instance creation in a managed instance group, and doing so could compromise security.

Option D is incorrect because it only suggests creating an instance template and adding it to an existing instance group. While this action is essential, it does not address the potential conflict from persistent disks with the same name as instance names. The incomplete solution may not resolve the instance creation failure entirely, making it an ineffective approach compared to Option A.

Solution to Question 25: C

The correct answer is C: Enable parallel composite uploads using gsutil on the file transfer.

Explanation:

To maximize the usage of the available 1 Gbps speed and transfer the 32 GB file as quickly as possible, it is essential to use the most efficient method of uploading the data. Parallel composite uploads using gsutil allow the large file to be divided into smaller chunks which can be uploaded concurrently, taking full advantage of the available bandwidth.

Here's an explanation for why other options will not work:

A. Increasing the latency on the machine initiating the transfer: Increasing latency would actually slow down the data transfer process. Lower latency allows for faster data transmission, so this option is counterproductive and will not help maximize the usage of the available 1 Gbps speed.

B. Disabling resumable uploads in gsutil: Resumable uploads are designed to continue an interrupted file transfer from where it left off, saving time and bandwidth. Disabling this feature would not improve the transfer speed and would not be beneficial in the case of a 32 GB file, since it increases the risk of having to restart the entire transfer process if the connection is disrupted.

D. Running multiple instances of gsutil in parallel without using composite uploads: Although this might increase file transfer speed in some cases, it could also lead to increased contention and inefficiencies resulting from independently managing multiple file transfers simultaneously, which will not significantly contribute to maximizing the usage of the available 1 Gbps speed limit. Parallel composite uploads, on the other hand, divide the file into smaller parts and

upload them concurrently using a single instance of gsutil, providing a more effective approach for large file transfers.

Solution to Question 26: C

The correct answer is C. Create a budget per project and configure budget alerts on all of these budgets.

Explanation: As a project manager overseeing individual Google Cloud Projects for each developer, your goal is to monitor and control costs on a per-project basis. By creating a separate budget for each project, you can ensure that each developer's expenditure stays within the $500 per month limit. Configuring budget alerts for each budget allows you to receive notifications when a project is close to or exceeding its limit. This granularity enables better cost management on an individual developer level.

Why other options will not work:

A. Configuring a billing notification with a spending threshold of $500 per month on the Organization level would track the overall spending for the organization, not each developer's project. The project manager would not be able to monitor the expenses of each individual project to ensure the required limitations.

B. Enabling VPC Flow Logs to monitor resource consumption in sandbox projects does not provide accurate cost information. VPC Flow Logs are designed to collect IP traffic-related data within the Virtual Private Cloud, not to monitor costs of resources used. Therefore, using VPC Flow Logs for cost management would not be efficient or reliable in this scenario.

D. Creating a single budget for all projects and configuring budget alerts on this budget would not provide individual cost control for each developer's project. By aggregating the spend for all projects, the project manager would miss crucial information on budget allocation per project and would not detect if a specific project exceeded the allocated $500 per month.

Solution to Question 27: C

The correct answer is C, to create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable, and use the BigQuery console to join these tables through user fields, applying appropriate filters. This option is the best solution for ad hoc requests that require merging data from Cloud Spanner and Cloud Bigtable as it provides a more efficient and cost-effective approach for merging data from two separate sources. By leveraging BigQuery's ability to query external tables and join the data, you can use SQL-like syntax to easily specify which users you need to merge the data for.

Option A is not suitable for this task as using Cloud Data Fusion to create a pipeline that reads data from Cloud Spanner and Cloud Bigtable is more suited for larger and continuous data integration processes, rather than ad hoc requests. This option adds an extra layer that might not be needed for a single request.

Option B is not ideal for ad hoc requests either because creating a Cloud Dataproc cluster that runs a Spark job to extract data from Cloud Spanner and Cloud Bigtable for specific users may be overkill. This approach would require spinning up additional resources and incurring costs that aren't necessary for the specific task. Additionally, this process would be more time-consuming as compared to using BigQuery external tables.

Option D is incorrect as a dataflow job that copies data from Cloud Bigtable and Cloud Storage for specific users would not efficiently merge the data. Instead, it would duplicate the data and lead to higher costs and increased processing time without providing the desired outcome.

In conclusion, the most efficient way to merge data from Cloud Spanner and Cloud Bigtable for specific users on an ad hoc request is option C, by using BigQuery external tables to join and filter the data based on user fields.

Solution to Question 28: A

The correct answer is A: Create a custom role by removing delete permissions, add users to the group, and then add the group to the custom role.

Explanation for A: Creating a custom role by removing delete permissions allows you to specifically grant your colleagues access to query datasets in BigQuery without giving them the ability to accidentally delete the datasets. This aligns with Google's recommended practices as it ensures you have full control over the permissions granted to your colleagues, thereby minimizing the risk of data loss.

B: Data Loss Prevention (DLP) is primarily used for detecting and preventing sensitive information from being exposed but does not control user access or permissions on the datasets. It doesn't provide a solution to the specific problem of granting query permissions while preventing the delete operation for your colleagues.

C: The roles/bigquery dataEditor role allows users to edit data and run queries but also grants them the ability to delete datasets, which is not what we want. By adding users only to this role, they would still have the ability to accidentally delete datasets, which goes against the purpose expressed in the question.

D: The roles/storage.objectViewer role only grants users the ability to view objects within Google Cloud Storage rather than controlling permissions on BigQuery datasets. This role will not help you grant your colleagues the appropriate access to query datasets in BigQuery without giving them the ability to accidentally delete those datasets.

Solution to Question 29: C

The correct answer is C. Enable Cloud IAP (Identity-Aware Proxy) for the Compute Engine instances and add the operations partner as a Cloud IAP Tunnel User. This is because Cloud IAP provides a secure way to manage access to your applications running on Compute Engine instances. By using

Cloud IAP, you can easily grant access to your external operations partner without the need for them to have a Google Account. Instead, they can use their existing identity for authentication. With Cloud IAP, you can control access to your applications using IAM (Identity and Access Management).

Option A, configuring a Google Cloud Pub/Sub topic to allow the operations partner to send and receive messages related to instance maintenance, is incorrect because Pub/Sub is a messaging service and is not designed for managing or providing access directly to Compute Engine instances.

Option B, implementing a dedicated Shared VPC and providing the operations partner with access to the subnets of the instances, is incorrect as well. While Shared VPC is intended for sharing network resources, this solution does not grant the required access to maintain the installed tooling on the Compute Engine instances. It only provides network access, which is insufficient for the given task.

Option D, enabling Cloud NAT and granting the operations partner access to the Cloud NAT gateway to allow traffic redirection, is incorrect because Cloud NAT is used for configuring Network Address Translation for outbound traffic from instances. It does not provide a means for granting external users access to maintain the installed tooling on those instances.

Hence, the most appropriate and effective solution for this scenario is Option C, enabling Cloud IAP for Compute Engine instances and adding the operations partner as a Cloud IAP Tunnel User.

Solution to Question 30: B

The correct answer is B, as it follows the Google-recommended practices for deploying a new instance in a different region while ensuring access to the existing application. Here's the explanation:

In option B, you start by creating a subnetwork in the same VPC but in the europe-west1 region. This is aligned with the goal of deploying a new instance in a different region but within the same project. Then, you create the new instance in the new subnetwork and use the first instance's private address as the endpoint. This allows the instances to communicate within the same VPC securely, without exposing the application to the public.

Option A is incorrect because it suggests setting up an instance group with only the new instance. Instance groups are typically used for load balancing and auto-scaling, which doesn't appear to be necessary for this task. Furthermore, using an instance group could unnecessarily complicate the deployment process.

Option C is not ideal because it proposes enabling global routing in the VPC, which is not necessary in this case. Inter-region communication can be achieved without enabling global routing. Enabling global routing could introduce potential security risks and is not a Google-recommended practice unless it is required for a specific use case.

Option D is not the best choice because it suggests creating an entirely new VPC and peering the two VPCs. While VPC peering can be used for connecting resources, it adds complexity and management overhead without providing a clear benefit for this task. Using a single VPC with multiple subnetworks is more in line with Google-recommended practices and simplifies the deployment process.

In conclusion, option B is the best choice as it adheres to Google-recommended practices, ensures efficient inter-region communication, and avoids unnecessary complexity.

Solution to Question 31: C

The correct answer is C: Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

The reasons why option C is the best course of action are:

1. The role requires permissions suitable for production. Using 'supported' support level for role permissions ensures that the permissions are stable and recommended for production use. Options A and B are not suitable because 'preview' and 'testing' support levels for role permissions are meant for evaluation and may not be suitable for production use.

2. The role needs to communicate the custom role version status clearly within the organization. Setting the role stage to ALPHA during testing allows the company to ensure that the role is still under development and may require changes. Once the role is ready for production, the role stage can be updated to GA, which means "General Availability" and indicates that the role is stable and suitable for production use. Option D is not suitable because setting the role stage to GA during testing may mislead the organization into thinking that the role is stable and ready for use when it is still under development.

Options A and B are not suitable because they use the 'preview' and 'testing' support levels for role permissions, which are not recommended for production use. By choosing the 'supported' support level, the team ensures that the role permissions are reliable and suitable for deployment in a production environment.

In conclusion, option C is the best course of action because it uses the 'supported' support level for role permissions and sets the role stage to ALPHA during testing. This combination ensures that the custom IAM role is suitable for production, and the role stage reflects its development status, allowing for clear communication within the organization.

Solution to Question 32: D

The correct answer is D. Deployment Manager.

Let us explain why other options are not suitable and why the Deployment Manager is the perfect choice.

A. Bigtable: Google Cloud Bigtable is a NoSQL database service used for big data projects. It provides a managed data storage solution with real-time data processing capabilities, but it does not supply a service for provisioning VMs. Thus, using Bigtable to provision VMs would not be practical or relevant to the task.

B. Managed Instance Group: Though it is a good option for managing VMs and automatically scaling up or down based on load, the Managed Instance Group does not offer a dynamic way to perform provisioning according to the dedicated configuration file mentioned in the task. It focuses mainly on scaling, and redundancy aspects rather than deploying complex configurations.

C. Cloud Composer: This is a fully managed workflow orchestration service built on Apache Airflow, which is used for data pipeline creation and management. While Cloud Composer provides some integration with Google Cloud services, it is not explicitly designed for provisioning VMs on Compute Engine following a dedicated configuration file.

D. Deployment Manager: This is the ideal choice for implementing a dynamic way of provisioning VMs, as it's a Google Cloud infrastructure management service that lets users create, delete, and manage resources in a structured and custom manner. With Deployment Manager, you can utilize a configuration file (based on YAML) to define your infrastructure's resources, properties, and policies. It follows Google's recommended practices, enabling efficient and scalable provisioning of VMs on Compute Engine. By using Deployment Manager, the lead engineer can achieve the exact specifications as required in the configuration file.

In summary, Deployment Manager (Option D) should be used for implementing a dynamic way of provisioning VMs on Compute Engine according to a dedicated configuration file since it fills the requirements and follows Google's recommended practices. Other options are unsuitable for the task as they either serve different needs or do not offer the desired level of configuration and management for VM provisioning.

Solution to Question 33: A

The correct answer is A. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

Here's why:

Option A: The company's data pattern involves writing objects once and accessing them frequently for the first 30 days. Using Standard storage during this period is appropriate, as it provides low latency and high throughput performance for frequently accessed data. After the first 30 days, moving the data to

Archive storage for the next three years is a cost-effective solution, given that the data will generally not be accessed again unless a particular need arises.

Option B: Using Nearline storage for the initial 30 days is not ideal in this scenario, as it is designed for data being accessed less frequently (approximately once a month). Additionally, moving data to Coldline storage for three years may incur higher costs than Archive storage as Coldline is targeted for data accessed less than once per quarter, while Archive is designed for longer-term data retention.

Option C: Coldline storage is not suitable for the initial 30-day period when objects are frequently accessed. This storage class is designed for infrequently accessed data, and it would incur high costs and longer retrieval times. While Archive storage might be appropriate for the three-year retention, this option's overall effectiveness is diminished due to its usage of Coldline storage for the first 30 days.

Option D: Similar to option B, using Nearline storage for the first 30 days is not optimal due to the frequent access requirements. Shifting to Coldline for one year and then to Archive storage for two years adds unnecessary complexity to the lifecycle policy without offering significant cost-saving compared to storing the data in Archive storage directly after the first 30 days.

In conclusion, the answer should be A, as it meets the company's needs for frequent access during the first 30 days (Standard storage) and cost-effective retention for the following three years (Archive storage). The other options either do not suit the company's access patterns or do not provide the most cost-effective storage solution.

Solution to Question 34: A

The correct answer is A, as the issue is related to permission issues in a specific project. By opening the Google Cloud console and checking the Identity and Access Management (IAM) roles assigned to the service account at the project, or inherited from the folder or organization levels, you can verify if the appropriate roles are granted to the service account.

Option B is not ideal because using the gcloud CLI to list the permissions assigned to the organization does not specifically target the required project permissions, as well as the roles specifically assigned to the service account in question.

Option C may be helpful in troubleshooting some issues, but in this case, since the problem is permission-related, checking CI/CD server logs wouldn't effectively resolve the problem. Identifying the issue with the service account's roles and permissions should be the priority.

Option D is not suitable for solving this issue, as it involves reviewing resource and service account quotas, which are not directly related to the permission problems the CI/CD server is facing in executing Google Cloud actions.

Hence, the best course of action to verify if the service account being used has the appropriate roles in the particular project is option A: Open the Google Cloud console and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

Solution to Question 35: B

The correct answer is B: Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

Explanation:

Option B adheres to the guidelines of least privilege and separation of duties, both of which are considered best practices for ensuring security and minimizing the risk of unauthorized access. By granting the service account the roles/bigquery.dataViewer role in the crm-databases project, the VMs in the web-applications project will be able to read the BigQuery datasets without having unnecessary permissions. Additionally, giving appropriate roles to the web-applications project allows it to maintain necessary access without being overly permissive.

Why other options will not work:

Option A: Granting "project owner" role to both crm-databases and the web-applications project is not a good practice because it provides excessive access rights to the service account. In doing so, it violates the principle of least privilege and increases the risk of unauthorized access.

Option C: Granting "project owner" role to crm-databases project and roles/bigquery.dataViewer role to web-applications project is not ideal. It still provides excessive rights ("project owner" role) to the crm-databases project, which can create security risks.

Option D: Similar to option A, this choice involves granting "project owner" role to both projects, which allows the service account to have unnecessary permissions, violating the principle of least privilege.

In conclusion, option B is the best choice because it grants appropriate permissions that follow Google-recommended practices while considering security, least privilege, and separation of duties.

Solution to Question 36: B

The correct answer is B, and here's why:

Option B: By setting metadata with enable-oslogin=true, you're enabling OS Login for the instance. This allows for a more streamlined process of managing SSH keys, as it associates the SSH keys directly with the user's Google identity. Granting the dev1 group the compute.osLogin role allows the users in the group to connect to the instance using their Google identity. Using Cloud Shell for

connecting via SSH ensures that users have appropriate access to the instance without any additional setup.

Now let's examine why the other options don't work:

Option A: Enabling block project-wide keys for the instance restricts access only to SSH keys that are explicitly associated with the specific instance. While generating SSH keys for each user and associating them with the instance might work, it is more cumbersome and not as streamlined as using OS Login. Additionally, directing users to use Cloud SDK doesn't guarantee that they will only be able to connect to that specific instance.

Option C: Creating a Cloud Storage bucket and granting the dev1 group the storage.objectAdmin role is irrelevant to the task at hand, as the goal is to configure SSH access to a Compute Engine instance and not manage storage permissions. This approach does not help in enabling SSH access to that instance, so it's not a proper solution.

Option D: Setting metadata to enable-oslogin=true enables OS Login for the instance, which is a correct step. However, setting the service account to "no service account" for that instance does not impact the SSH access required for dev1 group users, and it could potentially create issues with other services that rely on the service account. It's not a correct way to grant the dev1 group SSH access, so this option is also not a suitable solution.

Solution to Question 37: C

The correct answer is C. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Explanation:

A - Storing credentials for your user account in a config file and deploying it with your application violates Google's best practices for credential management. This approach can lead to unauthorized access if your config file is inadvertently exposed. Moreover, it might make your application less scalable and maintainable over time.

B - Creating a new Google account for the VM is not a suitable option because using a user account directly in a VM bypasses the benefits and security features of using a service account. Service accounts are recommended for application authentication as they provide more granular control, IAM permissions, and are not tied to a particular user.

C - Assigning appropriate access for Google services to the service account used by the Compute Engine VM is the best practice for authentication. This method follows Google's recommended guidelines for credential management, provides granular control over permissions, ensures app sustainability and flexibility, and offers the least amount of required changes, as the Application Default Credentials will automatically use the service account of the Compute Engine instance.

D - Manually generating an API key for each Google service and embedding them in your application code is not recommended because it increases the possibility of exposing sensitive information, makes the application less maintainable and scalable, and does not take advantage of the security benefits provided by service accounts.

Solution to Question 38: A

The correct answer is A. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network. The reasoning behind choosing this option is that creating a new VPC network allows you to overcome the lack of available private IP addresses in the existing VPC network. Enabling VPC Peering allows the VMs to communicate with the Dataproc cluster, ensuring that the communication stays within the Google Cloud's infrastructure. VPC Peering also enables low-latency, high-speed communication, which is essential for the data processing tasks of your project.

Option B is not the best choice because creating a VPN tunnel between the existing VPC network and a new VPC network adds overhead to the communication, which may result in slower and less efficient performance. Additionally, setting up a VPN tunnel can be more complex and time-consuming compared to VPC Peering.

Option C won't work because adding a new secondary IP range in the existing VPC would not resolve the issue of no available private IP addresses in the VPC network. The subnet provided still leads to the same limitation.

Option D is not recommended because adding VMs with public IP addresses increases the exposure of your project's resources on the internet. Configuring firewall rules to allow communication between VMs and the rest of the VPC adds extra maintenance and potential security risks.

Solution to Question 39: A

The correct answer is A. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

Here is the explanation for why this is the correct answer:

A: By creating a Kubernetes service of type NodePort, traffic is enabled to flow into the nodes in your cluster. The Kubernetes Ingress object provides rules to manage the traffic from the external world to the NodePort service created earlier. When using Google Kubernetes Engine (GKE) with autoscaling, the Ingress resource also automatically creates a Google Cloud Load Balancer, which will expose your application to the public via HTTPS on a public IP address. This ensures the requested task is achieved.

The other options are not suitable for this task for the following reasons:

B: A Kubernetes Service of type ClusterIP exposes your application within the cluster and assigns a cluster-internal IP. It does not expose the application to access it from the public internet via HTTPS, which is the required task.

C: While configuring a Google Compute Engine (GCE) instance with Nginx as a reverse proxy and connecting it to your GKE cluster might seem like a solution, it introduces unnecessary complexity and manual intervention. It also doesn't take advantage of Kubernetes native resources such as Ingress, which are more suitable for this task.

D: Deploying your application on Google Cloud Functions and using API Gateway would involve shifting from a containerized GKE deployment to a serverless architecture. This solution is not appropriate, given that the requirement is to deploy the application using Google Kubernetes Engine with autoscaling enabled.

Solution to Question 40: A

The answer should be A. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

The reason for choosing option A is that once an App Engine application is created, its serving region cannot be changed. To change the serving region, you need to create a new GCP project and a new App Engine application within it, specifying the desired new region, i.e., asia-northeast1.

Option B will not work because it suggests creating a Cloud Function to proxy requests to the App Engine application. The main purpose of Cloud Functions is to execute small, single-purpose functions in response to specific events. It would not help in changing the serving region of the App Engine application and might add unnecessary latency to application requests.

Option C is not suitable for this scenario because it focuses on creating a new Datastore instance in the desired region, not changing the serving region of the App Engine application. Datastore is a NoSQL database service used for storing data, and the task requires changing the App Engine application's serving region, not its datastore location.

Option D is incorrect because the region property setting of an existing App Engine application cannot be changed directly. A new App Engine application must be created in the desired region, as mentioned in option A.

Solution to Question 41: C

The correct answer is C: Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

Explanation: Setting up Google Cloud resources independently for the Marketing team is crucial to prevent any conflicts or dependencies with the Sales team's resources. Creating a new project specifically for the Marketing team ensures

proper resource organization, isolation, and easier management. It also prevents any potential access or permission issues by keeping the projects separate and easily manageable.

Here's why the other options will not work:

Option A: Creating a new marketing folder under the acme-data-digest project would not provide the desired resource separation. Instead, it would maintain the resources for both teams within a single project, which may lead to dependencies and complications in the long run. Additionally, granting folder editor access does not ensure that the Marketing team's resources would be independent of the Sales team's resources.

Option B: Utilizing Cloud Composer to build a pipeline transferring data from acme-data-digest to the Marketing team's resources doesn't address the need for independent organization of the resources. This approach would establish a dependency between the projects rather than ensuring their independence. It adds extra complexity and has a greater likelihood of leading to permission issues or conflicts between the teams.

Option D: Creating a separate organization for the Marketing team and migrating the acme-data-digest project there is both impractical and unnecessary. It would involve a significant re-organization of company resources and is not needed to achieve the desired separation of the projects. A simple project separation is more efficient in organizing and managing resources for the Marketing team independently of the Sales team.

Solution to Question 42: C

The correct answer is C. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

Explanation:

Option A is incorrect because using gcloud compute instances describe only gives you information about the instance, such as its IP address, system properties, and metadata, but not the username used to access the Windows VM via RDP.

Option B is incorrect because adding metadata to the instance with 'windows-password' as the key and a password as the value is not the recommended method for managing passwords for Windows VMs on Compute Engine. It can lead to security risks.

Option C is the correct answer because using gcloud compute reset-windows-password allows you to create new or reset existing login credentials for the VM. This method ensures secure and safe password management, allowing the IT specialist to provide seamless remote access to the team members.

Option D is incorrect because you cannot use your Google Account credentials to log in to a Windows VM on Google Compute Engine. Google Cloud uses project-level IAM permissions for access control, but you need an individual

Windows account with corresponding login credentials to access the Windows VM via RDP. The gcloud compute reset-windows-password command is used to generate the necessary login credentials.

Solution to Question 43: D

The correct answer is D: Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

Explanation:

In this scenario, you are required to create a new billing account and then link it to an existing GCP project. In order to do this, you need to have the Project Billing Manager role for the existing GCP project.

Option A is incorrect because the objective is to create a new billing account, not a new GCP project. Additionally, linking the new project to the existing billing account does not fulfill the requirement of linking the new billing account to an existing GCP project.

Option B is incorrect because you are supposed to create a new billing account, not a new project. While the Billing Administrator role is required to create or manage billing accounts, this option does not address the requirement of linking the new billing account to the existing GCP project.

Option C is incorrect because this option assumes that there is an existing billing account to link the existing GCP project to, but the task is to create a new billing account before linking it to the project.

Option D is correct because it ensures that you have the Project Billing Manager role for the existing GCP project and follows the required steps of creating a new billing account and linking it to the existing project. This will allow you to properly manage billing for the project through the newly created account.

Solution to Question 44: B

The correct answer is B. When creating the VM, use machine type n1-standard-96.

Explanation:

Option A is not appropriate because the Compute Engine default settings would not provide a VM with 96 vCPUs. Modifying the running instance to have 96 vCPUs may cause interruptions to the production-critical application, making it a less favorable choice.

Option B is the correct choice because it fulfills the requirement of having 96 vCPUs to ensure the application runs optimally on GCP. By directly creating the VM with the n1-standard-96 machine type, you provide a similar environment to the on-premises application without unnecessary adjustments or interruptions.

Option C is not suitable because relying on Rightsizing Recommendations is a slow and iterative process. It is not efficient to start with the default settings and adjust as you go, especially with a production-critical application. This approach may lead to suboptimal performance and disruptions during the migration.

Option D is incorrect because the n1-highmem-32 machine type offers only 32 vCPUs. This option does not meet the requirement of 96 vCPUs for the application, which will result in a less efficient environment compared to the on-premises application.

In conclusion, the best approach is to create the VM using the n1-standard-96 machine type, as it provides the required 96 vCPUs, ensuring the migrated application runs in a similar environment as it was on-premises.

Solution to Question 45: A

The correct answer is A, and here's why:

1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID.

Selecting option A will directly shut down all the configured services in a single action, making it the most efficient choice. Being assigned the Project Owners IAM role ensures that you have the necessary permissions to perform such actions.

Option B is not the best choice because it only involves deleting resources manually one by one, which is both time-consuming and inefficient.

Option C is incorrect because the Organizational Administrator IAM role is not required for this task; the Project Owners IAM role should be sufficient. Furthermore, simply entering the project ID in the GCP console will not allow you to shut down the services, as the option to shut down is missing in this choice.

Option D is also incorrect as it only focuses on deleting storage buckets. The question requires shutting down all configured services, which is not addressed by this option. Additionally, the Storage Administrator IAM role is not relevant to managing all services in the project in any case.

Solution to Question 46: B

The correct answer is B. You should assign the auditor the IAM role roles/logging.privateLogViewer and direct the auditor to also review the logs for changes to Cloud IAM policy. This is because the roles/logging.privateLogViewer role grants the necessary permissions to view Audit Logs and Data Access logs while adhering to the security principle of least privilege. In addition, asking the auditor to review logs for changes to Cloud IAM policy is a good practice to ensure that they have all the necessary information for a complete audit.

Option A is incorrect because roles/pubsub.editor is designed to manage Pub/Sub resources, which is not relevant to the task of giving the external auditor access to GCP Audit Logs and Data Access logs. Exporting logs to Cloud Storage is also unnecessary when the auditor has the appropriate role to view the logs directly on GCP.

Option C is incorrect for a couple of reasons. First, using a custom role would make it harder for the security analyst to maintain strict control over permissions and ensure that the auditor has only the necessary privileges. Second, roles/storage.objectViewer is an extra permission that the auditor does not need to fulfill their task, since they can access the required logs with the roles/logging.privateLogViewer role.

Option D is incorrect because roles/storage.admin grants excessive permissions to the external auditor, violating the principle of least privilege. The auditor only needs the roles/logging.privateLogViewer role for their task, and there is no need to export logs to Cloud Storage for the auditor's review.

In summary, the answer should be B, as it assigns the appropriate role to the external auditor, ensuring they have access to the necessary logs while maintaining strict control over permissions according to the least-privilege security principle.

Solution to Question 47: C

The correct answer is C. Enable the Cloud Spanner API.

Explanation:

As a database administrator assigned to develop a globally distributed application utilizing Cloud Spanner for data storage, the first step to take is to enable the Cloud Spanner API. Cloud Spanner is a highly scalable, globally distributed database service by Google Cloud, which is designed for mission-critical applications. Enabling the API is essential as it allows access to the service for your Google Cloud project. Without enabling the Cloud Spanner API, you will not be able to create, manage, or interact with the Spanner instances associated with your project.

Option A is incorrect because Google Cloud Firestore is a different NoSQL database service that is not globally distributed by default. Firestore is suitable for more straightforward use cases and does not provide the same globally distributed, horizontally scalable functionality as Cloud Spanner.

Option B is incorrect because Cloud SQL is a fully managed relational database service, but it is not designed for global distribution, unlike Cloud Spanner. Creating a Cloud SQL instance with global infrastructure does not meet the requirement of developing a globally distributed application with Cloud Spanner.

Option D is not the first step, although it may be an essential step in the overall process. Granting yourself the IAM role of Cloud Spanner Admin would allow you to manage instances, databases, and access, but it does not enable you to

utilize the Cloud Spanner service for your project. The IAM role should be set up after enabling the Cloud Spanner API to ensure that you have the necessary permissions to manage and configure the service for your needs.

Solution to Question 48: A

The correct answer is A. You should enable Private Google Access on the subnet within the custom VPC. This will allow Compute Engine VM instances with only internal IP addresses to access the Cloud Storage bucket without needing an external IP address while still following the company's security policies.

Here's why the other options will not work:

B. Private Service Access is used to establish a private connection between a VPC network and Google-managed services, but it doesn't help in allowing Compute Engine VM instances to access a Cloud Storage bucket over internal IP addresses. Cloud Storage buckets are accessible using Google APIs, which can be reached with Private Google Access.

C. Load Balancers are used to distribute network traffic across multiple backend systems to ensure high availability and reliability of applications. In this scenario, the task is to ensure that the application can access a file hosted in a Cloud Storage bucket, and configuring a Load Balancer would not be the appropriate solution.

D. While configuring a custom IAM policy is crucial in ensuring that the Compute Engine VM instances have the right permissions to access the Cloud Storage bucket, it does not address the connectivity issue that arises from disallowing connections to the internet. Enabling Private Google Access on the subnet solves this connectivity problem while adhering to the company's security policies.

Solution to Question 49: A

The correct answer is A.

Explanation for Answer A: By using a combination of Spot VM node pool and a node pool with standard VMs, you can optimize your costs while maintaining the necessary reliability for critical components. Spot VMs are cost-effective as they are created using spare Google Cloud compute capacity but can be interrupted by Google with short notice. This makes them suitable for non-critical, fault-tolerant deployments, where occasional downtime is acceptable. On the other hand, the node pool with standard VMs provides higher reliability for the critical components that must always be available, as they are not subjected to the same potential interruptions as Spot VMs.

Explanation for why Answers B, C, and D will not work:

Answer B: While both Custom VM node pool and standard VM node pool can offer higher reliability when compared to Spot VMs, choosing Custom VMs for fault-tolerant deployments does not contribute to cost optimization. Custom

VMs are primarily useful for specific resource configurations, not for minimizing costs for non-critical components.

Answer C: Creating a single node-pool with standard VMs does not optimize costs since it does not take advantage of the cheaper Spot VMs for the fault-tolerant deployments. Labeling the deployments with "spot_true" is also not a solution for cost optimization, as it only serves as an organizational label without any direct impact on the cost structure.

Answer D: Balanced Persistent Disks are focused on achieving a balance between performance and cost for storage solutions, rather than compute resources, which doesn't address the need for cost optimization and reliability concerning the VMs in the question. Moreover, labeling critical Deployments as "disk_balanced_false" neither results in cost optimization nor ensures higher availability for those deployments.

Solution to Question 50: C

The correct answer is C: Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

Here's why other options will not work and why Option C is the best choice:

Option A: Creating a global Cloud Spanner instance and configuring the VMs in the two zones to share the same Spanner database will make the application highly available from the database perspective. However, this does not directly address the problem of supporting the failure of a single Compute Engine zone. As a result, Option A may not fully eliminate downtime in case of a zone failure.

Option B: Creating an HTTP(S) Load Balancer with the global forwarding rules set up to direct traffic to your VMs can help in distributing the load, but it does not address the issue of deploying resources in multiple zones. If us-central1-a fails, there are no resources in us-central1-b to handle the load, leading to downtime. Therefore, this option does not meet the requirement of supporting the failure of a single Compute Engine zone.

Option D: Setting up a Kubernetes cluster in both zones us-central1-a and us-central1-b, and using Kubernetes services to balance the load across VMs in both zones, would involve migrating the application to the Kubernetes platform. This change might require additional resources and effort compared to other options, which may contradict the manager's desire to minimize additional costs.

Option C: Creating Compute Engine resources in us-central1-b and balancing the load across both zones addresses the requirement of supporting a single zone failure. Since the application is already hosted on Compute Engine VMs in the us-central1-a region, creating resources in us-central1-b and setting up a load balancer between these zones would provide high availability without incurring the need to migrate the application to another platform or make complex database changes. In the event of a single zone failure, this setup would ensure that the available zone continues to process requests and minimizes downtime

effectively. This also aligns with the manager's request of minimizing additional costs, as it leverages existing infrastructure and requires minimal modifications for the setup.

Practice Exam 7

Question 1: As a software engineer at a leading tech company, you have developed a complex application consisting of multiple microservices, where each microservice is packaged in its own Docker container image. To efficiently deploy the entire application on Google Kubernetes Engine and ensure that each microservice can be independently scaled, what should you do?

A. Create and deploy a Dataproc Cluster per microservice.

B. Create and deploy a Compute Engine Instance per microservice.

C. Create and deploy a Firestore Database per microservice.

D. Create and deploy a Deployment per microservice.

Question 2: You are working as a software engineer at a tech company, where you have developed a code snippet that needs to be executed each time a new file is uploaded to a Cloud Storage bucket. How should you deploy this code snippet to achieve the desired functionality?

A. Use AI Platform Training and configure a pre-processor to trigger the codeSnippet using Pub/Sub.

B. Use Dataflow as a batch job, and configure the bucket as a data source.

C. Use Cloud Functions and configure the bucket as a trigger resource.

D. Use App Engine and configure Cloud Scheduler to trigger the application using Pub/Sub.

Question 3: As a network administrator at a software development company, you've been tasked with setting up an application in a new VPC behind a firewall for a client who is particularly concerned about data egress. To address their concerns while ensuring the fewest open egress ports, what should be your approach?

A. Implement an HTTP(S) Load Balancer to restrict egress traffic.

B. Configure custom routes to block egress traffic on undesired ports.

C. Use a shared VPC to limit egress ports without configuring firewall rules.

D. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

Question 4: As a system administrator at a software company, you have been asked to determine when users were added to Cloud Spanner Identity Access Management (IAM) roles on the company's Google Cloud Platform (GCP) project. What should you do in the GCP Console to accomplish this?

A. Open the BigQuery console, and check audit logs for Cloud Spanner IAM roles.

B. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

C. Go to the Stackdriver Monitoring console and set up dashboards for Cloud Spanner IAM roles.

D. Open the Cloud Spanner console and review the schema tab.

Question 5: As an IT manager in a software development company, you are responsible for handling multiple Google Cloud projects efficiently. To simplify the management process and configure the Google Cloud SDK CLI to easily manage multiple projects, what should be your approach?

A. 1. Create a separate installation of Google Cloud SDK for each project you need to manage. 2. Use alias commands to switch between the SDK installations when working with different projects.

B. 1. Use the default configuration for all projects you need to manage. 2. Manually update the project ID within the configuration file each time you need to switch projects.

C. 1. Create a configuration for each project you need to manage. 2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

D. 1. Create a configuration for each project you need to manage. 2. Use gcloud init to update the configuration values when you need to work with a non-default project

Question 6: As an IT administrator in a software development company, your team members have Google accounts. You are responsible for managing numerous Compute Engine instances, and your operational team members require administrative access to servers. The security department insists on an efficient deployment of credentials and the ability to track who has accessed specific instances. What approach should you take?

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

B. Create a shared Gmail account for the team and use its Google account to generate an SSH key pair. Add the public key to each member's Google account and grant 'compute.osAdminLogin' role to the shared Gmail account.

C. Ask each member of the team to generate a new SSH key pair and add the public key to a shared Google Sheet. Use a configuration management tool to deploy those keys on each instance and grant 'compute.osAdminLogin' role to the Google group corresponding to this team.

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

Question 7: As a security analyst at a tech company, you need to confirm the IAM users and roles assigned within a GCP project named my-project for an internal audit. What is the most appropriate course of action to take?

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

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

C. Navigate to the project and then to the APIs & Services section in the GCP Console. Review the roles and project settings.

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

Question 8: You are working as a Cloud Engineer for a company that relies on multiple VPC-native Google Kubernetes Engine clusters in the same subnet. Your company is growing rapidly, and you need to ensure that the clusters can expand with additional nodes when required. However, the IPs available for the nodes have been exhausted. What is the best course of action to resolve this issue?

A. Configure Flexible PodCIDR to allow for more IP addresses.

B. Expand the CIDR range of the relevant subnet for the cluster.

C. Migrate one or more GKE clusters to a different VPC.

D. Decrease the number of nodes per GKE cluster.

Question 9: As a DevOps Engineer in a software development company, you are tasked with using Deployment Manager to create a Google Kubernetes Engine cluster. Alongside the same Deployment Manager deployment, you also need to create a DaemonSet in the kube-system namespace of the cluster. The objective is to find a solution that utilizes the least number of services. What approach should you take?

A. Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

B. In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value.

C. Use Anthos Config Management to create a config that sets up the DaemonSet in the kube-system namespace, and reference this config in the Deployment Manager template.

D. Update the Deployment Manager configuration to include a Cloud Logging sink that deploys the DaemonSet to the kube-system namespace whenever a log entry is created.

Question 10: As a software developer working in a technology company, you have successfully set up a development environment for an application utilizing

Compute Engine and Cloud SQL. Your next task is to create a production environment for the same application, adhering to the security team's guidelines which include avoiding network routes between the development and production environments and following Google-recommended practices. What steps should you take in this situation?

A. Create a production environment within the same project by setting up the necessary firewall rules to restrict traffic between development and production environments.

B. Create a new project, modify your existing VPC to be a Shared VPC, share that VPC with your new project, and replicate the setup you have in the development environment in that new project in the Shared VPC.

C. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

D. Utilize Identity-Aware Proxy (IAP) to restrict access to application resources between the development and production environments in the same project.

Question 11: You are working for a reputable financial organization that requires maintaining audit log records for 3 years and handles numerous Google Cloud projects. To efficiently implement a log file retention strategy without incurring high costs, what action should be taken?

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

B. Create an export to the sink that saves logs from Cloud Audit to Firebase Realtime Database.

C. Export logs from Cloud Audit to Cloud Firestore and configure data retention for 3 years.

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

Question 12: As a software developer working for a tech company, you are managing a development project with the appropriate IAM roles defined. Now, you need to create a production project and want to replicate the same IAM roles from the development project to the new one, using the fewest possible steps. What should you do?

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

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

C. Use gcloud iam roles copy, specifying both the development and production projects as the source projects.

D. Use gsutil iam setaclexamples for multiple projects with a single command.

Question 13: As a leading construction equipment rental company, you offer a variety of large-scale equipment fitted with multiple sensors that send event information regarding engine status, distance traveled, fuel level, and more. This data is used for customer billing and with each device generating thousands of events per hour, consistent data retrieval based on event timestamps is crucial. Moreover, storing and retrieving individual signals must be atomic. How should you handle this data efficiently?

A. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

B. Create a file in Google Sheets per device and append new data in it.

C. Create a file in Cloud SQL per device and append new data to that table.

D. Use Memorystore to cache incoming sensor data and periodically batch write them to Cloud Spanner.

Question 14: As a software developer in a fast-paced tech company, you are working on a project that utilizes Google Cloud and have set up a developer laptop with the Cloud SDK installed on Ubuntu from the Google Cloud Ubuntu package repository. You need to test your application locally with Cloud Datastore on your laptop. What is the best course of action to take?

A. Create a Cloud Datastore index using gcloud datastore indexes create.

B. Use the gcloud datastore emulator start command to launch the emulator without installing it.

C. Install the google-cloud-sdk-datastore-emulator component using the apt get install command.

D. Install the cloud-datastore-emulator component using the gcloud components install command.

Question 15: As a manager of a tech company in the software development industry, you are responsible for overseeing the organization and billing administration. The engineering team has been assigned the Project Creator role within the organization, but you wish to restrict their ability to link projects to the billing account. You want the finance team to have exclusive access to link a project to a billing account while ensuring they cannot make any other changes to projects. What approach should you take?

A. Assign the engineering team the Billing Account Administrator role on the billing account.

B. Assign the finance team both the Billing Account User and the Project Editors role on the organization.

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

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

Question 16: You are working at a software development company and manage both development and production projects on Google Cloud Platform. Your manager asks you to set up an automated process that lists all compute instances in both projects every day. How should you accomplish this task?

A. Create a BigQuery table for each project, and export all the compute resources information daily using the Dataflow service.

B. Create two separate folders in Google Cloud Storage for production and development projects, then write a script to export the list of compute instances daily using Google Cloud Storage Transfer Service.

C. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

D. Create a Firestore database for each project and store all compute instances information in it, then use Firestore Export to backup the data daily.

Question 17: You are working as a software engineer at a tech company and have been tasked with developing a new application. As part of the development process, you need to find a Jenkins installation to build and deploy your source code while ensuring that the installation is automated in the most efficient way. What approach should you take?

A. Install and configure Jenkins on a Cloud Run instance.

B. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application.

C. Deploy Jenkins through the Google Cloud Marketplace.

D. Connect Jenkins to Firestore and deploy your application using the integration.

Question 18: As a software engineer working for a start-up that relies on cloud storage for their applications, a feature has been built to store files using the Standard Storage class. However, access to files created more than 30 days ago is unnecessary. In order to save costs on these older files and maintain efficiency in the system, what is the most appropriate solution?

A. Create a cron job in Cloud Scheduler to call a Cloud Functions instance every day to delete files older than 30 days.

B. Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

C. Create a Cloud Pub/Sub topic to trigger a Cloud Function that deletes files older than 30 days.

D. Enable transfer service in GCP to move files older than 30 days to another bucket with a lower storage class.

Question 19: As a rapidly growing tech company, your firm enforces stringent access control measures for Google Cloud projects. In line with Google's recommended practices, you must enable your Site Reliability Engineers (SREs) to approve requests from the Google Cloud support team when they open a support case. How should you proceed?

A. Add your SREs to roles/iam.roleAdmin role.

B. Add your SREs to a group and then add this group to roles/accessapproval.approver role.

C. Add your SREs to a group and then add this group to roles/cloudfunctions.admin role.

D. Add your SREs to a group and then add this group to roles/logging.admin role.

Question 20: As a data engineer at a large tech company, your team has a massive 5-TB AVRO file stored in a Cloud Storage bucket that the data analysts need to access. However, the analysts are only proficient in SQL. Your task is to find the most cost-effective and quickest solution to allow the analysts to access the data. What should you do?

A. Create a BigQuery table and load data in BigQuery. Run a SQL query on this table and drop this table after you complete your request.

B. Convert the AVRO file to a CSV file and upload it to Google Sheets, giving analysts the ability to query the data with SQL functions.

C. Create a Memorystore instance and use Cloud Functions to process the AVRO file, storing the data in the Memorystore for SQL querying.

D. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

Question 21: As a software engineer in a tech company, you are assigned to a team responsible for maintaining the cloud infrastructure. Lately, you have realized that the current infrastructure needs to be updated and are required to share your proposed changes with your colleagues. To ensure a seamless process, you have decided to follow Google's recommended best practices. How should you communicate the proposed changes to your team?

A. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

B. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.

C. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

D. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Pub/Sub. Create a Shared VPC in the organization and apply the proposed changes for team review. Store the Deployment Manager templates describing the proposed changes in Firestore. Discuss the proposed changes in a Google Meet session. Use Cloud Logging to share the proposed changes with the rest of the team. Migrate the existing infrastructure to Anthos and then share the proposed changes using Anthos Config Management. Use Cloud Functions to automatically apply the proposed changes for team review. Create a diagram of the proposed changes and share it through Google Drive or Google Docs.

Question 22: As a software engineer working for a tech company, you have been assigned the task of ensuring that the DevOps team has full control of Compute Engine resources within the development project. However, they must not have the ability to create or update any other resources in the project. To stay compliant with Google's recommended practices, what steps should you take?

A. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

B. Grant the basic role roles/owner and the predefined role roles/compute.admin to the DevOps group.

C. Grant the basic role roles/viewer and the predefined role roles/storage.admin to the DevOps group.

D. Create a custom role at the folder level and grant all compute.diskAdmin.* permissions to the role. Grant the custom role to the DevOps group.

Question 23: As a database administrator at a software company, you need to choose and configure a cost-efficient solution on the Google Cloud Platform for handling relational data. Your company deals with a small set of operational data in a single geographical location, and point-in-time recovery is a requirement. What should be your preferred approach?

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

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

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

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

Question 24: As a software developer in a technology company, you have been assigned to a newly-created Google Cloud project with an attached billing account. Your tasks involve creating instances, setting up firewalls, and storing data in Cloud Storage. In order to adhere to Google-recommended practices, what should be your approach?

A. Open the Google Cloud console and enable all Google Cloud APIs from the API dashboard.

B. Open the Google Cloud console and run gcloud init –project in a Cloud Shell.

C. Open the Google Cloud Console and manually create instances, set firewalls, and store data in Cloud Storage without enabling any APIs.

D. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

Question 25: During your recent audit as a project manager at a cloud-based software development company, you discovered that last month's costs exceeded the budget due to a development GKE container generating excessive logs. To quickly disable the logs using the minimum number of steps, what action should be taken?

A. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

B. 2. Go to the Log Router in Stackdriver Logging, and create a sink with a no-op destination for the GKE container resource.

C. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE Cluster Operations resource.

D. 7. Use the Kubernetes API to update the container's logging configuration and disable Stackdriver Logging.

Question 26: As a software engineer at a leading tech company, you are tasked with deploying an application on Google Cloud using serverless technology. You want to test a new version of the application by rerouting a small percentage of production traffic. What should you do?

A. Deploy the application to Firebase. Use Cloud Firestore for traffic splitting.

B. Deploy the application to Cloud Storage. Use object ACLs for traffic splitting.

C. Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

D. Deploy the application to Cloud Pub/Sub. Use message filtering for traffic splitting.

Question 27: As a DevOps engineer at a tech company, you have recently set up a Deployment with 2 replicas in a Google Kubernetes Engine cluster that has a single preemptible node pool for your microservices. After waiting for a few minutes, you decide to use kubectl to check the status of your Pods and notice that one of them is still in Pending status. What could be the most likely cause for this situation?

A. Google Cloud Load Balancer failed to register the pending Pod's backend service, causing the Pod to remain in Pending status.

B. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

C. The pending Pod was originally scheduled on a node that has been preempted between the creation of the Deployment and your verification of the Pods' status. It is currently being rescheduled on a new node.

D. The Deployment has an affinity or anti-affinity rule that conflicts with existing Pods, causing the scheduling failure.

Question 28: As an IT specialist working for a multinational company, you have recently downloaded and installed the gcloud command line interface (CLI) and authenticated it with your Google Account. Most of the Compute Engine instances in your company's projects run in the europe-west1-d zone. To minimize effort and simplify the CLI commands when managing these instances, what should you do to avoid specifying this zone each time?

A. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

B. Create a folder called europe-west1-d in the CLI installation directory to act as the default zone.

C. Reinstall the gcloud CLI using the flag –default-zone=europe-west1-d during installation.

D. Create a text file named default_zone.txt containing europe-west1-d and place it in the .config folder of your user directory.

Question 29: As a Database Administrator for a media company, you are responsible for managing video storage costs. You need to create a policy that moves videos stored in a specific Cloud Storage Regional bucket to Coldline after 90 days, and then deletes them one year after their creation. How should you set up the policy?

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

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

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

D. Use Cloud Scheduler to execute a script that moves objects to Coldline after 90 days and deletes them after 275 days.

Question 30: You are an IT manager at a software development company and are deploying a critical production application on Google Compute Engine.

To ensure your team doesn't accidentally destroy the instance by clicking the wrong button, which feature should you enable?

A. Enable maintenance migrations on the instance.

B. Create a custom image with a longer deletion protection period.

C. Enable autohealing on the instance group.

D. Enable delete protection on the instance.

Question 31: You are an IT specialist working for a pharmaceutical research company that stores its sensitive research images in an on-premises data room. The company decides to utilize Cloud Storage for archival storage of these research images while requiring an automated process to upload newly generated images to Cloud Storage. How should you design and implement an effective solution?

A. Create a Pub/Sub topic, and enable a Cloud Storage trigger for the Pub/Sub topic. Create an application that sends all medical images to the Pub/Sub topic.

B. Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

C. Create a Cloud SQL instance and develop a script to import the image files into the database. Schedule the script as a cron job.

D. Use Datastore to store the medical images and create a script that transfers the images from on-premises storage to Datastore. Schedule the script as a cron job.

Question 32: You work in a gaming company and have developed a single binary application to be hosted on Google Cloud Platform. To handle player traffic, you decide to scale the application based on underlying infrastructure CPU usage automatically. As per your company's policies, you must use virtual machines directly. To make the application scaling operationally efficient and to complete it as quickly as possible, what should you do?

A. Create multiple Google Compute Engine instances with anti-affinity policies and manually adjust the number of instances based on CPU usage.

B. Use Cloud Dataflow to manage the scaling of the application based on CPU usage.

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

D. Use Google App Engine flexible environment to deploy the application and configure dynamic scaling based on CPU usage.

Question 33: In a software development company, the finance department requests access to view the billing reports for various projects without receiving additional permissions. How should you grant them the required access?

A. Add the group for the finance team to roles/datastore admin role.

B. Add the group for the finance team to roles/compute.viewer role.

C. Add the group for the finance team to roles/container admin role.

D. Add the group for the finance team to roles/billing viewer role.

Question 34: As a Cloud Storage specialist working in a financial services company, your internal auditor wants to review your organization's use of data in Google Cloud, specifically focusing on who accessed the data in Cloud Storage buckets. To assist the auditor, what should you do?

A. Assign the appropriate permissions, and then create a Data Studio report on Admin Activity Audit Logs.

B. Enable VPC Flow Logs for the organization's VPC networks to monitor data access.

C. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

D. Use the export logs API to provide the Admin Activity Audit Logs in the format they want.

Question 35: You work as a software engineer at an animation company that heavily relies on a Kubernetes Engine cluster for managing multiple microservices. One of the microservices is responsible for rendering high-quality images which demands significantly more CPU time compared to memory it requires, while other microservices are workloads that are optimized for n2-standard machine types. In order to maximize resource efficiency for all workloads, what adjustments should you make to your Kubernetes cluster?

A. Assign the pods of the image rendering microservice a higher pod priority than the other microservices.

B. Set up autoscaling for the image rendering microservice, but use the same general-purpose machine type nodes for all microservices.

C. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

D. Configure the required amount of CPU and memory in the resource requests specification of the image rendering microservice deployment. Keep the resource requests for the other microservices at the default.

Question 36: You're working as a cloud engineer for a company with multiple teams using Compute Engine instances in two separate GCP projects. Your task is to enable traffic between the groups of instances located in distinct VPCs. What should you do to achieve this?

A. Create a new VPC peering connection between the two existing VPCs and update route tables to allow traffic between the instances.

B. Verify that you are the Project Administrator of both projects. Create two new VPCs and add all instances.

C. Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.

D. Create a new Shared VPC with all instances from both projects and configure firewall rules to allow traffic between them.

Question 37: You are working as a software engineer at a tech company and are responsible for deploying an App Engine application for a client. After using gcloud app deploy, you realize it did not deploy to the intended project. To investigate why this happened and where the application was deployed, what should you do?

A. Review the gcloud app deploy command for any typos or incorrect parameters.

B. Confirm that App Engine is enabled in the API Library for the intended project.

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

D. Run gcloud projects list to verify the proper project ID for the intended project.

Question 38: You work as a system administrator for a large company that relies heavily on Linux instances hosted on Google Cloud. Your manager has asked you to find a secure and cost-effective solution for your team to log into these instances. What method should you employ for this purpose?

A. Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

B. Grant all users Compute Engine Instance Admin role to manage instances and access them through Google Cloud Console SSH.

C. Use a proxy server with public internet access and allow traffic on port 22 for SSH. Allow ingress traffic from the proxy server's IP range.

D. Create a GCP load balancer and forward all incoming connections to instances on port 22.

Question 39: As a software engineer in a tech company, you need to develop a Compute Engine instance in a new project for one of your clients. The project hasn't been created yet. What course of action should you follow?

A. Enable App Engine API in the Cloud Console and create a new project with Compute Engine instances as part of the default configuration.

B. Enable the Firestore API in the Cloud Console, create a new project, and then use the Cloud SDK to create a Compute Engine instance.

C. Create a service account with permissions to create Compute Engine instances and then use it to create instances in the new project.

D. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

Question 40: You are working as a data engineer at a media company and tasked with migrating your on-premises data to Google Cloud. Your data includes 200 TB of video files in SAN storage, data warehouse data stored on Amazon Redshift, and 20 GB of PNG files stored in an S3 bucket. Your goal is to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud Storage bucket. To accomplish this, you want to follow Google-recommended practices and avoid writing any code for the migration. How should you proceed?

A. Use Cloud SQL for the video files, Dataflow for the data warehouse data, and Cloud Storage for the PNG files.

B. Use Dataflow for the video files, Cloud Data Fusion for the data warehouse data, and Transfer Appliance for the PNG files.

C. Use Storage Transfer Service for the video files, Dataproc for the data warehouse data, and Storage Transfer Service for the PNG files.

D. Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

Question 41: As an IT manager at a rapidly growing software company, you are responsible for managing a nightly batch workload that utilizes a large number of virtual machines (VMs). Although the process is fault-tolerant and can endure some VMs being terminated, the current cost of VMs is too high. What should you do to reduce cost without compromising the workload's fault tolerance?

A. Run a test using Compute Engine Autoscaler. If the test is successful, use Autoscaler with N2 Standard VMs when running future jobs.

B. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

C. Run a test using Cloud Run with the same workload. If the test is successful, migrate the workload to Cloud Run.

D. Run a test using Cloud Dataproc with preemptible VMs enabled. If the test is successful, use Cloud Dataproc with N2 Standard VMs for future jobs.

Question 42: You are the project manager at a software development company that relies on Google Cloud for various projects. Your team has a specialist responsible for creating and managing all service accounts within these Google Cloud projects. In order to grant the appropriate minimum role to this individual for effective project organization, which role should you assign them?

A. Add the user to roles/iam.serviceAccountAdmin role.

B. Add the user to roles/iam.securityAdmin role.

C. Add the user to roles/iam.serviceAccountSecurityManager role.

D. Add the user to roles/iam.serviceAccountCreator role.

Question 43: You are working as a Security Analyst in a software company. One of the employees was terminated, but their access to Google Cloud was not revoked until two weeks after the termination. It is crucial to determine if the terminated employee accessed any confidential client data during that time. How should you proceed to investigate this issue?

A. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

B. View System Event Logs in Cloud Logging. Search for the user's email in the resource.labels values.

C. View VPC Flow Logs in Cloud Logging. Search for the IP address associated with the user.

D. View Admin Activity logs in Cloud Auditing. Search for the user's email as the principal.

Question 44: As a database engineer in a financial company, you are managing a Bigtable instance with three nodes that store sensitive customer PII data. You are required to log all read and write operations, including any metadata or configuration reads of this database table, in the company's Security Information and Event Management (SIEM) system. How should you accomplish this?

A. • Navigate to Cloud Monitoring in the Google Cloud console, and create a custom monitoring job for the Bigtable instance to track all changes. • Create an alert by using webhook endpoints, with the SIEM endpoint as a receiver.

B. Create a custom log-based metric in Cloud Monitoring to track Bigtable operations and export it to your SIEM system.

C. Apply a Cloud Identity Access Management (IAM) policy on the Bigtable instance to require custom roles for-read/write actions and track these actions in your SIEM system.

D. • Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.

Question 45: As a system administrator for a rapidly growing company, you recently received an alert from your managed instance group, stating that the creation of new instances has failed. You need to ensure that there are enough running instances as specified by the template to handle the expected application traffic in your company infrastructure. What should you do?

A. Delete the current instance template and replace it with a new instance template. Verify that the instance name and persistent disk name values are not the same in the template. Set the disks.autoDelete property to true in the instance template.

B. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

C. Update the instance group's autoscaling policy with a different scaling metric and create an instance template that contains valid syntax.

D. Change the instance group's region and create an instance template that contains valid syntax that will be used by the instance group.

Question 46: As an IT administrator in a software development company, you are tasked with providing three developers the ability to view and edit table data on a Cloud Spanner instance for a project they are working on. What should you do?

A. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to the role.

B. Run gcloud iam roles describe roles/spanner.databaseUser –project my-project. Add the users to a new group.

C. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

D. Run gcloud projects add-iam-policy-binding my-project –member user:email@example.com –role roles/spanner.databaseUser.

Question 47: You are working as a cloud engineer in a tech company and you have recently made significant changes to a complex Deployment Manager template. You need to ensure that the dependencies of all defined resources are properly met before committing it to the project, and you want the quickest feedback on your changes. What should you do?

A. Create a separate Deployment Manager branch with the new configuration and use GitHub integration to monitor for conflicts before merging.

B. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

C. Leverage a custom Cloud Function to validate the Deployment Manager template's resource dependencies before executing it.

D. Copy the Deployment Manager template to a separate storage bucket and set up object versioning to track changes over time.

Question 48: You are working as an IT specialist at a rapidly growing technology company, which has been using Google Workspace to manage employee accounts. The company expects to see an increase in workforce from 100 to 1,000 employees within the next 2 years. The majority of these employees will need access to the company's Google Cloud account. With this massive growth, the company's systems and processes must be able to accommodate a 10x increase without suffering from performance degradation, added complexity, or security risks. In order to achieve this, what should your approach be?

A. Turn on Google Cloud Directory Sync (GCDS) for Cloud Identity and skip Multi-Factor Authentication.

B. Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

C. Import and export all users manually to Google Cloud Storage.

D. Use the built-in GCP Admin Tools to manage accounts as they grow without integration.

Question 49: You're working as a software engineer in a tech company, and your team oversees a web application that's deployed as a managed instance group. While the application is receiving live web traffic, your team has developed a new version that requires a gradual deployment. To maintain the available capacity during the deployment, what approach should you take?

A. Perform a rolling-action start-update with maxSurge set to 0 and maxUnavailable set to 1.

B. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

C. Perform a rolling-action start-update with maxSurge set to 0 and maxUnavailable set to 0.

D. Manually update each VM instance within the managed instance group without using a rolling update.

Question 50: While working in a software company that heavily relies on containerization, you need to deploy a Dockerfile on Kubernetes Engine for a new project. How should you proceed?

A. Upload the Dockerfile to Cloud Storage and use kubectl create to deploy the application.

B. Create a docker image from the Dockerfile and upload it to Datastore. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

C. Use gcloud compute instances create with the Dockerfile as a parameter.

D. Create a docker image from the Dockerfile and upload it to Container Registry. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

Practice Exam 7 Solutions

Solution to Question 1: D

The correct answer is D. Create and deploy a Deployment per microservice.

Explanation: In this scenario, you have a complex application made up of multiple microservices, and you need to deploy it on Google Kubernetes Engine (GKE) to ensure efficient running and independent scaling for each microservice. Here's why option D is the best choice:

D. Create and deploy a Deployment per microservice: A Deployment in Kubernetes is a high-level object that manages and maintains a desired state for your application. It ensures that the specified number of replicas for each microservice is running, manages updates, and enables independent scaling as needed. Using a Deployment for each microservice allows you to manage each microservice's container images, lifecycle, and resources efficiently.

Here's why the other options won't work:

A. Create and deploy a Dataproc Cluster per microservice: Dataproc is a managed Apache Spark and Apache Hadoop service that allows you to process vast amounts of data quickly. It's not meant to manage microservices and containerized applications; hence, it is not suitable for deploying and managing your Docker containers in this scenario.

B. Create and deploy a Compute Engine Instance per microservice: Compute Engine provides Virtual Machines (VMs) to run your applications. Although you can run Docker containers in Compute Engine instances, managing multiple VMs for each microservice would not be as efficient as using Kubernetes Deployments. Deployments in GKE provide more straightforward management and scaling, whereas Compute Engine instances would require manual scaling and individually managed VMs.

C. Create and deploy a Firestore Database per microservice: Firestore is a NoSQL document database provided by Google Cloud for storing and syncing data. It is not a container orchestration platform and doesn't handle deploying or managing your Docker containers or microservices. Thus, it is not suitable for your requirements in this scenario.

Solution to Question 2: C

The correct answer is C. Use Cloud Functions and configure the bucket as a trigger resource.

Explanation:

Option A - Using AI Platform Training and configuring a pre-processor to trigger the code snippet with Pub/Sub is not the correct approach. AI Platform Training is specifically designed for training and deploying machine learning

models. While Pub/Sub messaging can be used to trigger actions, it should not be applied for this requirement in the context of AI Platform Training.

Option B - Using Dataflow as a batch job and configuring the bucket as a data source is also not a suitable solution. Dataflow is designed for processing and transforming large data sets, which is not necessary for executing a code snippet whenever new files are uploaded. While it might work, it would be an inefficient use of resources for this specific requirement.

Option C (correct answer) - Using Cloud Functions and configuring the bucket as a trigger resource is the most suitable option. Cloud Functions are serverless and can be triggered by events such as a new file being uploaded to a Cloud Storage bucket. This directly meets the requirement of executing the code snippet upon every file upload, making it the best solution for this use case.

Option D - Using App Engine and configuring Cloud Scheduler to trigger the application using Pub/Sub is not an appropriate solution. App Engine is a platform for building scalable web applications, and Cloud Scheduler is for running jobs at specified intervals. This combination would not be able to trigger the code snippet whenever a new file is uploaded, which means it would not satisfy the desired functionality.

Solution to Question 3: D

The correct answer is D. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports. This approach is best because it directly addresses the client's concerns about data egress by limiting open egress ports to only what is necessary for the application to function. By combining these two rules, you will block unnecessary egress traffic but still allow essential traffic to pass through the specified open ports.

Option A, implementing an HTTP(S) Load Balancer, is incorrect because it focuses on distributing inbound traffic and does not manage egress traffic restrictions. Moreover, load balancers are designed to balance incoming connections and not to control outgoing traffic.

Option B, configuring custom routes to block egress traffic on undesired ports, is not ideal because it is a more complex solution and not as efficient as working with firewall rules. Custom routes focus on directing traffic within a VPC or between VPCs and primarily govern how traffic is routed, rather than managing port restrictions.

Option C, using a shared VPC to limit egress ports without configuring firewall rules, is incorrect because shared VPCs are used for sharing resources across projects and don't inherently limit egress ports. Using a shared VPC alone would not address the client's concern over data egress.

Solution to Question 4: B

The correct answer is B. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

Explanation:

Option A is incorrect because BigQuery console is used for analyzing and visualizing large datasets using SQL-like queries. It is not the place to check audit logs for Cloud Spanner IAM roles.

Option B is the correct answer. Stackdriver Logging (now called Cloud Logging) is a part of Google Cloud Platform that enables you to store, search, analyze, and monitor log data and events. In this scenario, you should review admin activity logs, which record IAM operations such as adding or removing users from roles in the organization, and then filter them for Cloud Spanner IAM roles to determine when users were added.

Option C is incorrect because Stackdriver Monitoring (now called Cloud Monitoring) focuses on monitoring application performance, like observing latency, error rates, or other custom metrics. It is not suitable for tracking changes in IAM roles.

Option D is incorrect because the Cloud Spanner console is mainly used for managing Cloud Spanner database instances, schemas, and querying data. It does not provide access to the IAM roles history or any information about when users were added to IAM roles.

In conclusion, the best approach to determine when users were added to Cloud Spanner IAM roles is by going to the Stackdriver Logging console, reviewing admin activity logs, and filtering them specifically for Cloud Spanner IAM roles.

Solution to Question 5: C

The answer should be option C because it allows for efficient management of multiple Google Cloud projects through the Google Cloud SDK CLI by creating a dedicated configuration for each project, and activating the appropriate configuration as needed. This streamlined approach reduces the complexities involved in handling multiple projects and minimizes the risk of errors.

Option A is not efficient because creating a separate installation of Google Cloud SDK for each project would consume unnecessary space and increase system complexity. In addition, managing a large number of installations with alias commands can be cumbersome and time-consuming.

Option B is not an optimal approach because using the default configuration for all projects could lead to confusion, as it requires the manual update of the project ID in the configuration file each time you switch projects. This manual process is error-prone and inefficient, especially when dealing with multiple projects.

Option D is not suitable because, while it does create a configuration for each project, it incorrectly suggests using the "gcloud init" command to update configuration values when working with non-default projects. Instead, the appropriate method for managing multiple projects is to activate the corresponding

configuration. The "gcloud init" command is typically used to initialize, authenticate, and set up a new configuration, not for switching between configurations of existing projects.

Solution to Question 6: D

The correct approach to ensure efficient deployment of credentials and the ability to track who has accessed specific instances is option D. Here's why:

Option D: By asking each member to generate their SSH key pair and adding the public key to their Google account, you ensure that each user has a unique key tied to their personal account. This eliminates the risk of a shared key being compromised and gives a clear understanding of who accessed a particular instance. Further, by granting the 'compute.osAdminLogin' role to the Google group corresponding to the team, you make it easy to provide or revoke access in the future, as needed.

Option A: Although using a configuration management tool to deploy public keys helps manage the keys efficiently, this method falls short in terms of security and tracking access. Individual SSH keys could be misplaced, and if a team member leaves the company, it may be hard to ensure their key is removed from each instance.

Option B: Creating a shared Gmail account presents a significant security risk, as multiple individuals would have access to the same SSH key pair. Additionally, it would be nearly impossible to determine who accessed specific instances, since the same credentials would be used by multiple people.

Option C: While this method allows each team member to generate their own SSH key pair, storing public keys in a shared Google Sheet can be insecure and pose a risk of unauthorized access. The tracking of access to specific instances would also be more complicated than in Option D.

In conclusion, option D is the best choice to maximize security, efficiency, and tracking of individual access to Compute Engine instances.

Solution to Question 7: D

The most appropriate course of action to confirm the IAM users and roles assigned within a GCP project named my-project for an internal audit is to select option D. Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles. This approach allows you to easily view and manage users, roles, and permissions directly within the project, providing a convenient and centralized method for auditing access on the platform.

The other options will not work as efficiently for this specific case:

Option A: Run gcloud iam service-accounts list. Review the output section. Although this command allows you to list service accounts, it does not provide a complete overview of all IAM users and roles within the project. It only lists

service accounts, while users, groups, and other types of members will not be listed.

Option B: Navigate to the project and then to the Roles section in the GCP Console. Review the roles and status. This option only provides information about the roles available in the GCP project. It does not display the members these roles are assigned to, nor does it provide an easily accessible snapshot of all the roles assigned within the project.

Option C: Navigate to the project and then to the APIs & Services section in the GCP Console. Review the roles and project settings. This option is primarily for managing APIs and services and their respective quotas within a project. It does not provide an overview of the IAM users and roles assigned to the project.

In conclusion, Option D is the most appropriate course of action as it provides a centralized location to review the IAM users, roles, and permissions within the GCP project. It allows the security analyst to perform a thorough internal audit of the project's access and identity management settings.

Solution to Question 8: B

The correct answer is B. Expand the CIDR range of the relevant subnet for the cluster.

Explanation: An increase in the CIDR range of the subnet linked to the cluster will allow more IP addresses for nodes and will enable the GKE clusters to scale with additional nodes when required.

Reasons why other options will not work:

A. Configure Flexible PodCIDR to allow for more IP addresses. Flexible PodCIDR is not a valid option in Google Kubernetes Engine. CIDRs are assigned to clusters during creation, and it is not possible to change the PodCIDR range or allocate additional IP addresses for an existing cluster.

C. Migrate one or more GKE clusters to a different VPC. Migrating GKE clusters to a different VPC will not solve the IP exhaustion issue in the current VPC. It may be a temporary fix, but it doesn't guarantee a long-term solution for the growing company. Additionally, migration can be complex and time-consuming, which isn't optimal for this situation. The best solution is to address the issue in the existing VPC by expanding the CIDR range for the subnet.

D. Decrease the number of nodes per GKE cluster. Decreasing the number of nodes per GKE cluster is not an ideal solution for a growing company. Reducing the number of nodes might impact the performance and reliability of the services provided by the GKE clusters. The long-term solution is to allow the clusters to scale, which can be achieved by expanding the CIDR range of the subnet.

Solution to Question 9: A

The correct answer is A: Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

Explanation:

Option A is the appropriate approach because it directly integrates the deployment of the Google Kubernetes Engine cluster and the DaemonSet within the same Deployment Manager deployment. By adding the cluster's API as a new Type Provider, Deployment Manager can directly communicate with the Kubernetes API server and allow the creation of the DaemonSet within the kube-system namespace. This method results in the least number of services used, which is the primary objective.

Option B will not work because adding metadata to the cluster's definition does not necessarily create a DaemonSet within the kube-system namespace. The metadata added does not directly communicate with the Kubernetes API server and therefore will not achieve the desired result.

Option C involves using Anthos Config Management, which adds an extra service, going against the objective of utilizing the least number of services. Additionally, this option would require you to set up and manage external configuration repositories which is more complex than Option A.

Option D is not suitable because using Cloud Logging as a means to deploy the DaemonSet to the kube-system namespace is not its intended purpose. This approach is highly dependent on the log entry trigger and does not directly interact with the Kubernetes API server, which is not an efficient way to achieve the goal. Moreover, it would add an unnecessary dependency on Cloud Logging services.

Solution to Question 10: C

The correct answer is C, and here's why:

Creating a new project, enabling the Compute Engine and Cloud SQL APIs in that project, and replicating the setup you have created in the development environment ensures that the production environment is isolated from the development environment. This follows both the security team's guidelines and Google-recommended practices.

Here's why the other options are not suitable:

Option A: Creating a production environment within the same project might seem like a straightforward solution, but it doesn't adhere to Google-recommended practices of keeping development and production environments in separate projects. Firewall rules could help restrict traffic, but the possibility of configuration errors can still lead to security risks.

Option B: While creating a Shared VPC may improve resource sharing between projects, it doesn't provide the necessary level of isolation as it contradicts the security team's guidelines of avoiding network routes between the development and production environments.

Option D: Identity-Aware Proxy (IAP) is for controlling access to application

resources based on the identity of the users and their groups. This option does not address the requirement of avoiding network routes between the development and production environments, and therefore is not suitable for this situation.

Solution to Question 11: D

The correct answer is D because it satisfies the organization's requirements for maintaining audit log records for 3 years and managing multiple Google Cloud Projects cost-efficiently. Let's explore why the other options don't work:

Option A: Writing a custom script that uses the Logging API to copy logs from Stackdriver logs to BigQuery could be time-consuming and might not be as efficient as using an export sink. Additionally, BigQuery is more suitable for data analytics rather than long-term storage, which could result in higher costs when storing data for 3 years.

Option B: Exporting logs from Cloud Audit to Firebase Realtime Database is not suitable as it is designed for real-time data synchronization and does not natively support long-term storage or cost-effective data retention policies. Firebase Realtime Database has a maximum 1 GB storage limit and may not be able to store the data logs for the required time without exceeding that limit.

Option C: Exporting logs to Cloud Firestore and configuring data retention for 3 years might not be the most cost-effective solution. Firestore is designed for highly scalable document storage and querying, which may not be necessary for merely storing audit logs. Retaining data for 3 years in Firestore could lead to higher costs compared to Coldline Storage.

Option D (The correct answer): Creating an export to a sink that saves logs from Cloud Audit to a Coldline Storage bucket is the most suitable solution. Coldline Storage is a cost-effective Google Cloud Storage class explicitly designed for long-term data storage with infrequent access, like audit logs. By exporting logs to a Coldline Storage bucket, you can efficiently implement the required log retention policy for a lower cost and easily manage logs for numerous Google Cloud projects in one place.

Solution to Question 12: A

The correct answer is A: Use gcloud iam roles copy and specify the production project as the destination project. This is the most efficient method because it allows you to copy the IAM roles directly from the development project to the production project in the fewest steps. gcloud is the command-line interface for Google Cloud Platform which provides flexibility and ease of automation. Using the 'copy' functionality ensures that the same IAM roles will be duplicated in the production project, without having to redefine the roles manually.

Option B: In the Google Cloud Platform Console, use the 'create role from role' functionality. This option might work, but it would not be the most efficient method. It requires manual intervention through the Console, which involves

more steps and potentially more room for error compared to running a single gcloud command.

Option C: Use gcloud iam roles copy, specifying both the development and production projects as the source projects. This option doesn't make sense because you don't want to copy roles between two source projects. The goal is to replicate the IAM roles from the development project to the new production project, so specifying both as source projects won't achieve that.

Option D: Use gsutil iam setaclexamples for multiple projects with a single command. This option is not relevant to the situation, as 'gsutil' is a command-line tool for managing Google Cloud Storage buckets and objects, not IAM policies across the projects. It doesn't provide the functionality to copy IAM roles between projects as required in the question.

Solution to Question 13: A

The correct answer is A: Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

Explanation:

Option A is correct because Cloud Bigtable is designed to handle large-scale, high-velocity data ingestion efficiently. It can provide low-latency, high-throughput read and write access to your data, making it suitable for handling thousands of events per hour. By creating a row key based on the event timestamp, you ensure consistent data retrieval, as well as atomic operations for storing and retrieving individual signals.

Option B is not suitable for various reasons. Google Sheets is not designed for handling high-volume, high-velocity data generated by IoT devices. It has limitations in terms of maximum cells, real-time update frequency, and concurrent users. Additionally, it does not provide atomic operations for storing and retrieving individual signals.

Option C is also not optimal. Cloud SQL is a fully managed relational database service, which is not designed to handle the high ingestion rate and scale of data generated by IoT devices. Appending new data to a table might not be efficient enough at scale and could cause issues such as slow query performance and increased maintenance overhead.

Option D is not appropriate for this scenario. Using Memorystore to cache sensor data could address some latency concerns. However, Memorystore is an in-memory data store primarily used for caching and not a long-term storage solution. Periodically batch writing cached data to Cloud Spanner could introduce latency and inconsistency in terms of data retrieval based on event timestamps. Also, this option does not guarantee the atomicity of storing and retrieving individual signals.

Solution to Question 14: D

The correct answer is D, as it involves installing the cloud-datastore-emulator component using the gcloud components install command. This is the best course of action for testing your application locally with Cloud Datastore on your laptop, as it allows you to mimic the actual environment of the Google Cloud Datastore without further configurations or installations. Furthermore, installing the emulator through the gcloud command ensures that the emulator remains compatible with the Cloud SDK and other Google Cloud services.

Option A is not suitable because creating a Cloud Datastore index using gcloud datastore indexes create will only set up an index on an actual Cloud Datastore. The objective here is to test the application locally, not to create an index on the cloud.

Option B is incorrect because it suggests using the gcloud datastore emulator start command without installing the emulator. But it is essential to install the emulator before starting it, which is lacking in this option.

Option C might seem reasonable, but using the apt-get install command to install the google-cloud-sdk-datastore-emulator component is not the correct method. This option may lead to inconsistencies between the SDK components and might not always guarantee compatibility with the latest Google Cloud SDK updates. The best practice is to use the gcloud components install command, as stated in option D, to ensure compatibility.

Solution to Question 15: C

The correct approach is C: Assign the finance team the Billing Account User role on the billing account and the Project Billing Manager role on the organization.

The reason for this choice is because it fulfills both criteria mentioned in the question:

1. Restricting the engineering team's ability to link projects to the billing account: The engineering team is not assigned any billing related role which ensures they cannot make any changes related to billing.
2. Granting the finance team exclusive access to link a project to a billing account while ensuring they cannot make other changes: Assigning the Billing Account User role to the finance team ensures they can have access to billing information and perform limited management tasks. The Project Billing Manager role grants them permission to link projects to the billing accounts without giving them editing privileges on the entire project.

Let's analyze why the other options do not work:

Option A: Assign the engineering team the Billing Account Administrator role on the billing account. This would give the engineering team too much control over billing, which is contrary to the goal of restricting their ability to link projects to the billing account.

Option B: Assign the finance team both the Billing Account User and the Project

Editors role on the organization. This option does not meet the requirement of ensuring the finance team cannot make other changes to projects. The Project Editors role would give them too much control over all aspects of the projects, not just the billing aspect.

Option D: Assign the engineering team the Billing Account User role on the billing account and the Project Billing Manager role on the organization. This option would not restrict the engineering team's ability to link projects to the billing account as intended, and it doesn't grant any permissions to the finance team as required.

Solution to Question 16: C

The correct answer is C because this method automates the process of listing all compute instances in both projects daily by using gcloud configurations, which are specifically designed for managing multiple projects within Google Cloud Platform. This approach allows you to create configurations for both development and production projects and then switch between them, making it easy to list instances for each project.

Option A is not suitable because BigQuery is a data warehouse solution primarily used for analyzing large datasets, and Dataflow service is for processing and transforming data streams in real-time. Both of these services are not the right tools for listing compute instances.

Option B is not appropriate because it suggests using Google Cloud Storage Transfer Service. This service primarily focuses on transferring data between different cloud storage buckets, not specifically listing compute instances within a project.

Option D is not accurate because Firestore is a flexible, scalable NoSQL cloud database designed for mobile and web applications. Although it is possible to store compute instances information in Firestore, using Firestore Export to backup the data daily is not a practical solution for listing compute instances in multiple projects.

Solution to Question 17: C

The correct answer is C. Deploy Jenkins through the Google Cloud Marketplace.

Explanation for C: Using the Google Cloud Marketplace to deploy Jenkins is the most efficient and automated approach. The Google Cloud Marketplace provides pre-built solutions, like Jenkins, that are ready for deployment. This ensures that Jenkins is optimally configured for the Google Cloud environment, allowing you to focus on application development instead of managing and maintaining the Jenkins installation.

Reasons why other options will not work:

A. Install and configure Jenkins on a Cloud Run instance: While Cloud Run is a useful service for deploying containerized applications, it is not designed

specifically for deploying a Jenkins installation. Deploying Jenkins using Cloud Run would require manual configuration and would not be guaranteed to be as efficient or automated as deploying through the Google Cloud Marketplace.

B. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application: This approach involves manually setting up a Cloud Storage bucket, which is unnecessary for deploying a Jenkins installation. Additionally, Cloud Storage is designed for storing and managing unstructured data, such as large media files, rather than deploying applications or executing processes in the cloud.

D. Connect Jenkins to Firestore and deploy your application using the integration: Connecting Jenkins to Firestore does not address the installation and configuration of Jenkins for the Google Cloud environment. Firestore is a NoSQL database service designed for storing and retrieving data associated with Firebase applications and would not be useful for deploying Jenkins. Instead, it is better to use the Google Cloud Marketplace for the automated and efficient deployment of Jenkins.

Solution to Question 18: B

The most appropriate solution for this scenario is option B: Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

Option B is a cost-effective and efficient solution for the problem because it automates the process of managing the storage class of the objects stored in the bucket. This way, you don't have to worry about manually managing your file storage, and the transition will occur automatically when the files reach the specified age. Google Cloud Storage's Archive Storage class offers lower costs for files that do not need to be accessed frequently, which meets the requirement of saving costs for files older than 30 days.

Option A is not ideal because it involves creating a cron job to call a Cloud Functions instance every day to delete older files. This approach might not be cost-effective, since you are continuously executing serverless functions, and it permanently deletes the files instead of moving them to a lower cost storage class.

Option C is also not efficient because it requires setting up and managing a Cloud Pub/Sub topic to trigger a Cloud Function for deleting files. Similar to option A, this would mean executing serverless functions, incurring additional costs, and deleting the files instead of preserving them with a lower-cost storage solution.

Option D is not the best choice because, while enabling transfer service to move files to a different bucket with a lower storage class can save costs, it may also add complexity due to the management of multiple buckets. Meanwhile, object lifecycle management (Option B) provides a more efficient way of achieving the same goal without requiring additional bucket management.

Therefore, the best solution is option B, which allows you to create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days. This way, the system will automatically manage the files, ensure low cost, and maintain efficiency without the need for additional services or manual intervention.

Solution to Question 19: B

The correct answer is B. By adding your SREs to a group and then adding this group to the roles/accessapproval.approver role, you are providing them with the necessary permissions to approve requests from the Google Cloud support team when a support case is opened. This directly addresses the requirement specified in the question.

Here is why other options are not suitable:

Option A: While adding SREs to roles/iam.roleAdmin role would give them the ability to manage IAM roles, it does not specifically grant them the ability to approve access requests from the Google Cloud support team when they open a support case. This role is too broad and unrelated to the requirement.

Option C: Adding SREs to a group and then adding this group to roles/cloudfunctions.admin role would give them access to manage Google Cloud Functions resources, such as creating, updating, and deleting functions. However, this role would not grant them the required permissions to approve access requests from the Google Cloud support team when they open a support case. This role is not related to the requirement.

Option D: Adding SREs to a group and then adding this group to roles/logging.admin role would give them access to manage Cloud Logging resources, including writing logs, creating sinks, and configuring metrics. Still, it would not provide the necessary permissions to approve access requests from the Google Cloud support team when they open a support case. This role is unrelated to the requirement.

In conclusion, Option B is the best choice as it directly addresses the requirement of enabling the SREs to approve access requests from the Google Cloud support team when they open a support case.

Solution to Question 20: D

The correct answer is D. Here's why:

A. Creating a BigQuery table and loading data into it might work, but it can be both expensive and time-consuming, especially for such a massive 5-TB file. Dropping the table after the request is completed would also mean that the process would have to be repeated each time the analysts need access to the data.

B. Converting a 5-TB AVRO file to a CSV file is impractical and would take a significant amount of time. Moreover, Google Sheets has limits on the number

of cells and rows, making it insufficient for handling such a large dataset. Also, SQL functions available in Google Sheets are limited compared to BigQuery.

C. Creating a Memorystore instance and using Cloud Functions to process the AVRO file is an unnecessary and complex approach for this task. Memorystore is designed for in-memory data storage, and with a 5-TB file, it would become prohibitively expensive. Additionally, it's not optimized for SQL querying like BigQuery.

D. Creating external tables in BigQuery that point to Cloud Storage buckets is the most cost-effective and quickest solution. This approach enables analysts to directly run SQL queries on the data residing in Cloud Storage using BigQuery's capabilities without the need to load or move the data. External tables also save storage costs on BigQuery, as the actual data remains in Cloud Storage. This method provides a seamless way for the analysts to access the massive 5-TB AVRO file using SQL while minimizing costs and time delays.

Solution to Question 21: A

Answer: A. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

Explanation:

Option A is the best choice because, following Google's recommended best practices, it involves using Deployment Manager templates to describe the proposed changes in a declarative and version-controlled manner. Storing the templates in Cloud Source Repositories ensures that the entire team can access the proposed changes, review them, and collaborate on the necessary modifications. This approach promotes transparency, traceability, and collaboration among the team members.

Option B and C are not the best choices because they involve applying the changes in a development environment and then running 'gcloud compute instances list' to save the output. While this provides information about the instances being used, it does not provide a clear and comprehensive description of the proposed changes and their impact on the infrastructure. Additionally, storing the output in a shared Storage bucket (option B) or in Cloud Source Repositories (option C) does not allow for effective version control and collaboration.

Option D relies on using Cloud Pub/Sub to share proposed changes, which is not the intended use of this service. Cloud Pub/Sub is a messaging service designed for real-time, at-scale message streaming, not for sharing infrastructure changes.

Other options like Shared VPC, Firestore, Google Meet, Cloud Logging, Anthos, Cloud Functions, and Google Drive or Google Docs do not provide the necessary infrastructure-as-code, version control, and collaboration features that Deployment Manager templates and Cloud Source Repositories offer. These options might be useful for other purposes in the software development life cycle,

but they aren't as effective for communicating infrastructure changes in a clear, organized, and collaborative manner as option A.

Solution to Question 22: A

The correct answer is A, granting the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group. This is because it fulfills the requirement of granting the DevOps team full control over Compute Engine resources while not allowing them to create or update other resources in the project.

Let's examine why the other options will not work:

B. Granting the basic role roles/owner and the predefined role roles/compute.admin to the DevOps group is not the recommended practice. The roles/owner role would grant far more permissions than necessary, which goes against the principle of least privilege. Providing the owner role allows the DevOps group to create, update, and manage any resource in the project, which is not the desired outcome.

C. Granting the basic role roles/viewer and the predefined role roles/storage.admin to the DevOps group would not provide them control over Compute Engine resources. The roles/storage.admin role gives control over storage resources, not compute resources. This option fails to meet the requirement of giving full control over Compute Engine resources.

D. Creating a custom role at the folder level and granting all compute.diskAdmin.* permissions to the role is not ideal. Though it does provide some level of control over Compute Engine resources, it only focuses on disk administration and misses out on other necessary permissions. Moreover, custom roles can be more complex and harder to maintain than predefined roles. In this case, using the predefined roles/compute.admin role is more appropriate and ensures full control over Compute Engine resources, as required.

Solution to Question 23: B

The correct answer is B.

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

The reason behind choosing this option is that Cloud SQL (MySQL) is the most cost-effective solution for handling relational data when the company's operational data is small and limited to a single geographical location. With the enable binary logging option, you ensure the point-in-time recovery requirement, which is essential for the company.

Now let's examine why the other options would not work:

Option A: Select Cloud SQL (PostgreSQL). Verify that the enable binary logging option is selected.

Cloud SQL for PostgreSQL is a more costly option compared to MySQL when dealing with a small set of operational data. PostgreSQL is highly configurable and may be perfect for handling large datasets, but it's not cost-efficient in this scenario.

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

Creating failover replicas ensures high availability and reduces downtime; however, failover replicas do not fulfill the point-in-time recovery requirement. Furthermore, adding a failover replica would increase the overall cost.

Option D: Select Cloud Spanner. Set up your instance with 2 nodes.

Cloud Spanner is Google Cloud's horizontally scalable, strongly consistent relational database service. However, it is more expensive than Cloud SQL (MySQL). It is designed to span multiple geographic regions for accommodating large datasets with low latency and high availability. In this scenario, the company only deals with a small operational dataset in a single geographic location, making Cloud Spanner a less cost-efficient choice.

Solution to Question 24: D

The correct answer is D, and here is why:

D. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

This approach aligns with Google-recommended practices because it only enables the APIs (Application Programming Interfaces) that are necessary for the tasks you need to perform. Enabling only the required APIs ensures minimal resource utilization, better security, and easier management. In this case, enabling Compute Engine allows you to create instances and set up firewalls, while enabling Cloud Storage APIs allows you to store and manage data in Cloud Storage.

Here is why the other options will not work:

A. Open the Google Cloud console and enable all Google Cloud APIs from the API dashboard.

Enabling all the Google Cloud APIs is not a best practice because it unnecessarily uses resources, complicates project management, and may raise security concerns. You should only enable the APIs you specifically need for your assigned tasks.

B. Open the Google Cloud console and run gcloud init –project in a Cloud Shell.

While this command initializes the local SDK environment and allows you to switch between projects, it does not enable the necessary APIs needed for your tasks. Although useful for managing multiple projects, it does not adhere to Google-recommended practices for enabling APIs.

C. Open the Google Cloud Console and manually create instances, set firewalls, and store data in Cloud Storage without enabling any APIs.

Manually creating instances, setting firewalls, and storing data in Cloud Storage without enabling any APIs is not possible or even recommended. APIs are required to facilitate communication between different components of the Google Cloud infrastructure to perform these tasks.

Solution to Question 25: A

The correct answer is A because it quickly and directly addresses the issue of disabling logs for the specific GKE container generating excessive logs, using the minimum number of steps. By going to the Logs ingestion window in Stackdriver Logging and disabling the log source for the GKE container resource, you can stop logs from being ingested for that specific container, thus resolving the budget overrun issue.

Option B is not the most efficient solution as it involves creating a sink with a no-op destination for the GKE container resource. While this would effectively disable the logs, it requires an additional, unnecessary step, making it less efficient than Option A.

Option C is incorrect because disabling the log source for the GKE Cluster Operations resource would stop logs ingestion for the entire cluster's operations, not just for the specific container generating excessive logs. This could negatively impact the project's overall logging and monitoring capabilities.

Option D is also not the best solution as using the Kubernetes API to update the container's logging configuration would require more steps and may also need changes in the container's code or deployment configurations. This approach would not only be more time-consuming but also might introduce unwanted complexity.

Therefore, the best course of action is Option A, as it directly addresses the issue in the least number of steps without affecting other parts of the project.

Solution to Question 26: C

The correct answer is C: Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

Explanation: C: Deploying the application to Cloud Run and using gradual rollouts for traffic splitting is the best option here because Cloud Run is a Google Cloud managed platform designed for serverless applications. Using gradual rollouts in Cloud Run allows you to test new versions of your application by configuring the distribution of traffic between the new version and the existing one. Cloud Run facilitates this process by easily adjusting the proportion of traffic assigned to the different revisions of your application.

Why other options will not work:

A: Firebase is focused on mobile and web development and not specifically designed for serverless applications. Cloud Firestore is a NoSQL database that also isn't ideal for traffic splitting management. Thus, it does not fulfill the requirements for deploying serverless applications and managing traffic, as needed by a software engineer in this scenario.

B: Cloud Storage is an object storage service and using object ACLs (Access Control Lists) for traffic splitting only sets permissions on individual objects. It doesn't provide the required functionality for serverless applications deployment and traffic management between application revisions.

D: Cloud Pub/Sub is a messaging service that allows you to send and receive messages between independent applications. Although message filtering can restrict the messages that get published, it isn't meant for traffic splitting and does not cater to the deployment of serverless applications in the scenario described.

Solution to Question 27: B

The most likely cause for this situation is option B: Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

In a Google Kubernetes Engine cluster with a single preemptible node pool, it is possible for node resources to be depleted, particularly if many other Pods are already running. When a new Pod is created, the scheduler attempts to find a suitable node to run it on. If no such node is found due to resource constraints, the Pod remains in Pending status.

Options A, C, and D are less likely causes for the described situation:

A. Google Cloud Load Balancer failing to register the pending Pod's backend service would result in an issue with its traffic distribution, not in a Pending Pod status. The Pod would still be scheduled and deployed if resources are available in the cluster.

C. While preemption could occur in a cluster with preemptible VMs, the Kubernetes scheduler is designed to quickly reschedule Pods to new nodes in such cases. As a result, it is unlikely that you would observe the Pending status due to this reason after waiting for a few minutes.

D. Although affinity and anti-affinity rules can affect the scheduling of Pods, such rules would typically result in a more specific error message. Additionally, considering you have recently set up the Deployment, it is less likely that a conflict with existing Pods would ultimately cause the pending status. Instead, resource constraints in the cluster are a more plausible explanation.

Solution to Question 28: A

The correct answer is A: Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

Explanation for why answer A should be selected:

Setting the default zone as europe-west1-d using the gcloud config subcommand allows you to automatically apply the specific zone when managing the Compute Engine instances without explicitly specifying it each time. The gcloud CLI is designed to recognize and utilize configurations set through its own subcommands. By setting the default zone using this method, you'll be saving time and effort when running CLI commands for your company's projects.

Reasons why other options will not work:

Option B: Creating a folder called europe-west1-d in the CLI installation directory is not a standard solution and is not recognized by the gcloud CLI. It would not change or impact the zones used by the CLI commands.

Option C: Reinstalling the gcloud CLI with the flag –default-zone=europe-west1-d is not a correct method for setting the default zone. The gcloud CLI installation process does not support setting default configurations using installation flags.

Option D: Creating a text file named default_zone.txt in the .config folder of your user directory is not a recognized method for setting the default zone by the gcloud CLI. As mentioned previously, it is best to use the gcloud CLI's own subcommands to set configurations, like using the gcloud config subcommand.

Solution to Question 29: B

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

Explanation:

As a Database Administrator managing video storage costs, you should use Google Cloud Storage's Object Lifecycle Management to set up the required policy. This service allows you to configure policies based on object properties, such as age or storage class, and automates actions to transition or delete objects when conditions are met.

Option B is the suitable choice because it utilizes both Age conditions and appropriate actions (SetStorageClass and Delete). The Age condition is used to specify the object's age in days before the action takes place. Setting the SetStorageClass action to 90 days will move the videos to Coldline after 90 days from their creation, which fits the requirement. The Delete action is set to 365 days, which ensures the objects are deleted one year after their creation.

The other options are incorrect for the following reasons:

Option A: This choice uses CreationDate conditions instead of Age conditions, which would not be ideal as the policy should be based on the age of the object rather than its creation date. Additionally, setting the Delete action to 275 days would incorrectly delete the objects early, before the one-year requirement is met.

Option C: This choice suggests using gsutil rewrite, a command-line tool for managing Cloud Storage objects. While it can be used to change the storage class, it is not ideal for automating the entire process, as required. Additionally, setting the Delete action to 275 days would result in premature deletion of the objects.

Option D: This choice suggests using Cloud Scheduler to execute a script, which would involve complex and manual configuration, not suitable for a scalable and robust solution. Also, it sets the deletion action to 275 days, which does not meet the one-year requirement.

Solution to Question 30: D

The correct answer is D. Enable delete protection on the instance.

Explanation:

D. Enable delete protection on the instance - When you enable delete protection on an instance, it prevents accidental deletion of the instance by ensuring that the instance cannot be deleted via the Google Cloud Console, gcloud command, or API until the delete protection is disabled. This is the most suitable option in this scenario to avoid the accidental destruction of the instance by the team members.

Incorrect options:

A. Enable maintenance migrations on the instance - Maintenance migrations are used to minimize the impact of maintenance events on your instances, but they do not provide protection against accidental destruction of the instance. This option doesn't directly address the issue described in the question.

B. Create a custom image with a longer deletion protection period - Custom images can be created with specific configurations for new instances, but they do not provide delete protection for instances themselves. Moreover, Google Cloud does not offer a "deletion protection period" feature for custom images. Thus, this option does not help in preventing accidental deletion.

C. Enable autohealing on the instance group - Autohealing ensures that the instances within an instance group remain healthy by automatically detecting and recreating failed instances. However, autohealing would not protect the instance against accidental destruction, as it is meant to handle hardware or software failures and not user actions.

Solution to Question 31: B

The correct answer is B, mainly because it effectively addresses the requirements of archival storage of sensitive research images and the need for an automated process to upload the newly generated images to Cloud Storage.

Option B involves creating a script that uses the `gcloud storage` command to synchronize the on-premises storage with Cloud Storage. The script will

automate the upload of new research images while retaining the original on-premises storage. By scheduling the script as a cron job, the solution ensures that the uploading process runs periodically and automatically.

The other options are not suitable for the following reasons:

Option A suggests creating a Pub/Sub topic with a Cloud Storage trigger and an application to send medical images to the topic. Although Pub/Sub is useful for real-time message delivery, it doesn't address the primary requirement of archival storage and synchronization between on-premises and Cloud Storage.

Option C proposes creating a Cloud SQL instance and developing a script to import image files into the database. This option does not meet the company's needs because Cloud SQL is a relational database service, which is not ideal for storing binary large objects (BLOBs) like images. It may also increase complexity and costs without providing the necessary archival storage benefits.

Option D recommends using Datastore to store medical images and creating a script for image transfer. However, Datastore is a NoSQL database designed to store structured data and is not suitable for storing binary objects such as images. Additionally, it does not simplify the archival storage requirement or sync with on-premises storage.

In conclusion, option B is the best choice because it enables effective archival storage and automated synchronization between on-premises storage and Cloud Storage while the other options do not fulfill the company's requirements.

Solution to Question 32: C

The correct answer is C, and here's why:

Creating an instance template and using it in a managed instance group with autoscaling configured is the best choice to achieve the desired outcome. Managed instance groups (MIGs) allow operational efficiency to scale virtual machines automatically while maintaining high availability. An instance template is necessary to define the machines' configurations, and autoscaling policies based on CPU usage efficiently create or delete instances from the group.

Option A is not suitable because it involves manual adjustment of the number of instances based on CPU usage. Manual intervention is operationally less efficient, time-consuming, and error-prone. Moreover, the use of anti-affinity policies in this context does not contribute to scaling the application.

Option B suggests using Cloud Dataflow, which is a service for processing and transforming massive data streams, rather than scaling virtual machines directly. It does not fulfill the requirement of using virtual machines to host the single binary application.

Option D is also incorrect because Google App Engine flexible environment, while providing a platform to deploy applications and configure dynamic scaling

based on CPU usage, does not allow direct use of virtual machines. It is a higher-level platform-as-a-service (PaaS) offering that abstracts the underlying virtual machine infrastructure.

In conclusion, option C is the best solution to make the application scaling operationally efficient and quick, as it uses instance templates and managed instance groups with autoscaling policies that automatically adjust the number of virtual machines based on CPU usage.

Solution to Question 33: D

The correct answer is D. Add the group for the finance team to roles/billing viewer role. The finance department needs access to view the billing reports of various projects without additional permissions. In this case, the most appropriate role is the billing viewer role, which is specifically designed for users who need access to view the billing information of projects without having the ability to modify them.

Option A is not correct because roles/datastore admin role is related to managing the Google Cloud Datastore, which is used for storing and managing data for applications. This would not give the finance department access to billing reports without additional permissions.

Option B is incorrect as roles/compute.viewer role is designed for users who need to have read-only access to Google Cloud Compute resources such as instances, networks, and other configuration and metadata. This role does not provide access to billing reports that are required by the finance department.

Option C is not suitable because roles/container admin role is for managing Kubernetes and container-related resources. This role is not related to billing reports, and the finance department would not be able to access the required information with this role.

In conclusion, option D is the appropriate choice as it grants the finance department access to the billing reports of various projects without receiving additional permissions. The other roles provided in Options A, B, and C are not aligned with the specific needs of the finance department concerning billing reports.

Solution to Question 34: C

The correct answer is C. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage. Here's why:

Option A is not suitable because Data Studio reports focus on Admin Activity Audit Logs, which capture high-level information on administrative actions, not data access events in Cloud Storage buckets. These logs do not record the details required to specifically review who accessed data in the buckets.

Option B isn't appropriate because VPC Flow Logs monitor network traffic, not data access. VPC Flow Logs collect metadata about every packet that enters

or leaves the VPC, which is useful for network troubleshooting and security but cannot provide insights about who accessed data within Cloud Storage buckets.

Option C is the correct choice because Data Access Logs can record events related to data access for Google Cloud services, including Cloud Storage. By turning on Data Access Logs for the relevant buckets and building a query in the log viewer, you can easily filter and provide the required information for the auditor.

Option D is not suitable because the export logs API deals with Admin Activity Audit Logs, which, as mentioned earlier, do not provide detailed information about data access events in Cloud Storage buckets.

Thus, to assist the auditor in reviewing data access events in Cloud Storage buckets, you should turn on Data Access Logs for the necessary buckets and build a query in the log viewer that filters specifically on Cloud Storage (Option C).

Solution to Question 35: C

The correct answer is C. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

The reason behind choosing option C is that it addresses the specific resource requirements of the image rendering microservice and the other microservices separately. The compute-optimized machine type nodes are better suited for the image rendering microservice's CPU-intensive tasks, while the general-purpose machine type nodes like n2-standard are suitable for the other workloads. By utilizing separate node pools with appropriate machine types, the cluster can maximize resource efficiency and maintain optimal performance for all the microservices.

Option A is incorrect because assigning a higher pod priority to the image rendering microservice does not solve the problem of resource efficiency. Pod priority affects scheduling decisions but does not change the hardware resources needed for an efficient workload.

Option B is not optimal because even though setting up autoscaling can help manage the demands of the image rendering microservice, using the same general-purpose machine type nodes for all microservices does not optimize resource efficiency for the CPU-intensive image rendering workload.

Option D is not the best solution because it only addresses resource allocation in the image rendering microservice deployment configuration but does not consider the specific resource requirements on different machine types. This approach could cause inefficient resource usage across the cluster.

In conclusion, option C provides the most efficient use of resources and best performance for both the image rendering microservice and the other microservices

by creating separate node pools with appropriate machine type nodes for each workload.

Solution to Question 36: C

The correct answer is C. To understand why the other options will not work, let's analyze each of them.

Option A proposes creating a new VPC peering connection between the two existing VPCs and updating route tables. VPC peering might be useful for connecting distinct VPCs, but it doesn't directly address the requirement of allowing traffic between Compute Engine instances across different GCP projects. Moreover, VPC peering requires that the IP address ranges do not overlap, which might be an issue depending on the existing infrastructure.

Option B suggests verifying your role as a Project Administrator and creating two new VPCs with all instances from both projects. This option will not solve the issue as it doesn't establish any connectivity between the new VPCs. Also, the instances are still in separate VPCs, and no communication pathway is created for them to communicate with each other.

Option C, the correct answer, suggests verifying that both projects are in a GCP Organization and sharing the VPC from one project. By using a shared VPC, you can enable Compute Engine instances from distinct projects within the same organization to communicate and use services across the VPCs, effectively solving the problem.

Option D advises creating a new Shared VPC and configuring firewall rules. However, this option would require moving all instances to the new Shared VPC, which might not be feasible due to several reasons such as IP address conflicts, migration complexities, and downtime concerns.

Hence, the best option to enable traffic between Compute Engine instances in two separate GCP projects is Option C, as it leverages shared VPC functionality to establish communication between instances in distinct projects within the same organization.

Solution to Question 37: C

The answer should be C: Go to Cloud Shell and run gcloud config list to review the Google Cloud configuration used for deployment.

Explanation: This option is the most relevant in this situation because it allows you to check the current active project configuration, which is used when deploying your App Engine application with gcloud app deploy. By examining the configuration, you can identify if the project is set to the intended project or another one. This will provide you with the necessary information to understand why the application was deployed to the wrong project.

Reasons other options won't work:

A: Review the gcloud app deploy command for any typos or incorrect parameters. Although checking for errors in the command is necessary, in this case, the error lies in the incorrect project being deployed to, not the command itself. Also, the issue could be caused by a misconfigured gcloud environment rather than a typo or incorrect parameter in the command.

B: Confirm that App Engine is enabled in the API Library for the intended project. This option is not directly related to the issue of deploying to the wrong project. While you would need App Engine enabled in the project you intended to deploy to, it wouldn't prevent a deployment to a different project if your gcloud configuration was set to that other project.

D: Run gcloud projects list to verify the proper project ID for the intended project. While this option might help identify the correct project ID, it does not address the problem of the App Engine application being deployed to the wrong project. The main issue lies in the Google Cloud configuration itself, and not verifying the proper project ID. Even if you knew the correct project ID, it wouldn't help if your gcloud configuration was set to another project.

Solution to Question 38: A

The correct answer is A. The use of the gcloud compute ssh command with the –tunnel-through-iap flag ensures a secure and cost-effective solution for logging into Linux instances hosted on Google Cloud. The Identity-Aware Proxy (IAP) works as an intermediary that helps to authenticate users and validate their access without the need for public exposiure of the instances. By allowing ingress traffic from the IP range 35.235.240.0/20 on port 22, you restrict access only to connections coming through Google's IAP, enhancing security.

Reasons why the other options will not work:

Option B: Granting all users the Compute Engine Instance Admin role to manage instances and access them through Google Cloud Console SSH may not be cost-effective and secure. By providing all users this level of permissions, you can increase the risk of unauthorized changes to your instances, and it does not follow the least privilege principle.

Option C: Using a proxy server with public internet access and allowing traffic on port 22 for SSH might initially seem like a good solution, but it introduces additional complexities in managing proxy server security and can be prone to misconfiguration or public exposure. It also incurs costs for managing and maintaining the proxy server, making it a less cost-effective solution compared to using IAP.

Option D: Creating a GCP load balancer for forwarding connections to instances on port 22 is not a suitable solution for this use case. Load balancers are designed for distributing network traffic to multiple instances for the purpose of balancing loads or ensuring high availability. This method would not increase the security of instance access and would not be cost-effective, as you would have to pay for the load balancer service.

Solution to Question 39: D

The correct answer is D: Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

Explanation:

Option A is not correct because App Engine API is used for developing and hosting web applications, not for managing Compute Engine instances. Additionally, creating instances in Compute Engine is not part of the default configuration of App Engine.

Option B is incorrect because Firestore API is used for a NoSQL database service provided by Google Cloud, and it is not necessary for creating Compute Engine instances. Although you can use the Cloud SDK to create a Compute Engine instance after creating the new project, enabling the Firestore API is irrelevant and not needed in this case.

Option C is also incorrect because creating a service account is an intermediate step that is not necessary for developing a Compute Engine instance. The main goal here is to create a project, enable Compute Engine API, and create an instance.

Option D is correct because it outlines a straightforward process to achieve the given task:

1. Create a new project using the Cloud SDK by executing `gcloud projects create [PROJECT_ID]`.
2. Enable the Compute Engine API with `gcloud services enable compute.googleapis.com --project=[PROJECT_ID]` in order to create Compute Engine instances in the new project.
3. Create the Compute Engine instance by running `gcloud compute instances create [INSTANCE_NAME] --project=[PROJECT_ID]`.

In this way, Option D correctly covers the steps needed to create a new project and then create a Compute Engine instance while enabling the required API in the project.

Solution to Question 40: D

The correct answer is D: Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files. Here's why:

D is correct because it follows Google-recommended practices and avoids writing any code for the migration:

1. Transfer Appliance: Moving 200 TB of video files from on-premises SAN storage to Google Cloud Storage is a large-scale task. Transfer Appliance is specifically designed for large-scale data transfers. It is more efficient

and secure than traditional migration methods, like internet transfers, and doesn't require any code.

2. BigQuery Data Transfer Service: This is a fully managed, no-code service designed to move data from external data sources, like Amazon Redshift, into Google's BigQuery, which is the right destination for data warehouse data. It is specifically designed for cases like this and doesn't require coding.
3. Storage Transfer Service: This is a managed, no-code service that moves data from external sources, like Amazon S3, to Google Cloud Storage, making it the perfect fit for transferring 20 GB of PNG files in an S3 bucket to another Cloud Storage bucket.

The other options are incorrect because they don't follow Google best practices and may require coding:

A. Cloud SQL is not designed for moving video files, and using it to migrate SAN storage data to Google Cloud Storage is not recommended. Dataflow can migrate data warehouse data, but using it to move data from Amazon Redshift would require writing custom code, which goes against the question's requirements. Cloud Storage is the correct choice for the PNG files, but the rest of the option is not appropriate.

B. Dataflow is a managed service for stream and batch data processing, but using it for transferring 200 TB of video files requires coding and is not ideal. Cloud Data Fusion is meant for data integration and transformation, but it requires coding and configuring pipelines, which goes against the question's requirements. Transfer Appliance would be a more efficient method for transferring the PNG files but using it for only 20 GB of data is not cost-effective and not its intended use case.

C. Storage Transfer Service is a good option for moving data between cloud storage services, like Amazon S3 to Google Cloud Storage, but not optimized for on-premises large-scale migrations like 200 TB of video files. Dataproc is designed for running Hadoop or Spark clusters and requires writing custom code for migrating data warehouse data from Amazon Redshift, which goes against the question's requirements.

Solution to Question 41: B

The correct answer is B. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

Explanation:

In the given scenario, the nightly batch workload can tolerate some VMs being terminated, but the current cost of VMs is high. This calls for a solution that reduces costs while maintaining fault tolerance. Spot N2 Standard VMs are known to offer significant cost savings compared to regular VMs because

they utilize spare compute capacity in Google Cloud. They can, however, be terminated with a short notice if a higher-priority workload is needed.

Option B is the correct choice because using Spot N2 Standard VMs would help reduce costs without compromising the workload's fault tolerance, given that it can endure some VMs' termination. By running a test with simulated maintenance events, you can ensure that the workload will still function as required even if some VMs are terminated.

Option A involves using the Compute Engine Autoscaler with N2 Standard VMs. However, it does not specifically address cost reduction, as the focus of Autoscaler is on adjusting the number of VMs based on demand rather than cost optimization.

Option C suggests running a test using Cloud Run and potentially migrating the workload to Cloud Run. This option may offer some cost savings due to its pay-per-use model. However, since the Cloud Run platform is optimized for stateless, short-lived tasks, it might not be compatible with a nightly batch workload that requires a large number of VMs. This makes it a less suitable option.

Option D recommends running a test using Cloud Dataproc with preemptible VMs and then using Cloud Dataproc with N2 Standard VMs for future jobs. While preemptible VMs might reduce costs, Cloud Dataproc is primarily designed for running Apache Spark and Hadoop workloads. If the nightly batch workload is not based on these frameworks, using Cloud Dataproc might not be applicable to the given scenario. Furthermore, using N2 Standard VMs in the long run does not guarantee cost reduction.

In conclusion, B is the most suitable option, as using Spot N2 Standard VMs helps reduce the cost of VMs without compromising the workload's fault tolerance, aligning well with the requirements of the given scenario.

Solution to Question 42: A

The correct answer is A. Add the user to roles/iam.serviceAccountAdmin role. This is because the Service Account Admin role allows the user to create, manage, and delete service accounts within the Google Cloud projects. This role aligns with the specialist's responsibilities, ensuring that they can effectively organize and manage the projects.

Here's why the other options will not work:

B. Add the user to roles/iam.securityAdmin role: The Security Admin role is broader in scope; it grants permissions to manage Identity and Access Management (IAM) policies, roles, and configurations. While it does include some service account-related tasks, it goes beyond the specialist's responsibility. Thus, assigning this role would not adhere to the principle of least privilege, which aims to limit users' access only to the resources they need.

C. Add the user to roles/iam.serviceAccountSecurityManager role: This role does not exist in Google Cloud IAM. Hence, it cannot be assigned to the specialist.

D. Add the user to roles/iam.serviceAccountCreator role: The Service Account Creator role only allows the user to create service accounts. It doesn't grant them the permissions to manage or delete existing service accounts, making it an insufficient choice for the specialist's responsibilities.

In conclusion, assigning the specialist the roles/iam.serviceAccountAdmin role (Option A) is the appropriate choice, as it grants them the necessary permissions to create, manage, and delete service accounts within Google Cloud projects while adhering to the principle of least privilege.

Solution to Question 43: A

The correct answer is A. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

Here's why A is the best option and the other options are not effective:

A: Data Access audit logs in Google Cloud Logging provide insights into which users accessed and/or modified data within specific Google Cloud services (such as Cloud Storage, BigQuery, and others). By searching for the terminated employee's email (used as their identity) in the principal field, you can filter the logs to reveal any data access events involving that user. This allows you to determine if the employee accessed any confidential client data during the period between their termination and access revocation.

B: System Event Logs focus on tracking changes to resource configurations and may not necessarily contain any information about data access by specific users. Searching for the user's email in resource.labels values would not yield the required information about the terminated employee accessing confidential client data.

C: VPC Flow Logs record network traffic within the Google Cloud Virtual Private Cloud (VPC), including the IP addresses involved in various network flows. However, these logs do not specifically track user-level data access events within Google Cloud services. Searching for the IP address associated with the user in VPC Flow Logs would not be sufficient to determine if the terminated employee accessed confidential client data.

D: Admin Activity logs in Google Cloud Auditing are focused on administrative activities, such as creating, modifying or deleting resources within Google Cloud services. This log type does not provide information about user-level data access events. Searching for the user's email as the principal in Admin Activity logs would not help you confirm whether the terminated employee accessed confidential client data during the specified period.

In conclusion, option A (viewing Data Access audit logs and searching for the user's email as the principal) is the most effective way to investigate whether

the terminated employee accessed any confidential client data during the two weeks when their access was not revoked.

Solution to Question 44: D

The correct answer is D, and here's why:

Option D allows you to effectively log all read and write operations, including metadata and configuration reads, of the Bigtable instance with the company's SIEM system. By enabling Data Read, Data Write, and Admin Read logs in the Audit Logs page for the Bigtable instance, you capture all the necessary access details. Then, by creating a Pub/Sub topic as a Cloud Logging sink destination and adding your SIEM as a subscriber to the topic, you ensure that these logs are forwarded to the SIEM system for analysis and monitoring.

On the other hand, the other options do not meet the requirements or work as efficiently:

Option A is not the best solution, as creating a custom monitoring job in Cloud Monitoring with a webhook alert does not provide the level of granularity needed to log all the read and write operations, including metadata or configuration reads. Additionally, this approach is more suitable for generating alerts based on specific metric thresholds, rather than logging all data operations.

Option B is not suitable because it involves creating custom log-based metrics in Cloud Monitoring to track the Bigtable operations, but this would only monitor specific log events and not all the required read and write operations, including metadata and configuration reads. Moreover, exporting log-based metrics would send only summarized metric data to the company's SIEM system instead of the detailed logs required.

Option C is not an appropriate solution, as applying a Cloud Identity Access Management (IAM) policy with custom roles for read/write actions only controls access permissions to the Bigtable instance and does not allow for extensive logging of all read and write operations, including metadata or configuration reads. Tracking these actions in your SIEM system would require additional steps that aren't mentioned in this option.

Solution to Question 45: B

The correct answer is B: Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

Explanation:

As a system administrator, it's important to ensure that your managed instance group is able to create new instances to handle the expected application traffic. In this situation, the creation of new instances has failed most likely because there's a conflict in the instance template syntax or naming, preventing the instances from being created.

Answer B is the best option because it tackles the problem by creating a new instance template containing valid syntax and deleting any potentially problematic persistent disks with the same names as the instances. This will resolve any conflicts and ensure that the instance group is able to create new instances as needed.

Option A is not correct because, while it does suggest creating a new instance template and checking for conflicts in instance names and persistent disk names, it also includes setting the disks.autoDelete property to true. This may not be necessary and could actually cause unwanted data loss if the instances are deleted automatically alongside their attached persistent disks.

Option C is not correct because, while it suggests updating the instance group's autoscaling policy and creating a new instance template with valid syntax, it does not address the potential issue of conflicting instance names and persistent disk names, which could still lead to instance creation failures.

Option D is not appropriate because changing the instance group's region is not guaranteed to resolve the instance creation issue. It may cause additional complications due to regional differences in services and resources. Moreover, just creating an instance template that contains valid syntax does not address the naming conflicts, which must be resolved as per the correct option B.

In conclusion, the most suitable course of action to ensure enough instances are running in your company's infrastructure is option B: create an instance template with valid syntax and delete any persistent disks with the same name as instance names. This will resolve naming conflicts and syntax issues, allowing the managed instance group to create new instances as needed.

Solution to Question 46: C

The correct answer is C. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

Explanation:

To provide the three developers with the ability to view and edit table data on a Cloud Spanner instance, you need to grant them the appropriate IAM role. In this case, the required role is roles/spanner.databaseUser.

Option A is incorrect because adding the users directly to the role without creating a group would make the IAM policy management more challenging, especially when there is a need to provide similar access to additional developers in the future.

Option B is incorrect because it is insufficient to just describe the IAM role in the context of a specific project (my-project). There should be a group created with the developers added to it, and the group should be added to the role.

Option C is correct because it involves describing the IAM role, creating a new group, adding the developers to the group, and then adding the group to the

role. This way, it makes IAM policy management easier and more efficient.

Option D is incorrect because it only adds one user (email@example.com) to the roles/spanner.databaseUser role. The question requires you to give access to three developers.

Solution to Question 47: B

The correct answer is B. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources. This is because the "-preview" option allows you to see the impact of your changes without actually modifying the running resources. It quickly validates the dependencies of all resources in the template, providing immediate feedback on whether or not the template is functioning properly. This approach is the most time-efficient and accurate way to verify that the interdependencies are met before committing the changes to the project.

Option A is not the right choice because creating a separate Deployment Manager branch and using GitHub integration is focused on avoiding conflicts in version control, rather than verifying resource dependencies. Although this might be helpful for managing changes in the code, it does not provide immediate feedback on the correctness of the template.

Option C is not ideal as leveraging a custom Cloud Function would be an over-engineered solution that involves writing additional code to validate the template's resource dependencies. While it may work, it does not provide the quickest and easiest way to test the changes, as it requires extra development work.

Option D is also incorrect because copying the Deployment Manager template to a separate storage bucket and setting up object versioning only tracks changes over time but does not validate the resource dependencies or ensure they are working as intended. This method focuses on historical tracking rather than providing immediate feedback on the correctness of the template.

Solution to Question 48: B

The correct approach in this scenario would be option B: Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity. This is because it provides a scalable, secure, and efficient solution for managing a rapidly growing workforce.

Option B is the best approach for the following reasons:

1. Scalability - Organizing users into groups in Cloud Identity makes it easier to manage a large number of employees. Instead of dealing with individual accounts, you can perform mass operations for a specific group, which simplifies administration and reduces the risk of human errors.
2. Security - Multi-factor authentication (MFA) strengthens security by requiring employees to verify their identity using multiple methods, such as

a password and a one-time code from a mobile device. This additional layer of security drastically reduces unauthorized access to the company's Google Cloud account.

3. Centralized management - By using Cloud Identity, you can set up centralized policies and permissions for your groups, making it easier to manage access rights without complex configurations and manual interventions.

The other options are not viable due to their limitations and potential risks:

Option A: Turning on Google Cloud Directory Sync (GCDS) for Cloud Identity may help with syncing users, but it is a one-way sync that doesn't provide real-time updates or handle permissions and policies. Skipping multi-factor authentication exposes the company to security risks, especially with a growing workforce.

Option C: Importing and exporting all users manually to Google Cloud Storage is not an efficient nor scalable solution, and it also poses security risks. As the workforce grows, managing user accounts manually would be time-consuming and error-prone, which increases the likelihood of unauthorized access.

Option D: Using the built-in GCP Admin Tools without integration may work for a small number of accounts, but it doesn't scale for a company expecting to grow to 1,000 employees. It would require substantial manual effort to manage configurations and access rights while potentially introducing human errors.

In conclusion, the most suitable approach to manage the growing workforce is option B, which allows for scalable, efficient, and secure user management in Google Cloud by organizing users into groups in Cloud Identity and enforcing multi-factor authentication.

Solution to Question 49: B

The correct answer is B: Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

Explanation:

A rolling update is an approach that allows you to apply updates to your running application instances in a managed instance group without causing any downtime, and without requiring you to manually control the updates. By performing a rolling-action start-update, you can ensure that your application remains available during the update process. In this situation, you need to maintain the available capacity during the deployment, which is why the maxSurge and maxUnavailable settings are important.

Option B is the best approach because setting maxSurge to 1 and maxUnavailable to 0 would allow for one additional instance to be created during the update, ensuring that there is no reduction in the overall instance capacity. This would enable the new instance to be brought online while the existing instances are

updated, allowing the application to continue functioning with minimal disruption.

Here's why the other options will not work:

Option A (maxSurge = 0, maxUnavailable = 1): This approach would mean that no additional instances would be created during the update, and one instance would be taken down for the update. This reduces the available capacity, violating the requirement to maintain available capacity during deployment.

Option C (maxSurge = 0, maxUnavailable = 0): This approach would not allow any instances to be removed or added during the update, which means that the instances would not be updated at all.

Option D: Manually updating each VM instance within the managed instance group without using a rolling update would be a time-consuming and error-prone process. Also, without the rolling update functionality, there is a significant risk of accidentally causing downtime or resource constraint issues during the deployment process.

In conclusion, option B is the most suitable approach because it maintains the available capacity throughout the deployment process and allows for a smooth, gradual update of the instances without any downtime.

Solution to Question 50: D

The correct answer is D.

Option A is incorrect because Kubernetes Engine cannot directly deploy a Dockerfile from Cloud Storage. Instead, you need to create a Docker image from the Dockerfile and host that image in a container registry, such as Google Container Registry.

Option B is incorrect because Datastore is not a container registry. Datastore is a highly-scalable NoSQL database used for storing structured data, not for hosting container images. In this case, you need to use Container Registry or another container image storage solution to store the Docker image.

Option C is incorrect because the 'gcloud compute instances create' command is used for creating Google Compute Engine instances, not for deploying Docker containers to Kubernetes Engine. To deploy Docker containers on Kubernetes Engine, you need to use 'kubectl' commands to create the deployments based on the deployment YAML file.

Option D is correct because it follows the proper procedure for deploying a Dockerfile on Kubernetes Engine. Firstly, you create a Docker image from the Dockerfile and then host it on a container registry such as Google Container Registry. Next, you create a deployment YAML file that references the uploaded Docker image. Finally, you use the 'kubectl' command to create the deployment, which will run the containers based on the provided YAML file.

Practice Exam 8

Question 1: You are working as a cloud engineer in a company that uses Google Cloud for managing multiple services. Your main responsibility is to ensure the security and accessibility of applications running on different Google Cloud projects. One such application is spread across web-applications and crm-databases-proj projects. Virtual machines (VMs) in the web-applications project require access to BigQuery datasets in the crm-databases-proj project. Your task is to grant access to the service account in the web-applications project following Google-recommended best practices. How should you proceed?

A. Grant bigquery.dataViewer role to crm-databases-proj and bigquery.dataOwner role to web-applications project.

B. Give project owner role to crm-databases-proj and the web-applications project.

C. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

D. Give project owner role to crm-databases-proj and bigquery.dataViewer role to web-applications.

Question 2: You are working as a Cloud Engineer at a software development company, and you need to start a new Compute Engine instance in two different Google Cloud Platform accounts managed by the company. One account is in the default region and zone, while the other is in a non-default region and zone. What is the most appropriate way to accomplish this task using the command line interface?

A. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud config list to start the Compute Engine instances.

B. Create separate shell scripts for each account and specify the gcloud command to start Compute Engine instances with specific zone and region flags.

C. Run gcloud config set compute/zone [ZONE] and gcloud config set compute/region [REGION] to set the default zone and region for each account before starting the Compute Engine instances.

D. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

Question 3: As a recently hired IT manager at a growing tech company, you've been tasked with merging the IT systems after acquiring a startup. The acquired startup has a production Google Cloud project within their organization that needs to be transferred to your company and billed under your organization's account. What is the most efficient method to complete this task?

A. Create Kubernetes manifests for all resources in the project, deploy them to

a Kubernetes cluster in your organization, and then delete the project from the startup's Google Cloud organization.

B. Create a Google Cloud Storage bucket for each organization, export all resources from the startup's project to a bucket, and import them into a new project in your organization.

C. Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

D. Create an infrastructure-as-code template for all resources in the project by using Terraform, and deploy that template to a new project in your organization. Delete the project from the startup's Google Cloud organization.

Question 4: As a leading software developer at a prominent AI research company, you are overseeing the management of a Google Kubernetes Engine (GKE) cluster utilized by various teams for non-production workloads. The Machine Learning (ML) team requires access to Nvidia Tesla P100 GPUs to effectively train their models. Your goal is to achieve this with minimal effort and cost. What strategy should you implement?

A. Ask your ML team to use TPUs instead of GPUs for their training.

B. Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

C. Ask your ML team to add the accelerator: gpu annotation to their pod specification.

D. Enable GPUs on the existing nodes, but don't create a dedicated node pool.

Question 5: As a software engineer at a tech company, you've been assigned a task to deploy a workload to a Kubernetes cluster by your manager. You're uncertain about the workload's resource requirements, which could vary based on usage patterns, external dependencies, or other factors. To make cost-effective recommendations for CPU and memory requirements while ensuring consistent performance in any situation, you need to follow Google-recommended practices. What should you do?

A. Configure the Cluster autoscaler for availability, and configure the Horizontal Pod Autoscaler for cost optimization.

B. Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

C. Configure the Vertical Pod Autoscaler recommendations for availability, and configure the Cluster autoscaler for suggestions.

D. Configure the Horizontal Pod Autoscaler for availability, and configure the cluster autoscaler for suggestions.

Question 6: In your company, you are managing a Compute Engine instance hosting a crucial business application, which is actively utilized between 9 AM and 6 PM on weekdays. For disaster recovery purposes, you need to perform daily backups of this instance and maintain them for a duration of 30 days. Your goal is to implement a Google-recommended solution that minimizes management overhead and requires the least number of services. What steps should you take?

A. 1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk. 2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM - 2:00 AM - Autodelete snapshots after: 30 days

B. 1. Create a Dataflow job that backs up the instance's disk to BigQuery daily. 2. Configure the Dataflow job to delete the backups older than 30 days.

C. 6. Create a Cloud Composer environment to schedule a DAG that creates and deletes snapshots of your instance's disk daily with a 30-day retention period.

D. 4. Set up Data Loss Prevention (DLP) on the instance's disk to automatically back up the data daily and delete backups older than 30 days.

Question 7: You are working as a cloud architect in a leading software company, and it's your task to set up a Google Kubernetes Engine cluster that ensures verifiable node identity and integrity. In addition, the nodes should not be accessible from the internet, and you must minimize the operational cost of managing the cluster while following Google-recommended practices. What should you do?

A. Deploy a private DataProc cluster and enable shielded nodes.

B. Deploy a private autopilot cluster.

C. Deploy a private zonal cluster and enable shielded nodes.

D. Deploy a public Cloud SQL instance with shielded nodes enabled.

Question 8: As a system administrator at a software development company, you are responsible for managing a critical workload running on Google Compute Engine. To ensure business continuity, you want to regularly back up the data on the boot disk and restore it as quickly as possible in case of disaster, while adhering to Google-recommended best practices. Additionally, you need to automatically clean older backups to save on cost. What approach should you take?

A. Create a Managed Instance Group using the existing instance as a template.

B. Create a snapshot schedule for the disk using the desired interval.

C. Create a Cloud Scheduler job to clone the VM instance at the desired interval.

D. Use Cloud Memorystore for Redis to keep regular copies of the boot disk data.

Question 9: As a software engineer in a tech company, you are managing a virtual machine configured with 2 vCPUs and 4 GB of memory. You notice that the machine is running out of memory, and you decide to upgrade it to 8 GB. What is the most appropriate action to take?

A. Rely on live migration to move the workload to a machine with more memory.

B. Upgrade the Cloud SDK to allow for increased memory usage.

C. Stop the VM, increase the memory to 8 GB, and start the VM.

D. Stop the VM, change the machine type to n1-standard-8, and start the VM.

Question 10: As a data engineer at a multinational corporation, you are tasked with handling a large quantity of unstructured data stored in various file formats. The company wants to perform ETL transformations on this data and process it using a Dataflow job on Google Cloud. What should be your approach to make the data accessible on Google Cloud?

A. Upload the data to BigQuery using the bq command line tool.

B. Upload the data to Cloud Pub/Sub using the gcloud command line tool.

C. Upload the data into Cloud SQL using the import function in the console.

D. Upload the data to Cloud Storage using the gsutil command line tool.

Question 11: You are working as a Cloud Infrastructure Specialist in a company that relies heavily on a single batch process, running on an on-premises server. This task takes around 30 hours to complete, runs monthly, and can be performed offline. However, it has to be restarted if interrupted. The company wants to migrate this workload to the cloud while keeping costs to a minimum. How should you proceed?

A. Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

B. Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.

C. Migrate the workload to Cloud SQL for batch processing.

D. Host the workload on a Cloud Storage bucket and use Pub/Sub for event-driven processing.

Question 12: As a data analyst at a marketing company, you rely on Looker Studio to visualize a table from your data warehouse built on BigQuery. The data is appended during the day, and the daily summary is recalculated at night by overwriting the table. You've just realized that the charts in Looker Studio are malfunctioning, and you need to diagnose the issue. What steps should you take?

A. Verify Cloud Dataflow pipeline for any data ingesting issues in the Google Cloud platform.

B. Inspect the data warehouse's schema in the BigQuery console to identify any inconsistencies.

C. Contact the Looker Studio support team for assistance in resolving the issue.

D. Use the BigQuery interface to review the nightly job and look for any errors.

Question 13: As an IT manager in a financial company, you are developing an application to handle transactions on Google Kubernetes Engine. You've decided MongoDB is the ideal database system and require a managed MongoDB environment with support SLA for the application. What is the best course of action?

A. Deploy MongoDB Atlas from the Google Cloud Marketplace.

B. Download a MongoDB installation package, and run it on a Managed Instance Group.

C. Create a Cloud Dataproc cluster and use the MongoDB connector for Hadoop.

D. Download a MongoDB installation package, and run it on Compute Engine instances.

Question 14: As a financial analyst at a technology company, you are responsible for monitoring and analyzing the costs associated with multiple projects linked to a single billing account in Google Cloud. You need to create visualizations with specific metrics that should be dynamically calculated based on company-specific criteria, and you want to automate this process. How should you achieve this?

A. Leverage Google Cloud Monitoring to create alerts based on cost metrics, and view cost breakdowns through the Monitoring dashboard.

B. Use Stackdriver Monitoring to create custom cost metrics for the projects and visualize them in the Google Cloud console.

C. Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery export.

D. Create a Cloud Function that pulls data from the billing account and sends it to Google Sheets for visualization.

Question 15: As a software engineer in a gaming company, you are tasked with developing a multiplayer gaming interface that would store game data in a database. The company aims to maintain consistent performance as the game gains popularity, without increasing management complexity. How can you ensure optimal gaming experience for users across the globe?

A. Use Cloud Bigtable to store game statistics with a hashed timestamp as the row key for global consistency.

B. Use Cloud Spanner to store user data mapped to the game statistics.

C. Use Cloud SQL database with cross-region replication to store game statistics in the EU, US, and APAC regions.

D. Use Firebase Realtime Database to store game statistics with a master-master replication system for global consistency.

Question 16: As part of your job at a software development company, you are tasked with managing a third-party application that will run on a Compute Engine instance. The company already has other Compute Engine instances running with default configuration, and the application installation files are stored on Cloud Storage. Your responsibility is to access these files from the new instance without allowing other virtual machines (VMs) to access them. What should you do?

A. Create a new service account and assign this service account to the new instance. Use Cloud Identity-Aware Proxy (IAP) to secure access to Cloud Storage objects.

B. Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

C. Create a new service account and assign this service account to the new instance. Change the storage class of objects on Cloud Storage to Nearline storage.

D. Create a new service account and assign this service account to all instances. Grant the service account permissions on Cloud Storage.

Question 17: As a project manager in a software development company, you recently found out that several team members have been initiating Cloud Platform projects and paying for them using their personal credit cards, which the company later reimburses. The management now intends to consolidate all these projects under a single, new billing account. What is the most appropriate course of action to achieve this?

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

B. Contact the GCP sales team to request a new, centralized billing account for your company's projects.

C. In the Cloud Console, create a new billing account and manually transfer each employee's project to the root Organization.

D. Create a Google Group for your company, and invite all employees to join. Use this group to combine all billing accounts.

Question 18: As a developer at a tech company, you are tasked with creating a list of the enabled Google Cloud Platform APIs for a project named "my-project" using the gcloud command line in the Cloud Shell. What is the appropriate course of action to take?

A. Run gcloud info to view the account value, and then run gcloud services list –account .

B. Run gcloud init to set the current project to my-project, and then run gcloud services describe my-project.

C. Run gcloud init to set the current project to my-project, and then run gcloud services list –available.

D. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

Question 19: You are a software engineer at a tech company, and your team's application is hosted on a general-purpose Compute Engine instance. The application is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk while reading large files. The disk size currently stands at 350 GB. Your task is to maximize throughput and minimize costs for the company. What action should you take?

A. Migrate to use a multi-regional Cloud Storage bucket.

B. Use Cloud Storage instead of a Zonal SSD Persistent Disk.

C. Migrate to use a Local SSD on the instance.

D. Increase the size of the disk to 2 TB.

Question 20: As a cloud engineer at a large company, you are responsible for monitoring resources distributed over different projects in Google Cloud Platform. Your goal is to consolidate reporting under a single Stackdriver Monitoring dashboard. What is the best approach to achieve this?

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

B. Install the Stackdriver Monitoring agent on each project and use Google Cloud Pub/Sub to aggregate the data.

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

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

Question 21: You are a security administrator at a tech company and have noticed that your development team is using numerous service account keys during their development process. To quickly implement a process that enforces short-lived service account credentials within the company, you need to meet the following requirements:

• All service accounts requiring a key should be created in a centralized project called pj-sa. • Service account keys should only be valid for one day.

Which Google-recommended solution should you choose to minimize cost?

A. Implement a Cloud Functions job to rotate all service account keys daily in pj-sa. Enforce an org policy denying service account key creation with an exception to pj-sa.

B. Implement a Cloud Run job to rotate all service account keys periodically in pj-sa. Enforce an org policy to deny service account key creation with an exception to pj-sa.

C. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

D. Use a custom App Engine task runner to rotate service account keys every day. Enforce an org policy to allow service account key creation with no exceptions across all projects.

Question 22: As an IT administrator at a large company, you have user identities stored in Active Directory. The company wants to continue using Active Directory as the primary source of truth for identities. At the same time, they wish to maintain full control over the Google accounts employees use for all Google services, including Google Cloud Platform (GCP) organization. What is the best course of action?

A. Set up a SAML Single Sign-On (SSO) connection between Active Directory and GCP without synchronizing users.

B. Export users from Active Directory as a CSV and import them to Cloud Identity via the Admin Console.

C. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

D. Use Active Directory Sync Protocol (ADSP) to synchronize users into Cloud Identity.

Question 23: As a data security analyst at a major financial company, you are responsible for monitoring sensitive data stored in three Cloud Storage buckets where data access logging is enabled. Your task is to verify activities for a specific user on these buckets, ensuring the addition of metadata labels and identification of the files accessed from those buckets. What is the most efficient way to accomplish this task?

A. Use Cloud Pub/Sub to access the logs and filter the activity you need to verify.

B. View the bucket in the Storage section of the GCP Console.

C. Using the GCP Console, filter the Activity log to view the information.

D. Enable and configure Google Cloud Armor to view the logs.

Question 24: As an IT expert in a company that is implementing the Cloud Identity platform, you need to add a group of new users, some of whom already

have existing Google accounts. In order to follow Google's best practices and prevent account conflicts, what should you do?

A. Ask the user to create a separate Google Workspace account and migrate their data.

B. Create a new Google account for each user.

C. Invite the user to transfer their existing account.

D. Tell the user that they must delete their existing account.

Question 25: As a network administrator at a tech company, you need to deploy a new Compute Engine instance on the Google Cloud Virtual Private Cloud (VPC) architecture that is connected to the company's WAN via a VPN. The new instance must not be accessible via public Internet traffic. What is the most appropriate course of action to achieve this?

A. Use VPC Service Controls to limit access to the instance.

B. Create the instance without a public IP address.

C. Create a subnet with Private Google Access and deploy the instance in it.

D. Restrict the instance to only allow traffic from on-premises WAN IP addresses.

Question 26: You are part of a software development company that specializes in building applications for various industries. One of your current projects involves running multiple microservices in a Kubernetes Engine cluster. The microservice in charge of image rendering demands more CPU time than memory. Meanwhile, the other microservices are optimized for n1-standard machine types. To ensure efficient resource utilization across all workloads, what should your team do?

A. Increase the number of replicas for the image rendering microservice without changing machine types.

B. Use memory-optimized machine type nodes for the image rendering microservice and compute-optimized machine type nodes for the other microservices.

C. Enable vertical pod autoscaling for the image rendering microservice and horizontal pod autoscaling for the other microservices.

D. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Question 27: As a leading software development company with clients in various industries, your business is transitioning from an on-premises setup to Google Cloud. With multiple teams of developers working on projects that use Cassandra environments as backend databases, it is essential to provide each of them with an isolated development environment. To swiftly move to Google

Cloud and minimize the need for support, what course of action should be taken?

A. 1. Set up a Cloud Dataproc cluster and install Cassandra on it. 2. Configure the cluster for each development team to access their own isolated environment.

B. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

C. 1. Deploy a Pub/Sub topic for each development team and use Dataflow to process the messages to simulate a Cassandra-like environment. 2. Restrict access using Cloud IAM policies.

D. 1. Build a Cassandra Compute Engine instance and take a snapshot of it. 2. Use the snapshot to create instances for your developers.

Question 28: As a web developer working in a technology company, you are designing a new web application that will be hosted on Google Cloud Platform. You need to implement a release cycle that allows you to test updates on real user traffic but only affect a small portion of the users, while most users should continue interacting with a stable version. How should you proceed?

A. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

B. Deploy the application on Cloud Functions and create a new function for each update. Update the HTTP trigger to direct a small percentage of traffic to the new function.

C. Deploy the application on Kubernetes Engine. For a new release, update the deployment to use the new version.

D. Deploy the application on Kubernetes Engine and use a StatefulSet for each update. Configure traffic splitting through a Kubernetes Ingress to direct a small percentage of traffic to the new StatefulSet.

Question 29: You are working as a cloud administrator at a software company, and you have been asked to add a new auditor to one of your company's Google Cloud Platform projects. The auditor needs to have read access to all project items without the ability to modify them. How should you configure the auditor's permissions?

A. Add the user to the IAM Billing Account Viewer role with project-wide permissions. Add the user's account to this role.

B. Select the built-in IAM service Viewer role. Add the user's account to this role.

C. Select the built-in IAM project Viewer role. Add the user's account to this role.

D. Assign the user to the IAM BigQuery Data Viewer role with project-wide permissions. Add the user's account to this role.

Question 30: You are working as a web developer for a tech company and have a website hosted on App Engine standard environment. The company wishes to target 1% of the users to see a new test version of the website while minimizing complexities. What is the most appropriate approach to achieve this?

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

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

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

D. Create a new GKE cluster and deploy the new version in that cluster. Configure your network load balancer to send 1% of the traffic to that new cluster.

Question 31: As an IT manager at a software development company, you are using a Compute Engine instance to host a critical production application. To ensure smooth operations, you need to receive an email notification when the instance's CPU resources exceed 90% usage for more than 15 minutes, using Google services. How should you proceed to set up this monitoring and alert system?

A. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Write a script that monitors the CPU usage and sends it as a custom metric to Cloud Monitoring. 3. Create an uptime check for the instance in Cloud Monitoring.

B. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Set up a Cloud Function to monitor the instance's CPU usage. 3. Trigger an email notification using Cloud Pub/Sub when the CPU usage exceeds the threshold.

2. Use Stackdriver Debugger to monitor the instance's CPU usage. 3. Set up an email notification channel to receive alerts when the CPU usage exceeds the threshold.

3. Configure a Cloud Scheduler job to monitor the instance's CPU usage. 2. If the CPU usage exceeds the threshold, set up a Cloud Task to send an email notification.

4. Use the Google Cloud Console to manually monitor the instance's CPU usage. 2. Set up a Google Groups mailing list to receive email notifications when the CPU usage exceeds the threshold.

5. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Monitor the CPU usage using a built-in Cloud Monitoring

agent. 3. Enable Google Workspace email notifications and configure alerts to be sent when the CPU usage exceeds the threshold.

6. Use a Cloud Run instance to monitor the CPU usage of the Compute Engine instance. 2. Set up a Cloud Storage bucket to store the results. 3. Configure email notifications for high CPU usage using Cloud Pub/Sub.

7. Use Google Kubernetes Engine to monitor the Compute Engine instance's CPU usage. 2. If the CPU usage exceeds the threshold, create a log entry in Google Cloud Logging. 3. Configure Cloud Logging to send email notifications for high CPU usage events.

8. Set up a Cloud Identity-Aware Proxy to monitor the CPU usage of the Compute Engine instance. 2. Configure the Identity-Aware Proxy to send email notifications after the CPU usage remains above the threshold for more than 15 minutes.

C. 1. Create a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it. 2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

D. 1. Create a consumer Gmail account. 2. Write a script that monitors the CPU usage. 3. When the CPU usage exceeds the threshold, have that script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.

Question 32: As a database administrator at a tech company, you are tasked with managing an application that utilizes Cloud Spanner as its backend database. The application experiences regular traffic patterns, and you need to develop a method for automatically scaling the number of Spanner nodes based on traffic. What is the most effective approach to accomplish this?

A. Create a Cloud Monitoring alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.

B. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

C. Create a Cloud Run service that listens to Cloud Monitoring alerts and resizes the Spanner nodes accordingly.

D. Create an instance group in Cloud Spanner to handle autoscaling based on traffic patterns.

Question 33: As a financial analyst working for a technology company with multiple products, you're responsible for managing resources in various Google Cloud projects. These projects are connected to different billing accounts, but you need to estimate future expenses in a single visual representation and update

it promptly whenever new cost data is available. How should you achieve this goal?

A. Create a Google Cloud Function to consolidate costs from multiple projects periodically.

B. Export cost data from each billing account to a Google Sheet, and use the Google Sheets API to combine them for visualization

C. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

D. Use Google Cloud Monitoring to track costs of each project and create dashboards.

Question 34: You are working as a DevOps engineer at a software development company and, after receiving user feedback about a specific error spiking in one of your applications, you discover the issue is caused by a Service Account having insufficient permissions. You resolve the issue, but you want to be notified if it happens again in the future. What should you do to ensure you receive these notifications?

A. Grant Project Owner access to the Service Account.

B. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

C. In the Log Viewer, filter the logs on severity 'Error' and the name of the Service Account.

D. Disable and enable the Service Account to reset permissions.

Question 35: As a financial manager in a fast-growing company, you are tasked with migrating the company's invoice documents from on-premises storage to Cloud Storage. The invoice documents have specific storage requirements:

• Documents must be preserved for five years. • Up to five revisions of the same invoice document should be maintained to allow for corrections. • Documents older than 365 days need to be moved to lower-cost storage tiers.

To minimize operational and development costs, you want to adhere to Google-recommended best practices. What course of action should you take?

A. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

B. Enable retention policies on the bucket, use Cloud Pub/Sub to trigger a Cloud Run instance to manage document revisions and storage classes.

C. Enable retention policies on the bucket, use lifecycle conditions to automatically delete old documents, and use Datastore to handle revisions of invoice documents.

D. Enable object versioning on the bucket, and use Cloud Scheduler to invoke a Cloud Functions instance to move or delete your documents based on their metadata.

Question 36: As an IT manager in a tech company, you oversee the nightly batch workload running on numerous virtual machines (VMs). The workload is fault-tolerant and can handle occasional VM terminations. However, the current VM cost is becoming a concern. What strategy should be implemented to reduce expenses?

A. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

B. Run a test using Cloud Scheduler. If the test is successful, use N1 Standard VMs triggered by Cloud Scheduler when running future jobs.

C. Run a test using Google Compute Engine (GCE). If the test is successful, use preemptible N1 Highmem VMs when running future jobs.

D. Run a test using simulated maintenance events. If the test is successful, use N1 Standard VMs when running future jobs.

Question 37: As a system administrator in a software development company, you are managing multiple Linux instances on Compute Engine and expecting to add more in the upcoming weeks. To access all of these instances via your SSH client over the internet without configuring specific access for the existing and new instances, while also avoiding the assignment of public IP addresses to the Compute Engine instances, what should you do?

A. Configure Cloud Identity-Aware Proxy for HTTPS resources.

B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

C. Configure an SSH bastion host to access instances through a private IP address.

D. Use a Cloud Interconnect connection to link your on-premises network to your instances.

Question 38: As a database administrator for a tech company, you have recently set up an SQL Server 2017 instance on Compute Engine to evaluate its latest features. You want to connect to this instance using the least number of steps. What should you do?

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

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

C. Set a Windows username and password in the GCP Console. Verify that a firewall rule for port 5432 exists. Click the RDP button in the GCP Console,

and supply the credentials to log in.

D. Set a SQL Server username and password in the GCP Console. Verify that a firewall rule for port 443 exists. Click the HTTPS button in the GCP Console, and supply the credentials to log in.

Question 39: As a network administrator at a rapidly-growing tech company, you've been tasked with creating a custom VPC with a single subnet. To accommodate the company's growth, the subnet's range must be as large as possible. Which range should you use?

A. 203.0.113.0/24

B. 10.0.0.0/8

C. 192.168.0.0/16

D. 198.51.100.0/24

Question 40: As a network engineer in the tech industry, you are tasked with transitioning your company's entire workload to Google Cloud Compute Engine. Some servers need to be accessible from the internet, while others should be restricted to internal network access only. All servers must communicate with each other using specific ports and protocols. The existing on-premises network is divided into a demilitarized zone (DMZ) for public servers and a Local Area Network (LAN) for private servers. How should you design your company's networking infrastructure on Google Cloud to meet these requirements?

A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

B. 2. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to block public ingress traffic for the DMZ.

C. 8. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up only specific traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for both the DMZ and the LAN.

D. 3. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to block all traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Question 41: As a database administrator at a tech company, you've been tasked with resolving read latency-related performance issues they've been experiencing on a Cloud Spanner table. This table is only accessed by their users

using a primary key. The table schema is shown below. What should you do to address the issue?

A. Create a secondary index using the following Data Definition Language (DDL):

B. Remove the profile_picture field from the table.

C. Change the primary key to not have monotonically increasing values.

D. Split the table into two tables, one for user data and one for the profile_picture field.

Question 42: As a software engineer at a tech company, you are responsible for managing your team's web application that runs on Cloud Run for Anthos. You need to evaluate an updated version of the application through a canary deployment, targeting a specific percentage of your production users. How should you proceed?

A. Create a new service with the new version of the application. Add an HTTP Load Balancer in front of both services.

B. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

C. Create a new Deployment in Kubernetes Engine with the new version of the application. Configure the percentage of traffic to be routed to the new deployment.

D. Create a new Cloud Firestore directory with the new version of the application. Use Google Cloud Endpoints to direct traffic to both directories.

Question 43: While working at a tech company, your team is managing several applications running on different Compute Engine instances within the same project. To ensure higher security and control over access to Google Cloud APIs, you need to assign specific service accounts to each instance. How should you proceed to achieve this?

A. When creating the instances, specify a Service Account for each instance.

B. After starting the instances, use gcloud compute instances update to assign the name of the relevant Service Account as instance metadata.

C. Use the default Compute Engine service account for all instances and handle API access through IAM policies.

D. Create a Shared VPC and connect each instance to it, then assign a Service Account to the Shared VPC.

Question 44: You are working as a cloud engineer at a tech company and have been given a JSON file with a private key for a service account to access resources in a Google Cloud project. After downloading and installing the Cloud

SDK, you need to use this private key for authentication and authorization while executing gcloud commands. What step should you take?

A. Place the private key file in the installation directory of the Cloud SDK and rename it to credentials.json.

B. Use the command gcloud config set account and point it to the private key.

C. Use the command gcloud auth activate-service-account and point it to the private key.

D. Place the private key file in the .config/gcloud folder in your home directory and rename it to active_credentials.json.

Question 45: While working as a cloud administrator in a large software company, you uncovered several users with email addresses outside of your Google Workspace domain during a routine audit of your company's Google Cloud resources. Your goal is to ensure that your company's resources are only shared with users whose email addresses match your own domain. Furthermore, you want to remove any mismatched users without regularly auditing your resources to identify them. What action should you take?

A. Implement a Google Cloud Function that monitors projects for mismatched users and automatically removes them.

B. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

C. Modify the Google Workspace SSO settings to prevent external users from accessing resources.

D. Create a Cloud Scheduler task to regularly scan your resources and delete mismatched users.

Question 46: As a network engineer in a tech company, you have recently set up an LDAP server on Compute Engine that can be accessed via TLS through port 636 using UDP. Your task is to ensure that clients can reach the server through this port. What should you do?

A. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag.

B. Create a VPC peering connection to allow access to the LDAP server on port 636 using UDP. Enable the 'Allow Secure LDAP access over the Internet' option in the Compute Engine settings. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow ingress on TCP port 636 for that network tag. Create a Cloud VPN tunnel and configure the LDAP server to be reachable only through the VPN. Create a firewall rule to allow ingress on UDP port 636 without specifying any specific network tags. Set the VM instance to use a shared VPC and enable ingress on UDP port 636 in the Shared VPC settings. Deploy an Identity-Aware Proxy for the LDAP server and allow access on UDP port 636 only for authorized users. Create a

Cloud NAT gateway and configure it to allow access to the LDAP server on port 636 using UDP.

C. Add the network tag allow-udp-636 to the VM instance running the LDAP server.

D. Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

Question 47: You are working as a software engineer in a global finance company and are tasked with developing a trading application that will be utilized by clients worldwide. The application's data is stored and queried using a relational structure, and it is crucial to ensure all users have the exact same state of data with minimized latency. The application will be deployed across multiple regions for the best user experience. Which storage option should you choose for the application data to achieve this goal?

A. Use Cloud Spanner for data storage.

B. Use Cloud Bigtable for data storage.

C. Use Cloud Datastore for data storage.

D. Use Cloud Memorystore for data storage.

Question 48: As a security engineer at a leading software company, you are tasked with implementing the company's security vulnerability management policy for a specific Compute Engine instance hosting a critical application in your Google Cloud project. This policy requires a member of the security team to have visibility into vulnerabilities and other OS metadata. What action should you take to achieve this objective?

A. Enable the VPC Service Controls for the Google Cloud project.

B. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Create a log sink to BigQuery dataset. • Provide the security team member with access to this dataset.

C. • Ensure that the Ops Agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.inventoryViewer permission.

D. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.vulnerabilityReportViewer permission.

Question 49: As a software developer in a rapidly growing e-commerce company, you are tasked with creating a backend service that can efficiently handle a large volume of global transactions, ensuring data persistence from mobile and web clients. The business analytics team is keen on running SQL queries to analyze transactional data. To meet these requirements, you need to develop a highly available and scalable data store for the platform. What approach should you take?

A. Use a multi-region Pub/Sub for streaming transaction data and analyze it using Dataflow.

B. Create a multi-region Cloud Spanner instance with an optimized schema.

C. Create a multi-region Cloud Storage bucket and save transaction data as CSV files.

D. Deploy a self-managed multi-region Cassandra database with limited scalability.

Question 50: You are a software engineer at a tech company and have been working on an App Engine application for the development environment. After successfully completing the required testing, it's time to create a new project to serve as your production environment so the application can go live. What is the best approach to achieve this?

A. Use Dataflow to copy the application code from one project to another for deployment.

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

C. Create a second App Engine application within the same project, and then deploy your application to the new App Engine app.

D. Export the App Engine application from the development project and import it into the newly created production project using the GCP Console.

Practice Exam 8 Solutions

Solution to Question 1: C

The correct answer is C: Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

Explanation: The situation requires granting access to BigQuery datasets in the crm-databases-proj project to the service account in the web-applications project. Following Google-recommended best practices, you should assign the least privilege necessary for the service account to perform its role, which in this case is bigquery.dataViewer. This role allows the service account to read the data from the BigQuery datasets without giving additional unnecessary privileges.

Option A is incorrect because giving BigQuery data owner role to the web-applications project is excessive and goes against the principle of least privilege. The service account should not be allowed to modify or delete the datasets since it only needs access to read the data.

Option B is incorrect because giving the project owner role to both crm-databases-proj and the web-applications project would grant excessive permissions, going against the principle of least privilege. The owner role would allow the service account to potentially make major changes in both projects, which is not needed.

Option D is incorrect because, although it gives the bigquery.dataViewer role to the web-applications project, it still assigns an unnecessary project owner role to crm-databases-proj, which again goes against the principle of least privilege.

In conclusion, the best choice is C: Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications. This approach allows the service account to access the datasets needed while adhering to the principle of least privilege, ensuring the security and accessibility of the applications running on different Google Cloud projects.

Solution to Question 2: D

The correct answer is D.

Here's why the answer is D and why the other options will not work:

A: Activating two configurations using `gcloud configurations activate [NAME]` and then running `gcloud config list` will only list the configurations, but it won't start the Compute Engine instances. You still need to run the appropriate gcloud commands to start the instances.

B: Creating separate shell scripts for each account and specifying the gcloud command to start Compute Engine instances with specific zone and region flags could work, but it is not the most appropriate way to accomplish the task. This

method may require additional configuration and maintenance, whereas using configurations simplifies the process.

C: Running `gcloud config set compute/zone [ZONE]` and `gcloud config set compute/region [REGION]` will only set the default zone and region for your current account. It does not allow you to work with two different Google Cloud Platform accounts.

D: (Correct) Creating two configurations for the two GCP accounts using `gcloud config configurations create [NAME]` allows you to set up different, isolated settings for each account. To switch between accounts, just run `gcloud config configurations activate [NAME]`, which ensures that you can use the appropriate settings for each account when running the commands to start the Compute Engine instances. This method is the most appropriate and efficient way to work with multiple GCP accounts and their corresponding instances.

Solution to Question 3: C

The correct answer is C: Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

Option C is the most efficient method because it enables you to transfer the entire project without requiring any additional infrastructure changes or resource redeployments. The Google Cloud Console provides a documented process for moving projects between organizations using the projects.move method. This method ensures that all resources in the project are shifted to your organization with minimum hassle. After moving the project, updating the billing account will ensure that the costs are being managed and billed under the correct account.

Option A involves creating Kubernetes manifests and deploying them to a Kubernetes cluster in your organization. This method is not suitable because it is time-consuming, requires additional infrastructure setup, and only focuses on Kubernetes-specific resources, which might not cover all the resources in the project.

Option B involves creating separate Google Cloud Storage buckets for each organization, exporting resources from the startup's project, and importing them into a new project in your organization. This approach is also time-consuming, and there is room for error during the manual export-import process.

Option D suggests creating an infrastructure-as-code template with Terraform, deploying that template to a new project in your organization, and deleting the startup's project from their Google Cloud organization. While this is a viable option, it is not as efficient as moving the entire project to your organization using the projects.move method. Creating, maintaining, and deploying Terraform templates can be a laborious and time-consuming process, especially if there are

numerous resources. Additionally, deleting the project in the startup's organization may lead to undesired side effects, such as loss of data and additional cleanup requirements.

In conclusion, option C is the most efficient and reliable method for transferring the startup's Google Cloud project to your organization while updating the billing account as needed.

Solution to Question 4: B

The best strategy to achieve access to Nvidia Tesla P100 GPUs with minimal effort and cost for the Machine Learning (ML) team is option B: Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification. This approach allows you to create a separate, dedicated node pool, specifically designed to handle GPU-intensive workloads. By using the nodeSelector, you ensure that the ML team's pods are scheduled to run on the GPU-enabled nodes, which optimizes resource utilization and keeps costs in check.

Option A is not viable because it asks the ML team to use TPUs instead of GPUs. Tensor Processing Units (TPUs) are specialized hardware designed by Google for machine learning tasks and may not be a suitable replacement for the Nvidia Tesla P100 GPUs that the ML team needs to train their models efficiently.

Option C is also not an ideal solution, as simply adding the accelerator: gpu annotation to the pod specification does not guarantee that the desired GPU will be available in the cluster. The Kubernetes cluster must be configured to support GPU-enabled nodes to satisfy the ML team's requirements, which is not achieved just by adding an annotation to the pod specification.

Option D, which suggests enabling GPUs on existing nodes without creating a dedicated node pool, can lead to resource contention between different workloads running on the same nodes. Non-GPU workloads might use resources required by GPU workloads, leading to degraded performance and affecting the overall efficiency of the Kubernetes cluster. Creating a dedicated node pool for GPU-enabled workloads, as proposed in option B, ensures that resources are correctly allocated and reduces the possibility of resource contention in the cluster.

Solution to Question 5: B

The correct answer is B. Configure the Horizontal Pod Autoscaler (HPA) for availability, and configure the Vertical Pod Autoscaler (VPA) recommendations for suggestions.

Here's why the other options will not work:

Option A: Configuring the Cluster Autoscaler for availability and the Horizontal Pod Autoscaler for cost optimization is not ideal because the Cluster Autoscaler focuses on the number of nodes in a cluster, while the HPA scales the number

of pods based on resource usage. Cost optimization will be achieved by using VPA for right-sizing the resources required for each pod.

Option C: Configuring the Vertical Pod Autoscaler recommendations for availability and the Cluster Autoscaler for suggestions is not the best approach because the VPA is responsible for adjusting resource requirements for consistent performance in varied situations, but it does not directly affect availability. HPA should be configured for availability to ensure that there are enough pod replicas running to handle the varying workload.

Option D: Configuring the Horizontal Pod Autoscaler for availability, and configuring the cluster autoscaler for suggestions is not the best option because it does not address cost-effective recommendations on CPU and memory requirements for the workload. By utilizing VPA recommendations, you ensure accurate and efficient allocation of resources based on the workload's usage patterns, thus optimizing costs.

To summarize, by choosing Option B, you will configure the HPA for availability, ensuring that enough replicas are available to handle varying workloads effectively. Additionally, by using the VPA recommendations for suggestions, you can optimize the resource requirements for each pod, improving the cost efficiency while maintaining consistent performance.

Solution to Question 6: A

The correct answer is A, and here's why:

Option A: This is the best solution because it minimizes management overhead by using the native snapshot scheduler in the Google Cloud Console. This ensures the daily backup of the instance's disk is scheduled between non-working hours (1:00 AM - 2:00 AM) and automatically deletes the snapshots after 30 days. This method requires no additional services and follows Google's recommendations for disaster recovery.

Option B: This option involves creating a Dataflow job, which is not the most efficient solution since it requires additional services and might introduce more complexity to the task. Moreover, Dataflow is intended for data processing, not for managing disk backups. Therefore, this method is not recommended by Google for this specific use case.

Option C: Creating a Cloud Composer environment involves additional services and overhead. Even though Cloud Composer can schedule backup processes using DAGs, it is more suitable for complex data pipelines and workflows. The task at hand can be achieved with a simpler solution as mentioned in option A.

Option D: Data Loss Prevention (DLP) is a service designed for discovering, classifying, and protecting sensitive data, but it's not suitable for managing disk backups and retention. DLP neither automatically creates daily backups nor manages deletion of older backups, so this option does not meet the requirements.

Solution to Question 7: B

The correct answer is B. Deploy a private autopilot cluster.

Explanation:

Option A: DataProc clusters are designed for running Apache Spark and Apache Hadoop workloads, not for running Kubernetes workloads. Although shielded nodes are enabled, deploying a private DataProc cluster will not fulfill the requirement of setting up a Google Kubernetes Engine cluster.

Option B: A private Autopilot cluster meets all the requirements. Autopilot clusters are fully managed by Google, reducing the operational cost for managing the cluster. They also follow Google-recommended practices automatically. Additionally, a private cluster ensures that the nodes are not accessible from the internet and provides a more secure environment. Autopilot clusters support features such as node auto-upgrades, auto-scaling, and maintenance windows, and they have built-in verifiable node identity and integrity.

Option C: Deploying a private zonal cluster and enabling shielded nodes would provide a secure environment and verifiable node identity. However, it doesn't minimize the operational cost of managing the cluster as it requires manual management of node upgrades and other configurations.

Option D: Cloud SQL is a managed database service, not a Kubernetes cluster. It's not suitable for this task, even with shielded nodes enabled.

Thus, the best option to meet all the requirements is option B: Deploy a private autopilot cluster.

Solution to Question 8: B

The correct answer is B. Create a snapshot schedule for the disk using the desired interval. This is the recommended approach for regularly backing up the boot disk in Google Compute Engine while ensuring quick restoration and cost optimization.

Creating a snapshot schedule allows you to define the frequency at which snapshots are created, such as hourly, daily, or weekly. This method adheres to Google's best practices for backing up critical workloads running on Google Compute Engine. Moreover, snapshot schedules automatically clean older backups based on the retention policy, saving costs on storage.

Here's why the other options do not work:

A. Creating a Managed Instance Group (MIG) is used for managing a group of instances, automatically scaling based on load and performing rolling updates. MIG is not designed for backing up the boot disk data and restoring it.

C. Creating a Cloud Scheduler job to clone the VM instance at the desired interval is an inefficient approach. This method will create full copies of the VM

and will incur higher storage and operational costs. While this could technically allow you to recover data, it isn't recommended as the most effective solution.

D. Using Cloud Memorystore for Redis involves storing data in an in-memory data store service for Redis. This is not suitable for backing up boot disk data and providing quick restoration capabilities for a system administrator, as it is intended for caching and real-time querying purposes rather than disaster recovery of disk data.

Solution to Question 9: C

The correct answer is C: Stop the VM, increase the memory to 8 GB, and start the VM.

Explanation for C: Stopping the VM, increasing the memory to 8 GB, and starting the VM is the most appropriate action because it directly addresses the issue of running out of memory. It allows you to allocate more memory resources to the VM while maintaining the existing configuration, such as vCPUs and machine types.

Explanation for why other options will not work:

A. Rely on live migration to move the workload to a machine with more memory: Live migration is a technique used for high availability of VM instances by moving running VMs to other hosts without any downtime. It does not allocate more memory to your existing VM, so this option will not resolve the issue of running out of memory in the current virtual machine.

B. Upgrade the Cloud SDK to allow for increased memory usage: The Cloud SDK is a toolset to manage resources and applications hosted on a cloud platform. Upgrading the Cloud SDK does not directly impact the allocated memory of a virtual machine. It does not change the memory allocations of your VMs, so upgrading it will not solve the problem of running out of memory.

D. Stop the VM, change the machine type to n1-standard-8, and start the VM: Changing the machine type to n1-standard-8 means changing the configuration of VM resources. An n1-standard-8 machine type comes with 8 vCPUs and 30 GB of memory. While it does increase the memory, it also increases the number of vCPUs, which might not be necessary depending on your use-case and workload. This option could lead to unnecessary usage of computing resources and increased costs. Additionally, you can simply change the VM's memory without changing the machine type (as in option C), which would be a better approach for this specific situation.

Solution to Question 10: D

The correct answer is D. Upload the data to Cloud Storage using the gsutil command line tool.

Here's why the other options won't work:

A. Upload the data to BigQuery using the bq command line tool.

This option is incorrect because BigQuery is primarily used for analyzing structured data in a serverless, highly scalable environment. Uploading unstructured data directly to BigQuery can be complex and inefficient, as it would require schema definition and transformation before storing and analyzing the data.

B. Upload the data to Cloud Pub/Sub using the gcloud command line tool.

This option is incorrect because Cloud Pub/Sub is a messaging service that is primarily used for ingesting event-driven data and handling real-time message streaming. It is not suitable for uploading and processing large quantities of unstructured data.

C. Upload the data into Cloud SQL using the import function in the console.

This option is incorrect because Cloud SQL is a managed relational database service, which is best suited for structured data. Uploading unstructured data into Cloud SQL would be difficult and time-consuming, as you would need to transform the data and map it to a relational schema.

D. Upload the data to Cloud Storage using the gsutil command line tool.

This is the correct option. Google Cloud Storage is a highly-scalable and cost-effective storage service that can hold any type of data, including unstructured data. Uploading the data to Cloud Storage using the gsutil command line tool is efficient and straightforward. Once the unstructured data is in Cloud Storage, you can perform the necessary ETL transformations and process it using a Dataflow job, which allows you to build and execute complex data analytics pipelines in Google Cloud.

Solution to Question 11: A

The most appropriate answer is A: Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

Explanation: Moving the single batch process to a Compute Engine VM offers the ability to start and stop the instance as needed, thus reducing costs. Additionally, Compute Engine VM provides the necessary reliability to ensure the process can run for 30 hours without being interrupted. This solution allows for a simple migration of the existing workload to the cloud and only incurs costs when the VM is running.

Why other options will not work:

B. Migrating the workload to a Google Kubernetes Engine cluster with Preemptible nodes is not the best choice because Preemptible VMs have a 24-hour maximum runtime and can be terminated earlier by Google with a 30-second notice, making them unsuitable for a long-running offline task that cannot be restarted if interrupted.

C. Migrating the workload to Cloud SQL for batch processing is not a suitable option since Cloud SQL is a managed database service and specifically designed

for online database workloads, not for long-running batch processes like the one described in the question.

D. Hosting the workload on a Cloud Storage bucket and using Pub/Sub for event-driven processing is not applicable, as the given scenario involves a long-running batch process that has to be executed offline without interruption. Cloud Storage is an object storage service, and Pub/Sub is a messaging service, neither of which is designed to support long-running offline batch tasks.

Solution to Question 12: D

The correct answer is D. Use the BigQuery interface to review the nightly job and look for any errors.

Explanation:

Option A: Verify Cloud Dataflow pipeline for any data ingesting issues in the Google Cloud platform. Cloud Dataflow is used for data processing and ETL operations. While it is relevant to the overall data processing pipeline, it doesn't directly impact the Looker Studio visualization based on data in BigQuery. The issue mentioned is related to Looker Studio charts malfunctioning, so checking data ingestion using Cloud Dataflow is not the most appropriate step to take in this case.

Option B: Inspect the data warehouse's schema in the BigQuery console to identify any inconsistencies. While examining the schema helps determine if there are any inconsistencies in the table structure that may affect data querying, it is not the most immediate step to identify the root cause of the malfunctioning charts in Looker Studio. The issue with the daily summary recalculation might not be directly caused by schema inconsistencies.

Option C: Contact the Looker Studio support team for assistance in resolving the issue. Although contacting the Looker Studio support team could be a possible step later on if the issue persists, it should not be the first action taken. As a data analyst, you should attempt to diagnose the problem and investigate potential causes within the BigQuery interface before seeking external support.

Option D: Use the BigQuery interface to review the nightly job and look for any errors. (Correct Answer) This option is the most appropriate step in diagnosing the issue with the malfunctioning charts in Looker Studio. Since the data is appended during the day and the daily summary is recalculated at night by overwriting the table, checking the nightly job for any errors in BigQuery will help identify any issues with the data processing or update that could be affecting the Looker Studio charts.

Solution to Question 13: A

The best course of action is A. Deploy MongoDB Atlas from the Google Cloud Marketplace.

Here's why:

A. Deploy MongoDB Atlas from the Google Cloud Marketplace - This is the ideal choice since MongoDB Atlas is the official, fully-managed, and supported MongoDB service. By deploying MongoDB Atlas directly from the Google Cloud Marketplace, you benefit from a seamless integration with Google Kubernetes Engine, as well as a dedicated support SLA provided by MongoDB, Inc. This ensures that you have a reliable and scalable MongoDB environment to handle your financial company's transactions.

B. Download a MongoDB installation package, and run it on a Managed Instance Group - Although this option could provide automatic scaling of instances, it doesn't guarantee that the MongoDB environment will be fully managed, or that you'll receive the required support SLA. Managing MongoDB yourself could lead to additional operational overhead and potential security and performance issues.

C. Create a Cloud Dataproc cluster and use the MongoDB connector for Hadoop - This option is not suitable because Cloud Dataproc is designed for running Apache Hadoop and Apache Spark workloads, not MongoDB databases. While the MongoDB connector for Hadoop can be used to integrate these two technologies, this setup would not provide a fully managed MongoDB environment or the necessary support SLA for your application.

D. Download a MongoDB installation package, and run it on Compute Engine instances - Although this would allow you to deploy MongoDB on Google Cloud, it wouldn't provide you with a fully managed environment or the required support SLA. Like option B, managing MongoDB yourself could result in additional operational overhead and potential security and performance issues.

Solution to Question 14: C

The correct answer is C: Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery export.

Explanation:

Option A is not suitable because Google Cloud Monitoring primarily focuses on monitoring performance, uptime, and health of applications and infrastructure. While it can be configured for cost alerts, it doesn't provide a full-fledged solution for automating visualizations based on company-specific criteria and cost metrics.

Option B doesn't work because Stackdriver Monitoring is now incorporated into Google Cloud Monitoring. Using it to create custom cost metrics for projects does not align with the specific requirements mentioned in the question.

Option C is the right choice as it involves configuring Cloud Billing data export to BigQuery, which enables having all the billing details in one place and allows for the creation of customizable visualizations. By using Looker Studio, a modern data platform, you can create a dashboard on top of the BigQuery export

and automate the visualization process based on specific metrics and company criteria.

Option D is not suitable because using Cloud Functions to pull data and send it to Google Sheets does not provide the same level of flexibility, efficiency, and automation as using BigQuery and Looker Studio does. Moreover, Google Sheets has limitations in terms of capacity and might not be the best choice for handling large amounts of billing data and providing complex visualizations.

Solution to Question 15: B

The best choice for ensuring an optimal gaming experience for users across the globe would be option B: Use Cloud Spanner to store user data mapped to the game statistics.

Option B is the ideal choice because Cloud Spanner is a fully managed, globally distributed relational database service that offers both horizontal scaling and strong consistency. It is well-suited for handling large amounts of data across multiple regions without any noticeable impact on performance or increasing management complexity. In a gaming application, this ensures that all users have a seamless experience regardless of their location and that the game data is always consistent.

The reasons why the other options will not work are:

Option A: Cloud Bigtable is a NoSQL key-value store designed for low-latency and high-throughput applications. Despite offering high performance, using a hashed timestamp as the row key does not guarantee global consistency. Moreover, Bigtable is not well-suited for handling complex relational data and transactions, which can be an issue in a gaming application where players interact with each other.

Option C: Cloud SQL database is a fully managed and highly available database service that supports cross-region replication. However, setting up the replication in multiple regions like the EU, US, and APAC would increase management complexity. In addition, cross-region replication can introduce additional latency and is not designed for guaranteeing strong global consistency, which is crucial for a seamless gaming experience.

Option D: Firebase Realtime Database is a NoSQL cloud-based database suited for real-time applications. However, the master-master replication system might not be the best solution for large-scale, globally distributed applications, as it can lead to conflicts, inconsistencies, and increased complexity. Additionally, the Realtime Database focuses primarily on real-time data rather than providing strong global consistency and is not designed for horizontal scaling as required for a popular multiplayer gaming application.

Solution to Question 16: B

The correct answer is B because it focuses on creating a new service account specifically for the new Compute Engine instance, which ensures that only that

instance will have access to the necessary files on Cloud Storage. By assigning this service account to the new instance and granting the service account permissions on Cloud Storage, you are able to create a secure and restricted access to the required files.

Option A is incorrect because Cloud Identity-Aware Proxy (IAP) is used to secure access to applications, not Cloud Storage objects. While this option also involves creating a new service account, it does not directly address securing access to Cloud Storage.

Option C is incorrect because changing the storage class of objects on Cloud Storage to Nearline storage affects data storage costs and retrieval times, but it does not limit the access of the files to the new instance. This choice does not mention granting any permissions on Cloud Storage for the new service account.

Option D is incorrect because it suggests assigning the new service account to all instances, which would give all virtual machines (VMs) access to the Cloud Storage files rather than restricting access to only the new instance. This does not meet the requirement of the initial task.

Solution to Question 17: A

The correct answer is A. In the Google Cloud Platform Console, create a new billing account and set up a payment method.

Explanation for choosing option A: Creating a new billing account in the Google Cloud Platform Console is the most appropriate course of action for consolidating all projects under one account. A new billing account allows the company to have control over all the projects' expenses, manage payments centrally, and avoid the use of personal credit cards by the employees. The ability to link projects to a billing account is a built-in feature of GCP that streamlines project management and cost monitoring.

Reasons why other options will not work:

Option B: Contacting the GCP sales team to request a new centralized billing account is not necessary because the company can create the account directly from the Cloud Platform Console. Besides, sales teams typically handle larger issues related to contracts and pricing negotiations, not setting up new billing accounts.

Option C: Creating a billing account and manually transferring each employee's project to the root Organization is not a feasible option. The Google Cloud billing system does not allow transferring projects to the root Organization. Instead, employees or project administrators can change the billing account associated with their project to the newly created company's billing account.

Option D: Creating a Google Group for the company and inviting all employees to join will not address the requirement of consolidating billing accounts. Google Groups are used for managing access to resources and sharing information, not

for merging or managing billing accounts. Billing accounts must be managed through the Google Cloud Platform Console.

Solution to Question 18: D

The correct answer is D. To explain why the answer should be D and why other options will not work, let's analyze each option:

A. Run gcloud info to view the account value, and then run gcloud services list –account .

This option is incorrect because gcloud info will provide information about the current environment, including the account, but not the enabled APIs for a specific project. Additionally, the –account flag is not applicable for gcloud services list, so this option will not work.

B. Run gcloud init to set the current project to my-project, and then run gcloud services describe my-project.

This option is incorrect because the gcloud services describe command is used for getting information about a specified service, not the enabled APIs for a specific project. Furthermore, the correct flag to use would be –project, not passing the project name as an argument.

C. Run gcloud init to set the current project to my-project, and then run gcloud services list –available.

This option is incorrect because the gcloud services list –available command shows the list of available services, not the enabled APIs for a specific project. Setting the current project does not change the output of the command in this case.

D. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

This option is correct because getting the project ID with gcloud projects list allows you to specifically target the "my-project" you are looking for. Then, running gcloud services list –project will display the enabled APIs for the specified project. This course of action aligns with the task you're given and will provide the desired output.

Solution to Question 19: C

The correct answer is C: Migrate to use a Local SSD on the instance.

Explanation:

Option A: Migrating to a multi-regional Cloud Storage bucket will not help in maximizing throughput or minimizing costs. In fact, it will potentially increase the latency while accessing the files due to the geographical distribution of the data. Additionally, the application's primary concern is the excessive disk read throttling, which Cloud Storage will not directly solve.

Option B: Using Cloud Storage instead of a Zonal SSD Persistent Disk may not be the most effective solution to maximize throughput. While Cloud Storage could help in storing and retrieving data, it is not optimized for high-performance applications that require low-latency disk access, such as the one described here.

Option C: Migrating to use a Local SSD on the instance is the optimal solution. Local SSDs are physically attached to the instance's host server, providing very high input/output operations per second (IOPS) and very low latency compared to Zonal SSD Persistent Disks. Local SSDs can significantly improve disk read performance and thus reduce the impact of throttling, resulting in maximized throughput while keeping costs at a minimum.

Option D: Increasing the size of the disk to 2 TB might seem like a viable option, but it is not the most optimal choice. While it could potentially improve the throughput due to increased IOPS, it also comes with higher costs without necessarily addressing the core issue of disk read throttling. Compared to Local SSDs, this option is less cost-effective and not guaranteed to provide the performance improvements the application needs.

In conclusion, the best choice for maximizing throughput and minimizing costs for the company would be to migrate to a Local SSD on the instance (Option C).

Solution to Question 20: C

The best approach to consolidate reporting under a single Stackdriver Monitoring dashboard is option C: Configure a single Stackdriver account, and link all projects to the same account. This is because Stackdriver supports multi-project monitoring natively, allowing you to view and manage metrics from different GCP projects in a single dashboard without having to create separate accounts for each project.

Option A (Use Shared VPC to connect all projects, and link Stackdriver to one of the projects) is not the best approach because Shared VPCs are designed for network management and resources sharing, not specifically for consolidating Stackdriver Monitoring dashboards. Although it may help to organize and manage resources across projects, it doesn't directly consolidate the monitoring dashboards.

Option B (Install the Stackdriver Monitoring agent on each project and use Google Cloud Pub/Sub to aggregate the data) is not the ideal approach because it's unnecessarily complex compared to linking all projects to a single Stackdriver account. While the Stackdriver Monitoring agent can help collect additional resource metrics, using Google Cloud Pub/Sub to aggregate the data increases the management overhead and possibly lead to additional costs, synchronization issues, and latency compared to the native multi-project dashboard.

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

that Group) is not the best approach because creating groups based on project names can help you organize the resources within your dashboard, but it doesn't link the other projects directly to the Stackdriver account for monitoring purposes. You'll still need to link each project to the same account for consolidated monitoring, as described in option C.

Solution to Question 21: C

The correct answer is C. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

Reasoning:

Option A and B both suggest implementing a Cloud Functions job or a Cloud Run job to rotate service account keys daily. While these options would enforce short-lived credentials, they would incur additional costs associated with the serverless functions and require manual work to create and maintain the function's code.

Option D suggests using a custom App Engine task runner to rotate service account keys and enforce an org policy to allow key creation with no exceptions across all projects. This solution would not meet the requirement to centralize service account creation in pj-sa and would also incur additional costs associated with the App Engine task runner.

Option C is the best solution because it enforces an organization policy (org policy) constraint allowing the lifetime of service account keys to be 24 hours. This would ensure that all keys are short-lived, as required. Additionally, it enforces an org policy constraint denying service account key creation across all projects, except for pj-sa, which would centralize the accounts and be consistent with the requirements. This solution is cost-effective and minimizes the need for continued maintenance and updates.

Solution to Question 22: C

The best course of action in this scenario would be option C: Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

Here's why option C is the best choice:

1. By using Google Cloud Directory Sync (GCDS), you can seamlessly synchronize users, groups, and other directory information from your Active Directory to Cloud Identity. This ensures that your company can maintain Active Directory as the primary source of truth for identities while also gaining control over the Google accounts employees use.
2. GCDS integrates with both Active Directory and Cloud Identity to provide a consistent and secure experience for your users. It is designed to work specifically with these services to keep your identity management processes centralized and efficient.

Now, let's discuss why the other options are not suitable:

A. Setting up a SAML Single Sign-On (SSO) connection between Active Directory and GCP without synchronizing users doesn't provide full control over employee Google accounts. SSO simplifies the login process, but it doesn't keep Active Directory and Cloud Identity in sync; therefore, you can't manage Google accounts as effectively in this setup.

B. Exporting users from Active Directory as a CSV and importing them to Cloud Identity via the Admin Console is a manual process prone to human error, and it would be inefficient for a large company. Moreover, keeping both directories in sync with any updates, deletions, or additions would become a time-consuming and complicated task.

D. Active Directory Sync Protocol (ADSP) is not a valid option because it doesn't exist as a synchronization method between Active Directory and Google Cloud Identity. Therefore, it cannot be used to synchronize users in this situation.

In conclusion, using Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity is the best course of action for an IT administrator at a large company that wishes to maintain full control over employee Google accounts while keeping Active Directory as the primary source of truth for identities.

Solution to Question 23: C

The correct answer is C. Using the GCP Console, filter the Activity log to view the information.

Option A is not the best choice because Cloud Pub/Sub is mainly used for real-time messaging and streaming data between applications. It is not designed specifically for monitoring Cloud Storage bucket activities or filtering logs. While it may be possible to use Cloud Pub/Sub to process and filter logs, it would require additional effort in setting up and connecting to the logs.

Option B is also not efficient as it only allows you to view the contents of a specific bucket and its metadata. You won't be able to see user-specific activities, access logs, or filter the logs by user to gather the required information.

Option D is incorrect because Google Cloud Armor is a security service designed to protect applications and websites against DDoS attacks and web attacks. It is not intended to monitor Cloud Storage activities or filter logs for specific users.

Option C, on the other hand, stands out as the most efficient way to accomplish the task. You can use the GCP Console to filter the Activity log to view the information. This provides you a specific interface that makes it easy to find and filter the logs for the activities you need to verify. This way, you can identify the files accessed by the user and the addition of metadata labels in the most efficient manner.

Solution to Question 24: C

The correct answer is C: Invite the user to transfer their existing account.

An explanation for why the answer should be C is that transferring an existing account helps avoid account conflicts and follow the best practices set by Google. It allows the users to keep their existing data, and at the same time, links their account to the company's Cloud Identity platform. This will ensure seamless integration and management for IT experts within the organization.

Option A is suboptimal as creating a separate Google Workspace account can cause confusion and inefficiency for users who have to manage two separate accounts and manually migrate their data. This can also lead to an increased likelihood of account conflicts.

Option B is not ideal because creating a new Google account may result in users having duplicate accounts and increased complexity in managing them. Moreover, the users would lose all the data and settings on their existing account, which is not recommended by Google.

Option D is not appropriate as it disregards the importance of users' data and settings on their existing account. It would result in data loss and disruption for the users, which Google best practices aim to prevent. This would also likely cause frustration and dissatisfaction among users.

Solution to Question 25: B

The correct answer is B. Create the instance without a public IP address. Here's why:

Option A is incorrect because VPC Service Controls are designed to manage data access and movement between services in your VPC, not to restrict network access to a Compute Engine instance. This option does not ensure that the instance is not accessible via public Internet traffic.

Option B is the most appropriate since by creating the instance without a public IP address, it will only be accessible via the internal company network or VPN. This ensures that the instance is not directly accessible via public Internet traffic, meeting the requirement specified in the question.

Option C is incorrect because Private Google Access allows VM instances with only internal IP addresses (i.e., no external IPs) to access Google APIs via the default route. This does not ensure that the desired VM instance is not accessible via public Internet traffic, as required in the question.

Option D is incorrect because, although it restrains incoming traffic to the instance from on-premises WAN IP addresses, it does not prevent public Internet traffic from reaching the instance. Additionally, this option still exposes the instance to the Internet with a public IP address, which increases the potential attack surface.

Solution to Question 26: D

The correct answer is D: Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Explanation: In this scenario, the image rendering microservice demands more CPU resources than the other services, which are optimized for n1-standard machine types. To ensure efficient resource utilization, it is necessary to allocate resources accordingly.

Option D addresses the specific requirements of the image rendering microservice by creating a dedicated node pool with compute-optimized machine type nodes. These machine types allocate more CPU resources, which is suitable for the processing-heavy task of image rendering. Additionally, using a separate node pool with general-purpose machine type nodes for the other microservices ensures that they receive adequate resources as well.

Option A is incorrect because merely increasing the number of replicas for the image rendering microservice without changing the machine types would not resolve the resource allocation issue. More replicas could increase performance, but they would still be running on machine types not tailored for their CPU-intensive workload.

Option B is incorrect because using memory-optimized machine type nodes for the image rendering microservice does not address its need for more CPU time. Memory-optimized machine types are designed for workloads that require a large amount of memory, not CPU resources.

Option C is incorrect because, while vertical pod autoscaling could help the image rendering microservice, it would not address the overall issue of utilizing appropriate machine types for each microservice. Additionally, horizontal pod autoscaling also does not consider the specific machine type needs of the various microservices.

In conclusion, the best solution is to create a node pool with compute-optimized machine type nodes for the image rendering microservice (D). This enables efficient resource utilization across all workloads by catering to the specific needs of each microservice.

Solution to Question 27: B

The best course of action in this scenario is to choose option B:

B. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

Why Option B should be chosen:

1. By using the Cloud Marketplace, developers can quickly deploy pre-configured Cassandra environments on Google Cloud, thus reducing setup time and potential errors.

2. Each of the development teams can have their own isolated Cassandra environment, ensuring that their work does not interfere with other teams.
3. Leveraging Cloud Marketplace simplifies management and minimizes the need for support in setting up and maintaining these environments.

Why other options will not work:

Option A: 1. Cloud Dataproc is primarily designed to run Hadoop and Spark workloads efficiently, not for Cassandra environments. It would require additional setup and configuration to support Cassandra. 2. Since multiple teams need isolated environments, sharing a single cluster may lead to overlapping work and potential conflicts.

Option C: 1. Pub/Sub and Dataflow are not meant for creating and managing Cassandra environments. They are designed for processing streaming data and message-based architectures. 2. Simulating a Cassandra-like environment in Dataflow could introduce unnecessary complications and is not suitable for development work requiring real Cassandra environments.

Option D: 1. Using Compute Engine instances might work, but it is more complex to set up and manage, compared to Cloud Marketplace. 2. Creating and maintaining snapshots for each developer or team would consume more resources and increase management overhead.

Solution to Question 28: A

The correct answer is A, and here's why: Deploying the application on App Engine and creating a new version of the same service for each update is the most suitable option for achieving the required release cycle. This approach allows you to utilize App Engine's built-in traffic splitting functionality, which lets you send a specified percentage of traffic to the new version, enabling testing of updates with real user traffic and limiting their impact to a small number of users. The majority of users will still interact with the stable version, ensuring a seamless experience for them.

Why the other options won't work:

Option B: Cloud Functions is designed for running individual functions in response to specific events, which is not suitable for hosting an entire web application. While you can create a new function for each update, it is not possible to control the percentage of traffic directed to a specific function using the HTTP trigger in Cloud Functions. Hence, this solution will not meet the desired release cycle objectives.

Option C: Deploying the application on Kubernetes Engine and updating the deployment to use a new version for each release would replace the existing version with the new one for all users. This approach does not support traffic splitting, meaning that all users would be affected by the updates, and you wouldn't be able to limit the impact to a small portion of users.

Option D: Using a StatefulSet in Kubernetes Engine for each update is not appropriate for handling traffic splitting with real user traffic. StatefulSets are designed for managing stateful applications with a fixed number of replicas and stable network identities. Traffic splitting through a Kubernetes Ingress could become overly complex to manage and maintain, and it is not the most suitable option for the required release cycle in this scenario.

Solution to Question 29: C

The correct answer is C, as you need to select the built-in IAM project Viewer role and add the auditor's account to this role. The project Viewer role provides read access to all project resources without the ability to modify them, which aligns with the access requirements for the auditor.

Option A is incorrect because the IAM Billing Account Viewer role is limited to viewing billing information only, not the entire resources of a project.

Option B is incorrect as there is no separate IAM service Viewer role; instead, it's a part of the IAM project Viewer role, which is given in option C.

Option D is not suitable because the IAM BigQuery Data Viewer role focuses specifically on the BigQuery service and will not provide the auditor with read access to all project resources as required.

So, to provide the auditor with the necessary read access to all project items without the ability to modify them, you should configure the auditor's permissions by selecting the built-in IAM project Viewer role (option C) and adding their user account to that role.

Solution to Question 30: B

The correct answer is B. Deploy the new version in the same application and use the –splits option to give a weight of 99 to the current version and a weight of 1 to the new version.

This option is the most appropriate for achieving traffic splitting for the new test version of the website while minimizing complexities. Using the –splits option allows you to control the traffic distribution between the existing version and the new version so that 1% of users are directed to the new version. This approach keeps everything in the same App Engine standard environment, ensuring consistency and easier management.

Option A, creating a new App Engine application and configuring the network load balancer, is not ideal because it adds unnecessary complexity. Setting up a separate application and managing the load balancer to direct the required percentage of traffic would be more difficult to maintain compared to using the –splits option available in App Engine.

Option C, deploying the new version in the same application and using the –migrate option, is not suitable because the –migrate option is meant for shifting

traffic 100% from an existing version to a new version, rather than just targeting 1% of users with the new test version.

Option D, creating a new Google Kubernetes Engine (GKE) cluster and configuring the network load balancer, is also not the most appropriate approach as it involves additional complexity in managing a new cluster and balancing traffic. Furthermore, it deviates from the existing App Engine standard environment, which may cause inconsistencies and additional complexities in deployment and management.

Solution to Question 31: C

The correct answer is C because it allows you to create a Cloud Monitoring Workspace, set up an alerting policy based on the CPU usage threshold, and configure email notifications for the alert. This is the most efficient and reliable way to monitor the Compute Engine instance's CPU usage and receive notifications when the usage exceeds 90% for more than 15 minutes using Google services.

Option A is not correct because it involves writing a custom script and creating an uptime check, which does not directly address the need for an alert based on CPU usage. Uptime checks are typically used for monitoring the availability of an instance, not resource utilization.

Option B is not correct because using a Cloud Function to monitor the instance's CPU usage may be unreliable and requires custom coding to handle the problem. Also, Cloud Pub/Sub is not intended for sending email notifications.

Options D, E, and F involve setting up third-party services, including Gmail, Google Groups, and Google Workspace, which are not the most efficient or practical way to monitor and send notifications using Google Cloud Platform.

Option G is not correct because using Google Kubernetes Engine to monitor the CPU usage of a Compute Engine instance is not the intended purpose of Kubernetes Engine and adds complexity to the solution.

Option H is not correct because Cloud Identity-Aware Proxy is typically used for authentication purposes and does not have built-in monitoring or alerting capabilities for instance CPU usage.

In summary, option C is the best choice for setting up a monitoring and alert system that sends an email notification when the instance's CPU resources exceed 90% usage for more than 15 minutes using Google Cloud Platform.

Solution to Question 32: B

The correct answer is B because it leverages both Cloud Monitoring and Cloud Functions to create an automated scaling solution specifically for Cloud Spanner based on its CPU usage. By creating an alerting policy that sends an alert to a webhook when the Cloud Spanner CPU is over or under your defined threshold, you'll be informed of the need to allocate more or fewer resources. Combining

this with a Cloud Function that listens to HTTP requests and resizes Spanner resources according to these alerts, you have a responsive, automatic scaling solution.

Option A is not the ideal choice because it relies on Google Cloud Support to handle scaling. This approach may have longer response times and does not provide the level of automation that option B does.

Option C might seem plausible, but it's not the best choice as Cloud Run is primarily used for running stateless containers, not directly managing database resources like Cloud Spanner. It may require more complex implementation compared to option B, which offers a more direct solution.

Option D does not work because Cloud Spanner itself doesn't have an instance group feature like some other Google Cloud services. The concept of instance groups is usually associated with Compute Engine, not Cloud Spanner. Therefore, it cannot be used to handle autoscaling based on traffic patterns.

In summary, the most effective approach to automatically scale the number of Spanner nodes based on traffic is to create a Cloud Monitoring alerting policy and combine it with a Cloud Function that resizes Spanner resources accordingly (Option B).

Solution to Question 33: C

The correct answer is C. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

Explanation:

Option A: Creating a Google Cloud Function to consolidate costs from multiple projects periodically would be a complex solution and may not provide real-time updates on the cost information when needed. It may also require extensive coding for aggregating data and handling various edge cases.

Option B: Exporting cost data from each billing account to a Google Sheet and using the Google Sheets API to combine them for visualization would be a manual, error-prone process that is not recommended for use in a professional environment. This method would also not scale well when dealing with numerous Google Cloud projects and billing accounts.

Option C: Configuring Billing Data Export to BigQuery enables you to store all the cost data from various projects and billing accounts in one place, providing a comprehensive and scalable solution. BigQuery is a powerful and cost-effective solution for data storage and analysis. By visualizing the data in Looker Studio, you can create a single visual representation for your company's expenses, keeping stakeholders informed and enabling proactive budget management. This option ensures real-time updates of cost data and better scalability for multiple projects.

Option D: Using Google Cloud Monitoring to track costs of each project and create dashboards would be insufficient because it does not inherently consolidate all the cost data into a single visual representation. Cloud Monitoring focuses on tracking application performance and availability, rather than providing a comprehensive billing visualization solution.

Therefore, the most appropriate choice for estimating future expenses while keeping data up-to-date and providing a single visual representation is to configure Billing Data Export to BigQuery and visualize the data in Looker Studio (Option C).

Solution to Question 34: B

The correct answer is B. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

Here's why option B is the correct answer:

Option B allows you to create a custom metric based on the specific error message. By doing so, it keeps track of the occurrence of that error and triggers an alert when the error occurs again. This way, you will be promptly notified of the issue, enabling you to resolve it quickly and minimize its impact on your application. This solution is efficient and focused on addressing the particular problem that has been identified.

Here's why the other options are incorrect:

Option A: Granting Project Owner access to the Service Account may initially seem like a solution, but it is not appropriate for this situation. Project Owner access gives the Service Account overly broad permissions, which might introduce security risks and is not a targeted solution to the problem at hand. Additionally, it doesn't provide a notification mechanism to alert you if the error reoccurs.

Option C: Filtering logs in the Log Viewer can be helpful for troubleshooting and identifying errors. However, this approach does not automatically notify you if the error occurs again in the future, rendering it a passive and manual method, which might be ineffective in a real-time context.

Option D: Disabling and enabling the Service Account is a futile action in this scenario, as it does not reset permissions, nor does it ensure you receive notifications of future occurrences of the specific error.

In summary, option B is the most appropriate solution for receiving notifications about the specific error occurring in the future, as it focuses on the error at hand rather than broad changes to permissions and provides an automated alerting mechanism.

Solution to Question 35: A

The correct answer to this question should be A. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects,

set the number of versions, and delete old files.

Here's the explanation for why this is the best option:

In option A, the use of object versioning on the bucket directly aligns with the requirement to maintain up to five revisions of the same invoice document for corrections. The lifecycle conditions can be used to change the storage class of objects, meeting the need to move documents older than 365 days to lower-cost storage tiers. You can set the number of versions and create a condition to delete old files, ensuring that documents are preserved for five years. This option follows Google-recommended best practices and keeps operational and development costs to a minimum.

Option B is not ideal because it relies on Cloud Pub/Sub to trigger a Cloud Run instance to manage document revisions and storage classes. This introduces additional complexity, cost, and potential failure points in the system. Additionally, retention policies do not allow for maintaining multiple revisions of the same invoice document.

Option C is not recommended because while retention policies are used to automatically delete old documents, they do not support maintaining multiple revisions of the same document. Moreover, using Datastore for handling revisions can be unnecessarily complex and lead to operational and development costs.

Option D is not suitable because although it offers the advantage of object versioning, using Cloud Scheduler to invoke a Cloud Functions instance is more complicated and costlier as compared to managing the storage classes and deleting old files via lifecycle conditions directly, making this option less efficient.

Solution to Question 36: A

The correct choice for reducing expenses when running nightly batch workloads on virtual machines (VMs) within a tech company, in this case, is option A: Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

The reason why option A is the most suitable choice is that preemptible VMs, in contrast to regular VMs, cost significantly less since they can be terminated at any time when resources are in high demand. For nightly batch workloads that are fault-tolerant and can handle occasional VM terminations, preemptible VMs provide a cost-effective solution. Furthermore, the N1 Standard VMs offer a balance between performance and memory, making them suitable for various tasks such as batch processing.

Option B suggests using Cloud Scheduler to trigger N1 Standard VMs. While Cloud Scheduler can help automate the process of creating and managing instances, it does not directly contribute to reducing the VM cost.

Option C recommends using preemptible N1 Highmem VMs. While preemptible VMs lower costs, the N1 Highmem VMs are specifically designed for memory-

intensive workloads, which is not mentioned as a requirement in the question. Thus, it is more appropriate to use the N1 Standard VMs.

Lastly, option D proposes using simulated maintenance events and regular (non-preemptible) N1 Standard VMs. While simulating maintenance events is a good approach to testing fault-tolerance, using regular VMs instead of preemptible VMs will not help reduce the costs as desired.

In conclusion, the answer is A, as the use of preemptible N1 Standard VMs allows the tech company to reduce their VM costs while still maintaining the performance necessary for handling the nightly batch workloads.

Solution to Question 37: B

The correct answer is B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

Explanation:

To access the multiple Linux instances without configuring specific access for the existing and new instances and also avoiding the assignment of public IP addresses to the Compute Engine instances, you should configure Cloud Identity-Aware Proxy (IAP) for SSH and TCP resources.

Cloud IAP enables you to authenticate users and manage access to SSH and TCP services running on your Google Cloud instances. This way, you can provide remote access to your instances securely, without needing to provide them with public IP addresses. Cloud IAP for SSH and TCP resources adds an extra layer of security for your Google Cloud environments and supports access to all instances.

Reasons why other options will not work:

A. Configure Cloud Identity-Aware Proxy for HTTPS resources: This option is not appropriate because Cloud IAP for HTTPS resources only provides secure access to web applications and doesn't support SSH access to instances. You need to configure IAP for SSH and TCP resources to achieve the desired result.

C. Configure an SSH bastion host to access instances through a private IP address: Using an SSH bastion host could allow you to SSH into your instances and reach them through their private IPs; however, it doesn't address the requirement to access all of these instances without configuring specific access for each instance. The bastion host also requires additional management, such as updating firewall rules and managing user access to the bastion host.

D. Use a Cloud Interconnect connection to link your on-premises network to your instances: Cloud Interconnect connects your on-premises network to Google Cloud through a dedicated, private network connection. While this could provide you access to your instances without using public IPs, it doesn't provide the same level of authentication and access control as Cloud IAP. Additionally,

this option doesn't match the requirement to access instances via an SSH client over the internet.

Solution to Question 38: A

The correct answer is A. Install a RDP client in your desktop. Set a Windows username and password in the GCP Console. Use the credentials to log in to the instance.

Explanation: As a database administrator, you want to connect to the SQL Server 2017 instance on Compute Engine using the least number of steps. Installing a Remote Desktop Protocol (RDP) client on your desktop and setting a Windows username and password in the Google Cloud Platform (GCP) Console will allow you to log in to the instance directly and access the SQL Server quickly and efficiently.

Here's why the other options will not work:

B. This option involves setting a Windows username and password in the GCP Console and verifying a firewall rule for port 3389, which is promising, since port 3389 is the standard port for RDP connections. However, it goes on to mention clicking the SSH button in the GCP Console to log in. SSH is mainly used for secure remote access to Linux-based systems, not Windows systems running SQL Server. Therefore, this option will not connect you to your SQL Server instance.

C. This option sets a Windows username and password in the GCP Console and suggests verifying a firewall rule for port 5432. Port 5432 is generally used for PostgreSQL databases, not for SQL Server instances. Although it continues with the instruction to click the RDP button in the GCP Console, the incorrect port specification makes this option unreliable for connecting to the SQL Server instance.

D. This option suggests setting a SQL Server username and password in the GCP Console and verifying a firewall rule for port 443. Port 443 is typically used for HTTPS connections, which are not suitable for connecting to SQL Server instances directly. Clicking the HTTPS button in the GCP Console will not provide the desired access to the SQL Server instance.

Solution to Question 39: B

The answer should be B (10.0.0.0/8) because it provides the largest address space compared to the other options.

Option B (10.0.0.0/8) will provide a range from 10.0.0.0 to 10.255.255.255, giving a total of 16,777,216 available IP addresses. This large range will accommodate the rapid growth of the company by providing enough IP addresses for all devices and services that will be connected to the network in the future.

Option A (203.0.113.0/24) is not suitable because its range is only from 203.0.113.0 to 203.0.113.255, offering just 256 IP addresses. This will not be

flexible enough to support a rapidly-growing tech company.

Option C (192.168.0.0/16) offers a larger range compared to Option A, but it is still smaller than option B. The range for Option C is 192.168.0.0 to 192.168.255.255, providing 65,536 IP addresses. Although this option may accommodate the current needs of the company, it might not be sufficient for future expansion.

Option D (198.51.100.0/24) provides the smallest range among all the options. Its range is from 198.51.100.0 to 198.51.100.255, offering only 256 IP addresses. This option will not support a rapidly-growing tech company in need of many IP addresses.

In conclusion, Option B (10.0.0.0/8) is the best choice to accommodate future growth with its large range of 16,777,216 IP addresses. The other options will not work because they provide smaller ranges that are not suitable for a rapidly-growing tech company.

Solution to Question 40: A

The correct answer is A. Here's why:

A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

This option is the most appropriate solution for the given requirements. By creating a single VPC with separate subnets for the DMZ and LAN, you are effectively mimicking the existing on-premises network structure in Google Cloud. By setting up firewall rules to open up relevant traffic between the DMZ and LAN subnets, you are enabling proper communication between your public and private servers using specific ports and protocols. Additionally, allowing public ingress traffic only for the DMZ ensures that only the servers in the DMZ can be accessed from the internet, while LAN servers remain restricted to internal network access.

Here's why the other options won't work:

B. This option is almost correct, but it has one major flaw: it states to block public ingress traffic for the DMZ. This contradicts the requirement to have some servers accessible from the internet. So, this option will not meet the necessary requirements.

C. This option is incorrect because it allows public ingress traffic for both the DMZ and the LAN. This would expose the private servers in the LAN to public access, which is against the requirements given. The LAN subnet should only be accessible internally and not from the internet.

D. Creating separate VPCs for the DMZ and the LAN might seem reasonable, but setting up firewall rules to block all traffic between the DMZ and LAN

subnets will prevent the required communication between the servers, which goes against the specified requirements. So, this option is not suitable for the given scenario.

Solution to Question 41: C

The correct answer is C - Change the primary key to not have monotonically increasing values.

Explanation:

Option A: Creating a secondary index using the following Data Definition Language (DDL) would not solve read latency issues for this table. In fact, it may make the issue worse, as secondary indexes are only helpful when the table is being accessed using other columns apart from the primary key. Since the table is only accessed by primary key reads, adding an index will only consume additional storage and processing resources without providing any performance benefits.

Option B: Removing the profile_picture field from the table would not address the read latency issues. The latency issue is related to how the primary key is organized within the table, not the size or structure of specific fields. Removing fields from a table can help with performance and storage optimization, but it would not provide a significant improvement in this case where the main issue lies in the primary key organization.

Option C: Changing the primary key to not have monotonically increasing values is the correct solution. Monotonically increasing primary key values can lead to performance problems in Cloud Spanner, as it often results in write hotspots where all new writes go to a single node. By changing the primary key values to be non-monotonic, data will be distributed more evenly across the nodes, leading to better load balancing and reducing read latency.

Option D: Splitting the table into two tables, one for user data and one for the profile_picture field, would not address the read latency issue. While normalizing the data can be useful for improving data management and storage, it does not specifically solve the read latency problem caused by monotonically increasing primary keys. Moreover, it would add complexity to data access, as joins would now have to be used to access the full set of user data.

Solution to Question 42: B

The correct answer is B, the other options should not be considered for the following reasons:

A. Creating a new service with the new version of the application and adding an HTTP Load Balancer in front of both services is not the right solution here. This option would require additional infrastructure setup and configuration. Cloud Run for Anthos already provides traffic splitting features, which allows canary deployments to be performed with less complexity. In this case, you should

utilize the features available in Cloud Run for Anthos to manage your canary deployment, as outlined in option B.

B. This is the correct option. By creating a new revision with the new version of the application and splitting traffic between this version and the currently running version, you can easily carry out a canary deployment. This allows you to test the updated version of your application with a specific percentage of your production users, adhering to the requirements stated in the question. Cloud Run for Anthos enables you to perform traffic splitting between revisions without the need for additional infrastructure or configuration.

C. Although Kubernetes Engine allows for traffic management in deployments, this solution does not use Cloud Run for Anthos, which is specifically mentioned in the question. Instead, it introduces an extra layer of complexity by deploying the application to a separate environment. It is more efficient and effective to use the built-in features of Cloud Run for Anthos to manage your canary deployments, as mentioned in option B.

D. Creating a new Cloud Firestore directory and using Google Cloud Endpoints to direct traffic to both directories is an incorrect solution. This does not address the question since Cloud Firestore is a NoSQL database, not a web application deployment platform. Additionally, Google Cloud Endpoints is an API management platform and is not specifically designed for managing canary deployments of web applications in the context of Cloud Run for Anthos. Option B is the most appropriate method for achieving the desired canary deployment.

Solution to Question 43: A

The correct answer is A. When creating the instances, specify a Service Account for each instance.

Explanation: By assigning specific service accounts to each Compute Engine instance when they are created, you ensure that each instance only has the necessary permissions to interact with the required Google Cloud APIs. This provides better security, as it follows the principle of least privilege, granting the minimum level of access needed for each instance to perform its tasks.

Reasons why other options will not work:

B. After starting the instances, use gcloud compute instances update to assign the name of the relevant Service Account as instance metadata. - Service accounts cannot be assigned as instance metadata through the update command. Assigning a service account to an instance should be done during its creation, as specified in option A.

C. Use the default Compute Engine service account for all instances and handle API access through IAM policies. - Using the default Compute Engine service account for all instances will not result in higher security and granular access control, as the default service account has broad permissions within the project

by default. It's better to create specific service accounts and assign them to instances to limit the access based on the individual instance requirements.

D. Create a Shared VPC and connect each instance to it, then assign a Service Account to the Shared VPC. - While Shared VPCs are useful for managing multiple projects, they are not relevant for managing service account access within a single project. Service accounts need to be assigned to each instance separately during their creation in order to provide the granularity and control required for higher security.

Solution to Question 44: C

The correct answer is C: Use the command gcloud auth activate-service-account and point it to the private key.

Explanation: In order to use the private key for authentication and authorization with the Cloud SDK, you must activate the service account by issuing the "gcloud auth activate-service-account" command. This command allows you to specify the service account email and private key file, establishing appropriate authentication for gcloud commands.

Why other options will not work:

A. Placing the private key file in the installation directory of the Cloud SDK and renaming it to credentials.json doesn't make the SDK use this file automatically for authentication. The SDK needs to be instructed which private key to use, and it's done using the "gcloud auth activate-service-account" command.

B. The "gcloud config set account" command sets the active user account, but it doesn't activate the service account with a private key. You need to use "gcloud auth activate-service-account" to specifically activate the service account and provide the private key file.

D. Placing the private key file in the .config/gcloud folder in your home directory and renaming it to active_credentials.json will not automatically activate the service account. You need to use the "gcloud auth activate-service-account" command to establish the correct authentication with the private key.

Solution to Question 45: B

The correct answer is B: Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

Explanation for B: By setting an organizational policy constraint to limit identities by domain, you ensure that only users with email addresses from your domain can access the company's Google Cloud resources. This prevents any future instances of mismatched users from accessing your resources without the need for continuous auditing. Additionally, removing the existing mismatched users retroactively aligns your current user base with the policy constraint, ensuring a secure environment for your company's resources.

Reasons why other options will not work:

A. Implement a Google Cloud Function that monitors projects for mismatched users and automatically removes them. While a Google Cloud Function could potentially identify and remove mismatched users, it requires continuous monitoring, which increases the administrative work. Furthermore, it doesn't prevent new mismatched users from accessing the resources.

C. Modify the Google Workspace SSO settings to prevent external users from accessing resources. While this option might seem like it could prevent some external users from access, it is not directly tied to Google Cloud resources and doesn't provide the level of granularity or control required for the stated goal. Additionally, it doesn't account for existing mismatched users.

D. Create a Cloud Scheduler task to regularly scan your resources and delete mismatched users. Although a Cloud Scheduler task might identify and delete mismatched users on a regular basis, it essentially involves continuously auditing resources, which increases administrative work. Furthermore, it doesn't prevent access to resources for new mismatched users between scheduled scans.

Solution to Question 46: D

The correct answer is D, and here's an explanation for why this should be chosen and why other options will not work:

Answer D: Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

Explanation: By adding a network tag of your choice to the instance running the LDAP server, you can specifically identify the instance in question. Creating a firewall rule to allow ingress on UDP port 636 for that specific network tag ensures that clients can reach the server through this port as mentioned in the task. This is the most appropriate and targeted solution to the problem.

Other options:

Option A: This option is incorrect because it suggests allowing egress on UDP port 636 rather than ingress. Since the objective is to ensure clients can reach the server, ingress should be allowed instead of egress.

Option B: This option combines several unrelated and unnecessary steps to address the task. Creating a VPC peering connection, using a VPN tunnel, and deploying an Identity-Aware Proxy add complexity and do not directly solve the problem. Moreover, the first part of this option refers to TCP instead of UDP.

Option C: This option is incorrect because simply adding a network tag itself will not influence connectivity. Even though the network tag name "allow-udp-636" implies allowing traffic on port 636, it must be combined with creating an appropriate firewall rule as described in answer D.

Thus, the best choice for ensuring clients can reach the LDAP server through port 636 using UDP is to choose answer D.

Solution to Question 47: A

The correct answer is A. Use Cloud Spanner for data storage.

Explanation for why the answer should be A: Cloud Spanner is a fully managed, mission-critical, relational database service built for the cloud that combines the benefits of a traditional relational database management system with non-relational scalability. It supports strong consistency, geographical replication, and global transactions, which are essential features for a trading application to be utilized by clients worldwide and require the exact same state of data with minimized latency. By deploying the application across multiple regions, Cloud Spanner will ensure optimal user experience with minimal delays.

Why other answers will not work:

B. Cloud Bigtable is a highly scalable NoSQL database designed for large, single-region real-time analytical workloads. It does not come with built-in multi-region support or provide strong consistency guarantees, which are crucial for a global finance trading application.

C. Cloud Datastore is a highly available and fully managed NoSQL document database designed for web and mobile apps that require robust data storage. While it does support multi-region deployment, it does not provide the strong consistency and relational structure needed for a global finance trading application, rendering it less suitable compared to Cloud Spanner.

D. Cloud Memorystore is a managed in-memory data store service primarily designed for caching and real-time use cases. It does not offer the structural support, strong consistency, and multi-region replication capabilities necessary for global finance trading applications that require all users to have the exact same state of data with minimized latency.

Solution to Question 48: D

Option D is the correct answer for the following reasons:

1. The OS Config agent is essential for enabling vulnerability management and OS metadata in Compute Engine instances. This agent scans and reports OS vulnerabilities, ensuring that the security team has visibility into the security status of the instance.

2. By providing the security team member with the roles/osconfig.vulnerabilityReportViewer permission, you are specifically granting them the required access to view the vulnerability reports generated by the OS Config agent. This aligns with the company's security vulnerability management policy.

Options A, B, and C are not correct for the following reasons:

Option A: VPC Service Controls help in securing your Google Cloud resources and data from unauthorized access, but they do not provide any vulnerability management functionality. Moreover, enabling VPC Service Controls does not provide the security team with the visibility into OS vulnerabilities and metadata.

Option B: This option is partially correct as it ensures the OS Config agent installation. However, creating a log sink to a BigQuery dataset is not necessary for managing OS vulnerabilities and does not provide the required access for the security team member to view the vulnerability reports.

Option C: The Ops Agent is primarily designed for logging and monitoring, but it does not provide the specific functionality required for managing OS vulnerabilities. Also, the roles/osconfig.inventoryViewer permission gives access to view inventory information, not vulnerability reports. Hence, this option will not fulfill the requirements of the company's security vulnerability management policy.

Solution to Question 49: B

The correct approach is B: Creating a multi-region Cloud Spanner instance with an optimized schema. Let's explain why this is the ideal solution and why the other options are not suitable.

The first option, using a multi-region Pub/Sub for streaming transaction data and analyzing it using Dataflow, is inefficient and not suitable for this case. Although Pub/Sub can handle real-time transactions, it does not provide the necessary data persistence or a highly available and scalable data store. Furthermore, it does not support SQL queries required by the business analytics team.

The second option, creating a multi-region Cloud Spanner instance with an optimized schema, is the best choice. Cloud Spanner is built for high availability, consistency, and global scaling. It is a fully managed relational database that supports SQL queries, making it appropriate for the requirements of both developers and the analytics team. Besides, as the company grows, it becomes even more essential to maintain a scalable data store that can handle an ever-increasing volume of transactions from multiple regions.

The third option, creating a multi-region Cloud Storage bucket and saving transaction data as CSV files, does not provide a suitable solution for the given problem. While data will be stored and made available in multiple regions, Cloud Storage is an object storage service and not a fully managed database. Saving transaction data as CSV files lacks the efficiency, consistency, and query support required by the analytics team.

Lastly, deploying a self-managed multi-region Cassandra database with limited scalability is not the ideal solution. Managing a database infrastructure by yourself can lead to increased workloads and risks, as the company would be responsible for handling the complexities of scaling, managing, and securing the database. Also, the option already talks about limited scalability, which is not suitable for a rapidly growing e-commerce company.

Considering the requirements, choosing option B: Creating a multi-region Cloud Spanner instance with an optimized schema is the most suitable solution. This way, the company can develop a highly available and scalable data store for

the platform that will serve the needs of both the development and business analytics teams.

Solution to Question 50: B

The best approach to achieve creating a new project to serve as your production environment and deploy the application is Option B: Use gcloud to create the new project, and then deploy your application to the new project.

Option B is the best approach because it ensures that your development and production environments are separated in different projects, following best practices to avoid any unwanted changes and enabling better manageability, access control, and resource allocation. Additionally, using gcloud (Google Cloud SDK) to create and manage the resources allows a more efficient, scripted, and automated control over your GCP projects.

Option A is not suitable because Dataflow is primarily used for data processing and transformation tasks and not for copying application code from one project to another.

Option C is not the best approach since creating a second App Engine application within the same project might make it harder to manage the separation of responsibilities, permissions, and resources between development and production environments. You should have separate projects for better isolation.

Option D is not a feasible approach because the GCP Console does not provide a native method to export and import App Engine applications directly between projects. This manual process would be more time-consuming and prone to errors than using gcloud as suggested in Option B.

Practice Exam 9

Question 1: In your company, you have been assigned the task of configuring IAM access audit logging in BigQuery for external auditors while adhering to Google-recommended practices within the tech industry. What is the appropriate course of action to achieve this?

A. Add the auditors group to the 'bigQuery.dataViewer' and 'logging.admin' predefined IAM roles.

B. Add the auditor user accounts to the 'bigQuery.projectViewer' and 'logging.writer' predefined IAM roles.

C. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

D. Add the auditor user accounts to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

Question 2: Working as a financial manager in a tech company, your organization, which already has an existing GCP organization with hundreds of projects and a billing account, recently acquired another company with hundreds of projects and its own billing account. Your goal is to consolidate all GCP costs from both GCP organizations onto a single invoice starting tomorrow. What should you do?

A. Link the acquired company's projects to your company's billing account.

B. Configure your company's billing account to access the acquired company's billing data using IAM roles.

C. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued.

D. Create a custom report in the GCP Console that shows the combined costs of both companies' GCP projects and use that as the invoice.

Question 3: As an IT specialist at XYZ company, you have been tasked with developing a new application that utilizes Google Cloud Platform (GCP) services like AutoML. The application will be run from the company's on-premises data center. You have already set up a service account which has the necessary access rights to AutoML. In order to authenticate API access from the company's on-premises environment, what steps should you take?

A. Use gcloud to create a key file for the service account that has appropriate permissions.

B. Go to the IAM & admin console, grant a user account permissions similar to the service account permissions, and use this user account for authentication from your data center.

C. Configure a Compute Engine instance with appropriate permissions and connect your on-premises application to it

D. Create a separate project for the on-premises application and use its default service account for authentication

Question 4: As an IT manager for a tech company, you are tasked with configuring 10 Compute Engine instances to ensure availability during maintenance. The instances must automatically restart in case of crashes and maintain high availability even during system maintenance. How should you proceed to achieve this requirement?

A. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Terminate VM instance. Add the instance template to an instance group.

B. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to None. Add the instance template to an instance group.

C. Create an instance group for the instances. Set the 'Autohealing' health check to healthy (HTTP).

D. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

Question 5: You are part of a software development company that specializes in creating containerized applications. Your team has developed an application and packaged it into a Docker image. Now, you need to deploy this Docker image as a workload on Google Kubernetes Engine for a client in the finance industry. What is the appropriate action to take?

A. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image.

B. Upload the image to Container Registry and create a Kubernetes DaemonSet referencing the image.

C. Upload the image to Container Registry and create a Kubernetes StatefulSet referencing the image.

D. Upload the image to Container Registry and create a Kubernetes Service referencing the image.

Question 6: You just started working at a tech company where they utilize Google Cloud for their projects. After installing the Google Cloud CLI on your office computer, you need to view the existing instances of your organization on Google Cloud. What actions should you take before executing the gcloud compute instances list command? (Choose two.)

A. Check that your system environment variables include GOOGLE_APPLICATION_CREDENTIALS.

B. Run gsutil config to authenticate the gcloud CLI with your Google Cloud Storage bucket.

C. Run gcloud config set project $my_project to set the default project for gcloud CLI.

D. Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI.

Question 7: As a finance analyst in a tech company, you are responsible for monitoring expenses across multiple Google Cloud projects, each linked to different billing accounts. You need to create a single visual representation of all costs incurred for more accurate budget forecasting and include the latest cost data as fast as possible. What approach should you take?

A. Create custom metrics for billing and track costs using Cloud Monitoring dashboards on a per-project basis.

B. Set up a Google Sheets-based billing dashboard for each billing account and combine them manually.

C. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

D. Visit the Cost Table page to get a CSV export and visualize it using Data Studio.

Question 8: As a project manager in a software development company, you've been tasked with estimating the total cost of running a three-tier web application on Google Cloud instances and Cloud SQL, considering that the application currently runs on virtual machines using a MySQL database. How should you proceed?

A. Look for a pre-existing pricing structure of a similar 3-tier web application on Google Cloud Platform Forums, and adapt this structure to your own use case.

B. Read through the Google Cloud documentation and determine the cost of resources using trial and error based on the structure of your web application.

C. Use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource you expect to use. Use similar size instances for the web server, and use your current on-premises machines as a comparison for Cloud SQL.

D. Use the Google Cloud Pricing Calculator and select the Cloud Operations template to define your web application with as much detail as possible.

Question 9: As a team lead in an IT company, you need to delegate control to your team members in managing buckets and files in Google Cloud Storage for the projects they are assigned to. In order to adhere to Google-recommended practices, which IAM role should you grant them?

A. Storage Admin

B. App Engine Admin

C. Pub/Sub Admin

D. Project Editor

Question 10: As an IT manager at a software company, you are in charge of a web application running on Compute Engine. Your goal is to ensure the support team gets automatically notified if clients experience high latency for a minimum of 5 minutes. Considering a Google-suggested solution with no development cost, what should be your course of action?

A. Use the Cloud Monitoring dashboard to observe latency and take the necessary actions when the response latency exceeds the specified threshold.

B. Use Cloud Armor to monitor and alert on high latency events in your Compute Engine instances.

C. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

D. Export Cloud Monitoring metrics to Cloud Storage and use Data Studio to create a dashboard for monitoring latency.

Question 11: As a DevOps engineer in a software company, you are responsible for setting up a Google Kubernetes Engine (GKE) cluster with the cluster autoscaler feature enabled. You must ensure that each node in the cluster runs a monitoring pod, which sends container metrics to a third-party monitoring solution. What's the right course of action to take in this situation?

A. Deploy the monitoring pod in a CronJob object.

B. Deploy the monitoring pod in a DaemonSet object.

C. Deploy the monitoring pod in a ConfigMap object.

D. Enable a GKE add-on for third-party monitoring integration.

Question 12: You are working in a software company as a cloud architect, and you're tasked with moving a mission-critical application from the company's local data center to Google Cloud. You need to make sure that any data used by the application will be readily accessible in the event of a zonal failure, in order to maintain high availability. What action should you take?

A. Store the application data on a zone-local SSD, and if an outage occurs, recover the lost data from the local SSD in another zone.

B. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

C. Store the application data on a regional persistent disk. Create a snapshot schedule for the disk. If an outage occurs, create a new disk from the most recent snapshot and attach it to a new VM in another zone.

D. Store the application data on a zonal persistent disk. Create a snapshot schedule for the disk. If an outage occurs, create a new disk from the most recent snapshot and attach it to a new VM in another zone.

Question 13: As a network engineer in a technology company, you are tasked with establishing a secure Virtual Private Network (VPN) connection between a newly created Virtual Private Cloud (VPC) and a remote location. The main requirements are dynamic routing, a shared address space of 10.19.0.1/22, and avoiding overprovisioning of tunnels during failover events. In order to adhere to Google's recommended practices and achieve a high availability Cloud VPN, what should be your approach?

A. Use a custom mode VPC network, configure static routes, and use active/passive routing.

B. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

C. Use an automatic mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and configure policy-based routing.

D. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and configure VPN tunnel over Interconnect.

Question 14: You are working as a cloud engineer in a tech company and have created a new project in Google Cloud through the gcloud command line interface (CLI), linking it to a billing account. Your manager asks you to set up a new Compute Engine instance using the CLI and to complete any necessary prerequisite steps. What should you do before creating the instance?

A. Create a VPC network in the project.

B. Enable the compute.googleapis.com API.

C. Create a Cloud Storage bucket in the project.

D. Create a Cloud Run service in the project.

Question 15: While working as a software developer in a well-known software company, you happen to deploy a new version of an application to App Engine. After the deployment, you find a bug in the new release and need to immediately revert to the prior version of the application. What should you do to accomplish this?

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

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

100% of the requests.

C. Stop the current version on the App Engine page, then restart the previous version. Use gcloud app migrations command to revert to the previous version. On the App Engine Services page of the GCP Console, delete the faulty version and select the prior version to be live. Use gcloud app versions command to switch to the previous version of the application.

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

Question 16: You are working as a data analyst in a tech company, where you manage an App Engine Service that consolidates and displays data from BigQuery. The application utilizes the default App Engine Service account. However, the data that needs to be visualized is in a separate project managed by another department in your company. You do not have access to their project, but you'd like your application to read data from their BigQuery dataset. What action should you take to achieve this?

A. Create your own BigQuery dataset in your project and ask the other team to sync their data with your dataset.

B. Request the other team to export their BigQuery dataset to Cloud Storage which your App Engine service can then read and visualize.

C. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

D. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Data Viewer in your project.

Question 17: Your organization, a software development company, is planning to move its on-premises workloads to Google Cloud. The existing on-premises workloads consist of the following components: a Flask web application, a backend API, and a scheduled long-running background job for ETL and reporting. To minimize operational expenses and abide by Google's recommended best practices, you have been assigned to migrate these workloads to serverless solutions on Google Cloud. What approach should you take?

A. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

B. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run. Use Cloud Tasks to run your background job on Compute Engine.

C. Run the web application on a Cloud Storage bucket and the backend API on Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

D. Run the web application on a Cloud Storage bucket and the backend API on App Engine. Use Cloud Tasks to run your background job on Cloud Functions.

Question 18: You are working as a DevOps Engineer in a technology company, and your manager has tasked you with updating a deployment in Deployment Manager without causing any downtime to the resources within that deployment. Which command should you execute to accomplish this?

A. gcloud deployment-manager deployments update –config

B. gcloud deployment-manager resources create –config

C. gcloud deployment-manager deployments stop –config

D. gcloud deployment-manager resources delete –config

Question 19: You are working as a cloud administrator in a company where multiple teams share access to a common project environment. You are tasked with hosting an application on a Compute Engine instance in this shared project. To secure the application and minimize the chances of other teams inadvertently causing downtime, which feature should you utilize in this scenario?

A. Restrict SSH access to the instance

B. Use a sole-tenant node.

C. Enable deletion protection on the instance.

D. Use an Instance Template

Question 20: You are working as a network administrator at a software development company and have noticed that the primary internal IP addresses in a subnet for a custom mode VPC are running out. This subnet uses the IP range 10.0.0.0/20, and the virtual machines in the project rely on these IP addresses. To ensure that you can provide more IP addresses for the virtual machines, what should you do?

A. Add a secondary IP range 10.2.0.0/20 to the subnet.

B. Add a secondary IP range 10.1.0.0/20 to the subnet.

C. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

D. Enable Private Google Access for the virtual machines.

Question 21: You are working as a cloud engineer at a company and managing their web application on Cloud Run, which is used by a few hundred clients. Some clients report that the initial load time of the web app is significantly longer than the subsequent pages. In order to address this issue while adhering to Google's recommendations, what should you do?

A. Set the minimum number of instances for your Cloud Run service to 3.

B. Set the concurrency number to 1 for your Cloud Run service.

C. Enable autoscaling on the Cloud Run service.

D. Decrease the request timeout for your Cloud Run service.

Question 22: As a software engineer at a technology-based company, you are tasked with integrating the company's single sign-on (SSO) identity provider that supports Security Assertion Markup Language (SAML) with service providers. The company has user accounts set up in Cloud Identity and wants users to authenticate using your organization's SSO provider. What is the best method for achieving this goal?

A. Create a custom SAML app in GCP, and configure it to work with your company's SSO provider.

B. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service consumer.

C. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

D. In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps.

Question 23: As a software engineer at a tech company, you are responsible for selecting and configuring compute resources for a set of nightly batch processing jobs that take around 2 hours to complete. Your primary objective is to minimize service costs for the company. What should you do?

A. Select Cloud Functions with maximum memory allocation.

B. Select App Engine with standard environment and manual scaling.

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

D. Select App Engine. Use flexible environment with automatic scaling.

Question 24: You are an IT manager at a tech company, and a team of data scientists occasionally needs to use a Google Kubernetes Engine (GKE) cluster under your supervision. They require GPUs for executing lengthy, non-interruptible tasks. How can you minimize the costs involved while meeting their requirements?

A. Use Compute Engine instances with GPUs for the data scientists' workloads.

B. Enable node auto-provisioning on the GKE cluster.

C. Create a node pool with regular VMs and GPUs attached to those VMs.

D. Create a VerticalPodAutoscaler for those workloads.

Question 25: As an IT administrator for a software company, you have an application that looks for its licensing server on the IP 10.0.3.21. You need to deploy the licensing server on Compute Engine without changing the configuration of the application, ensuring that the application can reach the licensing server. What should you do?

A. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

B. Create a load balancer with the backend pointing to the licensing server and use the IP 10.0.3.21 as the frontend IP address.

C. Reserve the IP 10.0.3.21 as a static public IP address using gcloud and assign it to the licensing server.

D. Create a custom routing rule to route traffic destined for 10.0.3.21 to the licensing server's actual IP address.

Question 26: As a software engineer at a rapidly growing tech company, you've been tasked with streamlining and standardizing the creation and management of multiple Google Cloud resources using Infrastructure as Code. The goal is to reduce the amount of repetitive code necessary for managing the environment efficiently. What is the best approach to achieve this?

A. Use curl in a terminal to send a REST request to the relevant Google API for each individual resource.

B. Use Google Cloud Run to manage resources via a stateless container implementation.

C. Develop templates for the environment using Cloud Deployment Manager.

D. Write custom Python code using the Google Cloud SDK to create and manage resources.

Question 27: You are working as a DevOps engineer at a software company and you have recently deployed a new application inside your Google Kubernetes Engine cluster using the YAML file specified below. After checking the status of the deployed pods, you notice one of them is still in PENDING status. To identify the reason why the pod is stuck in pending status, what should you do?

A. Check the Google Kubernetes Engine dashboard for any errors related to the cluster.

B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

C. View logs of the container in myapp-deployment-58ddbbb995-lp86m pod and check for warning messages.

D. View logs of the myapp-service Service object and check for error messages.

Question 28: As a network administrator in a software development company, you are responsible for managing two subnets (subnet-a and subnet-b) within the default VPC. The database servers reside in subnet-a, while application servers and web servers are in subnet-b. To enhance security, you need to implement a firewall rule that allows only database traffic from the application servers to access the database servers. What is the most appropriate course of action to achieve this configuration?

A. Create a network tags app-server and db-server. • Add the app-server tag to the database servers and the db-server tag to the application servers. • Create an egress firewall rule to allow network traffic from source network tag app-server to target network tag db-server.

B. Create a service account sa-app and a network tag db-server. • Associate the service account sa-app with the database servers and the network tag db-server with the application servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target network tag db-server.

C. • Create a service account sa-app and a network tag db-server. • Associate the service account sa-app with the application servers and the network tag db-server with the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-a IP addresses.

D. • Create service accounts sa-app and sa-db. • Associate service account sa-app with the application servers and the service account sa-db with the database servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

Question 29: As an IT specialist working in a financial company, you are tasked with developing an archival solution for your data warehouse using Cloud Storage. The company needs to access this archived data quarterly for regulatory compliance purposes. Which cost-efficient storage option should you choose?

A. Regional Storage

B. Multi-Regional Storage

C. Firestore

D. Cold Storage

Question 30: As a cloud engineer working for a tech company that heavily relies on Google Cloud Platform, you are asked to verify that a service account was created at a specific time. How should you accomplish this task?

A. Filter the Activity log to view the Configuration category. Filter the Resource type to BigQuery.

B. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

C. Filter the Activity log to view the Configuration category. Filter the Resource type to Google Project.

D. Filter the Audit logs to view the Configuration category. Filter the Resource type to Compute Engine.

Question 31: You work as a software engineer for a company that utilizes Google Cloud infrastructure. Your team has deployed an application in Google

Kubernetes Engine (GKE) with cluster autoscaling enabled, which exposes a TCP endpoint and has multiple replicas. There is a Compute Engine instance situated in the same region but in a different Virtual Private Cloud (VPC) called gce-network, with no overlapping IP ranges with the first VPC. This instance needs to establish a connection with the GKE application. To accomplish this with minimal effort, what strategy should you implement?

A. 1. In GKE, create a Service of type ExternalName that points to the GKE application's Pods. 2. Peer the two VPCs together. 3. Configure the Compute Engine instance to use the address of the ExternalName Service that has been created.

B. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal 3. Peer the two VPCs together. 4. Configure the Compute Engine instance to use the address of the load balancer that has been created.

C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add a custom annotation that allows access from gce-network. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

D. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Configure a VPN between the two VPCs. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

Question 32: As an employee of a leading transcription company, you must extract text from audio files using the Speech-to-Text API. Your clients upload audio files to a Cloud Storage bucket, and you need to create a fully managed, serverless compute solution that requires authentication and aligns with Google-recommended practices. To automate the process and ensure that the API is called for each file as it arrives in the bucket, what should you do?

A. Create a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

B. Configure a Cloud Pub/Sub subscription to listen for events from the Cloud Storage bucket and submit the file URI to the Google Speech-to-Text API.

C. Deploy a Cloud Shell script on a regular schedule to scan the bucket regularly for incoming files and call the Speech-to-Text API for each unprocessed file.

D. Run a Kubernetes job to scan the bucket regularly for incoming files, and call the Speech-to-Text API for each unprocessed file.

Question 33: You are an engineer at a major tech company, focusing on analyzing real-time data for predicting market trends in the digital industry. You've been tasked with developing an efficient pipeline for processing time-

series data using Google Cloud Platform services. Which combination of services should you utilize for boxes 1,2,3, and 4 in the pipeline?

A. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery

B. Cloud Pub/Sub, Cloud Dataflow, BigQuery, Cloud Spanner

C. Cloud Pub/Sub, Cloud Dataflow, Cloud Datastore, BigQuery

D. Cloud Pub/Sub, Cloud Dataproc, Cloud Storage, BigQuery

Question 34: As a software engineer working for a cloud-based company, you're responsible for developing a product utilizing Google Kubernetes Engine (GKE) with a single GKE cluster. Each customer has their own pod running within the cluster, with the ability to run arbitrary code inside their pod. Your task is to optimize the isolation between these customers' pods. Which strategy should you implement to achieve this goal?

A. Use the cos_containerd image for your GKE nodes. Add a nodeSelector with the value cloud.google.com/gke-os-distribution: cos_containerd to the specification of your customers' Pods.

B. Create a separate GKE cluster for each of your customers to run their Pods.

C. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

D. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

Question 35: You are working as an infrastructure engineer at a software company, and it's predicted that the company will experience a significant increase in application traffic due to a recent business acquisition. To prepare for the anticipated load, you need to create a copy of a custom Compute Engine virtual machine (VM). What is the recommended course of action?

A. Create a Compute Engine managed instance group from your base VM. Create your instances from that instance group.

B. Create a Google Kubernetes Engine cluster from your base VM. Create your instances from that cluster.

C. Create a custom Compute Engine image from a snapshot. Create your instances from that image.

D. Create a custom Compute Engine image from a snapshot. Create your instances from a Cloud Storage bucket.

Question 36: You are working as a Cloud Engineer in a software development company. You have been utilizing Google Cloud for various projects and initially set up the billing with your personal credit card. The company has decided to

simplify the billing process by charging project costs directly to their corporate account. What steps should you take to implement this change?

A. Set up BigQuery billing export and grant your financial department IAM access to query the data.

B. Export your project billing information to a spreadsheet and share it with your financial team.

C. Change the billing account of your projects to the billing account of your company.

D. Use Google Cloud Pub/Sub to send billing notifications to your finance team.

Question 37: As a software developer working in a multinational company that heavily relies on Google Cloud services centralized in a single project for smooth operations, your DevOps team requires access to all production services to effectively perform their tasks. You want to ensure that Google Cloud product changes do not inadvertently expand their permissions in the future and wish to adhere to Google's recommended best practices. What course of action should you take?

A. Create a custom role with Compute Admin permissions and grant all members of the DevOps team the custom role on the production project.

B. Create a service account with required permissions and provide the DevOps team with the credentials.

C. Grant all members of the DevOps team the role of Project Owner on the organization level.

D. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

Question 38: As a software engineer in a multinational company handling Google Cloud infrastructure, you need to permanently delete a Pub/Sub topic managed by Config Connector in the company's Google Cloud project. What is the appropriate action to take?

A. Use kubectl to rename the topic resource.

B. Use kubectl to create the label deleted-by-cnrm and to change its value to true for the topic resource.

C. Use kubectl to delete the topic resource.

D. Use kubectl to update the topic label deleted-by-cnrm to true.

Question 39: As a cloud administrator in a software development company, you have one project called proj-sa where you manage all your service accounts. You need to be able to use a service account from the proj-sa project to take snapshots of VMs running in another project called proj-vm. What should you do?

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

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

C. Grant the service account the IAM Role of Project Viewer in the project called proj-vm.

D. Grant the service account the IAM Role of Compute Instance Admin in the project called proj-vm.

Question 40: You're working as an IT administrator in a company that hosts an internal static website on Cloud Storage, which contains informative PDF files for employees. Recently, you decided to include links to these PDF files on the website. When employees click on the links, their browsers prompt them to save the file onto their local system. However, you want the PDF files to be displayed directly within the browser window without prompting users to save the files locally. What should you do?

A. Enable object versioning for the bucket containing PDF files.

B. Use Firebase Hosting instead of Cloud Storage for the static website.

C. Set Content-Type metadata to application/pdf on the PDF file objects.

D. Create a custom role with permissions to view the PDF files in-browser.

Question 41: You're working as a DevOps engineer at a growing tech company, and your team has decided to deploy a specific content management system (CMS) on Google Cloud to streamline content organization. To efficiently install and deploy the CMS solution, what should you do?

A. Use Cloud Build to build a Docker image of the CMS, then deploy the solution to Google Cloud Run.

B. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

C. Deploy the CMS solution using Kubernetes Engine and manually configure the solution using the YAML files.

D. Manually install the CMS on a new App Engine standard environment instance.

Question 42: As a data analyst at a leading tech company, you are tasked with setting up a cost-effective archiving solution for data stored in a Cloud Storage bucket. Multiple versions of the data should be archived after 30 days, and previous versions must be accessed once a month for reporting purposes. Additionally, the archived data is occasionally updated at the end of each month. How should you proceed?

A. Add a bucket lifecycle rule that archives data from multi-regional storage after 30 days to Coldline Storage.

B. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Nearline Storage.

C. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

D. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Coldline Storage.

Question 43: As a data analyst working in a large corporation using Google Cloud Platform and BigQuery for data warehousing, you have been tasked with making sure your data science team, which frequently changes and has a limited number of members, can perform essential queries while adhering to Google-recommended best practices. What should be your next course of action?

A. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery machineLearningAdmin user role to the group.

B. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery jobUser role to the group.

C. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery admin user role to the group.

D. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery dataEditor user role to the group.

Question 44: You are working for a software company specializing in web applications and are in charge of updating an application currently hosted in an App Engine environment. Your task is to first test the new version with 1% of users before fully transitioning the application to the new version. What is the appropriate course of action to achieve this?

A. Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic.

B. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

C. Use Cloud Pub/Sub to distribute 1% of your application's traffic to the new version deployed in App Engine.

D. Deploy the new version of your application in a separate project within App Engine and then use GCP Console to split traffic.

Question 45: You are the lead engineer at a rapidly growing software development company that was established 6 months ago. With a growing customer base and increased usage of Google Cloud for various tasks, you need to establish a way for your fellow engineers to create new projects without requiring their personal credit card details. What would be the most efficient approach to achieve this?

A. Apply for Google Cloud Startup credits and distribute them among the engineering team.

B. Set up a shared Google Cloud account with pre-purchased credits for all engineers to use for project creation.

C. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

D. Create a billing account, associate it with a monthly purchase order (PO), and send the PO to Google Cloud.

Question 46: As a web developer in a reputable tech company, you are tasked with creating a secure website with autoscaling for a client, based on the compute instance CPU load. To enhance the performance of the site, you've decided to store the static content in Cloud Storage. Which resources do you require to properly distribute user traffic?

A. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load, and Google Cloud Storage FUSE to serve static content from the compute instances.

B. An external HTTP(S) load balancer with managed SSL for the backend service and an additional Cloud Pub/Sub integration for distributing the requests for the static content to the Cloud Storage backend.

C. An external HTTP(S) load balancer to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend. Install the HTTPS certificates on the instance.

D. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

Question 47: As a software engineer at a leading tech company, you are responsible for maintaining an existing application running in Google Kubernetes Engine (GKE) that consists of several pods running on four GKE n1-standard-2 nodes. You need to deploy additional pods that require n2-highmem-16 nodes without causing any downtime. What should you do?

A. Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

B. Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

C. Use gcloud container clusters set-machine-type to change the node type to n2-highmem-16 and deploy the new pods.

D. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

Question 48: As a database administrator for a finance company that relies on a Cloud SQL MySQL database, you are required to maintain a month-end copy of the database for auditing purposes over a period of three years. What is the most appropriate course of action to achieve this?

A. Save the automatic first-of-the-month backup for three years. Store the backup file in an Archive class Cloud Storage bucket.

B. Set up an on-demand backup for the first of the month. Write the backup to an Archive class Cloud Storage bucket.

C. Convert the automatic first-of-the-month backup to an export file. Write the export file to a Coldline class Cloud Storage bucket.

D. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

Question 49: As a software developer in a tech company, you are deploying an application to App Engine for your client. They require the number of instances to scale according to the request rate and always want at least 3 unoccupied instances available. Which scaling type should you use?

A. Basic Scaling with target_cpu_utilization set to 3.

B. Basic Scaling with max_instances set to 3.

C. Automatic Scaling with min_idle_instances set to 3.

D. Manual Scaling with 1 instance.

Question 50: As a system administrator in a software company, you are managing multiple Google Cloud Platform (GCP) projects for different teams and need to have access to all logs from the past 60 days. To efficiently explore and analyze the log content while adhering to Google's best practices for obtaining combined logs across all projects, what should you do?

A. Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days.

B. Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

C. Configure a Stackdriver Logging Sink to stream logs directly to BigQuery. Use Dataflow to parse and process logs in real-time.

D. Use Stackdriver Logging Viewer to export logs to Cloud SQL and set the retention policy for log data to 60 days.

Practice Exam 9 Solutions

Solution to Question 1: C

The correct answer is C. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

The reasons why option C is the most appropriate course of action are as follows:

1. Combining 'logging.viewer' and 'bigQuery.dataViewer' provides the sufficient required access for external auditors to perform IAM access audit logging in BigQuery. The 'logging.viewer' role allows them to view Stackdriver logs to perform analysis and monitoring, while the 'bigQuery.dataViewer' role provides the necessary access to bigQuery datasets.

2. It is recommended to assign permissions to groups rather than individuals. Assigning IAM roles to an auditors group makes it easier to manage access and makes the process more efficient than adding individual user accounts (options B and D). This adheres to the Google-recommended principles of least privilege and streamlined role management.

The reasons why other options are not suitable:

A. The 'logging.admin' role is not required for external auditors. This role grants full control and management of the logs, which is not necessary for auditors who only need to view logs. Hence, option A will violate the principle of least privilege.

B. The 'bigQuery.projectViewer' role allows viewing the project-level metadata but doesn't provide the necessary access to datasets that auditors need. The 'logging.writer' role provides the ability to write logs, which auditors do not need, and violates the principle of least privilege. Assigning roles individually instead of using a group is also not optimal.

D. As explained earlier, assigning roles to individual user accounts instead of using a group is not an efficient way to manage access. Hence, option D is not the recommended choice.

Solution to Question 2: A

The correct option is A. Link the acquired company's projects to your company's billing account.

Explanation for A: By linking the acquired company's projects to your company's billing account, you'll be consolidating all GCP costs from both companies onto a single invoice. This allows for unified management and a clear view of the expenses across your organization.

Reasons why other options will not work:

B. Configure your company's billing account to access the acquired company's billing data using IAM roles: IAM roles manage access to different resources within GCP but do not consolidate billing accounts. Linking the projects to your organization's billing account is necessary for attaining a single invoice.

C. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued: While this keeps the finance team informed of new invoices, it doesn't consolidate the costs for both GCP organizations onto a single invoice. You will still receive separate invoices for each billing account, making it difficult to manage and track expenses effectively.

D. Create a custom report in the GCP Console that shows the combined costs of both companies' GCP projects and use that as the invoice: Although custom reports can help visualize combined expenses, they don't actually merge the billing accounts or create a single invoice. Hence, this option doesn't address the requirement of consolidating all GCP costs from both organizations onto a single invoice.

Solution to Question 3: A

The correct answer is A. Use gcloud to create a key file for the service account that has appropriate permissions.

Explanation for why A is the best option: Creating a key file for the service account with the necessary permissions is the most secure and straightforward way to authenticate API access from the company's on-premises environment. Utilizing the existing service account ensures that the IT specialist can manage the permissions separately, giving them more control over the resources that the new application can access within GCP. Key files can be generated using the gcloud command-line tool, and this key file can be securely stored and used in the on-premises environment to authenticate when interacting with the GCP APIs such as AutoML.

Reasons why other options do not work effectively:

Option B: Going to the IAM & admin console and granting a user account permissions similar to the service account is not a recommended method, as user accounts are managed separately and can create confusion with the management of access rights. It is also less secure, as user accounts may have unrelated permissions or change unexpectedly.

Option C: Configuring a Compute Engine instance with the appropriate permissions and connecting the on-premises application to it adds unnecessary complexity to the architecture. It introduces latency to the API calls and additional costs for running a Compute Engine instance. Moreover, it is potentially less secure as it could create an additional attack point.

Option D: Creating a separate project for the on-premises application and using its default service account for authentication may overcomplicate the setup. Not only would this require the extra task of creating and managing a new project,

but default service accounts often come with more permissions than necessary, creating potential security risks. Using existing service accounts with specific access rights, as described in Option A, provides better control and security.

Solution to Question 4: D

The correct answer is D. Here's why:

Option A: The 'On-host maintenance' setting as Terminate VM instance is not suitable for maintaining high availability during maintenance. If the option is set to 'Terminate', the instances will be terminated when maintenance occurs, and there will be downtime. This doesn't satisfy the requirement of ensuring availability during maintenance.

Option B: The 'On-host maintenance' setting as None means that the maintenance is never performed. While this may avoid immediate downtime, it could lead to potential security and performance issues over time. This is not a sustainable solution for high availability.

Option C: Creating an instance group and setting the health check to healthy (HTTP) alone is not enough to solve the requirement. Although the Autohealing process ensures instances are recreated if they fail the health check, it doesn't address the need for availability during system maintenance.

Option D: Creating an instance template with 'Automatic Restart' set to on ensures the instances restart automatically in case of crashes. Setting the 'On-host maintenance' to Migrate VM instance means that the instances will be live-migrated to another host during maintenance, maintaining high availability even during the system maintenance. Adding the instances to an instance group will help distribute incoming traffic and manage instance health effectively. This option meets all the requirements mentioned in the question.

Solution to Question 5: A

The correct answer is A. There are several reasons why this is the best course of action and why the others are not appropriate.

A. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image. This is the correct answer because Artifact Registry is a Google Cloud service designed to store and manage container images securely and privately. Uploading the Docker image to Artifact Registry ensures that it can be easily accessed and deployed within the Google Kubernetes Engine (GKE). When creating a Kubernetes Deployment, you are defining a scalable and resilient application by specifying the desired state (number of replicas) and how the application should be updated. This suits the needs of a finance industry client, as deployments ensure availability and fault tolerance in their applications.

B. Upload the image to Container Registry and create a Kubernetes DaemonSet referencing the image. This option is not appropriate because a DaemonSet is used when you need to run a single instance of a container on every node in

a Kubernetes cluster. This is useful for monitoring and logging purposes, but not for deploying a containerized application meant for end users in the finance industry.

C. Upload the image to Container Registry and create a Kubernetes StatefulSet referencing the image. This option is not suitable because a StatefulSet is used when the application requires stable network identity and persistent storage. StatefulSets are common in database applications, but there is no indication that the application in question has any specific stateful requirements. Therefore, using a StatefulSet would add complexity without any noticeable benefits for the client.

D. Upload the image to Container Registry and create a Kubernetes Service referencing the image. This option is incorrect because a Kubernetes Service is used to expose an application to other applications or users. While this is a necessary component in many deployments, creating a Kubernetes Service alone does not deploy the application itself. Consequently, this would not fulfill the requirement of deploying the application as a workload on GKE.

In summary, the appropriate action to take is to upload the Docker image to Artifact Registry and create a Kubernetes Deployment referencing the image, as it caters to the needs of a finance industry client, ensuring availability, fault tolerance, and easy management of their containerized applications within Google Kubernetes Engine.

Solution to Question 6: D

The correct answers are C and D. Here's why:

Answer A is incorrect because setting the GOOGLE_APPLICATION_CREDENTIALS environment variable is primarily used for applications and scripts to authenticate with Google Cloud APIs. It is not a requirement in this scenario where you want to view existing instances using gcloud CLI.

Answer B is incorrect because gsutil config is meant for configuring and authenticating with Google Cloud Storage. Since you want to work with Google Cloud instances, gsutil is not the right tool for this purpose.

Answer C is correct because, when using the gcloud CLI, it is essential to set the default project you would like to work with. Running "gcloud config set project $my_project" accomplishes this by setting the project you want to view instances from as the default.

Answer D is correct because, before using the gcloud CLI, you need to perform an initial authentication to access your organization's resources on Google Cloud. Running "gcloud auth login" prompts you to enter your credentials and a login token, giving you the necessary access to view instances in your organization.

Therefore, the right actions to take before executing the gcloud compute instances list command are C and D, which involve setting the default project and authenticating your account with gcloud CLI.

Solution to Question 7: C

The correct answer is C, which involves configuring Billing Data Export to BigQuery and visualizing the data in Data Studio. This approach allows you to consolidate and visualize expenses from multiple Google Cloud projects and billing accounts in a single, interactive report. Moreover, BigQuery enables real-time data processing, ensuring that you have the latest, most accurate cost information for budget forecasting.

Option A is not advisable because creating custom metrics for billing and tracking costs using Cloud Monitoring dashboards on a per-project basis does not provide a consolidated visual representation of costs across different billing accounts. This approach would require manual efforts to compile information from multiple dashboards to perform budget forecasting, making it less efficient than option C.

Option B relies on setting up a Google Sheets-based billing dashboard for each billing account and combining them manually. This method not only consumes significant time and effort but also increases the chances of human error and data inconsistencies. Using BigQuery and Data Studio, as suggested in option C, automates the data consolidation process and eliminates these concerns.

Lastly, option D entails visiting the Cost Table page to obtain a CSV export and visualizing it using Data Studio. However, this approach does not ensure real-time data processing, leading to potential delays and inaccuracies in budget forecasting. In contrast, option C utilizes BigQuery's real-time processing capabilities, thus providing the most accurate and up-to-date cost data.

Solution to Question 8: C

The correct answer is C. One should use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource they expect to use. By utilizing the Pricing Calculator, they can efficiently estimate the total cost of running the three-tier web application on Google Cloud instances and Cloud SQL based on their specific requirements. Additionally, using similar size instances for the web server and using their current on-premises machines as a comparison for Cloud SQL ensures an accurate estimation of the required resources and costs.

Option A is not suitable because relying on a pre-existing pricing structure of a similar 3-tier web application from Google Cloud Platform Forums may not accurately represent the specific requirements and use case of the project manager's application. This could lead to inaccurate cost estimations.

Option B is not efficient nor reliable, as reading through the Google Cloud documentation and determining the cost of resources using trial and error based on the application structure could be time-consuming and still result in inaccurate estimations.

Option D is not the right choice since the Cloud Operations template focuses on monitoring, logging, and troubleshooting, which are not relevant to the task

of estimating the cost of running a three-tier web application on Google Cloud instances and Cloud SQL. Using the template may not provide a precise cost estimation for the intended purpose.

Solution to Question 9: A

The correct answer is A. Storage Admin.

Here's an explanation for why the answer should be A, and why other options will not work:

A. Storage Admin - The Storage Admin role is the most appropriate IAM role for team members managing buckets and files in Google Cloud Storage for specific projects. This role provides necessary permissions to create, modify, delete, and control access to buckets and objects within Google Cloud Storage, ensuring that team members have the proper access to manage storage resources related to their assigned projects.

B. App Engine Admin - This IAM role is not suitable for managing buckets and files in Google Cloud Storage because it is specifically designed for managing App Engine applications. App Engine Admin role has permissions to create, configure, modify, and delete App Engine applications, but it doesn't provide the required permissions for managing storage resources.

C. Pub/Sub Admin - The Pub/Sub Admin IAM role is also not appropriate for managing buckets and files in Google Cloud Storage, as it is designed for managing Google Cloud Pub/Sub resources. This role allows users to create, configure, modify, and delete Cloud Pub/Sub topics and subscriptions, which are unrelated to management and access control for storage resources.

D. Project Editor - Although Project Editor IAM role has broad permissions to modify resources across a Google Cloud project, including storage resources, it may grant more access than necessary for team members just managing storage resources. Google's recommended practices involve the principle of least privilege, which suggests granting only the required permissions to perform specific tasks. By providing the Project Editor role, you would risk giving unnecessary permissions to your team members, opening potential doors for unintended actions and security vulnerabilities.

In conclusion, according to Google-recommended practices and the principle of least privilege, you should grant the Storage Admin IAM role (Option A) to your team members in order to delegate control to them for managing buckets and files in Google Cloud Storage related to their assigned projects, while keeping the access control secure and project-specific.

Solution to Question 10: C

The correct answer should be C, "Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold," and here's why:

Option A, "Use the Cloud Monitoring dashboard to observe latency and take the necessary actions when the response latency exceeds the specified threshold," is not the best solution because it involves manual monitoring. This method doesn't provide automatic alerts or notifications to the support team, making it inefficient and likely to cause delays in addressing latency issues.

Option B, "Use Cloud Armor to monitor and alert on high latency events on your Compute Engine instances," is not the appropriate solution. Cloud Armor is primarily used for securing applications against DDoS attacks and other malicious risks, not for monitoring latency.

Option C, "Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold," is the correct course of action. It allows the support team to receive automatic notifications when latency issues arise, which helps ensure a swift response to any problems clients might be facing.

Option D, "Export Cloud Monitoring metrics to Cloud Storage and use Data Studio to create a dashboard for monitoring latency," is not a suitable option because it is an unnecessarily complex and time-consuming process. This approach also lacks automated alerting features, making it inefficient for the specific issue at hand.

Solution to Question 11: B

The correct answer is B. Deploy the monitoring pod in a DaemonSet object.

Explanation:

Option B: A DaemonSet ensures that a copy of the monitoring pod runs on each node in the GKE cluster. This option is the best solution because it guarantees that the monitoring pod is scheduled on each node, including any new nodes added by the cluster autoscaler. It provides consistent monitoring coverage for the entire cluster, as well as seamless support for scalability.

Option A: Deploying the monitoring pod as a CronJob is not suitable because CronJobs are used for running periodic tasks at specific times or intervals, not for ensuring the continuous operation of a pod on each node in a cluster.

Option C: A ConfigMap object is used to store configuration data for applications running in containers within a Kubernetes cluster. While it is useful for managing application configuration, it is not appropriate for deploying and managing the monitoring pod across all cluster nodes.

Option D: Enabling a GKE add-on for third-party monitoring integration is not relevant in this case, as the question states that a custom monitoring pod (designed to send container metrics to a third-party monitoring solution) should be used. GKE add-ons are used to extend the functionality of GKE clusters with integrated services like logging and monitoring, but they do not provide a means to deploy custom monitoring pods across all nodes.

In summary, the most suitable course of action in this situation is to deploy the monitoring pod in a DaemonSet object, ensuring that it runs on each node in the cluster and automatically scales with the addition of new nodes.

Solution to Question 12: B

The answer should be B. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

Here's why option B is the best choice and why other options won't work:

Option A: Storing the application data on a zone-local SSD and recovering the lost data from the local SSD in another zone during an outage means that the data's survival depends on the availability of the local SSDs. In the event of a zonal failure, there's no guarantee that the data will be accessible in another zone or that it won't be lost. This option doesn't ensure high availability.

Option B: Storing the application data on a regional persistent disk ensures that the data is replicated synchronously across two zones. In the event of a zonal failure, another instance can be created in the other zone, and the data from the regional persistent disk can be readily attached, making the data available for the application. This provides high availability, hence it is the most suitable option.

Option C: Although storing data on a regional persistent disk helps maintain high availability, creating snapshot schedules adds latency to the recovery process. Additionally, newer data changes occurring between snapshot intervals might be lost during recovery. This approach may not provide the optimal availability desired for mission-critical applications.

Option D: Storing the data on a zonal persistent disk and using snapshot schedules means the data will only survive in a single zone. In the event of a zonal failure, time would be lost in creating the new disk from the most recent snapshot, and data changes between snapshot intervals could be lost. This method does not ensure high availability.

In conclusion, option B is the best choice, as it maintains high availability and ensures application data access during a zonal failure.

Solution to Question 13: B

The correct answer is B: Use a custom mode VPC network, use Cloud Router Border Gateway Protocol (BGP) routes, and use active/passive routing.

Here's why:

A. Using a custom mode VPC network is correct, but configuring static routes is not the best choice when dynamic routing is required. Static routes do not handle network changes well and would require manual updates. Also, active/passive routing is appropriate for avoiding tunnel overprovisioning, but this option does not use dynamic routing as required. Hence, option A is not adequate for this case.

B. This option satisfies all the requirements. Firstly, it uses a custom mode VPC network that provides more control over IP ranges and subnet creation. Secondly, it utilizes Cloud Router BGP routes for dynamic routing - a big advantage when dealing with network changes. Lastly, it uses active/passive routing that prevents overprovisioning of tunnels during failover events and ensures higher availability.

C. Using an automatic mode VPC network is not suitable for this case since it assigns pre-defined IP ranges and does not allow for a shared address space of 10.19.0.1/22 as required. Although using Cloud Router BGP routes (for dynamic routing) and configuring policy-based routing are appropriate for certain scenarios, not having control over IP ranges makes this option unsuitable.

D. This option uses a custom mode VPC network and Cloud Router BGP routes, which are suitable for the given requirements. However, configuring VPN tunnel over Interconnect introduces a different method of connecting your VPC to remote locations and is not part of the high availability Cloud VPN solution recommended by Google. Therefore, option D is not the best choice.

In conclusion, option B meets all the requirements and follows Google's recommended practices for establishing a high availability Cloud VPN with dynamic routing, shared address space, and optimized tunnel provisioning during failover events.

Solution to Question 14: B

The correct answer is B. Enable the compute.googleapis.com API.

Explanation:

Before creating a Google Compute Engine instance, you must ensure that the necessary API (compute.googleapis.com) is enabled in the project. This is because Google Compute Engine is a component offered by Google Cloud, and in order to access and use this service, you need to enable its API in the respective project. By enabling the API, you grant your project access to the Compute Engine resources and data. Once the API is enabled, you can proceed to create the Compute Engine instance using the gcloud CLI.

Reasons why other options are not correct:

A. Create a VPC network in the project: While creating a Virtual Private Cloud (VPC) network is necessary for Compute Engine instances to communicate within the project, it is not a prerequisite step. When you create a Compute Engine instance, if a VPC is not specified, the instance will automatically be connected to the default VPC network that is created for each project. Thus, you don't need to create a VPC network before creating the instance. However, it might be needed based on your specific networking requirements.

C. Create a Cloud Storage bucket in the project: Cloud Storage buckets are used to store data objects and are not directly related to setting up a Compute Engine instance. Creating a Cloud Storage bucket is not a prerequisite for

creating a Compute Engine instance and is independent of the Compute Engine service. Moreover, Cloud Storage uses a separate API (storage.googleapis.com) from Compute Engine.

D. Create a Cloud Run service in the project: Cloud Run is a managed compute platform for deploying containerized applications. It is separate from Compute Engine and is not a prerequisite for creating a Compute Engine instance. Both services cater to different use cases; Cloud Run targets stateless containers, while Compute Engine targets virtual machines (VM) based infrastructure. Enabling the Cloud Run service does not impact the creation of a Compute Engine instance.

Solution to Question 15: D

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

Explanation: In App Engine, you can deploy multiple versions of your application and then manage the traffic distribution between them. When you encounter a bug in the newest release, you can quickly revert to the previous version by changing the traffic allocation, ensuring that your users are not affected by the buggy version. Answer D provides the quickest and most effective way to revert to the previous version.

Here's why the other options will not work:

A. This option does not exist in GCP Console. App Engine doesn't have a "Revert" button, but rather provides an easy way to route traffic to different versions of your application.

B. Deploying the original version as a separate application would be unnecessary, time-consuming, and may lead to confusion. Plus, it would require more complex traffic management. In App Engine, you can manage traffic between different versions of the same application, which is more efficient.

C. Stopping the current version and restarting the previous version will not accomplish the desired goal. App Engine doesn't have a gcloud app migrations command. Additionally, deleting the faulty version can be risky, as you may want to fix the bugs and redeploy the fixed version later. The gcloud app versions command does exist, but you'll still need to route the traffic to the previous version through the GCP Console or using the command "gcloud app services set-traffic".

Thus, the best approach is to follow option D, which ensures the prior version serves all the requests immediately after you change the traffic allocation.

Solution to Question 16: C

The correct answer is C: Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

Explanation for answer C:

In order to allow your App Engine Service to access the BigQuery dataset in a separate project managed by another department, you need to have appropriate permissions in that project. The default App Engine Service account is used to manage this access. By asking the other team to grant the BigQuery Job User role to your default App Engine Service account, you are giving your application the necessary permissions to read data from their BigQuery dataset.

Reasons why other options do not work:

A. Creating your own BigQuery dataset in your project and asking the other team to sync their data with your dataset would create a redundant and possibly inefficient synchronization process between both datasets. It is unnecessary because you can access the data directly from the original dataset by setting the proper permissions as explained in option C.

B. Requesting the other team to export their BigQuery dataset to Cloud Storage implies additional complexity and, like option A, an unnecessary data transfer process. This option would also require you to manage access to Cloud Storage. Instead, it's better to give your App Engine Service account the proper permissions to access the dataset directly, as described in option C.

D. Granting a newly created service account from the other team the role of BigQuery Data Viewer in your project would not help in this scenario. In order to access their dataset, your App Engine Service account needs permissions in the other team's project, not the other way around. Additionally, creating a new service account is not necessary when you can use the default service account that the App Engine Service is already using.

Solution to Question 17: A

The correct approach is A: Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

Here's why option A is the best choice and why the other options will not work:

A - Migrating the Flask web application to App Engine allows you to take advantage of App Engine's fully managed environment, which is designed to handle web applications with minimal configuration and operational overhead. By using Cloud Run for the backend API, you can benefit from its ability to scale seamlessly while only paying for the actual usage. Cloud Tasks is a serverless solution for task queues, and it integrates well with Cloud Run, allowing you to offload the long-running background job and ensure it operates efficiently.

B - Running the web application on a Cloud Storage bucket is not suitable for a dynamic, server-side rendered Flask application. Cloud Storage is designed for static websites and does not support server-side scripting. Additionally, using Compute Engine for the background job goes against the serverless requirement as it involves provisioning and managing VM instances, which increases operational expenses.

C - Similar to option B, using a Cloud Storage bucket for running the web application is not an appropriate solution because it is not suitable for a dynamic Flask application that requires server-side rendering.

D - Running the web application on a Cloud Storage bucket is not suitable for a Flask application, as explained in options B and C. While using App Engine for the backend API would work, it doesn't provide some of the containerization benefits that Cloud Run offers. Moreover, using Cloud Functions for the background job might lead to issues because of its maximum execution timeout (currently 9 minutes), which may not be sufficient for long-running ETL and reporting tasks.

Solution to Question 18: A

The correct option is A. gcloud deployment-manager deployments update –config

Explanation for option A: Using the 'gcloud deployment-manager deployments update' command with the '–config' flag allows you to update the specified Deployment Manager deployment using a configuration file at the path . This command enables the Deployment Manager to perform an in-place update of the resources, ensuring that no downtime is inflicted on the deployment.

Why other options will not work:

Option B: The 'gcloud deployment-manager resources create' command creates new resources as specified in the given configuration file. However, this option doesn't update the resources within the existing deployment. It will not meet the requirement of updating the deployment without causing downtime.

Option C: The 'gcloud deployment-manager deployments stop' command is used to stop an ongoing operation on a deployment. This command is not intended for updating a deployment and will not affect resources within the deployment in the manner required.

Option D: The 'gcloud deployment-manager resources delete' command deletes resources specified in the given configuration file. This option will remove resources instead of updating them and could cause downtime rather than preventing it.

Solution to Question 19: C

The correct answer is C. Enable deletion protection on the instance.

The main reason to choose C over other options is because the primary concern mentioned in the scenario is the risk of other teams inadvertently causing downtime to the shared project environment. Enabling deletion protection on the instance helps to prevent accidental deletion of the instance, thus minimizing the chances of application downtime caused by other teams.

No other options are as effective at addressing this specific scenario:

A. Restrict SSH access to the instance: While restricting SSH access is a recommended security practice and may minimize the chances of unauthorized access, it does not address the core concern of the scenario, which is the inadvertent deletion of the instance by other teams working in the common project environment.

B. Use a sole-tenant node: Sole-tenant nodes are excellent when you require dedicated hardware for specific compliance or data management needs, but they will not specifically address the issue of downtime caused by the unintended actions of the other teams working in the shared project environment.

D. Use an Instance Template: Instance templates are useful for efficiently deploying uniform groups of instances. However, they are not designed to address the key concern of protecting the instance from unintended deletion or actions by the other teams.

In summary, enabling deletion protection on the instance (Option C) is the most suitable feature as it addresses the main concern in the scenario, which is minimizing the chances of application downtime due to inadvertent actions by other teams sharing the project environment.

Solution to Question 20: C

The correct answer is C because changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 will effectively increase the number of available IP addresses within the subnet. This is because a /18 subnet has a larger address space in comparison to a /20 subnet.

Let's see why other options will not work:

A. Adding a secondary IP range 10.2.0.0/20 to the subnet would create a new pool of IP addresses, but this option would not help increase the number of primary internal IP addresses in the subnet that the virtual machines rely on.

B. Adding a secondary IP range 10.1.0.0/20 to the subnet would also create a new pool of IP addresses, but again, this would not help increase the number of primary internal IP addresses in the subnet needed for the virtual machines.

D. Enabling Private Google Access for the virtual machines would allow VM instances with private IP addresses to access Google APIs and services without an external IP address or needing to traverse the public internet. However, this would not address the problem of running out of primary internal IP addresses within the subnet.

Solution to Question 21: A

The correct answer is A. Set the minimum number of instances for your Cloud Run service to 3.

Explanation for A: In Cloud Run, instances are responsible for serving requests to your web application. By setting a minimum of 3 instances, you ensure that there are always at least three instances ready to respond to incoming requests.

According to Google's recommendations, having more than 1 instance running prevents cold starts, which cause the initial load time to be longer. Increasing the minimum number of instances to 3 ensures that the initial load time is faster and matches the subsequent load times.

Reasons why other options will not work:

B. Set the concurrency number to 1 for your Cloud Run service: Concurrency is the number of requests that can be processed simultaneously by an instance. Setting the concurrency number to 1 means that each instance can only handle one request at a time, which might not be optimal for load management and may result in slow response times during periods of high traffic. In fact, decreasing concurrency may exacerbate load times instead of mitigating them.

C. Enable autoscaling on the Cloud Run service: Autoscaling is already a default feature in Cloud Run; each service automatically scales based on the incoming traffic as long as you don't set the concurrency and minimum number of instances to 1. Enabling autoscaling can help adjust instance count during high traffic, but it does not address the issue of cold starts, which happen when there are no instances available to respond to the incoming requests.

D. Decrease the request timeout for your Cloud Run service: Decreasing request timeout limits the amount of time the Cloud Run service has to process and return a response. While this might encourage your service to respond faster, it also increases the risk of requests timing out if instances are processing slower-than-average requests. This option does not address the issue of cold starts or initial load time and may negatively impact the user experience.

Solution to Question 22: C

The correct answer is C - In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

Explanation:

C is the best option because it directly meets the requirement of integrating the company's SSO identity provider with the service providers. By setting up SSO with a third-party identity provider in Cloud Identity and having Google as a service provider, users can authenticate using the organization's SSO provider, while Google takes care of the connection with the service providers that support SAML.

A - Create a custom SAML app in GCP, and configure it to work with your company's SSO provider: This option doesn't necessarily help in connecting with the service providers directly. It just creates a custom SAML application in GCP that works with the company's SSO provider but doesn't mention how it will be integrated with the existing service providers who support SAML.

B - In Cloud Identity, set up SSO with a third-party identity provider with Google as a service consumer: This option doesn't take advantage of Google's infrastructure to connect with service providers that support SAML. It's an

indirect solution as Google would act as a service consumer and not as a service provider, so it doesn't align with the company's goal of authenticating users with service providers by using the organization's SSO provider.

D - In Cloud Identity, set up SSO with Google as an identity provider to access custom SAML apps: This option doesn't work because it makes Google the identity provider, which is not the goal of the company. The company already has an SSO identity provider that supports SAML and wants to integrate with service providers, so using Google as an identity provider would not be appropriate in this situation.

Solution to Question 23: C

The correct answer is C because using Compute Engine with preemptible VM instances of appropriate standard machine types is the most cost-effective solution for running nightly batch processing jobs.

Option A is incorrect because although Cloud Functions can be used for short tasks and event-driven functions, using them with the maximum memory allocation for lengthy batch processing jobs is not the best solution to minimize cost. Additionally, Cloud Functions have a maximum execution timeout, which may not be sufficient for a 2-hour batch processing job.

Option B is incorrect because although App Engine standard environment with manual scaling gives you fine-grained control over the instances, it is not the most cost-effective solution for batch processing jobs that run during a specific time period. Also, you would need to manually adjust the number of instances to meet demand, which could lead to underutilization or overprovisioning of resources.

Option D is incorrect because App Engine's flexible environment with automatic scaling is more suitable for handling variable user loads and web applications. The cost for the resources used in the flexible environment is generated on a per-minute basis, which may increase the overall service cost for a 2-hour long nightly batch processing job.

By selecting the Compute Engine and using preemptible VM instances (option C), you are able to minimize the service cost because these instances are short-lived and up to 80% cheaper than regular instances. This is an appropriate choice for batch processing jobs that can tolerate possible interruptions since preemptible instances can be terminated with a short notice. You can also select an appropriate standard machine type that provides the proper balance between performance and cost.

Solution to Question 24: B

The correct answer is B. Enable node auto-provisioning on the GKE cluster. Here's the explanation for why this is the right answer and why the other options will not work:

B. Enabling node auto-provisioning on the GKE cluster will ensure that your cluster automatically manages the number of nodes and their associated GPUs in the most efficient way possible. Node auto-provisioning allows GKE to create or delete node pools based on the requirements of the workloads running on the cluster. This feature helps in avoiding underutilized or overprovisioned resources, leading to cost optimization. The data scientists can create GPU-intensive workloads, and GKE will take care of providing requisite resources without manual intervention, thus minimizing costs while meeting their requirements.

Now, let's consider why the other options are not suitable:

A. Using Compute Engine instances with GPUs for the data scientists' workloads involves manual management of resources. The unnecessary overhead of manually managing the instances would increase costs and create room for errors, such as failing to turn off idle instances. Moreover, data scientists might not be able to access the GPU resources as quickly, leading to delays in their projects.

C. Creating a node pool with regular VMs and GPUs attached to those VMs might seem like a good solution, but it does not necessarily minimize costs. With a fixed node pool, you may end up with underutilized or overprovisioned resources, leading to higher costs and resource inefficiencies compared to using auto-provisioning.

D. Creating a VerticalPodAutoscaler (VPA) for those workloads would not really help in minimizing costs related to GPUs as it adjusts the resources (CPU and memory) allocated to a pod based on its utilization, rather than the nodes in the GKE cluster. VPA does not address the efficient provisioning of GPU resources, making it unsuitable for the specific needs of the data scientists in this scenario.

Solution to Question 25: A

The correct answer should be A. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server. This is because the application needs to reach the licensing server on IP 10.0.3.21 without changing its configuration. By reserving the specified IP address as a static internal IP and assigning it to the licensing server, you will ensure that the application can communicate with the licensing server as required.

Option B is incorrect because creating a load balancer with the backend pointing to the licensing server and using the IP 10.0.3.21 as the frontend IP address will not help since the application is specifically looking for the licensing server on IP 10.0.3.21. Load balancers are used for distributing network traffic and are not suitable for this use case.

Option C is incorrect because reserving the IP 10.0.3.21 as a static public IP address using gcloud and assigning it to the licensing server will not work as the application is looking for an internal IP address, not a public one. Public

IP addresses are designed for external access, while internal IPs are meant for communication within the private network.

Option D is incorrect because creating a custom routing rule to route traffic destined for 10.0.3.21 to the licensing server's actual IP address is not advisable. This would require modifying the routing tables, which can be complex and can lead to undesired consequences if not properly managed. Moreover, it would not directly fulfill the requirement of ensuring that the application can reach the licensing server without any configuration changes.

Therefore, the best solution is to reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server. This will enable the application to communicate with the licensing server as required without making any configuration changes to the application itself.

Solution to Question 26: C

The correct answer is C. Develop templates for the environment using Cloud Deployment Manager.

Here's why each answer is correct or incorrect:

A. Using curl in a terminal to send a REST request to the relevant Google API for each individual resource would be inefficient and not a best practice. This method does not scale well as the environment grows and becomes more complex. It would also require keeping track of resource management configurations and status outside of any version-controlled system, making it harder to maintain and extend.

B. Google Cloud Run is a service designed for containerized applications. It is not meant for streamlining and standardizing the creation and management of multiple Google Cloud resources. Cloud Run focuses on executing stateless containers in response to events, like HTTP requests, and not on helping maintain infrastructure resources.

C. Developing templates for the environment using Cloud Deployment Manager is the best approach. Cloud Deployment Manager is a Google Cloud service designed specifically for creating, managing, and updating cloud resources using declarative templates. Reusability and consistency can be achieved through this method as a template can be applied to many different projects, reducing repetitive code and keeping everything centralized in version control. This helps in managing the environment efficiently and ensures standardization.

D. Writing custom Python code using the Google Cloud SDK is not the most efficient approach. Although this method allows for more flexibility in resource management, it also adds unnecessary complexity, which increases development time and maintenance costs. It lacks the simplicity, reusability, and consistency that IAC (Infrastructure as Code) provides through Cloud Deployment Manager templates, which makes it an inferior choice for streamlining and standardizing the creation and management of multiple Google Cloud resources.

Solution to Question 27: B

The correct answer is B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

Option B is the best choice because when a pod is stuck in a Pending status, it usually indicates that there is an issue in the configuration or resource allocation for that specific pod. Reviewing the details of the pod with its warning messages will help identify the source of the problem and provide information for necessary adjustments.

Option A is not suitable since the Google Kubernetes Engine dashboard might not give detailed information about the exact pod(s) in question, while the issue here is with the specific pod "myapp-deployment-58ddbbb995-lp86m."

Option C is not suitable since a container's logs are primarily aimed to provide information about the running application rather than the status of the pod or its deployment. Since the pod is still in Pending status, the container inside the pod may not have started yet. Thus, viewing logs at this stage may not provide helpful information regarding the cause of the Pending status.

Option D is not suitable since it suggests viewing logs of the "myapp-service" Service object. The issue here is not with the service itself but with the pod's Pending status. The pod is not yet scheduled for executing, so checking logs of the service object would not give relevant insights about the current problem.

Solution to Question 28: D

Answer: D.

Explanation: To enhance security in the given scenario, you should create separate service accounts for the application servers (sa-app) and the database servers (sa-db). This ensures proper isolation and prevents unauthorized access between the two subnets.

Option D provides the most suitable approach for achieving this configuration. By associating the service account sa-app with the application servers and the service account sa-db with the database servers, you maintain a clear separation of their roles and responsibilities. Then, you can create an ingress firewall rule that allows network traffic from the source service account sa-app to the target service account sa-db, effectively permitting only legitimate database traffic from the application servers to the database servers.

Option A is incorrect because it involves creating network tags instead of service accounts. While network tags can be used to facilitate communication between instances, they do not provide the same level of security and access management as service accounts.

Option B fails to provide the desired security as it only associates a service account (sa-app) with the database servers, and a network tag (db-server) with the

application servers. This does not define proper permissions for the application servers and may leave the environment vulnerable.

Option C is not the best choice because it allows network traffic from source VPC IP addresses instead of specifying the source service account (sa-app). This configuration could potentially allow any IP address within the VPC to access the database servers in subnet-a, reducing the overall security of the system.

In summary, option D is the most appropriate and secure course of action to achieve the desired configuration as it uses service accounts to segregate the roles, and sets up an ingress firewall rule allowing only the application servers to access the database servers.

Solution to Question 29: D

The correct answer is D. Cold Storage, also known as Google Cloud Storage Nearline, because it is a cost-effective storage solution for data that is accessed infrequently, such as the data warehouse in this scenario.

Option A, Regional Storage, is not the most cost-efficient choice for this situation as it is designed for storing data that remains within a specific region only. This storage class provides lower latency and higher throughput as compared to Cold Storage, but it also incurs higher costs. Since the company needs to access the data only quarterly, it doesn't require low-latency storage.

Option B, Multi-Regional Storage, is also not the most cost-efficient choice. It is designed for storing data that needs to be accessed frequently and within multiple regions. This storage class provides high availability and low latency, but it also has higher costs. Multi-Regional Storage would be overkill for the company's quarterly access needs.

Option C, Firestore, is a NoSQL document database designed for real-time data synchronization and scalable infrastructure for web and mobile applications. Firestore is not an optimal solution for large-scale archival storage, and it is typically more expensive compared to Cold Storage when used for infrequently accessed data, like in this scenario.

In conclusion, Option D, Cold Storage, is the most cost-effective solution for this financial company's requirements, as it is specifically designed for infrequently accessed data, and it provides significant savings when compared to other storage options.

Solution to Question 30: B

The correct answer should be B. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

Explanation: Service Accounts help manage resources and permissions in Google Cloud Platform. In order to verify the creation of a service account, you need to focus on the logs related to service accounts and their configurations. The

Activity log provides you with information about the actions performed on resources in your project. By filtering the Activity log to view the Configuration category, you will be able to see logs related to the setup and management of resources. To look specifically for service accounts, you need to further filter by Resource type to Service Account. This will provide you with the necessary information to determine when a service account was created.

Here's why the other options do not work:

Option A: Filtering the Resource type to BigQuery will only show you logs related to BigQuery services and configurations and does not yield any information on service accounts.

Option C: Filtering the Resource type to Google Project will provide you with logs related to overall project configuration, but it will not specifically display service account-related information.

Option D: Filtering the Audit logs for the Configuration category and Compute Engine as Resource type will give you logs about Compute Engine resources and not service accounts.

Solution to Question 31: B

The correct answer is B because it provides a seamless and efficient way to establish a connection between the GKE application in one VPC and the Compute Engine instance in another VPC. Here's why each step in option B is important:

1. Creating a Service of type LoadBalancer in GKE automatically provisions and configures an internal TCP/UDP load balancer that distributes traffic to the application's Pods.
2. Adding the annotation "cloud.google.com/load-balancer-type: Internal" ensures that the load balancer created is an internal load balancer, confined to the scope of your VPC network.
3. Peering the two VPCs together allows the Compute Engine instance to reach the load balancer's internal IP address, even though it is in a different VPC.
4. Configuring the Compute Engine instance to use the address of the created load balancer enables connectivity to the GKE application.

The reasons why other options will not work:

Option A: Creating a Service of type ExternalName in GKE does not create a load balancer or reserve an IP address. ExternalName services simply provide a way to map a service to an external DNS name. While VPC peering is a good idea to enable connectivity between the two VPCs, using an ExternalName service does not provide the required connectivity to the GKE application.

Option C: While creating a LoadBalancer Service will create a load balancer, using a custom annotation does not provide a way to specify the VPC or access scope, and therefore will not enable the required connectivity. You need the specific "cloud.google.com/load-balancer-type: Internal" annotation to ensure

an internal load balancer, and peering the VPCs together is still needed for access between the VPCs.

Option D: Creating a LoadBalancer Service is a good start, but configuring a VPN between the two VPCs requires additional effort compared to VPC peering. Additionally, creating a VPN still exposes the GKE application publicly accessible through the internet-facing load balancer, which is not an ideal solution when the Compute Engine instance is in the same region and only needs internal access to the GKE application.

Solution to Question 32: A

The correct answer is A because it offers the most efficient and reliable solution for the given use case, which is to create a fully managed, serverless compute solution that automatically processes incoming files in the Cloud Storage bucket using the Google Speech-to-Text API.

A. Creating a Cloud Function triggered by Cloud Storage bucket events allows you to submit the file URI directly to the Google Speech-to-Text API as soon as a new file is uploaded. This solution is fully managed and serverless, so you don't need to worry about provisioning infrastructure or maintaining the underlying systems. It also provides authentication and is in line with Google-recommended practices, ensuring that the solution is secure without any additional effort required.

B. Configuring a Cloud Pub/Sub subscription to listen for events from the Cloud Storage bucket seems like an appropriate solution at first, but it will not work effectively because Cloud Pub/Sub handles general-purpose messaging and orchestration, not file processing. It also adds complexity and latency to the process as you have to manage and coordinate both the subscription and its associated code, instead of directly utilizing the Speech-to-Text API.

C. Deploying a Cloud Shell script on a regular schedule to scan the bucket for incoming files adds unnecessary overhead and complexity to the solution. It also makes the service less responsive, as it depends on a fixed time interval to process incoming files. In contrast, a Cloud Function that automatically triggers upon file arrival allows for immediate processing and is fully managed, aligning better with the requirements.

D. Running a Kubernetes job to scan the Cloud Storage bucket regularly for new files is not the optimal solution because it requires potentially unnecessary maintenance and management of a Kubernetes cluster. It also involves regularly scanning the bucket, adding latency to the process, and doesn't follow the requirements of a fully managed and serverless solution. The Cloud Function in option A provides a more efficient, responsive, and simpler setup compared to this approach.

Solution to Question 33: A

The correct answer is A: Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, and

BigQuery.

Here's why each component of option A is the right choice:

1. Cloud Pub/Sub: This is a messaging service that allows you to send and receive real-time data from various sources. In our case, it's the perfect choice to ingest the time-series data from different sources asynchronously.
2. Cloud Dataflow: This service is designed to process, transform, and analyze data using parallel processing. When dealing with time-series data, extracting relevant information and performing computations is crucial. Cloud Dataflow can handle these tasks efficiently and at scale, which is paramount for real-time data.
3. Cloud Bigtable: Time-series data is typically high volume and requires high write and read performance. Cloud Bigtable is a NoSQL database that provides low-latency and high-throughput, making it the perfect choice for managing such data. It is especially suitable for time-series data storage as it supports a wide column store that can efficiently handle the data's dynamic nature.
4. BigQuery: This is a fully managed data warehouse designed for analyzing large datasets and generating actionable insights. In the context of predicting market trends, real-time data analysis is essential. BigQuery's ability to run ad-hoc queries and handle large-scale analytics makes it the right choice for the last step of the pipeline.

Here's why the other options will not work:

Option B: Cloud Spanner is used for handling transactional data in a relational database. It is not suitable for time-series data, which is better managed using wide column stores like Cloud Bigtable.

Option C: Cloud Datastore is a NoSQL database service designed for web and mobile applications, mostly focusing on key-value storage. In comparison, Cloud Bigtable has specific optimizations to efficiently handle time-series data.

Option D: Cloud Dataproc is a managed Apache Hadoop and Apache Spark service for batch processing, while our requirement is for real-time processing achieved by Cloud Dataflow. Additionally, Cloud Storage is an object storage service that wouldn't provide the real-time querying and performance needed for time-series data like Cloud Bigtable does.

Solution to Question 34: C

The correct strategy to optimize the isolation between customers' pods is option C, which involves creating a GKE node pool with a sandbox type configured to gvisor and adding the runtimeClassName: gvisor parameter to the specification of the customers' Pods. This approach provides strong isolation for each customer, as gvisor is a container runtime that runs containers inside a lightweight, fully-virtualized environment using kernel and user-space isolation.

This makes it more difficult for one customer's pod to affect another, even if they run arbitrary code.

Option A, using the cos_containerd image and adding a nodeSelector, is not the best strategy for optimizing isolation between customers' pods. Though cos_containerd is a secure container-optimized operating system, it doesn't provide the necessary isolation between multiple customers running arbitrary code in the same cluster.

Option B, creating a separate GKE cluster for each customer, is an inefficient and costly solution. GKE clusters are designed for managing multi-tenant workloads, and scaling to such an extent would lead to significant resource and management overhead.

Option D, using Binary Authorization and whitelisting only the container images, is not an effective method in this scenario. Although Binary Authorization can help improve the security of your CI/CD process, it doesn't provide the isolation required between multiple customers' pods running arbitrary code within the same cluster.

Solution to Question 35: C

The recommended course of action is option C: Create a custom Compute Engine image from a snapshot. Create your instances from that image.

Here's why option C is the correct answer and why the other options will not work:

Option A: Create a Compute Engine managed instance group from your base VM. Create your instances from that instance group.

While creating a managed instance group can be useful for scaling and controlling multiple VMs, to prepare for the increased application traffic, it is still necessary to create a custom Compute Engine image from a snapshot in order to have a consistent disk state across all instances. This option doesn't involve image creation and, therefore, may result in inconsistent configurations in newly created instances.

Option B: Create a Google Kubernetes Engine cluster from your base VM. Create your instances from that cluster.

Google Kubernetes Engine (GKE) is a service mainly used for container orchestration and management, whereas the question is focused on creating a copy of a custom Compute Engine VM. While GKE can scale and manage workloads, it requires a different infrastructure design revolving around containers, making it inadequate for the given problem.

Option C: Create a custom Compute Engine image from a snapshot. Create your instances from that image.

This is the recommended course of action because it involves creating a custom Compute Engine image from a snapshot of the existing VM. That way, you can

ensure consistent disk states across all instances, which is essential for maintaining uniformity within a scaled environment, especially during an anticipated increase in application traffic.

Option D: Create a custom Compute Engine image from a snapshot. Create your instances from a Cloud Storage bucket.

Creating a custom Compute Engine image from a snapshot is a good idea; however, using a Cloud Storage bucket to create instances is not the correct approach. This option would involve storing the image data in the Cloud Storage bucket and then creating instances with that data, which is unnecessarily complex and less efficient. Option C is a more straightforward and effective solution since it does not involve the additional step of interacting with a Cloud Storage bucket.

Solution to Question 36: C

The correct answer is C: Change the billing account of your projects to the billing account of your company.

Explanation: Since the company wants to simplify the billing process by charging project costs directly to their corporate account, the best course of action is to change the billing account associated with your projects. This will allow Google Cloud to charge the company's account directly, making it easier for the finance team to manage and pay for the cloud usage.

Reasons why other options are not the correct choices:

A. Setting up a BigQuery billing export and granting financial department IAM access to query the data is not the optimal solution because it doesn't change the billing account used for the projects. While this option allows the finance team to view and analyze the billing data, it would not charge the company's corporate account directly.

B. Exporting your project billing information to a spreadsheet and sharing it with your financial team would not change the billing account associated with your projects. This option only shares the billing information with the finance team and not the responsibility of paying the bill directly to the company's corporate account.

D. Using Google Cloud Pub/Sub to send billing notifications to your finance team is also not the best solution, as it only alerts the financial department to billing changes or updates. This option does not change the actual billing account to the company's corporate account.

In summary, by changing the billing account of your projects to the billing account of your company (Option C), you will be able to implement the change desired by the company and create a simplified billing process where the costs will be charged directly to their corporate account.

Solution to Question 37: D

The correct course of action is D. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

Here's why the other options don't work:

Option A: Create a custom role with Compute Admin permissions and grant all members of the DevOps team the custom role on the production project. This option is not the best because it only grants Compute Admin permissions. This may not be sufficient for the DevOps team, as they may require other permissions to access different Google Cloud services used by the company. Additionally, this might inadvertently expand their permissions in the future if new services are introduced.

Option B: Create a service account with required permissions and provide the DevOps team with the credentials. This option is not recommended because sharing service account credentials among team members is a security risk. Service accounts are intended for non-human, service-to-service communication rather than for direct use by the DevOps team.

Option C: Grant all members of the DevOps team the role of Project Owner on the organization level. This option is not ideal because it would give the DevOps team broad and potentially excessive access to every project in the organization, which might be unnecessary for their tasks. It could also lead to an increase in accidental privilege escalation in the future, as Google Cloud product changes might grant additional permissions to the project owner role.

Option D is the best choice because it allows you to create a custom role tailored for the DevOps team's requirements and prevent inadvertent expansion of their permissions in the future. By implementing a custom role, you can control which Google Cloud services the DevOps team can access and ensure they have the proper permissions for smooth operations while adhering to Google's recommended best practices.

Solution to Question 38: C

The correct answer is C: Use kubectl to delete the topic resource.

Explanation:

As a software engineer handling Google Cloud infrastructure, you need to use Kubernetes-native declarative management using Config Connector. When it comes to the task of permanently deleting a Google Cloud Pub/Sub topic managed by Config Connector, you should use the appropriate action to achieve the desired outcome (permanent deletion).

A. Using kubectl to rename the topic resource would not accomplish the desired task, as it only changes the name of the topic and does not lead to the deletion of the topic.

B. Creating the label "deleted-by-cnrm" and setting its value to "true" is not

a valid approach either. Config Connector does not use this label to determine if a resource should be deleted. This action would only add the label to the resource without deleting the topic.

C. By using kubectl to delete the topic resource, you are leveraging Config Connector's ability to manage Google Cloud resources by using Kubernetes-native declarative management. Therefore, deleting the Kubernetes resource using kubectl will also delete the corresponding Google Cloud resource, in this case, the Pub/Sub topic. This is the appropriate action to take.

D. Updating the topic label "deleted-by-cnrm" to "true" would not accomplish the desired goal, as Config Connector does not use this label to determine if a resource should be deleted. This action would only update the label on the resource without actually deleting the topic.

In summary, to permanently delete a Pub/Sub topic managed by Config Connector in the company's Google Cloud project, you should opt for Option C: Use kubectl to delete the topic resource, as it directly deletes the Kubernetes resource and its corresponding Google Cloud resource. The other options would not accomplish the desired goal of deleting the topic.

Solution to Question 39: B

The correct answer is B. Grant the service account the IAM Role of Compute Storage Admin in the project called proj-vm.

Explanation: In this scenario, the requirement is to use a service account from the proj-sa project to take snapshots of VMs running in another project called proj-vm. To achieve this task, the service account needs to have the necessary permissions in the proj-vm project.

Option B is correct because granting the service account the IAM Role of Compute Storage Admin in the proj-vm project will provide the required permissions to manage snapshots and disks in the Google Cloud project. Compute Storage Admin is a pre-defined role that allows managing the Persistent Disk resources, which includes creating, deleting, and managing snapshots.

Option A is incorrect because setting the service account's API scope for Compute Engine to read/write when creating the VMs has no influence on taking snapshots. API scopes are used to control access to the APIs used by the VMs themselves and are not related to cross-project permissions.

Option C is incorrect because granting the service account the IAM Role of Project Viewer in the project called proj-vm provides read-only access to view the resources but does not grant the necessary permissions to manage snapshots.

Option D is incorrect because granting the service account the IAM Role of Compute Instance Admin in the project called proj-vm allows the user to manage virtual machine instances, but not manage the snapshots for those virtual machine instances.

To summarize, the correct answer is option B, as it provides the necessary permissions for the service account to take snapshots of VMs in the proj-vm project.

Solution to Question 40: C

The correct answer is C: Set Content-Type metadata to application/pdf on the PDF file objects.

Explanation: By setting the Content-Type metadata to application/pdf for the PDF objects stored in the Cloud Storage bucket, you are explicitly instructing web browsers to treat those files as PDF documents when downloading or streaming. Consequently, web browsers like Google Chrome, Mozilla Firefox, or Microsoft Edge will display the PDF files directly within the browser when accessed through the static website, instead of prompting users to save the file locally.

Reasons why other options will not work: A. Enable object versioning for the bucket containing PDF files - Object versioning is a Cloud Storage functionality that keeps a history of revisions made to an object in the bucket. However, it does not modify the behavior of browser downloads or affect how files are displayed in the browser.

B. Use Firebase Hosting instead of Cloud Storage for the static website - Firebase Hosting is tailored towards hosting web applications and not just static content. While it could be used to host the website, migrating to Firebase Hosting would not inherently change the behavior of PDF files when accessed through the links. The core issue of PDF files prompting users to save them would remain, as this behavior is determined by the Content-Type metadata, not the hosting solution.

D. Create a custom role with permissions to view the PDF files in-browser - Creating a custom role with specific permissions might be beneficial when determining whether users can access the files or not, but it does not address the issue of PDF files prompting users to save them locally. The desired behavior of displaying the PDF directly in the browser depends on the correct Content-Type metadata rather than the users' permission roles.

Solution to Question 41: B

The correct answer is B: Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from the Cloud Marketplace. Here's the explanation for why it's the best choice and why other options are not recommended:

A. Use Cloud Build to build a Docker image of the CMS, then deploy the solution to Google Cloud Run. This option is less efficient compared to B because it requires you to manually build a Docker image and deploy it to Cloud Run. This process can be time-consuming and you may not be leveraging optimizations and integrations available via the Cloud Marketplace.

B. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace. (Correct) This is the recommended approach because it is the most efficient and streamlined method for deploying a CMS on Google Cloud. Google Cloud Marketplace offers numerous pre-configured solutions that can be deployed directly onto the platform, often with just a few clicks. These solutions come with optimizations and best practices for the Google Cloud environment. Deploying the CMS directly from the Cloud Marketplace saves time, reduces manual configuration, and ensures a stable, optimized environment.

C. Deploy the CMS solution using Kubernetes Engine and manually configure the solution using the YAML files. This option is not recommended because it requires a higher level of expertise and manual configuration effort. While Kubernetes Engine can be a valid choice for deploying a CMS, the manual configuration process can be time-consuming and prone to errors. Additionally, you might not be taking full advantage of available optimizations if you are not using a pre-configured solution from the Cloud Marketplace.

D. Manually install the CMS on a new App Engine standard environment instance. This option is not recommended because it requires unnecessary effort and may not fully utilize the capabilities of App Engine. Manually installing a CMS solution onto an App Engine instance can be a time-consuming process, and it doesn't leverage the full range of features and optimizations that come with deploying from the Cloud Marketplace.

In conclusion, deploying a pre-built CMS solution from the Google Cloud Marketplace (Option B) provides the most efficient and optimized way to install and deploy the required content management system on Google Cloud.

Solution to Question 42: C

The best option is C, adding a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage. Here's why:

Option A (archiving data from multi-regional storage to Coldline Storage) does not meet requirements because Coldline Storage is intended for infrequent access, typically only once or twice a year. Since you need to access the archived data once a month for reporting purposes, this is not suitable.

Option B (archiving data from regional storage to Nearline Storage) does not meet requirements because it does not take into account the need to store multiple versions of the data. As a data analyst, you need to ensure you can access the different versions of the data and this option doesn't cater to that requirement.

Option C (archiving data with newer versions to Nearline Storage) meets all requirements. It allows you to manage multiple versions of the data, accessing the archived data once a month which suits Nearline Storage's purpose (it is designed to be accessed approximately once per month) and provides a cost-effective solution compared to the other storage classes. Additionally, occasional updates to the archived data at the end of each month can be managed.

Option D (archiving data from regional storage to Coldline Storage) has the same issue as Option A – Coldline Storage is not suitable for monthly access, it is designed for very infrequent access (once or twice a year).

In summary, Option C best meets the requirements for setting up a cost-effective archiving solution while managing versioning and providing access to previous versions once a month for reporting.

Solution to Question 43: B

The correct answer is B, as it ensures that the data science team members can perform essential queries while adhering to the Google-recommended best practices.

Option B suggests creating a dedicated Google group in Cloud Identity and adding each data scientist's user account to this group. By assigning the BigQuery jobUser role to the group, the data scientists will have the necessary permissions to run queries and jobs, while limiting their permissions to solely performing these essential tasks as suggested in the question.

Here's why the other options will not work:

Option A: Assigning the BigQuery machineLearningAdmin user role to the group would provide the data scientists with administrative privileges for machine learning resources within the BigQuery. However, it won't grant them the required permissions to perform essential queries, which is the primary function needed.

Option C: Assigning the BigQuery admin user role to the group would give the data scientists full control over BigQuery resources, including the ability to manage datasets and tables, and even delete them. This level of access goes beyond the requirements of the question and may pose a security risk, as it is not considered a recommended best practice by Google.

Option D: Assigning the BigQuery dataEditor user role to the group would grant the data scientists the permission to edit and delete datasets and tables. While they would be able to perform essential queries with this role, it again provides excessive permissions and goes beyond the scope of the question. Additionally, this is not a Google-recommended best practice.

Therefore, option B is the most suitable approach for ensuring the data scientists can perform essential queries while adhering to Google-recommended best practices when using Google Cloud Platform and BigQuery for data warehousing.

Solution to Question 44: B

The correct answer is B, and here is why:

Option B is the appropriate course of action because deploying a new version of your application in App Engine and then using GCP Console to split traffic between the current version and the newly deployed version is a standard

practice when needing to test new versions with a portion of users. This allows you to control the percentage of user traffic that reaches the new version of the application and provides data on how the new version is performing before rolling it out to all users.

Option A is not a good choice because deploying a new version of your application in a Compute Engine instance instead of App Engine would require additional work to manage, configure, and scale the infrastructure. Moreover, performance and resource usage may differ between the two, leading to inaccurate testing results.

Option C is not suitable because Cloud Pub/Sub is a messaging service used for asynchronous messaging between independent systems, not for distributing application traffic between different versions of a web application. So, even though Cloud Pub/Sub is a useful service, it does not serve our purpose here.

Option D is also incorrect because creating a separate project for the new version within App Engine would cause unnecessary complexity and cost implications with multiple projects. Furthermore, it would not be efficient to split traffic between projects for this purpose, as you can manage multiple versions and traffic splitting within a single project in App Engine itself.

Thus, the best course of action to achieve the task is Option B: Deploy a new version of your application in App Engine and use GCP Console's App Engine settings to split traffic between the current and newly deployed versions accordingly.

Solution to Question 45: C

The correct answer is C. Here's why:

A. Applying for Google Cloud Startup credits and distributing them among the engineering team may provide some short-term financial assistance for the engineers, but it is not an efficient or sustainable way of managing project billing. The credits allocated through the startup program are limited and may expire, requiring engineers to find alternative means of payment once the credits run out.

B. Setting up a shared Google Cloud account with pre-purchased credits for all engineers to use for project creation may seem like a practical solution at first glance, but it is not the most efficient approach. This method would require engineers to share login credentials and could make it difficult to maintain control over the account or accurately attribute project costs to individual team members.

C. Creating a Billing account, associating a payment method with it, and providing all project creators with permission to associate that billing account with their projects is the most efficient approach to achieve the goal. This method allows engineers to create projects without needing their personal credit card

details, while maintaining the autonomy of their individual Google Cloud accounts. Moreover, it simplifies the process of tracking costs and expenses, as all the projects are consolidated under a single billing account that can be managed centrally.

D. Creating a billing account and associating it with a monthly purchase order (PO) would not directly solve the problem as it does not provide an easy way for the engineers to create new projects without requiring their personal credit card info. While it may help with the company's financial management, it does not address the primary concern outlined in the question.

Solution to Question 46: D

The correct answer is D. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

Here's why other options will not work:

Option A: This option suggests using Google Cloud Storage FUSE to serve static content from the compute instances. However, this method is not optimal for serving web content to users and could impact performance. FUSE introduces additional latency and unnecessary overhead compared to serving content directly from Cloud Storage.

Option B: In this case, an external HTTP(S) load balancer with a managed SSL certificate for the backend service is a good option. However, adding Cloud Pub/Sub integration for distributing requests for static content is unnecessary and over-complicated. A URL map is a more efficient way to route traffic for static content to Cloud Storage backend.

Option C: The external HTTP(S) load balancer for distributing the load and a URL map for targeting the static content is a good choice. However, installing HTTP certificates on individual instances instead of using managed SSL certificates is not efficient. With managed SSL certificates, you can have automated provisioning, renewal, and management of certificates, which is much more convenient and secure.

Option D is the best choice, as it combines the advantages of the external HTTP(S) load balancer, managed SSL certificate for secure connection, and URL map to efficiently route static content requests to Cloud Storage backend. This setup ensures the optimal performance of the site and ensures a secure connection for the users.

Solution to Question 47: D

The correct answer is D. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

Here's the explanation for why D is the correct answer and why other options don't work:

Option D: Creating a new node pool and specifying the machine type as n2-highmem-16 will allow you to deploy the new pods on the desired nodes without causing any downtime in your existing application. GKE supports the use of multiple node pools within a single cluster, and Kubernetes will automatically schedule the new pods on the appropriate nodes. This method allows for seamless deployments and management.

Option A: While creating a new cluster with both n1-standard-2 and n2-highmem-16 nodes is possible, it would involve redeploying the existing application pods and deleting the old cluster. This could cause downtime, and it is unnecessary because you can employ multiple node pools in a cluster as explained in option D.

Option B: Creating a new cluster with only n2-highmem-16 nodes and redeploying the pods would be inefficient because it would require the movement of the existing application to the new cluster, which could cause downtime and increased costs. Also, having separate clusters for different types of nodes would generally have higher management overhead.

Option C: Using gcloud container clusters set-machine-type to change the node type to n2-highmem-16 is not a viable option. The command is used to change the properties of GKE clusters, not individual nodes or node pools. Additionally, doing this would require you to delete and recreate the nodes, causing potential downtime in the application.

In summary, option D is the best choice because it allows you to deploy the additional pods on the needed n2-highmem-16 nodes without impacting the existing application running on n1-standard-2 nodes and avoids any downtime.

Solution to Question 48: D

The most appropriate course of action to achieve the requirement of maintaining a month-end copy of the database for auditing purposes over a period of three years would be option D: Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

Option A is not ideal because it relies on automatic backups, which might not always fall on the exact first day of the month. This could result in missing the exact month-end copy required for auditing purposes. In addition, backups are not specifically designed for long-term archival storage.

Option B is better than option A as it involves setting up an on-demand backup. However, backups are still not designed explicitly for long-term archival storage. Instead, the primary purpose of backups is for disaster recovery.

Option C has a better approach to long-term storage by converting the automatic backup to an export file, but it writes to a Coldline class Cloud Storage bucket. Although Coldline storage is suitable for long-term storage, it is more expensive than Archive storage and offers slightly faster retrieval times. Since

the requirement is primarily for auditing purposes and not frequent access, the increased cost and speed of Coldline storage are unnecessary.

Option D is the best approach for a few reasons. First, it involves setting up an export job, which is designed explicitly to store and manage database exports. Second, it writes the export file to an Archive class Cloud Storage bucket, which is the most cost-effective storage class for long-term storage of infrequently accessed data, such as the month-end copies required for auditing purposes in this scenario. Thus, option D satisfies both the time-based and storage requirements in the most efficient and cost-effective manner.

Solution to Question 49: C

The correct answer is C: Automatic Scaling with min_idle_instances set to 3.

An explanation for why option C is the correct answer:

Automatic Scaling is the best choice in this scenario because it allows the number of instances to scale according to the request rate, which is a requirement specified by the client. Additionally, by setting the min_idle_instances property to 3, you are ensuring that there will always be at least 3 unoccupied instances available to handle incoming requests, as required by the client.

Reasons why the other options will not work:

A. Basic Scaling with target_cpu_utilization set to 3: Basic Scaling is not ideal for this situation because it scales the number of instances based on their CPU utilization, rather than the request rate. Additionally, setting the target_cpu_utilization to 3 will not guarantee that there will always be at least 3 unoccupied instances available.

B. Basic Scaling with max_instances set to 3: This option is not suitable for two reasons. Firstly, Basic Scaling does not fully fulfill the client's requirement to scale according to the request rate. Secondly, setting the max_instances property to 3 will limit the number of instances to 3, which contradicts the client's need for 3 unoccupied instances to always be available in addition to those handling requests.

D. Manual Scaling with 1 instance: Manual Scaling does not align with the client's requirement for the number of instances to scale according to the request rate. Moreover, setting the number of instances to 1 does not meet the requirement to always have at least 3 unoccupied instances available.

Solution to Question 50: B

The correct answer is B because it allows for efficient exploration and analysis of log content from multiple Google Cloud Platform projects while following Google's best practices. When you create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset, you are centralizing all logs from different GCP projects in one place. Configuring the table expiration to 60 days

ensures that you have access to all logs from the past two months, which meets the requirement specified in the question.

Option A is not ideal because, although it exports the logs to Cloud Storage and satisfies the 60-day retention period, it does not support efficient exploration and analysis of the logs as required. Log data in Cloud Storage is not as easily queryable as it is in BigQuery.

Option C is not suitable because streaming logs directly to BigQuery through Stackdriver Logging Sink would not be as efficient in handling combined logs across multiple projects as creating a Logging Export with a Sink destination. Additionally, using Dataflow to parse and process logs in real-time may result in processing overhead and latency, which is not necessary for a simple log analysis scenario.

Option D is incorrect because exporting logs to Cloud SQL using Stackdriver Logging Viewer is not in line with Google's best practices for obtaining combined logs across multiple projects. Cloud SQL is a relational database service, which is not designed for efficient handling of large-scale log data. Additionally, using Cloud SQL for log analysis might not be as cost-effective and scalable as BigQuery.

Practice Exam 10

Question 1: You are working as a Cloud Administrator at a large tech company that has recently acquired a smaller startup with its own Google Cloud organization. In order to maintain a consistent working environment, you need to make sure that your Site Reliability Engineers (SREs) have identical project permissions in both your organization and the startup company's organization. How should you achieve this?

A. Use the gcloud iam roles copy command, and provide the project IDs of all projects in the startup company's organization as the destination.

B. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

C. In the Google Cloud console for the startup company, select Create role from selection and choose source as the startup company's Google Cloud organization.

D. Use the gcloud iam org-policies set-policy command and enforce the same role policies for the startup company's organization as your organization.

Question 2: You're a software developer at a growing tech company working on a new application that will store relational data for users worldwide. Your manager is unsure of the potential user base size and wants a database solution that can easily scale with user growth without frequently adjusting configurations. Which storage solution should you choose for this project?

A. Cloud Pub/Sub

B. Cloud Spanner

C. Firestore

D. Kubernetes Engine

Question 3: In your software development company, it is mandatory for all developers to possess identical permissions across every Google Cloud project they work on. Additionally, the company's security policy limits developer permissions exclusively to Compute Engine, Cloud Functions, and Cloud SQL. To efficiently enforce this security policy, what action should you take?

A. • Manually grant individual Compute Engine, Cloud Functions, and Cloud SQL permissions to each developer for each project.

B. • Assign the predefined roles of Compute Engine Admin, Cloud Functions Invoker, and Cloud SQL Client to the Google group at the Google Cloud project level.

C. • Enable API access to Compute Engine, Cloud Functions, and Cloud SQL for all developers, without creating custom roles or assigning Google group permissions.

D. • Add all developers to a Google group in Cloud Identity. • Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level. • Assign the custom role to the Google group.

Question 4: You are an IT administrator at a software company that relies on a critical application running on a managed instance group in Compute Engine. This application accepts TCP traffic on port 389 and needs to preserve the IP address of the client sending the request. To provide access to the application over the internet using a load balancer, which approach should you take?

A. Expose the application by using an external TCP Network Load Balancer.

B. Expose the application by using an external UDP Network Load Balancer.

C. Expose the application by using an external Serverless Network Endpoint Group Load Balancer.

D. Expose the application by using an SSL Proxy Load Balancer.

Question 5: You are working for a fast-growing media company, and your task is to host the company's video encoding software on Compute Engine. The company's user base is constantly increasing, and the users require uninterrupted access to encode their videos without any CPU limitations. You are responsible for ensuring the high availability of the encoding solution while also adhering to Google's best practices for automating operations. How should you proceed?

A. Deploy your solution on multiple Compute Engine instances, and use Google Cloud Functions to handle high CPU utilization.

B. Deploy your solution on multiple standalone Compute Engine instances, and replace existing instances with high-CPU instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

C. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

D. Deploy your solution to an instance group, but set the maximum number of instances lower than the expected peak demand.

Question 6: You've recently joined a company specializing in ecommerce hosting solutions and are working on a project that involves an on-premises ecommerce application. The application is built on a complex set of Python-based microservices, each running on Docker containers, with configurations injected using environment variables. Your task is to migrate this on-premises application to a serverless Google Cloud solution. What approach should you take for a seamless and efficient deployment?

A. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Kubernetes Engine. Use the same configuration as on-premises.

B. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

C. Use your existing codebase and deploy each service as a separate Cloud Run. Use the same configurations as on-premises.

D. Migrate the code to App Engine Flexible Environment and deploy each microservice as separate services. Update the configurations and the required endpoints.

Question 7: You are working as a cloud engineer for a company that uses Linux VMs to connect to Cloud SQL. You have recently created a service account with the necessary access rights. To ensure that your Linux VM utilizes the newly created service account instead of the default Compute Engine service account, what step should you take?

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

B. Configure an environment variable to override the default Compute Engine service account on the VM.

C. Create an external IP address for the VM and add it to the Authorized Networks of the Cloud SQL instance.

D. Add the service account email address as a tag to the VM and restart it.

Question 8: You are working as a network administrator at a tech company, and you need to load balance an instance group serving a public web application over HTTPS. Your goal is to terminate the client SSL session and adhere to the Google-recommended practices. What should be your approach?

A. Configure a global external forwarding rule.

B. Configure an external SSL proxy load balancer.

C. Configure a Cloud NAT gateway.

D. Configure an HTTP(S) load balancer.

Question 9: You are working as a network administrator in a large-scale software company. Your company's application is running on bare-metal servers in their own data center, and it needs to access Google Cloud Storage. However, the company's strict security policies do not permit the servers hosting the application to have public IP addresses or access to the internet. In order to provide the application with access to Google Cloud Storage while adhering to Google-recommended best practices, what should you do?

A. 6. Deploy a Kubernetes cluster on your on-premises servers using Anthos, then configure the application to access Cloud Storage using the Anthos Service Mesh.

B. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in Google Cloud. 2. Use Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through

the VPN tunnel. 3. In your on-premises network, configure your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com.

C. 3. Deploy a Filestore instance in the same VPC as the servers and configure the application to use the Filestore instead of Cloud Storage, while synchronizing the data between Filestore and Cloud Storage manually.

D. 4. Use Cloud Pub/Sub to send messages containing your servers' data to Google Cloud, then process these messages with a Cloud Function that stores the data in Cloud Storage.

Question 10: As an IT manager at a growing tech company, you are overseeing an application development team that has produced Docker images for an application set to launch on Google Cloud. The team prefers not to handle the infrastructure related to this application and expects it to automatically scale with increasing popularity. What course of action should you take to meet these requirements?

A. Deploy the application on Google Compute Engine with a Preemptible VM.

B. Configure a Google Cloud Function to run the Docker image on a schedule using Cloud Scheduler.

C. Create and launch Cloud Dataflow jobs with the container image.

D. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Question 11: You are working as a DevOps engineer at a software development company. Your team uses Google Container Registry to store container images centrally in a separate project. Now, you are tasked to create a Google Kubernetes Engine (GKE) cluster in another project. In order to ensure that the Kubernetes can successfully download the images from the Container Registry, which action should you perform?

A. Configure an Identity-Aware Proxy for the Container Registry and allow access to the service account used by the Kubernetes nodes.

B. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

C. Grant the Storage Object Viewer IAM role to the default service account of the project where the GKE cluster is being created.

D. Enable the Cloud Storage API in the project where the GKE cluster is being created.

Question 12: You are working as a system administrator in a tech company that relies on running an application on multiple virtual machines within a managed instance group with autoscaling enabled. The autoscaling policy is configured to add additional instances when the CPU utilization exceeds 80%. The group has a maximum limit of five VMs or until CPU utilization lowers

to 80%. The initial delay for HTTP health checks is set to 30 seconds, while the VM instances take about three minutes to become available. You notice that during autoscaling, the instance group adds more instances than required to support the user traffic. How can you effectively maintain the instance group size when autoscaling?

A. Decrease the autoscaling cooldown period to 60 seconds.

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

C. Increase the instance group's maximum limit to 10.

D. Decrease the autoscaling threshold to 50%.

Question 13: As a software engineer at a technology company, you need to examine the configured Kubernetes Engine cluster of an inactive configuration in gcloud using the fewest possible steps. What should you do?

A. Use kubectl get nodes to review the output.

B. Use gcloud config set compute/zone and gcloud config set compute/region to review the output.

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

D. Use gcloud auth list to review the output.

Question 14: As a data engineer for an international pharmaceutical firm, you've been tasked with selecting and configuring a solution for storing and archiving research data on Google Cloud Platform. The firm needs to comply with regulations for data from a specific geographic location. The data will be archived after 30 days and accessed annually. What should you do?

A. Select Regional Storage. Add a bucket lifecycle rule that archives data after 60 days to Coldline Storage.

B. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

C. Select Nearline Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

D. Select Regional Storage. Add a bucket lifecycle rule that moves data to Bigtable after 30 days.

Question 15: You are working at a tech company and you need to share an object containing sensitive data stored in a Cloud Storage bucket with a client from an external company. The client does not have a Google account for granting specific user-based access privileges, and you want to ensure that the content access is removed after four hours. To achieve this with the most secure method and the fewest steps, what should you do?

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

B. Use Cloud Functions to create an endpoint that provides temporary read access to the object. The external company will be allowed access for only four hours before the endpoint stops working.

C. Use VPC Service Controls to limit access to the Cloud Storage bucket from a specific IP address associated with the external company. Remove the IP address after four hours.

D. Create an API key with access to Cloud Storage and share this key with the external company to access the object. Delete the API key after four hours.

Question 16: As a financial manager for a tech company in the software industry, you are responsible for monitoring expenses. You have been asked to establish a budget alert for Compute Engineer services on one of the three Google Cloud Platform projects your company is currently working on. All three of these projects are linked to a single billing account. What is the appropriate course of action?

A. Verify that you are project administrator. Select the associated billing account and create a budget and a custom alert.

B. Verify that you are the project administrator. Select the associated billing account and create a budget for the appropriate project with additional padding for potential overruns.

C. Verify that you are the project billing administrator. Select the associated billing account and create a separate budget for each project.

D. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

Question 17: In your rapidly growing healthcare technology company, you've recently experienced a security breach and have decided it's crucial to better monitor activities within your Google Cloud environment. Your main focus is tracking unexpected firewall changes and instance creation, while keeping the solution as simple as possible. What should you do?

A. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

B. Use Cloud Debugger to monitor and analyze unexpected changes in firewall rules and instances, and set up custom alerts for violations.

C. Use Cloud Data Loss Prevention (DLP) to monitor sensitive data and set up alerts for abnormal patterns in firewall rules and instance creation.

D. Set up a cron job on a compute instance to periodically check for changes in firewall rules and instances, and send email notifications if any discrepancies are found.

Question 18: You are working as a cloud specialist in a tech company, and your latest assignment involves setting up the billing configuration for a new

Google Cloud client. The client wants to efficiently organize their resources based on shared common IAM policies. What strategy should you implement to achieve this?

A. Set up separate Cloud SQL instances for resources with common IAM policies.

B. Set up separate billing exports for resources with common IAM policies.

C. Use folders to group resources that share common IAM policies.

D. Set up a proper billing account structure to group IAM policies.

Question 19: You work for a software company that utilizes a 3-tier solution deployed on Compute Engine. The infrastructure consists of the following configuration: each tier has its own service account associated with all instances within it. Your task is to enable communication on TCP port 8080 between tiers in the following manner: * Instances in tier #1 must communicate with tier #2. * Instances in tier #2 must communicate with tier #3. What action should be taken in order to achieve this?

A. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #1 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #3 service account • Protocols: allow TCP: 8080

B. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow all 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow all

C. 1. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow all 2. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow all

D. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP: 8080

Question 20: As a software developer in a large company, you have created a containerized web application intended for internal colleagues to use during business hours. To minimize costs outside of operating hours, you have recently established a new Google Cloud project for deploying the application. What

actions should be taken to prevent additional costs beyond these designated hours?

A. Deploy the container on Cloud Functions, configuring the function to trigger during business hours only.

B. Use Datastore to implement time constraints on access to the containerized application during non-business hours.

C. Deploy the container on Google Compute Engine (GCE) with VM instance scheduling to automatically shut down during non-business hours.

D. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

Question 21: You are working as a Cloud Engineer at a tech company, and your application runs on Google Cloud within a managed instance group (MIG). While monitoring Cloud Logging, you notice errors for one VM, indicating that one of the processes has become unresponsive. To swiftly replace this problematic VM in the MIG, what action should you take?

A. Use the gcloud compute instances restart command to restart the VM.

B. Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

C. Enable autoscaling for the MIG based on CPU utilization.

D. Select the MIG from the Compute Engine console and, in the menu, select Replace VMs.

Question 22: You are working as a cloud infrastructure engineer at a software development company. Your manager has assigned you the task of deploying production and test workloads on Compute Engine. The production VMs must be in a different subnet than the test VMs, and all the VMs should be able to communicate with each other using Internal IP without creating additional routes. To accomplish this, you need to set up VPC and two subnets. What is the appropriate configuration that fulfills these requirements?

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

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

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

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

Question 23: As an IT manager in a tech company, what action should you take to allow an external auditor to only view but not modify resources in a

project where Domain Restricted Sharing is enabled, without compromising the security of your organization?

A. Give the auditor BigQuery Data Viewer role on the project.

B. Ask the auditor for their Google account, and give them the Viewer role on the project.

C. Create a temporary account for the auditor in Cloud Identity, and give that account the Storage Object Viewer role on the project.

D. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

Question 24: As a developer at a startup company, you need to deploy a low-traffic application within a new project. The application, packaged in a container image, exposes an HTTP endpoint and receives very few requests per day. To minimize costs while deploying this application, what solution should you implement?

A. Deploy the container on Firebase Hosting.

B. Deploy the container on Cloud Run.

C. Deploy the container on Dataflow.

D. Deploy the container on Cloud Functions with HTTP trigger.

Question 25: As a financial analyst at a tech company, you are responsible for analyzing Google Cloud Platform service costs across three different departments. Your task is to estimate service costs by service type, on a daily and monthly basis, for the upcoming six months using standard query syntax. How should you proceed?

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

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

C. Export your bill to a Cloud Storage bucket, and then import into Cloud Spanner for analysis.

D. Use Cloud Pub/Sub to stream billing data to Google Sheets for analysis.

Question 26: As a data analyst for a multinational corporation, you are responsible for managing extensive data stored in BigQuery. The company has accumulated over 1000+ datasets across various projects, created by different business units. The Chief Information Officer has tasked you with identifying all tables containing the employee_ssn column. To accomplish this task efficiently, what approach should you take?

A. Write a script that loops through all the projects in your organization and runs a query on INFORMATION_SCHEMA.COLUMNS view to find the employee_ssn column.

B. Create a Pub/Sub topic and configure Data Catalog to send all the dataset metadata updates to this topic, then filter the messages to find those containing employee_ssn.

C. Go to Data Catalog and search for employee_ssn in the search box.

D. Manually check each dataset in all the projects for the presence of an employee_ssn column.

Question 27: You are working in a growing tech company, and you have been tasked with migrating the company's on-premises data management solutions to Google Cloud. Currently, the company is utilizing the following setup:

• A MySQL cluster for the primary database • Apache Kafka for event streaming • A Cloud SQL for PostgreSQL for analytics and reporting.

In order to align with the global scalability and minimal operational and infrastructure management requirements, you have been asked to implement the recommended Google Cloud solutions.

Which migration path should you follow?

A. Migrate from MySQL to Cloud SQL, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

B. Migrate from MySQL to Firestore, from Kafka to Cloud Tasks, and from Cloud SQL for PostgreSQL to BigQuery.

C. Migrate from MySQL to Firestore, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to Bigtable.

D. Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

Question 28: As a data analyst working for a retail company, you have an on-premises data analytics set of binaries that processes large inventory data files ranging from 1 gigabyte to 16 gigabytes in memory for about 45 minutes every midnight. To optimize resources and minimize costs, your company is looking to migrate this application to Google Cloud with minimal effort. What should you do?

A. Upload the set of binaries to BigQuery and use Cloud Scheduler to run a SQL query on the data files every midnight.

B. Use Dataflow to host the set of binaries and schedule the processing for every midnight.

C. Upload the code to Cloud Run and use Cloud Scheduler to trigger the execution every midnight.

D. Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

Question 29: As a DevOps engineer working at a software development company, you are responsible for creating a new Google Kubernetes Engine (GKE) cluster that consistently runs a supported and stable version of Kubernetes. What should you do to ensure this?

A. Enable the "Network Policy" feature for your GKE cluster.

B. Select the "Autoscaling" option for your GKE cluster.

C. Use "Ubuntu" as a node image for your GKE cluster.

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

Question 30: As a database administrator in a tech company managing a Cloud Spanner instance for the best query performance, your production instance runs in a single Google Cloud region. To enhance performance in the least possible time while adhering to Google's best practices for service configuration, what approach should you take?

A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 75%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

B. Increase the number of nodes in your Cloud Spanner instance by 50% and monitor the impact on high priority CPU utilization, adjusting nodes as needed.

C. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 45%. If you exceed this threshold, add nodes to your instance.

D. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

Question 31: As a network administrator for a large e-commerce company, you are tasked with configuring Cloud DNS to host your company's website. You need to create DNS records to direct home.mydomain.com, mydomain.com, and www.mydomain.com to the IP address of your Google Cloud load balancer. What should you do?

A. Create one CNAME record to point mydomain.com to the load balancer, and create two AAAA records to point WWW and HOME to mydomain.com respectively.

B. Create one CNAME record to point mydomain.com to the load balancer, and create two A records to point WWW and HOME to mydomain.com respectively.

C. Create one SOA record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com

respectively.

D. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively. Most Voted

Question 32: As a software engineer working in a major tech company, you need to ensure the security of the database by refactoring the configuration in a way that the database password is not stored in plain text. You decide to follow Google-recommended practices. What step should you take next?

A. Store the database password in the Compute Engine instance metadata and use a startup script to extract it.

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

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

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

Question 33: As an IT specialist at a software company, you've been tasked with configuring autohealing for network load balancing for a group of Compute Engine instances operating in multiple zones. To ensure efficiency, you must complete this task in the fewest possible steps and configure re-creation of the VMs if they are unresponsive after 3 attempts of 10 seconds each. What should you do?

A. Create an HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10.

B. Create an HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP)

C. Create a managed instance group. Set the Autohealing health check to healthy (HTTP)

D. Create an HTTP(S) load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (TCP)

Question 34: As a software engineer in a tech company, you are tasked with enabling your development team to deploy new features to an existing Cloud Run service in production. In order to minimize the risk associated with a new revision and reduce the number of customers potentially affected by an outage, you need to adhere to Google-recommended practices for managing revisions to a service without introducing any development or operational costs to your customers. What should your approach be?

A. Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

B. Enable Cloud Scheduler to perform periodic health checks on the new revision and reroute traffic to the old revision if issues are detected.

C. Create multiple Cloud Run staging environments for testing before deploying to production, but maintain the same traffic allocation.

D. Deploy your application to a second Cloud Run service, and ask your customers to use the second Cloud Run service.

Question 35: As a DevOps engineer at a growing tech company, you are responsible for managing the Google Kubernetes Engine (GKE) cluster named 'dev' deployed on Google Cloud. In order to manage the GKE configuration using the command line interface (CLI), you've recently downloaded and installed the Cloud SDK. To make sure that by default, your future CLI commands address this specific cluster, what action should you take?

A. Create a file called gke.settings in the ~/.google folder that contains the cluster name.

B. Use the command gcloud config set project/cluster dev.

C. Use the command gcloud container clusters update dev.

D. Use the command gcloud config set container/cluster dev.

Question 36: As an IT manager at a global tech company, you need to ensure that all development teams in your organization, based in the United States, are restricted to creating Google Cloud resources within the US only. How should you proceed to implement this limitation?

A. Create an Identity and Access Management (IAM) policy to restrict the resources locations in all dev projects. Apply the policy to all dev roles.

B. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations. Most Voted

C. Create a VPC network in US regions and restrict all dev projects to use only that network.

D. Configure Cloud Monitoring to alert the organization if resources are created outside of the US. Set up manual deletion for those resources.

Question 37: As an IT manager in the healthcare industry, your company's infrastructure is on-premises and all machines are running at maximum capacity. You want to burst to Google Cloud to handle additional workloads, but it's crucial that the workloads on Google Cloud can directly communicate with the workloads on-premises using a private IP range. What should you do?

A. In Google Cloud, configure the VPC as a host for Shared VPC.

B. Configure Firewall rules only on the on-premises environment to allow all traffic between both networks.

C. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

D. Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses.

Question 38: In your company, you are responsible for managing a latency-sensitive website within the IT department. Your task is to run a single caching HTTP reverse proxy on GCP that consumes minimal CPU. With the requirement of a 30-GB in-memory cache plus an additional 2 GB of memory for other processes, and a goal to minimize cost, how should you run this reverse proxy?

A. Create a Cloud Filestore with 32 GB of storage, and use it as the cache for the reverse proxy.

B. Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

C. Create a Cloud Datastore with 32 GB of storage and utilize Cloud Datastore for caching.

D. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

Question 39: You are the lead developer at a growing tech company and want to deploy an application on Cloud Run to handle the processing of messages from a Cloud Pub/Sub topic, in compliance with Google-recommended practices. What steps should you take to achieve this?

A. 6. Deploy a Compute Engine instance that consumes messages from the Cloud Pub/Sub topic and forwards them to your Cloud Run application using HTTP requests.

B. 7. Use Cloud IoT Core to subscribe to the Cloud Pub/Sub topic and then configure it to push messages to your Cloud Run application using the REST API.

C. 1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run. 2. Create a Cloud Pub/Sub subscription for that topic. 3. Make your application pull messages from that subscription.

D. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

Question 40: You are working as a software engineer in a multinational company and are tasked with developing an application to manage customer relations. The application will be used by customers worldwide, and the company's CTO is concerned about potential scalability issues due to unpredictable user

growth. To ensure proper scaling with minimal configuration changes, which storage solution should you implement?

A. Cloud Spanner

B. Cloud Memorystore

C. Cloud Bigtable

D. Cloud Datastore

Question 41: As a member of a software solutions company that manages multiple Google Cloud projects, you've been assigned to set up billing for the Marketing department's new initiative, which requires using Google Cloud services. What steps should you follow to accomplish this task?

A. 1. Verify that you are assigned the Billing Account Creator role for your organization's Google Cloud account. 2. Assign the Marketing department users to the new Billing Account, but don't create a new project.

B. 1. Verify that you are assigned the Project Creator IAM role for your organization's Google Cloud account. 2. Create a new Marketing project and share the billing account with other projects.

C. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud Project for the Marketing department. 2. Link the new project to a Marketing Billing Account.

D. 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account. 2. Assign quotas to Marketing department's project and manually calculate billing based on resource usage.

Question 42: You are working as a system administrator at a tech company, and you recently deployed an application on a single Compute Engine instance within your organization's network. The application writes logs to disk. Now, users are reporting errors with the application, and your task is to diagnose the problem. What should you do?

A. Connect to the instance using Cloud Identity-Aware Proxy (IAP) and view the application logs.

B. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

C. Enable Stackdriver Trace to trace and analyze application logs.

D. Navigate to Cloud Logging and view the application logs.

Question 43: You are working as a Project Manager at a company in the retail industry. Your task is to handle a project for the Data Analytics department, which needs to execute custom SQL queries on the most recent data in BigQuery, as the data pipeline continuously streams data into the platform. How should you enable the department to access and query the latest data in BigQuery?

A. Configure the BI team's API keys to have read and write access to BigQuery, allowing them to query and analyze data.

B. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

C. Create a service account with BigQuery Data Transfer Service role and share the private key with the BI team to copy data from BigQuery.

D. Use Cloud Composer to schedule a daily workflow that synchronizes the data in BigQuery with their internal database.

Question 44: You're working as an IT specialist at a large corporation that relies on Cloud Storage for storing critical backup files for disaster recovery. In order to comply with Google's best practices, which storage option should you choose?

A. Bigtable

B. Coldline Storage

C. Archive Storage

D. Filestore

Question 45: As a recently hired IT specialist at a multinational tech company, you are given responsibility for maintaining a Google Cloud Platform project that your colleague previously managed. To ensure the project's security, you want to inspect which users have been granted the Project Owner role. What is the most appropriate step to take in this situation?

A. In the GCP Console, navigate to the VPC Network Peering page and check the permissions for network resources.

B. Use the command gcloud projects get-iam-policy to view the current role assignments.

C. Check the Cloud Identity Groups settings to find the groups with the Project Owner role.

D. In the console, validate which SSH keys have been stored as project-wide keys.

Question 46: As a data storage specialist in a tech company based in Boston, MA, you need to configure the optimal data storage for files stored in Cloud Storage for minimal cost. These files are used in a mission-critical analytics pipeline that is used continually. How should you set up the storage configuration?

A. Configure multi-regional storage for the multi-region closest to the users. Configure a Standard storage class.

B. Configure regional storage for the region closest to the users. Configure a Nearline storage class.

C. Configure regional storage for the region closest to the users. Configure a Standard storage class.

D. Configure multi-regional storage for the multi-region closest to the users. Configure a Nearline storage class.

Question 47: As a database administrator for a leading tech company that utilizes a hybrid cloud strategy, some of your applications are deployed on Google Cloud. Your Virtual Private Cloud (VPC) in Google Cloud is connected to your company's on-premises network via a Virtual Private Network (VPN) tunnel. You need a solution that enables multiple applications in Google Cloud to connect to your on-premises database server without having to change the IP configuration in all applications when the IP of the database server changes. What should you do?

A. Create a Cloud Storage bucket and store the IP of the database, which can be accessed by all applications.

B. Configure a static public IP for the database on your on-premises network.

C. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

D. Create an external Cloud DNS zone to ensure all applications can resolve the database's IP address.

Question 48: You are working as a cloud engineer for a company that heavily relies on Google Cloud. Your manager asks you to set up application performance monitoring for projects A, B, and C, in order to have a single unified view for monitoring CPU, memory, and disk usage. What should you do to achieve this?

A. Use Firebase Performance Monitoring to track metrics across the three projects.

B. Enable API and then use default dashboards to view all projects in sequence.

C. Enable API, create a workspace under project A, and then add projects B and C.

D. Enable BigQuery API, export metrics data to BigQuery, and then analyze it there.

Question 49: As a data analyst at a leading tech company, you need to send the logs from all Compute Engine instances to a BigQuery dataset called platform-logs for analysis purposes. You have already installed the Cloud Logging agent on all the instances and your aim is to minimize cost. What is the most cost-effective method to accomplish this task?

A. 1. In Cloud Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the platform-logs dataset as Sink Destination.

B. 1. Give the BigQuery Data Editor role on the platform-logs dataset to the service accounts used by your instances. 2. Update your instances' metadata to add the following value: logs-destination: bq://platform-logs.

C. 1. In Cloud Logging, create a logs export with a Cloud Pub/Sub topic called logs as a sink. 2. Create a Cloud Function that is triggered by messages in the logs topic. 3. Configure that Cloud Function to drop logs that are not from Compute Engine and to insert Compute Engine logs in the platform-logs dataset.

D. 7. Modify your instances' startup scripts to send the logs directly to the BigQuery dataset (platform-logs) using the bq command-line tool. 8. Grant BigQuery Data Editor role on the dataset to the service accounts used by your instances.

Question 50: As a network engineer for a global company, you're managing an application that handles SSL-encrypted TCP traffic on port 443 with clients from all around the world. Your main goal is to minimize latency for these clients. Which load balancing option should you implement?

A. Cloud VPN Load Balancer

B. SSL Proxy Load Balancer

C. HTTPS Load Balancer

D. NAT Gateway Load Balancer

Practice Exam 10 Solutions

Solution to Question 1: B

The correct answer is B. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination. This approach enables you to copy identical roles from your organization to the startup company's organization, ensuring that your SREs have the same project permissions in both organizations. Providing the Organization ID as the destination ensures that the roles are applied at an organizational level instead of individual projects, covering all current and future projects within the startup company's organization.

Option A is incorrect because it requires you to provide the project IDs of all projects in the startup company's organization, which can be time-consuming and error-prone. This approach would also not apply to future projects created within the organization, causing inconsistency with the roles.

Option C is incorrect because "Create role from selection" is not a valid option in the Google Cloud console. Additionally, choosing the source as the startup company's Google Cloud organization would not result in identical role permissions since it would be copying roles from the startup company's organization, not from your organization.

Option D is incorrect because the "gcloud iam org-policies set-policy" command deals with organization policies rather than IAM roles and permissions. While it may help maintain policy consistency between the two organizations, it will not address the project permissions for SREs specifically.

Solution to Question 2: B

The correct answer is B. Cloud Spanner.

Explanation: Cloud Spanner is a fully managed, highly scalable, relational database designed to support global online transaction processing (OLTP) workloads. It combines the benefits of horizontal scalability, powerful transactions, and strong consistency with ease of management, making it an ideal choice for the given use case.

Why other options will not work:

A. Cloud Pub/Sub: Cloud Pub/Sub is a messaging service that facilitates communication between various components of an application via publish-subscribe pattern. It does not serve as a relational data storage solution and is not designed for managing the kind of data storage needs specified in the question.

C. Firestore: Firestore is a NoSQL database designed for document-based storage. While it can handle scalability and real-time data synchronization, it is not a relational database. The question specifically requires a relational data storage solution, which Firestore cannot provide.

D. Kubernetes Engine: Kubernetes Engine (GKE) is a managed, production-ready environment for deploying and managing containerized applications. It is not a database solution, making it unsuitable for the project's relational data storage needs.

In conclusion, Cloud Spanner is the best choice for relational data storage, as it can easily scale with user growth without frequently adjusting configurations, making it an ideal solution for a growing tech company with an undefined user base size.

Solution to Question 3: D

The correct answer is D because it is the most efficient and secure way to enforce the company's security policy across the organization.

D: This option allows you to create a custom role specifically tailored for your developers that has permissions for Compute Engine, Cloud Functions, and Cloud SQL, which is in line with the company's security policy. By adding developers to a Google group in Cloud Identity, you ensure that permissions are identical across the team. Assigning the custom role to this Google group at the organization level guarantees that the permission scheme is applied consistently to all relevant projects, simplifying management and ensuring compliance.

A: Manually granting individual permissions for each developer, and for each project, is error-prone and time-consuming. This method does not scale well and will introduce inefficiencies as the team and project list grow. It also increases the risk of human error when assigning permissions, potentially violating the company's security policy.

B: Although using predefined roles might seem like a convenient solution, it is not the most secure or efficient choice. In this case, the predefined roles included may provide more permissions than required by the company's security policy. This could lead to security breaches and expose resources to unauthorized actions. Additionally, assigning the roles at the Google Cloud project level increases management overhead when new projects are added.

C: Enabling API access to only the specified services ensures that developers have the ability to access data and perform operations, but it does not enforce identical permissions for all developers. Moreover, this approach does not consider custom roles or Google group permissions, which allow for a more efficient and structured method of managing permissions.

In conclusion, the best approach to enforce identical permissions between developers, specifically for Compute Engine, Cloud Functions, and Cloud SQL, requires creating a custom role at the organization level and assigning it to a Google group that contains all developers. This ensures that permissions are uniform across the company and it simplifies access management.

Solution to Question 4: A

The correct answer is A, and here's why:

A. Expose the application by using an external TCP Network Load Balancer.

An external TCP Network Load Balancer is the appropriate approach because it meets both requirements: it supports the necessary TCP traffic on port 389 and preserves the client IP address. Network Load Balancers operate at Layer 4 (transport layer) and can handle millions of requests per second while maintaining low latency. This makes it the most efficient and suitable choice for managing the critical application's traffic.

B. Expose the application by using an external UDP Network Load Balancer.

A UDP Network Load Balancer would not be suitable in this scenario since the application requires TCP traffic on port 389, not UDP. The UDP protocol is different from TCP and not suitable for applications that need guaranteed delivery of packets.

C. Expose the application by using an external Serverless Network Endpoint Group Load Balancer.

Although a Serverless Network Endpoint Group Load Balancer supports TCP traffic and operates at Layer 4, it is specifically designed for serverless applications and not suitable for our use case. Additionally, there is no direct indication that it preserves the client IP address for incoming requests.

D. Expose the application by using an SSL Proxy Load Balancer.

An SSL Proxy Load Balancer is not the right choice as it operates at Layer 7 (application layer) and deals with SSL/TLS traffic. While it supports TCP traffic, it doesn't preserve the client IP address for incoming requests, which is a necessary requirement for the critical application in this scenario.

In conclusion, option A (using an external TCP Network Load Balancer) is the most suitable approach for this case, as it fulfills both requirements by supporting TCP traffic on port 389 and preserving the client IP address of incoming requests.

Solution to Question 5: C

The correct answer is C. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

Here's why the other options will not work:

Option A: Deploy your solution on multiple Compute Engine instances, and use Google Cloud Functions to handle high CPU utilization. Using Google Cloud Functions for video encoding is not suitable, as they are designed for lightweight and short-duration tasks (up to a maximum of 9 minutes). Furthermore, they are not optimized to handle high CPU utilization.

Option B: Deploy your solution on multiple standalone Compute Engine instances, and replace existing instances with high-CPU instances when CPU

utilization on Cloud Monitoring reaches a certain threshold. Manually replacing instances with high-CPU instances is not adhering to Google's best practices for automating operations. Moreover, this method is inefficient and may cause downtime during the replacement process, impacting the users' experience.

Option D: Deploy your solution to an instance group, but set the maximum number of instances lower than the expected peak demand. This approach does not ensure the high availability of the encoding solution. Setting the maximum number of instances lower than the expected peak demand will cause performance issues and unacceptable delays when the demand surpasses the available resources.

So the best option is C, which leverages the power of Instance Groups and autoscaling based on CPU utilization. This will automatically scale the number of instances depending on the resource demand, thus ensuring high availability and adhering to Google's best practices for automating operations.

Solution to Question 6: B

The best approach for this scenario is option B: Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

Here's why option B is the most suitable choice and why other options are not ideal:

Option A: While using Kubernetes Engine would allow you to deploy Docker containers, it is not a serverless solution as required by the task. In addition, using the same on-premises configuration might not fully leverage the benefits and optimizations that Google Cloud provides.

Option C: Deploying each service as a separate Cloud Run without utilizing the existing Docker images would involve more manual work and could potentially cause inconsistencies during deployment. Additionally, applying the same on-premises configurations could lead to suboptimal performance in a serverless cloud environment.

Option D: While App Engine Flexible Environment can be used for deploying containerized applications, it is not the most efficient choice for serverless deployment of the Python-based microservices as required by the task. Moreover, the migration process to App Engine would require additional work and changes to the codebase, which might not be cost-effective and time-efficient.

Option B, on the other hand, allows you to leverage the existing CI/CD pipeline and deploy Docker containers seamlessly to a serverless Google Cloud solution using Cloud Run. This approach provides the benefits of autoscaling, easy configuration updates, and integration with other Google Cloud services - all without requiring substantial modifications to your application or deployment process. By updating the configurations and endpoints, you ensure that the application is optimized for the cloud environment, thus achieving a more efficient

and seamless deployment.

Solution to Question 7: A

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

Explanation: When you want your Linux VM to use the newly created service account instead of the default Compute Engine service account, you need to specify it during the VM creation process. By doing this, you are ensuring that the VM will use the new service account for authentication and accessing the respective resources, including Cloud SQL.

Why other options will not work:

B. Configure an environment variable to override the default Compute Engine service account on the VM. This option will not work because the association between a VM instance and its service account is determined during the instance creation process. Overriding the default service account with an environment variable within the system is not a supported method.

C. Create an external IP address for the VM and add it to the Authorized Networks of the Cloud SQL instance. While this option may provide your VM access to the Cloud SQL instance, it does not address the issue of using the correct service account with the proper access rights for the Linux VM. This option only manages the network access rules, not the service account association.

D. Add the service account email address as a tag to the VM and restart it. Adding the service account email address as a tag to the VM does not change the service account associated with the VM. Tags are used for networking and resource organization purposes, and they do not have any direct impact on the access and identity management of the VM.

Solution to Question 8: D

The correct answer is D. Configure an HTTP(S) load balancer.

Explanation:

To achieve the goal of load balancing an instance group serving a public web application over HTTPS and terminating the client SSL session, you need a service capable of handling SSL termination and adhering to Google-recommended practices. Given the options provided, an HTTP(S) load balancer is the best solution.

D. Configure an HTTP(S) load balancer - This is the correct choice because Google Cloud's HTTP(S) load balancer is a global, managed service that provides SSL termination, utilizes Google's backbone for efficient traffic routing, offers multi-region support, is compliant with Google-recommended practices, and allows you to load balance traffic over HTTPS. By implementing an HTTP(S)

load balancer, you meet both your requirements of load balancing over HTTPS and terminating the client SSL session.

A. Configure a global external forwarding rule - This option is incorrect because global external forwarding rules are used to forward traffic to target proxies, which in turn route the traffic to the backend services. This alone will not suffice for SSL termination and load balancing over HTTPS as required in the scenario.

B. Configure an external SSL proxy load balancer - This option is not suitable because an SSL proxy load balancer is a regional service and typically used for load balancing non-HTTP(S) traffic with SSL termination. This will not be ideal for a public web application and may not adhere to Google's recommended practices for this specific scenario.

C. Configure a Cloud NAT gateway - This option is incorrect because a Cloud NAT gateway is a regional, managed Network Address Translation (NAT) service for providing internet access to private instances without assigning them individual public IPv4 addresses. It does not provide SSL termination or load balancing capabilities required in this scenario.

In summary, the best approach for load balancing an instance group serving a public web application over HTTPS with SSL termination and adhering to Google-recommended practices is to configure an HTTP(S) load balancer.

Solution to Question 9: B

The correct answer is B, which involves creating a tunnel to a VPC in Google Cloud using Cloud VPN or Interconnect and using Cloud Router to create a custom route advertisement. This approach allows your on-premises servers hosting the application to access Google Cloud Storage without requiring public IP addresses or internet access. The DNS server configured in your on-premises network resolves *.googleapis.com as a CNAME to restricted.googleapis.com, further ensuring that the required security policies are maintained. This approach adheres to Google-recommended best practices.

Option A is incorrect because the deployment of a Kubernetes cluster using Anthos does not address the company's security policies disallowing public IP addresses or internet access on the servers hosting the application. Additionally, just implementing the Anthos Service Mesh does not directly provide access to Google Cloud Storage.

Option C is not optimal as it requires manual synchronization between Filestore and Cloud Storage, which can be inefficient and prone to errors. Furthermore, this option does not address the security concerns associated with providing access to Google Cloud Storage without public IP addresses or internet access.

Option D is incorrect because using Cloud Pub/Sub and Cloud Functions introduces additional complexity and management overhead, as well as extra costs.

Moreover, this solution does not directly address the requirement of accessing Google Cloud Storage in compliance with the company's strict security policies.

Solution to Question 10: D

The correct answer is D - Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Here's why D is the best option and the other choices are not suitable:

D: Google Cloud Run is the most tailored solution for your requirements. By uploading the Docker images to Artifact Registry and deploying the application on Cloud Run, you can provide the infrastructure and auto-scaling capabilities your development team is looking for. Cloud Run is designed to automatically handle the underlying infrastructure, scaling, and operational tasks, allowing your team to focus solely on the application code. Furthermore, Cloud Run supports container-based applications, making it a perfect fit for your Docker images.

A: Deploying the application on Google Compute Engine with a Preemptible VM is not ideal for these requirements. While Compute Engine provides virtual machines, Preemptible VMs have a maximum runtime of 24 hours and can be terminated at any moment with short notice. This option does not offer automatic scaling to accommodate an increasing popularity and requires more hands-on management of the infrastructure when compared to Cloud Run.

B: Configuring a Google Cloud Function to run the Docker image on a schedule using Cloud Scheduler is not suitable, as Cloud Functions are designed for serverless applications and do not natively support Docker containers. This option also lacks the necessary automatic scaling functionality, since Cloud Functions are typically used for single-purpose tasks or short-lived operations.

C: Creating and launching Cloud Dataflow jobs with the container image is not appropriate for this application. Cloud Dataflow is a stream/batch data processing service designed specifically for data transformation and analysis use cases. While it does support containerized processing functions, it is not well-suited for deploying and managing the infrastructure required by an entire application with a need for automatic scaling.

In conclusion, the best course of action to meet your requirements is to upload the Docker images to Artifact Registry and deploy the application on Google Cloud Run, as it is designed for container-based applications, handles underlying infrastructure, provides automatic scaling, and allows the team to focus on application development without infrastructure management.

Solution to Question 11: B

The correct answer is B. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes. This ensures that the Kubernetes nodes have the appropriate access to view and download the container images stored in the Google Container Registry.

Option A does not work because Identity-Aware Proxy is designed for authentication and access control to web applications. While it handles identity-based access management, it is not suitable for providing direct access to storage objects like container images in the Google Container Registry.

Option C is not the correct solution because granting the Storage Object Viewer IAM role to the default service account of the project where the GKE cluster is being created does not necessarily grant access to the service account used by the Kubernetes nodes themselves. The Kubernetes nodes might be using a different service account for pulling the container images.

Option D is also not suitable because enabling the Cloud Storage API in the project where the GKE cluster is being created does not automatically provide access to download the container images from the Google Container Registry. The appropriate IAM role must still be granted to the service account used by the Kubernetes nodes.

Solution to Question 12: B

The correct answer is B, which suggests increasing the initial delay of the HTTP health check to 200 seconds.

The reason for choosing Option B is that the virtual machine instances take about three minutes (180 seconds) to become fully available. If the initial delay for the HTTP health check is only 30 seconds, the health check might not recognize that a new instance is already working properly. Thus, the autoscaler may continue to add more instances than required. By increasing the initial delay of the HTTP health check to 200 seconds, you give the newly created instances enough time to become available before the health check starts monitoring their status, preventing unnecessary scaling.

Option A is incorrect because decreasing the autoscaling cooldown period to 60 seconds would make the autoscaler more aggressive, which can result in more instances added than required.

Option C is incorrect because increasing the instance group's maximum limit to 10 would not address the issue of having more instances than needed. Instead, it would allow even more instances to be added, which may further exacerbate the problem.

Option D is incorrect because decreasing the autoscaling threshold to 50% would cause the autoscaler to add instances even when the CPU utilization is lower, likely leading to more instances being added than necessary to support the user traffic.

In summary, increasing the initial delay of the HTTP health check to 200 seconds (Option B) best addresses the issue of adding excessive instances during autoscaling while maintaining the desired performance of the managed instance group.

Solution to Question 13: C

The correct answer is C: Use kubectl config use-context and kubectl config view to review the output.

Explanation:

Option A: Using kubectl get nodes will only give you information about the nodes of the currently active Kubernetes cluster, not an inactive one.

Option B: Using gcloud config set compute/zone and gcloud config set compute/region sets the default region and zone for all gcloud commands, but it does not provide any insights into a particular Kubernetes Engine cluster.

Option C: Using kubectl config use-context allows you to switch between different Kubernetes contexts, so you can change to the context of the inactive configuration you want to examine. Then, using kubectl config view allows you to review the output of that context, providing you with the relevant information about the configured Kubernetes Engine cluster. This option is the most direct and efficient way to achieve the desired result.

Option D: Using gcloud auth list will display the available authenticated accounts, but it does not provide any information about the configured Kubernetes Engine clusters.

Solution to Question 14: B

The correct answer is B: Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

Explanation:

Option A is not suitable because it suggests archiving data after 60 days, which does not meet the requirement to archive data after 30 days.

Option B is the correct choice because it meets the requirements by selecting Regional Storage to store the data while complying with the specific geographic location regulation. It also adds a bucket lifecycle rule that archives data after 30 days to Coldline Storage, which is suitable for the annual access frequency.

Option C is not the right choice because Nearline Storage is recommended for data that is accessed at least once a month. In this scenario, the firm needs to access the archived data annually, which is less frequent than Nearline Storage's intended usage. Coldline Storage is more appropriate as it is designed for infrequent access, such as annual access.

Option D is not suitable because Bigtable is not the right service for archiving data. Bigtable is a high-performance, scalable NoSQL database designed for real-time data processing, whereas Coldline Storage is specifically designed for archiving purposes with lower costs and infrequent access requirements.

In conclusion, Option B holds the correct solution for the given scenario by selecting Regional Storage and archiving data to Coldline Storage after 30 days

in compliance with the specified regulations, and for the required accessing frequency.

Solution to Question 15: A

The recommended approach for sharing an object containing sensitive data with a client from an external company without a Google account and with access removal after four hours is option A: Create a signed URL with a four-hour expiration and share the URL with the company. This method is the most secure and involves the fewest steps.

A signed URL is a way to grant temporary access to resources in your Cloud Storage bucket. The URL is valid only for a specific time period, in this case, four hours, after which it expires. This ensures that sensitive data access is limited and automatically removed without manual intervention. Additionally, generating a signed URL doesn't require the client to have a Google account to access the content.

Option B suggests using Cloud Functions to create an endpoint for temporary access. However, this method would require extra effort and resources to develop, deploy, and maintain the Cloud Function during its lifecycle. Moreover, it doesn't provide any substantial security benefits over the signed URL approach.

Option C is not as feasible because VPC Service Controls restrict access at the perimeter level rather than limiting access to specific resources within a Cloud Storage bucket. Although it can limit access to a specific IP address, implementing and managing the IP address restrictions can be complex and time-consuming. It also requires manual intervention to remove the IP address after four hours, unlike the auto-expiring signed URLs.

Option D involves creating an API key for Cloud Storage and sharing it with the external company. However, this method is less secure as the API key can be exposed to unauthorized users if not handled carefully. Additionally, it requires manual deletion of the API key after four hours to revoke access, while using signed URLs automatically enforces this limitation.

In conclusion, option A is the best choice for securely sharing sensitive data stored in a Cloud Storage bucket with a client from an external company without a Google account while ensuring access removal after four hours.

Solution to Question 16: D

The correct answer is D. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

Here's the explanation for why the answer should be D and why other options will not work:

Option A: While verifying project administrator status is essential, it is not enough for managing the billing account. The role of a project billing admin-

istrator is required for handling financial aspects like budget and alerts. Thus, option A is incorrect.

Option B: This option is incorrect because, although verifying the project administrator role, the main focus should be on the project billing administrator role in this context. Additionally, while creating a budget with additional padding for potential overruns can be helpful, it doesn't specifically address the requirement of establishing a budget alert.

Option C: While it is true that you should verify project billing administrator status, creating separate budgets for each project is not the required action, as you need to establish a budget alert for Compute Engineer services for only one project among the three. Therefore, option C is incorrect.

Option D: This option is correct because it states that you should verify your role as the project billing administrator, which is crucial for managing budgets and alerts. It also specifies creating a budget and alert for the appropriate project, meeting both the budget and alert requirements for the Compute Engineer services on the specific project.

Solution to Question 17: A

The correct answer is A: Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

Here's why option A is the best choice and why the others will not work:

A. Using Cloud Logging filters to create log-based metrics for firewall and instance actions is the right solution for your requirements. This approach allows you to specifically monitor the activities related to firewall changes and instance creation, which are your main focus. You can quickly set up alerts to notify you of unexpected actions, making it easy to respond to any potential security threats. This solution keeps things simple, as it leverages an existing service designed to track these activities.

B. Cloud Debugger is not suitable for this purpose, as it's designed for debugging applications in real-time, rather than monitoring security-related actions in your infrastructure. While Cloud Debugger can help identify issues in your application code, it doesn't have the capabilities to monitor firewall changes and instance creation in your Google Cloud environment.

C. Cloud Data Loss Prevention (DLP) is primarily focused on preventing the exposure of sensitive information and ensuring data compliance, rather than monitoring infrastructure-related activities. While DLP can help protect your data, it doesn't directly address the monitoring of firewall changes and instance creation, which are your primary concerns in this scenario.

D. Setting up a cron job on a compute instance to periodically check for changes in firewall rules and instances would technically work, but it would be a less

efficient and less scalable solution compared to using Cloud Logging filters. Creating custom scripts to perform these checks requires additional maintenance and increases complexity. Moreover, the periodic nature of a cron job means that potential security issues might go unnoticed between checks, whereas Cloud Logging filters will provide near real-time monitoring and alerting.

Solution to Question 18: C

The correct answer is C: Use folders to group resources that share common IAM policies.

Explanation:

A: Setting up separate Cloud SQL instances is not a valid solution for organizing resources based on shared IAM policies. Cloud SQL instances are used to manage and store data in databases, but they do not provide a means to directly manage or group resources based on common policies. This option does not address the client's requirements.

B: Setting up separate billing exports for resources with shared IAM policies would not help in organizing resources efficiently. It could provide a way to track costs for resources with common policies, but it wouldn't have any impact on the actual management and organization of those resources within the Google Cloud environment.

C: The best option for efficiently organizing resources that share common IAM policies is to use folders. Folders in Google Cloud provide a hierarchical way to group resources, making it easier to apply and manage common policies. By organizing resources into folders based on shared IAM policies, you can ensure that all the resources in the same folder will inherit the same set of policies. This streamlines the management and organization of resources in a manner that aligns with the client's requirements.

D: Setting up a proper billing account structure would not directly address the problem of organizing resources based on shared IAM policies. While a well-organized billing account structure can provide a clearer view of costs and account usage, this strategy does not help with organizing resources that share common IAM policies.

Therefore, the most effective strategy to achieve the client's goal is to use folders to group resources that share common IAM policies, making option C the correct answer.

Solution to Question 19: D

The correct answer is D, as it precisely specifies the required communication between the respective tiers and limits the allowed protocol to only TCP:8080, which is the requirement mentioned in the question. Let's analyze why the other options are not suitable:

Option A: This option incorrectly reverses the targets and source filters for both

firewall rules. The tier #1 instances should be allowed to communicate with tier #2, not the other way around. The same issue applies to the second rule. This would result in the wrong communication setup between the tiers.

Option B: Though this option correctly specifies the required communication setup by targeting the right tier instances and source filters, it allows all protocols instead of limiting it to only TCP:8080, which is the requirement mentioned in the question. This would result in an insecure configuration, allowing any protocol to pass through the firewall.

Option C: This option uses IP ranges as source filters, which is not as secure and specific as using service accounts, like in option D. Additionally, it allows all protocols instead of limiting it to TCP:8080, posing security and specificity issues.

In conclusion, only option D meets the requirements by enabling communication on TCP port 8080 between the specified tiers using service accounts to target instances, ensuring both the proper communication setup and the required level of security and specificity.

Solution to Question 20: D

The correct answer is D. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

Here's why option D is the most appropriate:

1. Cloud Run (fully managed) allows you to deploy containerized applications without managing the underlying infrastructure. This effectively reduces management overhead and operational costs.
2. By setting the minimum number of instances to zero, your application will scale down to zero when idle. This means that no instances will run during non-business hours, saving costs as you only pay for the actual usage, not the idle instances.

Now let's see why the other options will not work:

A. While Cloud Functions provide a cost-effective way to run smaller pieces of code, deploying a containerized web application on Cloud Functions is not possible, as they are intended for serverless, single-purpose code functions rather than full containerized applications.

B. Datastore is a NoSQL database for storing data, and it does not have the capacity to implement time constraints on an entire application. It is not a solution to reduce operating costs outside business hours.

C. While Google Compute Engine (GCE) gives you more control over your container deployment, VM instance scheduling might not be the best option for minimizing costs for this specific use case. Although you can schedule VM instances to automatically shut down during non-business hours, you might still have to pay for the allocated resources, even when the instances are not

running. Additionally, automated stopping and starting of instances adds more management overhead compared to Cloud Run.

Solution to Question 21: B

The correct answer is B. Using the gcloud compute instance-groups managed recreate-instances command to recreate the VM is the most appropriate action in this scenario. This is because this command specifically targets and recreates a problematic VM within a managed instance group. The process of recreating the VM involves deleting the existing instance and creating a new one, which ensures that the issue with the unresponsive process gets resolved without manually intervening in the VM's configuration.

Option A is not ideal because using the gcloud compute instances restart command to restart the VM may not actually resolve the issue with the unresponsive process. This is because restarting the VM does not necessarily guarantee a fresh state for all processes running on the VM.

Option C is not suitable because enabling autoscaling for the MIG based on CPU utilization does not directly address the issue of the unresponsive process on a specific VM. Autoscaling is designed to manage the number of instances in the group based on demand but does not have the ability to identify or rectify issues with individual instances.

Option D is also not suitable because selecting the MIG from the Compute Engine console and using the Replace VMs option recreates all the instances within the MIG, not just the problematic VM. This approach causes unnecessary downtime for healthy VMs in the MIG and wastes resources by replacing functioning instances.

In conclusion, using the gcloud compute instance-groups managed recreate-instances command (option B) effectively targets and resolves the issue with the unresponsive process on a specific VM in the managed instance group, making it the best choice in this situation.

Solution to Question 22: A

The correct answer is A: Create a single, custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range. This option will appropriately fulfill all the requirements because it allows you to separate the production and test workloads in distinct subnets while ensuring internal communication.

Here are the reasons why other options do not work:

B. Create 2 custom VPCs, each with a single subnet. Create each subnet in the same region and with the same CIDR range. This option does not allow internal communication between VMs in different VPCs without additional routes. The same CIDR range would also cause IP conflicts, making communication between VMs impossible.

C. Create a single custom VPC with 2 subnets. Create each subnet in different zones within the same region and with a different CIDR range. Although it separates workloads in distinct subnets with different CIDR ranges, creating subnets in different zones within the same region does not provide enough isolation between production and test workloads. A regional outage may affect both subnets simultaneously.

D. Create a single custom VPC with 2 subnets. Create each subnet in the same region and with a different overlapping CIDR range. Overlapping CIDR ranges will lead to IP conflicts and make it difficult for VMs to communicate with one another without additional routes. Introducing overlapping CIDR ranges can cause a significant amount of confusion and operational difficulties.

In conclusion, Option A is the most suitable configuration to meet the given requirements, as it offers proper isolation between production and test workloads while still allowing internal communication without creating additional routes.

Solution to Question 23: D

The correct answer is option D: Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project. By creating a temporary account in Cloud Identity, the IT manager can ensure that the external auditor only has access to the resources required for the duration of the audit, without compromising the security of the organization. The Viewer role on the project provides the auditor with the required read-only access to project resources.

Option A would not work because the BigQuery Data Viewer role only grants read access to BigQuery resources in the project. It does not provide read-only access to other resources that the auditor might need to review during the audit.

Option B is not a secure option because adding the auditor's Google account as a Viewer directly to the project might lead to the potential exposure of sensitive information beyond the scope of the audit. Additionally, this approach does not allow the IT manager to easily control the duration of the auditor's access.

Option C is inappropriate because the Storage Object Viewer role only provides read access to storage objects in the project. This does not provide read-only access to other resources that the auditor might need to view during the course of the audit.

In summary, the best option for granting an external auditor read-only access to project resources without compromising the security of the organization is option D: Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

Solution to Question 24: B

The answer should be B, Deploy the container on Cloud Run, and here's why:

Google Cloud Run is designed specifically for running stateless containers and

automatically scales to handle the number of incoming requests. Since it is a fully managed service, it also handles the underlying infrastructure management, making it ideal for low-traffic applications, such as the one mentioned in the question. Cloud Run implements a pay-per-use model, which means you only pay for the compute resources actually utilized by your application, minimizing costs for low-traffic applications.

Here's why the other options are not preferable:

A. Deploy the container on Firebase Hosting: Firebase Hosting is a static and dynamic web content hosting service, which is ideal for serving static assets (HTML, CSS, JavaScript, images, etc.) but not for running containerized applications. In this case, since we need to deploy a container image that exposes an HTTP endpoint, Firebase Hosting will not work.

C. Deploy the container on Dataflow: Google Cloud Dataflow is a fully managed service for executing data processing workflows, such as ETL (Extract, Transform, Load). While it could potentially run containerized applications, it is not meant for hosting low-traffic HTTP services. Using Dataflow could result in higher costs and additional complexity, making it unsuitable for this use case.

D. Deploy the container on Cloud Functions with HTTP trigger: Google Cloud Functions is a Function-as-a-Service (FaaS) platform that enables you to run individual functions in response to events. While it can be triggered via HTTP, it requires your code to be written as functions rather than containerized applications like our use-case. Additionally, when compared to Cloud Run, Cloud Functions might have limitations in terms of resource customization options and may not be ideal for a containerized application.

Solution to Question 25: B

The correct answer is B because it effectively fulfills the requirements of the task, which is estimating service costs by service type on a daily and monthly basis for the upcoming six months using standard query syntax. BigQuery is a serverless data warehouse that provides super-fast SQL queries and supports managing large datasets. By exporting your bill to a BigQuery dataset and writing time window-based SQL queries, you will be able to access, analyze, and process the needed data effectively and efficiently.

Option A is not suitable because Cloud Datastore is a NoSQL database, which does not support standard query syntax, and, therefore, does not fulfill the task requirements.

Option C is also not suitable because Cloud Spanner is a globally distributed database used for high-scale, mission-critical applications. It is not designed for analyzing billing data or writing standard query syntax for that purpose.

Lastly, option D is improper because using Cloud Pub/Sub to stream billing data to Google Sheets for analysis would be impractical and inefficient when

dealing with large datasets. Additionally, Google Sheets does not support standard query syntax, and it is not designed for advanced data analysis.

Solution to Question 26: C

The correct answer is C: Go to Data Catalog and search for employee_ssn in the search box.

Explanation: As a data analyst managing extensive data stored in BigQuery, using Data Catalog makes the most sense for this task. Data Catalog is specifically designed for such tasks as it is a fully managed and scalable metadata management service that helps with discovering, understanding, and managing data.

Why the other options will not work:

A. Writing a script to loop through all the projects in your organization and running a query on INFORMATION_SCHEMA.COLUMNS view to find the employee_ssn column is an option, but it is time-consuming and might introduce errors. Using Data Catalog's search functionality is a more efficient way of accomplishing this task.

B. Creating a Pub/Sub topic and configuring Data Catalog to send all dataset metadata updates to this topic, then filtering the messages to find those containing employee_ssn is not the right approach for this problem. This option is useful when you want to track real-time updates on dataset metadata changes, but it is not the best approach for efficiently finding all tables containing a specific column like employee_ssn.

D. Manually checking each dataset in all projects for the presence of an employee_ssn column is highly inefficient and error-prone. With over 1000+ datasets across multiple projects, it would be a significant time investment and prone to human errors. The Data Catalog feature offers a more efficient and accurate way to accomplish the task.

In conclusion, using the Data Catalog and searching for employee_ssn in the search box (Option C) is the most efficient and accurate approach for identifying all tables containing the employee_ssn column.

Solution to Question 27: D

The correct migration path is Option D: Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

Here's why:

1. Migrate from MySQL to Cloud Spanner: Cloud Spanner is a fully managed, strongly consistent, horizontally-scalable, and globally distributed relational database service. It is designed to handle massive-scale, mission-critical workloads with effortless concurrency and high availability. It has familiar SQL semantics making migration from MySQL easier, and is

better suited for aligning with the global scalability requirements of the growing tech company compared to the other options.

2. Migrate from Apache Kafka to Pub/Sub: Google Cloud Pub/Sub is a scalable, reliable, and real-time messaging service that allows you to send and receive messages between independent applications. It is a suitable replacement for Apache Kafka when migrating to Google Cloud, as it offers a similar publish-subscribe pattern for event streaming. Pub/Sub handles real-time event processing and analytics while offering at-least-once delivery with global availability making it the perfect fit for the company's needs.

3. Migrate from Cloud SQL for PostgreSQL to BigQuery: BigQuery is a fully managed, serverless, and highly-scalable data warehouse solution for analytics and reporting, designed to enable super-fast SQL queries across petabytes of data. It integrates easily with other Google Cloud services, has built-in ML capabilities, and supports real-time inserting and streaming of data. This makes it an ideal choice for migrating the analytical workload from Cloud SQL for PostgreSQL.

Now, let's analyze why the other options will not work:

Option A: Migrating from MySQL to Cloud SQL might not provide the required global scalability. Also, migrating from Cloud SQL for PostgreSQL to BigQuery would be redundant, as we're already using Cloud SQL for PostgreSQL for analytics and reporting.

Option B: Firestore is a NoSQL document database that is not designed for large-scale, globally distributed relational workloads, and might not be the best fit for a primary database. Additionally, Cloud Tasks is a task management service and not a suitable replacement for event streaming, which requires Pub/Sub.

Option C: Firestore and Bigtable are both NoSQL databases that don't adhere to the company's requirement of minimal operational and infrastructure management. Also, Bigtable is not designed for analytics and reporting, lacking the SQL support and serverless-ness of BigQuery.

Solution to Question 28: D

The correct answer is D. Lift and shift to a VM on Compute Engine and use an instance schedule to start and stop the instance at the appropriate times.

The reason option D is the most appropriate solution is that it allows for minimal changes during migration while optimizing resources and minimizing costs. By simply lifting and shifting the existing on-premises data analytics set of binaries to a Virtual Machine (VM) on Google Compute Engine (GCE), migration to the Google Cloud becomes straightforward and quick. The instance scheduling feature can be utilized to automate the start and stop of the VM instance, ensuring that it only runs during the period when the data processing is required. This helps in minimizing costs as the VM will only incur usage costs when active.

Option A is not suitable because BigQuery is not designed to host sets of binaries. BigQuery is a serverless, highly scalable, and cost-effective multi-cloud data warehouse meant for running complex SQL-based analytics queries, not for running custom code or housing binaries. Cloud Scheduler could be useful in triggering the data processing, but it doesn't solve the issue of hosting and processing large files in memory.

Option B is also not apt as Dataflow is primarily used for streaming and batch data processing via complex data pipelines. It is used to create, schedule, and manage data processing jobs, but it is not designed to host an external set of binaries or run them directly. Additionally, the migration would require significant effort, which goes against the "minimal effort" requirement.

Option C is not an ideal choice because Cloud Run is designed for hosting and running containerized applications. It would require effort in containerizing the on-premises binaries, which goes against the minimal effort requirement. Moreover, the given scenario of processing large data files for a fixed duration does not fit well with the serverless nature of Cloud Run, which is meant for stateless request-response style applications.

Being a data analyst at a retail company, to optimize resources, minimize costs, and migrate the application to Google Cloud with minimal effort, it is advisable to opt for option D - Lifting and shifting the binaries to a VM in Compute Engine and using instance scheduling to start and stop the instance as needed.

Solution to Question 29: D

The correct answer is D. Enable the Node Auto-Upgrades feature for your GKE cluster.

Explanation: As a DevOps engineer, your main goal is to maintain a stable and consistently updated Kubernetes environment on the Google Kubernetes Engine (GKE). Enabling the Node Auto-Upgrades feature for your GKE cluster ensures that your Kubernetes nodes are automatically upgraded to the latest stable and supported Kubernetes version as per the cluster's release channel. This helps you keep your environment up-to-date with security patches and feature enhancements, which is essential for running a stable Kubernetes environment.

Reasons why the other options are not appropriate:

A. Enabling the "Network Policy" feature for your GKE cluster - Network policies are useful for controlling traffic between Kubernetes components, but they don't guarantee that you will run a consistently updated and supported version of Kubernetes.

B. Selecting the "Autoscaling" option for your GKE cluster - Autoscaling helps in managing the scaling of your Kubernetes resources by adding or removing nodes from the cluster based on current demand. While it's a valuable feature for efficiently managing resources, it has no direct influence on ensuring that your Kubernetes environment consistently runs a supported and stable version.

C. Using "Ubuntu" as a node image for your GKE cluster - The choice of node image impacts the operating system running on your Kubernetes nodes, but it does not guarantee that your GKE cluster will always have the latest supported and stable version of Kubernetes. Although the node image is important, it doesn't directly influence the Kubernetes version being used.

Solution to Question 30: D

The correct answer is D.

Creating an alert in Cloud Monitoring when the percentage of high priority CPU utilization reaches 65% is the best approach to enhance performance in the least possible time while adhering to Google's best practices for service configuration. If you exceed this threshold, adding nodes to your instance will help distribute the load among the nodes, improving overall system performance. This approach ensures that you are monitoring and optimizing your database system in real-time.

Option A is not the best choice because simply rewriting queries to optimize their resource usage is insufficient in itself. While it can help alleviate some CPU usage, it doesn't take into account the need to scale the database infrastructure to handle increasing loads, which is crucial for maintaining optimal query performance.

Option B is not optimal as it recommends increasing the number of nodes in the Cloud Spanner instance by 50% without monitoring the CPU utilization. This approach might cause over-provisioning or under-provisioning, resulting in resource waste or insufficient performance improvements.

Option C is also not the best choice because setting an alert at 45% of high priority CPU utilization might lead to premature node addition, resulting in possible resource overprovisioning and increased costs. Monitoring the CPU utilization at 65% strikes a better balance, allowing for more accurate scaling decisions.

Solution to Question 31: D

The correct answer is D: Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

Explanation:

Option A is incorrect because it uses AAAA records instead of CNAME records. AAAA records are used to map a domain to an IPv6 address. In this case, we need to use CNAME records to create aliases for the primary domain (mydomain.com) which already points to the Google Cloud Load Balancer's IP address.

Option B is incorrect because it uses A records to point WWW and HOME instead of CNAME records. While A records can map a domain to an IPv4

address, it is better to use CNAME records for aliases because it requires less DNS maintenance if the IP address of the load balancer changes.

Option C is incorrect because it uses an SOA record instead of an A record. SOA (Start of Authority) records are used to declare the authoritative DNS server for a particular domain, not to point a domain to an IP address or another domain.

Option D is correct because it starts with creating an A record, which maps the primary domain (mydomain.com) to the ip-address of your Google Cloud load balancer. After that, it creates two CNAME records for the subdomains, WWW and HOME, to point to the primary domain. This ensures that all three domains (mydomain.com, www.mydomain.com, and home.mydomain.com) will resolve to the same IP address of the Google Cloud load balancer. Additionally, using CNAME records for the subdomains simplifies DNS management, as only the A record needs to be updated if the IP address of the load balancer changes.

Solution to Question 32: B

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

Explanation: Option B is the best choice since it adheres to the Google-recommended practices for managing sensitive data like database passwords. By storing the password in a Kubernetes Secret object, it will be encrypted at rest and only accessible to authorized users or applications. Modifying the YAML file ensures the population of the environment variable from the Secret, decoupling sensitive information from code.

Option A is not suitable as it involves storing the database password in the Compute Engine instance metadata, which is a less secure method compared to using a Secret object. Moreover, startup scripts can become unmanageable in complex systems.

Option C is not ideal because it stores the database password in a Kubernetes persistent volume, which is primarily designed for storing application data, not sensitive information. Using a persistent volume claim to mount the volume adds unnecessary complexity and may be less secure than using a Secret object.

Option D is not recommended as it suggests storing the database password inside the Docker image of the container. This exposes sensitive information to everyone who has access to the image and makes updating the password more difficult, as it requires rebuilding and redeploying the container. It also violates the principle of separating code from sensitive data.

Solution to Question 33: C

The correct answer is C: Create a managed instance group. Set the Autohealing health check to healthy (HTTP).

Explanation:

Creating a managed instance group (MIG) is the correct way to configure autohealing for network load balancing on Compute Engine instances operating in multiple zones. MIGs have several benefits over unmanaged instance groups, including automatic instance management, such as creation, autohealing, and deletion, as needed. The autohealing health check monitors the instances to determine if they are unresponsive and, if needed, will re-create them when they fail the health check.

In this specific scenario, you should set the Autohealing health check to healthy (HTTP), which means that it will monitor the HTTP traffic of the instances. If an instance does not respond to 3 consecutive checks (10 seconds each), the autohealing feature will trigger a re-creation of that unresponsive VM.

Now let's take a look at the other options and why they are not suitable:

A: Creating an HTTP load balancer with a backend configuration that references an existing instance group, defining a balancing mode and setting the maximum RPS to 10, would not address the autohealing requirement of the question. The emphasis here is on load balancing traffic rather than ensuring the instances are healthy and autohealing when required.

B: Creating an HTTP load balancer with a backend configuration that references an existing instance group and setting the health check to healthy (HTTP) will help monitor instances' health, but it will not take care of autohealing them when they fail the health check. This approach focuses on forwarding traffic to healthy instances but does not address the autohealing requirement.

D: Creating an HTTP(S) load balancer with a backend configuration that references an existing instance group and setting the health check to healthy (TCP) will again help monitor instances' health, but only at the transport layer and not with HTTP traffic specifically. Like option B, it will not take care of autohealing unresponsive VMs when they fail the health check, making it an unsuitable solution for the given task.

Solution to Question 34: A

The correct answer is A: Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs. This is because following Google-recommended practices for managing service revisions involves slowly rolling out changes and monitoring for any issues to minimize potential negative impact on customers. By gradually rolling out the revision and splitting traffic, you give yourself the flexibility to identify issues and rollback to a previous revision if needed, ensuring minimal disruption to your users.

B: Enabling Cloud Scheduler to perform periodic health checks on the new revision and reroute traffic to the old revision if issues are detected is not the best approach. While Cloud Scheduler can be useful in triggering periodic tasks, it is not designed specifically for managing deployment revisions or traffic allocation. On the other hand, Cloud Run provides built-in traffic splitting and rollback features that are more suitable for this purpose.

C: Creating multiple Cloud Run staging environments for testing before deploying to production is a good practice for catching bugs and issues before they impact end-users. However, maintaining the same traffic allocation across these environments will not minimize the risk associated with introducing a new revision to the production environment. Gradual rollout and splitting traffic, as mentioned in option A, would be a better approach.

D: Deploying your application to a second Cloud Run service and asking your customers to use the second Cloud Run service is not an appropriate solution. This approach places the burden on your customers to switch to the new service and can introduce unnecessary complexity and potential downtime. Furthermore, it does not follow Google-recommended practices for managing revisions to a service. The best approach is to use traffic splitting and gradual rollout, as described in option A.

Solution to Question 35: D

The correct answer is D.

Option D: Using the command "gcloud config set container/cluster dev" ensures that by default, your future CLI commands will address the 'dev' GKE cluster. By setting this configuration within the gcloud CLI, you are indicating the default cluster to be used for operations related to Google Kubernetes Engine, making it easier and more efficient to manage resources within this specific cluster.

Option A: Creating a file called gke.settings in the ~/.google folder that contains the cluster name is an incorrect approach. Gcloud CLI configurations are not stored in this way, and it won't serve the purpose of setting a default configuration for GKE.

Option B: The command "gcloud config set project/cluster dev" is incorrect because it attempts to set the configuration related to the project when, in fact, we need to set the configuration related to the GKE cluster. Using this command will result in an error.

Option C: Using the command "gcloud container clusters update dev" is not the right choice because this command is meant to update an existing cluster's properties, not to set it as the default cluster for gcloud CLI commands. This command will not help establish the correct default configuration for managing the GKE cluster.

In conclusion, the correct action to take is to use the command "gcloud config set container/cluster dev", as stated in option D. This ensures that future CLI commands will be executed against the 'dev' GKE cluster by default, making resource management more efficient for the DevOps engineer.

Solution to Question 36: B

The correct answer is B: Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations

Explanation: Creating a folder containing all the dev projects and then creating an organization policy to restrict resources to US locations would effectively enforce the desired limitation. Organization policies offer a powerful way to centrally manage and enforce constraints on resources in the Google Cloud platform. By establishing such a policy, you can ensure that any resource created in the projects within that folder will adhere to the location restriction set by the policy.

Why other options will not work:

A) Creating an IAM policy to restrict the resources locations in all dev projects and applying the policy to all dev roles would not be as effective. IAM policies control who has access to what resources, rather than governing the location of the creation of resources. So, while you can use IAM policies to grant different access levels to users, they are not designed to enforce restrictions on resource locations.

B) Creating a VPC network in US regions and restricting all dev projects to use only that network will not limit the creation of resources in other regions. VPC networks are a virtual version of a physical network, and although they help provide network connectivity among resources, they do not control resource creation restrictions based on location. Developers could still create resources outside of the US even if they are connected to a VPC network in a US region.

C) Configuring Cloud Monitoring to alert the organization if resources are created outside of the US and setting up manual deletion for those resources is not a proactive approach. Rather than enforcing restrictions, this option only allows you to react to resources created outside the desired boundaries, leading to additional manual work. It also carries the risk of human error in processing the alerts and the potential for associated delays.

Solution to Question 37: C

The correct answer is C: Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Explanation: Setting up Cloud VPN between your on-premises infrastructure and Google Cloud allows you to securely connect your on-premises network to your Google Cloud VPC network. This will enable workloads on Google Cloud and on-premises machines to securely communicate using their private IP addresses.

Why the other options will not work:

A. In Google Cloud, configure the VPC as a host for Shared VPC: Shared VPC is used to share one VPC network across multiple projects within an organization, not with on-premises networks. This option would not enable communication with on-premises machines using private IP addresses.

B. Configure Firewall rules only on the on-premises environment to allow all traffic between both networks: Configuring firewall rules on the on-premises environment alone wouldn't be enough to establish a secure and private connection between the on-premises machines and Google Cloud. A private connection like VPN is needed to securely transfer data between both environments.

D. Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses: Bastion hosts are used to access private instances through a public instance, but they don't ensure direct and private communication between on-premises and Google Cloud workloads. Public IP addresses usually don't provide the same level of security as a private connection like VPN. Therefore, relying on bastion hosts with public IP addresses doesn't meet the security requirements for healthcare workloads.

Solution to Question 38: D

The correct answer is D, and here's why:

A. Create a Cloud Filestore with 32 GB of storage and use it as the cache for the reverse proxy.

This option is not ideal because Cloud Filestore is a managed file storage service for applications that require a file system interface and shared access to the file system. It is intended for use with applications like content management systems, websites with static content, or shared file systems. It is not designed for in-memory caching and is not the most efficient solution for a latency-sensitive website.

B. Run it on Compute Engine, choose the instance type n1-standard-1, and add an SSD persistent disk of 32 GB.

n1-standard-1 instance type has only 3.75 GB of memory, which will not suffice to meet the 30 GB in-memory cache requirement plus an additional 2 GB for other processes. This option will, therefore, not work for the given scenario.

C. Create a Cloud Datastore with 32 GB of storage and utilize Cloud Datastore for caching.

Cloud Datastore is a NoSQL database service for web and mobile applications that need to store and manage non-relational data. While it can be used for caching, it is not the most optimal solution for a latency-sensitive website that requires an in-memory cache. Additionally, Cloud Datastore does not provide the same performance as an in-memory caching solution like Redis.

D. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

This is the best option for managing a latency-sensitive website within the given requirements. Cloud Memorystore for Redis is a managed in-memory data store service built on the popular open-source Redis. It provides fast and scalable caching to minimize latency, and it fully manages the service for

you, eliminating the need for manual administration. With a 32-GB capacity instance, it meets the required memory specifications and provides an efficient, cost-effective solution.

Solution to Question 39: D

The correct answer is D, and here's why:

Option A is incorrect because it introduces unnecessary complexity by adding a Compute Engine instance as an intermediary between the Cloud Pub/Sub topic and the Cloud Run application. This goes against the principle of reducing components and maintaining simplicity in a system.

Option B is also not the best approach, as Cloud IoT Core is specifically designed for managing and communicating with IoT devices, rather than simply subscribing to a Cloud Pub/Sub topic and pushing messages to Cloud Run applications. Using Cloud IoT Core in this scenario would not follow Google-recommended practices and could lead to inefficiencies or added complexity.

Option C might seem reasonable, but it mandates a pull-based approach for fetching messages from the Cloud Pub/Sub subscription. Cloud Run is designed to work with push-based messaging, which enables better scaling and resource management. Additionally, this option doesn't mention creating a service account and giving it the Cloud Run Invoker role.

Option D is the most suitable method as it adheres to the Google-recommended best practices. It involves creating a dedicated service account, granting the appropriate Cloud Run Invoker role, and using the push-based messaging system for processing messages from the Cloud Pub/Sub topic. This approach ensures proper authentication, authorization, and efficient processing of the messages in the Cloud Run application.

Solution to Question 40: A

The answer should be A: Cloud Spanner.

Here's why each option is either the correct choice or not ideal in this scenario:

A. Cloud Spanner: Cloud Spanner is a fully managed, horizontally scalable, relational database service that provides strong consistency across rows, regions, and continents. It automatically handles replication and load balancing, making it a perfect choice for an application that will be used by customers worldwide and whose user growth is unpredictable. With minimal configuration changes, it ensures proper scaling and high availability. It is also fully ACID (Atomicity, Consistency, Isolation, Durability) compliant, which is important for managing customer relations.

B. Cloud Memorystore: Cloud Memorystore is a fully managed, in-memory data store service built on the popular Redis. Although it is suitable for caching, it is not appropriate for the main storage solution required by the application, especially considering the need for worldwide access. Additionally, it is not

designed to provide horizontal scaling and global distribution like Cloud Spanner. Thus, this option is not ideal for the given scenario.

C. Cloud Bigtable: Cloud Bigtable is a fully managed, NoSQL, wide-column database service that provides high throughput and low latency at any scale. It is designed for real-time analytics and high-write-volume workloads, but it lacks strong consistency guarantees for multi-row transactions in comparison to Cloud Spanner. This means that Cloud Bigtable may not be suitable for managing customer relations that require strong multi-row consistency guarantees, making it less suitable for the given scenario.

D. Cloud Datastore: Cloud Datastore is a fully managed, schemaless, NoSQL database service for building highly scalable applications. Although it offers high throughput and consistency, it does not provide fully global relational consistency like Cloud Spanner. Cloud Datastore is built for web and mobile apps that require highly available, flexible, and consistent storage but does not cater to the horizontal scalability and strong relational consistency guarantees required in this scenario as effectively as Cloud Spanner.

In conclusion, Cloud Spanner is the best choice for a storage solution in this scenario due to its ability to guarantee proper scaling with minimal configuration changes, strong consistency across rows, regions, and continents, global replication, and ACID compliance, making it the optimal solution for managing customer relations in an application used by customers worldwide.

Solution to Question 41: C

The correct answer is C, and here's why:

Option A is incorrect because verifying that you are the "Billing Account Creator" role is not enough. Additionally, assigning marketing department users to the new Billing Account without creating a new project will not enable them to use and manage Google Cloud services for their initiative.

Option B is incorrect because having the "Project Creator" IAM role does not give you the required permissions to manage billing. Also, sharing the billing account with other projects is not the right approach; it is essential to create a dedicated Billing Account for the Marketing department's initiative to manage costs separately.

Option C is the correct answer. Firstly, you need to verify that you have the "Billing Administrator" IAM role for your organization's Google Cloud Project for the Marketing department. This role gives you the appropriate permissions to manage billing. Then, you should link the new project to a Marketing Billing Account, ensuring that the billing process is tailored to the Marketing department's needs and keeping their usage separate from other departments.

Option D is incorrect because having the "Organization Administrator" IAM role is not sufficient to manage billing for a specific project. Additionally, assigning quotas and manually calculating billing based on resource usage is not the

recommended method, as Google Cloud has built-in billing management tools to make this process more efficient and accurate.

In conclusion, the best approach to set up billing for the Marketing department's new initiative is to have the Billing Administrator IAM role and link the new project to a dedicated Marketing Billing Account (Option C).

Solution to Question 42: B

The correct answer should be B: Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

Reasoning for choosing B: Since the application is writing logs to disk, installing and configuring the Cloud Logging Agent will enable you to view and analyze the logs from Cloud Logging. This process will streamline log management, aggregation, and analysis, helping you to diagnose and resolve the reported errors more quickly.

Reasons for discarding other options:

A. Connect to the instance using Cloud Identity-Aware Proxy (IAP) and view the application logs: Cloud IAP is a service that secures your application running on Google Cloud, but it doesn't provide a log management solution. Even though you can connect to the instance and view logs directly, it's not the optimal way of managing logs within Google Cloud.

C. Enable Stackdriver Trace to trace and analyze application logs: Stackdriver Trace is used to analyze the performance of applications by visualizing traces. However, it is not designed to manage and analyze logs that are written to disk, which is what the question's scenario is about.

D. Navigate to Cloud Logging and view the application logs: Simply navigating to Cloud Logging will not allow you to view the logs written to disk without first installing and configuring the Cloud Logging Agent. Thus, option B is required to ensure that the logs are aggregated and viewable within Cloud Logging.

Solution to Question 43: B

The correct answer is B: Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

Explanation: Option B is the best solution because it ensures that the Data Analytics department can access and query the latest data in BigQuery while adhering to the principle of least privilege. By assigning the BigQuery User role to the Google Group containing the BI team members, you are granting them the necessary permissions to execute queries on the data. The access can be managed easily by adding or removing members from the group, ensuring security and compliance with company policies.

Option A is not ideal because configuring the BI team's API keys with read and write access does not adhere to the principle of least privilege. This configura-

tion would grant the team broader access than necessary, potentially leading to unintended changes or exposing sensitive data.

Option C is not suitable because creating a service account with the BigQuery Data Transfer Service role is primarily for transferring data between locations and is not focused on granting access to execute queries. Additionally, sharing the private key with the BI team introduces security risks and makes it difficult to manage access control.

Option D is not a practical solution because using Cloud Composer to schedule a daily workflow for synchronizing BigQuery data with an internal database does not provide real-time access to the latest data as it arrives. This approach would add unnecessary complexity to the project and would not satisfy the department's need for continuous access to the most recent data for custom SQL queries.

Solution to Question 44: B

The correct answer is B. Coldline Storage, as it is best suited for storing critical backup files for disaster recovery purposes in compliance with Google's best practices. Coldline Storage is a cost-effective, reliable, and long-term storage option designed for data that can be stored for a minimum of 90 days. It provides fast response times and durable storage, making it perfect for disaster recovery and backup scenarios.

Here's why the other options are not suitable:

A. Bigtable is not an ideal choice for critical backup files in this context. Bigtable is a managed NoSQL database service designed for handling large amounts of structured, semi-structured, and unstructured data. While it may be suitable for certain use cases that require high-performance data storage and retrieval, it is not primarily focused on long-term backup and disaster recovery.

C. Archive Storage is another cost-effective storage class that offers long-term storage. However, it is designed for data that can be stored for a minimum of 365 days and has a higher retrieval time - up to several hours. While it may be suitable for some archival purposes, it is not the optimal choice for disaster recovery scenarios where quick data retrieval is necessary.

D. Filestore is a fully managed, network-attached storage system that is designed for applications that require shared file systems. It provides a high-performance, low-latency file system that can be accessed by multiple applications. However, Filestore is not specifically designed for long-term backup storage and as such, is not the best option for storing critical backup files in compliance with Google's best practices.

In conclusion, Coldline Storage is the most suitable option for storing critical backup files for disaster recovery in a large corporation, as it offers the necessary balance between cost-effectiveness, reliability, and accessibility required in this context.

Solution to Question 45: B

The correct answer is B. Use the command gcloud projects get-iam-policy to view the current role assignments.

Explanation:

Option B is the correct choice because the gcloud projects get-iam-policy command enables you to view the Identity and Access Management (IAM) policy for a Google Cloud Platform project. This command will list the current role assignments, including the Project Owner role, which is what you want to inspect.

Option A is not correct because the VPC Network Peering page focuses on Virtual Private Cloud (VPC) network configurations, not project role assignments or permissions.

Option C is not correct because Cloud Identity Groups settings are used to manage group membership and permissions, but the most appropriate step to directly view role assignments, including the Project Owner role, is to use the gcloud command specified in option B.

Option D is not correct because checking for stored SSH keys deals with Secure Shell (SSH) authentication for Compute Engine instances, not with project role assignments or permissions.

Solution to Question 46: C

The answer should be C: Configure regional storage for the region closest to the users. Configure a Standard storage class.

Explanation:

Option A is not optimal because it suggests configuring multi-regional storage, which is more expensive than regional storage. Multi-regional storage is typically suited for data that is frequently accessed from around the world. However, in this case, our focus is on a tech company based in Boston, MA. Therefore, configuring regional storage would be more cost-effective for this company.

Option B is not the best choice because it suggests configuring a Nearline storage class, which is designed for infrequent access to data storage. As the question mentions that this is a mission-critical analytics pipeline with constant use, the Nearline storage class would actually increase costs due to higher access fees for frequent use.

Option C is the correct answer because it recommends configuring regional storage, which focuses on storing data in a specific region. This option reduces the cost compared to multi-regional storage while still ensuring that data is stored close to the users for efficient access. Additionally, it suggests a Standard storage class which is designed for providing low-latency and high-throughput performance at a balanced cost. This makes it ideal for this analytics pipeline application that needs continuous access.

Option D is not a suitable choice because it suggests a multi-regional storage class, which increases costs for a company based in a specific location. Additionally, it also uses Nearline storage class, which is not optimal for frequently accessed data, as mentioned earlier.

Thus, considering the need for low-latency, high-throughput performance, and continuous access to the data stored in Cloud Storage, Option C offers the most cost-effective and efficient configuration for the tech company's analytics pipeline.

Solution to Question 47: C

The correct answer is C: Create a private zone on Cloud DNS, and configure the applications with the DNS name.

The reason why option C is the best answer is because it allows you to set up a private DNS zone in Google Cloud that is only accessible to your VPC and applications within it. By creating a private zone in Cloud DNS, you can map the on-premises database server's IP address to a DNS name. This way, all applications can use that DNS name instead of the IP address. If the IP address of the database server changes, you only need to update the DNS record instead of having to reconfigure each application individually.

Option A would not be effective because storing the IP address in a Cloud Storage bucket would not automatically update the applications when the IP of the database server changes. In addition, retrieving the IP from a storage bucket would add unnecessary latency to the application's connection to the database.

Option B is not suitable because, even though configuring a static public IP address for the database server in your on-premises network could make the IP address less likely to change, it would not prevent the need for IP configuration changes in all applications if it did change. Furthermore, exposing an on-premises database with a public IP brings with it potential security risks.

Option D is incorrect because creating an external Cloud DNS zone would make the DNS records publicly accessible, which is unnecessary for an internal database connection and could potentially lead to security risks. The private zone in Cloud DNS, as mentioned in option C, would be the proper choice for this scenario.

Solution to Question 48: C

The correct answer is C: Enable API, create a workspace under project A, and then add projects B and C. This is because, by doing this, you will create a unified monitoring space where all three projects' performance metrics will be visible in a single location, giving a better overview for analyzing and comparing the performance data.

Here's why the other options will not work:

A: Firebase Performance Monitoring is used to monitor user-centric performance for mobile applications. This is not suitable for monitoring CPU, memory, and disk usage of Google Cloud projects. Therefore, using Firebase Performance Monitoring will not help in achieving the objective mentioned in the question.

B: Using the default dashboards can provide useful insights into the performance of individual projects, but they do not provide a unified view for monitoring multiple projects at the same time. So the objective of having a single view for all projects cannot be achieved without creating a workspace and adding all the projects to it as stated in option C.

D: Enabling BigQuery API and exporting metrics data to BigQuery could potentially provide an avenue for detailed analysis of performance metrics, but this method would require extra effort in setting up queries, managing exported data, and creating visualization tools. This method also lacks real-time monitoring, making it less practical than the solution provided by option C where you simply need to create a workspace and add projects to have a live, unified monitoring view.

Solution to Question 49: A

The most cost-effective method to accomplish this task is option A, and here's why:

Option A details a direct method to export logs specifically from Compute Engine instances to the BigQuery dataset using Cloud Logging. By creating a filter that only targets Compute Engine logs, and then using the Create Export feature with BigQuery as the sink service and the platform-logs dataset as the sink destination, you minimize the cost of transferring logs, because you are only dealing with relevant logs directly. The Cloud Logging agent is already installed, which makes this process even more efficient.

Option B is not suitable because updating the metadata and giving the Data Editor role to the service accounts will not be enough to accomplish the task. Exporting logs to BigQuery needs to be configured either via Cloud Logging or other mechanisms. The metadata update proposed won't trigger the transfer on its own.

Option C introduces additional complexity and costs. By using Cloud Pub/Sub and Cloud Functions, multiple services are added to the process, thus increasing costs in terms of data transfer, data storage for the Pub/Sub topic, and executing Cloud Functions. This approach is not justified when there's a straightforward solution available in Cloud Logging.

Option D requires modifying instances' startup scripts and utilizing the `bq` command-line tool to send logs directly to the BigQuery dataset. This method demands more maintenance, configuration efforts, and computing resources for every instance, which may lead to increased costs and potential discrepancies in the logging process. Also, granting the Data Editor role to service accounts for

manual logs insertion is tedious and less efficient compared to utilizing Cloud Logging.

In conclusion, option A is the most cost-effective method as it directly exports only the relevant logs to the BigQuery dataset using Cloud Logging, without introducing unnecessary complexity or additional costs.

Solution to Question 50: B

The correct answer is B: SSL Proxy Load Balancer.

Explanation for choosing B: SSL Proxy Load Balancer is specifically designed for handling SSL-encrypted TCP traffic (which is your main concern as mentioned in the question). It operates at the transport layer (Layer 4), enabling it to minimize latency by effectively distributing incoming SSL traffic among backend services and instances. An SSL Proxy Load Balancer provides built-in SSL offloading, letting your backend instances focus on processing requests instead of handling SSL termination - which reduces overall latency.

Why other options will not work: A. Cloud VPN Load Balancer: This option is not suitable for your requirement since its primary function is to provide consistent availability and performance for VPN connections. It doesn't deal specifically with SSL-encrypted TCP traffic, and its focus on VPN traffic means it's not optimized for preventing latency in SSL traffic scenarios like your use case.

C. HTTPS Load Balancer: While the HTTPS Load Balancer does provide load balancing for encrypted traffic, it operates at the application layer (Layer 7). This means it inspects the contents of the incoming request to make routing decisions, adding an additional layer of processing that can increase latency compared to Layer 4 SSL Proxy Load Balancer.

D. NAT Gateway Load Balancer: A NAT Gateway Load Balancer primarily deals with translating private IP addresses in the network to public ones for traffic destined to the internet or external networks. Its focus is on IP address translation, which is unrelated to your requirement of minimizing latency for SSL-encrypted TCP traffic on port 443.

Practice Exam 11

Question 1: You are working as a security manager in a tech company and are responsible for the monthly security review of your organization's Google Cloud environment. During your routine check, you need to identify who has access to view the data stored in the company's Google Cloud Project. What should be your next step?

A. Enable Audit Logs for all APIs that are related to data storage.

B. Enable the Security Command Center for the project.

C. Review the IAM permissions for any role that allows for data access.

D. Check the Access Transparency Logs for unusual activities.

Question 2: In your software development company, you are in charge of migrating the continuous integration and delivery (CI/CD) pipeline to Compute Engine instances for a more efficient cloud infrastructure management. What steps should be taken to guarantee the pipeline's proper permissions while maintaining adherence to security best practices?

A. • Create multiple service accounts, one for each pipeline with the appropriate minimal Identity and Access Management (IAM) permissions. • Use a secret manager service to store the key files of the service accounts. • Allow the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline.

B. Grant full project level permissions to the service account attached to the Compute Engine instances.

C. • Attach a single service account to the compute instances. • Add all required Identity and Access Management (IAM) permissions to this service account to create, update, or delete resources.

D. Use API keys for authentication on compute instances.

Question 3: You are working as a DevOps engineer in a software development company, and you have recently deployed an application on a Compute Engine instance. Your company has hired an external consultant who needs to access the Linux-based instance for maintenance purposes. The consultant is connected to your company's network via a VPN connection but does not have a Google account. How should you grant the consultant access to the instance?

A. Instruct the external consultant to use the gcloud compute ssh command line tool by using Identity-Aware Proxy to access the instance.

B. Instruct the external consultant to generate an SSH key pair, and request the public key from the consultant. Add the public key to the instance yourself, and have the consultant access the instance through SSH with their private key.

C. Use Google Cloud IAM to create a temporary service account and provide the consultant with the JSON key file to access the instance.

D. Instruct the external consultant to generate an SSH key pair, and request the private key from the consultant. Add the private key to the instance yourself, and have the consultant access the instance through SSH with their public key.

Question 4: As a software engineer in a large tech company, you are assigned to set up a new Jenkins server for your development team's upcoming project. Your manager insists on deploying the server as quickly and efficiently as possible. What is the most suitable approach for accomplishing this task?

A. Try deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service.

B. Use GCP Marketplace to launch the Jenkins solution.

C. Create a Jenkins instance using Cloud Functions.

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

Question 5: As a software engineer at a fast-growing tech company, you are working on a new application consisting of various microservices. You have been tasked with deploying the application to Google Kubernetes Engine (GKE) in a way that supports automatic scaling as more applications are added in the future, minimizing manual intervention for each deployment. What strategy should you adopt to achieve this?

A. Use Google Cloud Run instead of GKE and create multiple replicas of the application to provide automatic scaling.

B. Create a custom GKE cluster without autoscaling and manually add nodes when needed.

C. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

D. Deploy the application on GKE and add both a HorizontalPodAutoscaler and VerticalPodAutoscaler to cover all scaling possibilities.

Question 6: You are working in a software development company, and you recently installed the Google Cloud CLI on your office workstation and set up the proxy configuration. However, you want to ensure that your proxy credentials do not get recorded in the gcloud CLI logs to maintain security. How can you prevent your proxy credentials from being logged?

A. Create a .gcloudignore file in your home directory, and add the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD property names to it.

B. Encrypt your proxy credentials using asymmetric encryption and set them in the gcloud CLI by using gcloud config set proxy/username and gcloud config set proxy/password commands.

C. Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

D. Use the base64 encoding for your username and password, then configure them using gcloud config set proxy/username and gcloud config set proxy/password commands.

Question 7: You are working as an IT specialist for a radiology clinic that keeps its medical imaging data in an on-premises server. The clinic wants to utilize Cloud Storage for archiving these images and requires an automated method to upload new medical images to Cloud Storage. How should you design and implement this solution?

A. Create a Compute Engine instance with the gsutil command line tool installed, and use it to manually copy the medical images from the on-premises storage to Cloud Storage.

B. Use Cloud Functions with the Cloud Storage trigger to automatically transfer medical images from on-premises storage to Cloud Storage.

C. Create a Data Fusion pipeline to transfer medical images from the on-premises storage to Cloud Storage on a scheduled interval.

D. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

Question 8: You are a software engineer at a tech company responsible for developing a crucial application that requires deployment on a Kubernetes cluster. This application is critical to the company's core business functions and needs to be optimized for reliability. In order to follow Google-recommended practices for provisioning a Kubernetes cluster, what should you do?

A. Create a zonal GKE standard cluster. Enroll the cluster in the stable release channel.

B. Create a regional GKE standard cluster. Enroll the cluster in the stable release channel.

C. Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

D. Create a GKE Autopilot cluster. Enroll the cluster in the preview release channel.

Question 9: As the lead software engineer for a fast-growing video streaming company, you need to host your video encoding software on Compute Engine. The user base is rapidly expanding, and they require uninterrupted access to encoding services without any CPU limitations. It's crucial to ensure the high availability of your encoding solution and adhere to Google-recommended practices for automating operations. What is the best course of action?

A. Deploy your solution using Cloud Run services without autoscaling, and monitor CPU utilization using Cloud Monitoring.

B. Deploy your solution to an instance group, and increase the number of available instances whenever you see high CPU utilization in Cloud Monitoring.

C. Deploy your solution on multiple standalone Compute Engine instances, and replace existing instances with high-CPU instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

D. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

Question 10: You work as a data engineer for a multinational company that specializes in IoT-enabled products, serving millions of customers worldwide. The company is building a data lake on Google Cloud to analyze and manage the data generated by its IoT devices. To meet the high demand and ensure a robust architecture following best practices, which approach should you adopt when handling structured and unstructured data from the IoT devices?

A. Stream data to IoT Core, and use Cloud Functions to send data to Bigtable.

B. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

C. Stream data to Pub/Sub, and use Storage Transfer Service to send data to Firestore.

D. Stream data to Cloud Pub/Sub, and use Dataflow to send data to Cloud SQL.

Question 11: As a software engineer working in a company that uses Google Cloud Platform, you are asked to permanently delete a Pub/Sub topic managed by Config Connector in your company's Google Cloud project. What is the recommended approach to accomplish this task?

A. Use kubectl to delete the topic resource.

B. Use Firebase CLI to delete the topic resource.

C. Use kubectl to create a new topic with the same name to replace the old one.

D. Use kubectl to rename the topic resource.

Question 12: As an IT manager at a tech company, you have recently overseen the acquisition of a startup and are now responsible for merging the IT systems of both companies. The startup has a production Google Cloud project within their organization, which needs to be transferred to your organization and billed accordingly. What is the most efficient method to accomplish this task?

A. Create a VPC Network Peering between the startup's Google Cloud project and your organization's project, then configure Billing Export to send billing data from the startup's project to your organization's project.

B. Create a Private Catalog for the Google Cloud Marketplace, and upload the resources of the startup's production project to the Catalog. Share the Catalog with your organization, and deploy the resources in your company's project.

C. Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

D. Create Kubernetes manifests for all resources in the project, deploy them to a Kubernetes cluster in your organization, and then delete the project from the startup's Google Cloud organization.

Question 13: You are working as a Cloud Solutions Architect at a software company that wants to implement a particular content management system (CMS) on Google Cloud in a fast and simple way. What method should you use for deploying and installing it?

A. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

B. Deploy the CMS to a Firebase hosting environment, then manually configure the solution using the Cloud Functions.

C. Deploy the CMS solution using Kubernetes Engine and manually configure the solution using the YAML files.

D. Create a custom VM image with the CMS pre-installed, then deploy the image to a new Compute Engine instance.

Question 14: As a Cloud Architect at an e-commerce company, you have developed a solution on Google Cloud that incorporates multiple Google Cloud products. Your manager has assigned you to estimate the monthly total cost of the solution. What approach should you take to provide this cost estimation?

A. Check customer testimonials or case studies and use their cost estimates as a base for your solution's monthly costs.

B. Estimate the costs by conducting a blind test among different team members and averaging their guesses, without using the pricing calculator.

C. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Use Cloud Monitoring to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

D. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

Question 15: You've recently joined a tech company and are responsible for managing their resources on Google Cloud. You've installed the Google Cloud CLI on your office computer and need to review all the current instances running on Google Cloud. What steps should you take before executing the gcloud compute instances list command?

A. Run gcloud compute instances create to create a new instance before listing existing instances.

B. Check that your system environment variables include GOOGLE_APPLICATION_CREDENTIALS.

C. Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI.

D. Enable the required APIs by running gcloud services enable compute.googleapis.com.

Question 16: As a software engineer working in a tech company, you need to grant access to an external team member so they can view compute images and disks in one of your ongoing projects while adhering to Google's recommended practices. How should you provide the required permissions to this individual?

A. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

B. Create a custom role, and add all the required compute.disks.list permissions as includedPermissions. Grant the custom role to the user at the organization level.

C. Grant the Project Viewer role without including the required compute.images.list and compute.disks.list permissions at the project level.

D. Create a custom role based on the Compute Storage Admin role. Exclude unnecessary permissions from the custom role. Grant the custom role to the user at the project level.

Question 17: As a software engineer at a leading technology company, you need to deploy an application in Google Cloud using serverless technology and test a new version with a small percentage of production traffic. How should you proceed?

A. Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

B. Deploy the application to Google Kubernetes Engine. Use Anthos Service Mesh for traffic splitting.

C. Deploy the application to Bigtable. Use data replication for traffic splitting.

D. Deploy the application to Cloud Functions. Specify the version number in the function's name.

Question 18: As an IT specialist in a tech company, you have been assigned to set up application performance monitoring for three projects (A, B, and C) on Google Cloud, providing a single overview for CPU, memory, and disk usage. What action should you take to accomplish this task?

A. Create a custom Cloud Functions service to gather metrics data from projects A, B, and C.

B. Create separate monitoring dashboards for each project and switch between them.

C. Enable API, create a workspace under project A, and then add projects B and C.

D. Set up Google Kubernetes Engine for projects A, B, and C with a single dashboard.

Question 19: As a financial analyst for an e-commerce company, you're tasked with monitoring multiple projects that are connected to a single billing account in Google Cloud. The company requires custom metrics and dynamic calculations based on unique company criteria to visualize costs effectively. To automate this process, which approach should you take?

A. Manually download the billing data in JSON format, and create a custom visualization using Google Data Studio.

B. Use Stackdriver Monitoring to create custom cost metrics for the projects and visualize them in the Google Cloud console.

C. In the Google Cloud console, use the export functionality of the Cost table. Create a Looker Studio dashboard on top of the CSV export.

D. Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery export.

Question 20: As a database administrator at a tech company, you've set up an instance of SQL Server 2017 on Compute Engine to evaluate its features for potential implementation. To efficiently connect to this instance, what should you do?

A. Create a VPN tunnel between your desktop and the GCP environment. Verify that a firewall rule for port 3389 exists. Use your existing RDP client to connect to the SQL Server instance using the internal IP address.

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

C. Enable Windows authentication in the GCP Console. Verify that a firewall rule for port 3389 exists. Click the RDP button in the GCP Console and select "Connect using Windows Authentication".

D. Set a Windows username and password in the GCP Console. Verify that a firewall rule for port 5900 exists. Click the VNC button in the GCP Console, and supply the credentials to log in.

Question 21: As a database administrator at a tech company, you maintain an application that relies on Cloud Spanner to store the current state of user information. In addition, user-triggered events are logged in Cloud Bigtable,

and daily backups of Cloud Spanner data are exported to Cloud Storage. An analyst from your team requests that you join data from Cloud Spanner and Cloud Bigtable for specific users in the most efficient way possible. How should you accomplish this task?

A. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

B. Create a Cloud Dataproc cluster that runs a Spark job to extract data from Cloud Bigtable and Cloud Storage for specific users.

C. Create a Cloud Functions trigger to automatically copy specific data from Cloud Spanner to Cloud Bigtable whenever a backup occurs.

D. Create a temporary table in Cloud Spanner to store Cloud Bigtable data for specific users, then query the data using SQL queries.

Question 22: As an IT manager at a software development company, you oversee two projects: proj-sa, which handles service accounts, and proj-vm, which runs virtual machines. You need to enable a service account from proj-sa to take snapshots of VMs in proj-vm. What action should you take?

A. Enable Google Cloud Storage JSON API in proj-vm and use the proj-sa service account JSON key for authentication.

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

C. Use the Google Cloud SDK to create a service account key and add it to the VM's boot disk.

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

Question 23: As a lead engineer in a software development company, you manage a Google Kubernetes Engine (GKE) cluster utilized by a team of data scientists who occasionally require GPUs for running long-duration, non-restartable jobs. Your goal is to minimize expenses without impacting their work. What approach should you take?

A. Create a node pool with preemptible VMs and GPUs attached to those VMs.

B. Enable Cluster Autoscaler on the existing GKE cluster without adding GPU-enabled VMs.

C. Enable node auto-provisioning on the GKE cluster.

D. Create a VerticalPodAutoscaler for those workloads.

Question 24: As a technical team lead working at a software development company, you're responsible for managing access provisioning for Google Cloud users in your organization. Recently, your company acquired a smaller startup

that has its own Google Cloud organization. To ensure your Site Reliability Engineers (SREs) have the same project permissions in the acquired startup's organization as in your own organization, what steps should you take?

A. Use the gcloud iam roles copy command, and provide the project IDs of all projects in the startup company's organization as the destination.

B. In the Google Cloud console for the startup company, select Create role from selection and choose source as the startup company's Google Cloud organization.

C. In the Google Cloud console for the startup company, copy the roles and permissions, then manually create custom roles in your organization's console.

D. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

Question 25: As a DevOps engineer at a software development company, you are given a Dockerfile to deploy on the company's Kubernetes Engine. What is the correct way to do this?

A. Create a docker image from the Dockerfile and upload it to Cloud SQL. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

B. Use gcloud app deploy .

C. Create a docker image from the Dockerfile and upload it to Bigtable. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

D. Create a docker image from the Dockerfile and upload it to Container Registry. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

Question 26: You're working in a technology-focused company that has built a brand new application which is essential for their business operations. This application needs to be deployed on Kubernetes while ensuring maximum reliability. In order to provision a Kubernetes cluster, you want to adhere to Google's recommended guidelines. What action is the most appropriate to take?

A. Create a GKE standard cluster with no availability preference. Enroll the cluster in the stable release channel.

B. Create a regional GKE standard cluster. Enroll the cluster in the rapid release channel.

C. Create a GKE Autopilot cluster without enrolling in any specific release channel.

D. Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

Question 27: You are working for a tech company and have been assigned a project that consists of a single Virtual Private Cloud (VPC) and a single subnetwork in the us-central1 region. There is a Compute Engine instance hosting an application in this subnetwork. Your task is to deploy a new instance in the same project in the europe-west1 region, which requires access to the application. Following Google-recommended practices, what steps should you take?

A. 1. Create a subnetwork in the same VPC, in europe-west1. 2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

B. 1. Create a subnetwork in the same VPC, in europe-west1. 2. Use Cloud VPN to connect the two subnetworks. 3. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

C. Create a VPC and a subnetwork in europe-west1. Configure VPC peering between the two VPCs. Create the new instance in the new subnetwork and use the first instance's public address as the endpoint.

D. Create a subnetwork in the same VPC, in europe-west1. Use Cloud Interconnect to connect the two subnetworks. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

Question 28: You are working as a cloud specialist for a company that runs their applications on Compute Engine VM instances within a custom Virtual Private Cloud (VPC). The company's security policies require only the use of internal IP addresses on VM instances and prohibit connecting to the internet. To comply with these policies, you need to configure the application to access a file hosted in a Cloud Storage bucket within your project. How should you proceed?

A. Deploy a Cloud NAT instance and route the traffic to the dedicated IP address of the Cloud Storage bucket.

B. Enable Private Google Access on the subnet within the custom VPC.

C. Set up a Cloud Storage FUSE mount on the VM instances to access the Cloud Storage bucket.

D. Create a VPN tunnel between Compute Engine VMs and Cloud Storage bucket.

Question 29: As a cybersecurity analyst at a financial services company, you are tasked with granting an external auditor the necessary access to review your company's Google Cloud Platform (GCP) Audit Logs and Data Access logs. How should you proceed in assigning the appropriate Cloud Identity and Access Management (Cloud IAM) role to the auditor?

A. Assign the auditor the IAM role roles/logging.privateLogViewer and roles/pubsub.editor. Perform the export of logs to Cloud Storage.

B. Assign the auditor's IAM user to a custom role that has logging.logEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

C. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

D. Assign the auditor's IAM user to a custom role with the permission monitoring.logsWriter. Perform the export of logs to Cloud Storage.

Question 30: As an IT professional working in the software development industry, you are tasked with migrating your company's continuous integration and delivery (CI/CD) pipeline to Compute Engine instances. This pipeline will be responsible for managing the entire cloud infrastructure using code. How can you ensure the pipeline has appropriate permissions while adhering to security best practices within your organization?

A. Create individual user accounts for each pipeline and use them for respective infrastructure provisioning.

B. Grant full project level permissions to the service account attached to the Compute Engine instances.

C. Use Application Default Credentials for accessing resources, without setting any specific IAM permissions.

D. • Create multiple service accounts, one for each pipeline with the appropriate minimal Identity and Access Management (IAM) permissions. • Use a secret manager service to store the key files of the service accounts. • Allow the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline.

Question 31: As a Database Administrator at a large tech company, you are responsible for managing a Cloud Spanner instance to ensure optimal query performance in your production environment. Your instance currently operates in a single Google Cloud region, and you need to enhance its performance quickly while adhering to Google's best practices for service configuration. What is the most suitable course of action to take in this situation?

A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 55%. If you exceed this threshold, add nodes to your instance.

B. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

C. Increase the percentage of high priority CPU utilization threshold to 85% and create an alert in Cloud Monitoring to check for performance degradation.

D. Migrate your Cloud Spanner instance to a multi-region configuration and create an alert in Cloud Monitoring to alert when the percentage of high priority

CPU utilization reaches 65%.

Question 32: You are working as a project manager in a tech company and have been tasked with managing a GCP project. Your goal is to delegate control to your team members so that they can efficiently manage buckets and files in Cloud Storage while adhering to Google-recommended practices. Which IAM roles should you assign to your colleagues?

A. Storage Admin

B. Storage Object Admin

C. Bigtable Admin

D. API Gateway Admin

Question 33: As a leading software development company in the industry, you must maintain strict access control to your Google Cloud projects. To enable your Site Reliability Engineers (SREs) to approve requests from the Google Cloud support team whenever an SRE opens a support case, while adhering to Google-recommended practices, what should you do?

A. Add your SREs to roles/storage.admin role.

B. Add your SREs to a group and then add this group to roles/iam.roleAdmin.role.

C. Add your SREs to a group and then add this group to roles/cloudfunctions.admin role.

D. Add your SREs to a group and then add this group to roles/accessapproval.approver role.

Question 34: You are working as a cloud engineer for a startup company operating in one geographic location and require a cost-effective solution for managing relational data on Google Cloud Platform. The system must support a small set of operational data and point-in-time recovery. Which configuration should you choose?

A. Select Firestore (Native Mode). Set up your instance as multi-regional.

B. Select Cloud Datastore. Set up your instance with 2 nodes.

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

D. Select Bigtable. Create a backup schedule for your operations.

Question 35: As a project manager for a tech company's Business Intelligence department, you are given the responsibility of enabling the team to run custom SQL queries against the most recent data ingested into BigQuery via a data pipeline through streaming. How can you accomplish this?

A. Create a Data Studio dashboard that uses the related BigQuery tables as a source and give the BI team view access to the Data Studio dashboard.

B. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

C. Grant the BI team access to Cloud Pub/Sub to receive real-time data updates from the data pipeline, without querying BigQuery.

D. Configure the BI team's API keys to have read and write access to BigQuery, allowing them to query and analyze data.

Question 36: As a software engineer at a tech company, you've developed an application that's been packaged into a Docker image. Now, you need to deploy the Docker image as a workload on Google Kubernetes Engine. What's the right approach to accomplish this task?

A. Upload the image to Container Registry and create a Kubernetes StatefulSet referencing the image.

B. Upload the image to Container Registry and create a Kubernetes DaemonSet referencing the image.

C. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image.

D. Upload the image to Cloud Storage and create a Kubernetes StatefulSet referencing the image.

Question 37: You are working as a system administrator in a tech company. The company uses a single sign-on (SSO) identity provider compatible with Security Assertion Markup Language (SAML) integration for service providers. You have users in Cloud Identity, and you want to enable them to authenticate via your company's SSO provider. What step should you take to achieve this?

A. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Web Server Applications.

B. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps.

C. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

D. Enable the G Suite Domain-Wide Delegation feature in Cloud Identity to use your company's SSO provider.

Question 38: As a project manager in a software development company, you are responsible for selecting and configuring compute resources for a set of batch processing jobs that are key to your daily operations. The jobs take around 2 hours to complete and are run every night. Your goal is to minimize service costs while effectively managing these jobs. What should you do?

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

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

C. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types.

D. Select Cloud Functions with maximum memory allocation.

Question 39: As a data recovery specialist working in a technology company, you are responsible for securely storing application backup files using Cloud Storage following Google's recommended practices. What storage option should be employed for effective disaster recovery management?

A. Coldline Storage

B. Persistent Disk

C. Local SSD

D. Datastore

Question 40: You are working at a company as a Data Analyst and are using Looker Studio to visualize a table from your company's data warehouse that is built on Google BigQuery. Data is appended during the day, and at night, the daily summary is recalculated by overwriting the table. You recently noticed that the charts in Looker Studio are not displaying correctly, and you need to investigate the issue. What should you do?

A. Use the BigQuery interface to review the nightly job and look for any errors.

B. Check the performance of the Data Transfer Service for any delays in data replication.

C. Check the Stackdriver Monitoring dashboard for any issues related to Looker Studio.

D. Inspect the data warehouse's schema in the BigQuery console to identify any inconsistencies.

Question 41: As a cybersecurity specialist working in a company that utilizes Linux instances on Google Cloud, you are tasked with implementing a method that ensures your team can securely and cost-effectively log in to these instances. What is the most suitable approach to achieve this?

A. Use a third party tool to provide remote access to the instances.

B. Use Google Cloud VPN to connect directly to the instances and use SSH over VPN connection.

C. Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

D. Create a bastion host with public internet access. Create the SSH tunnel to the instance through the bastion host.

Question 42: You are working as a software engineer at a creative design company, overseeing the deployment of multiple microservices in a Kubernetes Engine cluster. The cluster includes a microservice responsible for rendering images, which requires more CPU time than memory. The other microservices in the cluster are optimized for n1-standard machine types. In order to ensure optimal resource usage across all workloads, what steps should be taken?

A. Assign the pods of the image rendering microservice a higher pod priority than the other microservices.

B. Deploy the image rendering microservice on App Engine Flexible Environment while keeping the other microservices on Kubernetes Engine.

C. Configure the required amount of CPU and memory in the resource requests specification of the image rendering microservice deployment. Keep the resource requests for the other microservices at the default.

D. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Question 43: At your company in the retail industry, you utilize Google Cloud Platform for your data warehousing needs through BigQuery. Your data science team has high turnover and consists of only a few members who require access to perform queries. In order to adhere to Google's recommended practices, what steps should you take?

A. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery machineLearningDeveloper user role to the group.

B. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery jobUser role to the group.

C. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery dataEditor user role to the group.

D. 1. Create an IAM entry for each data scientist's user account. 2. Assign the BigQuery user role to the group.

Question 44: As a network administrator at a software development company, you have an Apache web server running on a Compute Engine instance, along with other applications in the Google Cloud project. You need to receive an email notification when the egress network costs associated with the server surpass 100 dollars for the current month. How should you accomplish this task?

A. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the

Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

B. Configure a Google Cloud Monitoring agent on the Apache web server and create a custom dashboard in Monitoring to track egress network costs. Set an hourly reminder to manually review the dashboard and send an email if costs exceed 100 dollars for the current month.

C. Use the Cloud Logging Agent to export the Apache web server logs to Cloud Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Cloud Logging for the current month and sends an email if the size of all HTTP responses, multiplied by current Google Cloud egress prices, totals over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

D. Create an App Engine application that retrieves the billing data via the Cloud Billing API, calculates egress costs for the Apache web server, and sends an email if costs exceed 100 dollars for the current month. Set up a cron job to run the application hourly.

Question 45: You're working as a cloud engineer in a software development company and have recently deployed an App Engine application using gcloud app deploy. However, the application did not deploy to the intended project. To determine why this happened and where the application was deployed, what should you do?

A. Go to Deployment Manager and review settings for deployment of applications.

B. Check the Google Cloud SDK installation on your computer for proper configuration.

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

D. Review logs in the App Engine dashboard in Google Cloud Console to check any deployment issues.

Question 46: You are working as a data engineer in a large e-commerce company, and your team utilizes a data warehouse on BigQuery. A partner company specializing in AI solutions is offering to improve your business's product recommendations using their sophisticated engine, which relies on the data stored in your data warehouse. Both companies operate on Google Cloud, with each managing resources in separate projects. To facilitate the integration of the recommendation engine, the partner company needs access to your BigQuery dataset. How can you provide them the necessary access?

A. Create a Service Account in your own project, and ask the partner to grant this Service Account access to Cloud Functions in their project.

B. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

C. Ask the partner to create a Service Account in their project, and have them give the Service Account access to Compute Engine in their project.

D. Ask the partner to create a Service Account in their project, and have them give the Service Account access to Cloud Storage in their project.

Question 47: You are working as a data engineer for a company that relies heavily on efficient data storage and management. The company needs you to quickly upload a 32 GB single file to a Nearline Storage bucket. In your company, you have access to an exclusive WAN connection rated at 1 Gbps. Your goal is to utilize the maximum possible capacity of the 1 Gbps to expedite the file transfer process. How should you proceed with the file upload?

A. Enable parallel composite uploads using gsutil on the file transfer.

B. Upload the file using Google Cloud Pub/Sub streaming.

C. Run multiple instances of gsutil in parallel without using composite uploads.

D. Disable resumable uploads in gsutil.

Question 48: As a data analyst at a large corporation, you are responsible for managing the company's data warehousing using BigQuery. The organization has grown significantly, with over 1,000 datasets created by various business units across multiple projects. The CIO has tasked you with identifying any tables containing an employee_ssn column across all these datasets, while minimizing the effort required for this task. How should you proceed in order to efficiently locate the information required?

A. Write a shell script that uses the bq command line tool to loop through all the projects in your organization.

B. Create a Pub/Sub topic and configure Data Catalog to send all the dataset metadata updates to this topic, then filter the messages to find those containing employee_ssn.

C. Write a Cloud Run service that accepts dataset information, scans for employee_ssn column, and automatically respond with the results to find desired tables.

D. Go to Data Catalog and search for employee_ssn in the search box.

Question 49: You are working as a cloud consultant at a financial firm, which requires the storage of audit log files for a period of 3 years across their hundreds of Google Cloud projects. Your task is to devise a cost-effective strategy for log file retention. What would be the best approach to achieve this in your company?

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

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

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

D. Export logs to Cloud Pub/Sub and utilize Cloud Dataflow pipeline to store logs in Cloud Bigtable.

Question 50: You are working as a network engineer in a technology company and have been assigned the task of ensuring secure and robust VPN connectivity between a new Virtual Private Cloud (VPC) and a remote site in your organization. The key requirements for this project include dynamic routing, a shared address space of 10.19.0.1/22, and no overprovisioning of tunnels during a failover event. In order to implement a high availability Cloud VPN setup that adheres to Google-recommended practices, what steps should you take?

A. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/active routing with Cloud NAT.

B. Use an automatic mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

C. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

D. Use an automatic mode VPC network, configure static routes, and use active/active routing.

Practice Exam 11 Solutions

Solution to Question 1: C

The correct answer is C. Review the IAM permissions for any role that allows for data access.

Here's why other options will not work:

A. Enable Audit Logs for all APIs that are related to data storage - Audit logs help in monitoring how resources and services are being accessed in your Google Cloud environment. Although they provide valuable insights into individual API calls, they do not directly identify who has access to view the data stored in the company's Google Cloud Project. Thus, enabling Audit logs will not fulfill the requirement of identifying who has access to view the data.

B. Enable the Security Command Center for the project - The Security Command Center is a tool for monitoring and managing security risks and vulnerabilities in your Google Cloud environment. While it helps to provide an overview of an organization's security posture, it does not directly identify specific user permissions or roles for data access.

D. Check the Access Transparency Logs for unusual activities - Access Transparency Logs provide information about the actions taken by Google personnel on user data and system configurations. They do not directly provide insight into the users and roles within the organization that have access to view data in the Google Cloud Project.

Therefore, reviewing the IAM permissions for any role that allows for data access (Option C) is the best way to identify who has access to view the data stored in the company's Google Cloud Project. IAM (Identity and Access Management) allows for configuring access control for resources, services, and applications. By reviewing the permissions assigned to different roles, you can determine who has access to view the data in the project.

Solution to Question 2: A

The correct answer is A for the following reasons:

1. Creating multiple service accounts for each pipeline with minimal IAM permissions adheres to the principle of least privilege. By ensuring that each service account only has the necessary permissions to carry out specific tasks, you reduce the risk of unauthorized access and maintain a higher level of security.

2. Using a secret manager service to store key files of the service accounts adds an extra layer of security and protection. By managing and centralizing secrets, it minimizes the risk of unauthorized access and simplifies the access management process.

3. Allowing the CI/CD pipeline to request appropriate secrets during the execution of the pipeline ensures that access is granted only when needed, further following the principle of least privilege and improving security.

Option B is incorrect because granting full project-level permissions to the service account increases the potential for unauthorized access. It fails to adhere to the principle of least privilege and is a violation of security best practices.

Option C is incorrect because using a single service account for all compute instances with a broad scope of permissions will not follow the principle of least privilege. This approach can lead to a higher risk of unauthorized access due to the elevated permissions, making it less secure.

Option D is incorrect because API keys are not suitable for authentication and authorization in this scenario. API keys can be easily leaked and do not provide the fine-grained access control required for managing a CI/CD pipeline's permissions according to security best practices.

Solution to Question 3: B

The correct answer is B, and here's why:

Option B suggests instructing the external consultant to generate an SSH key pair, and providing you with their public key. You will then add this public key to the Compute Engine instance, granting the consultant secure access through SSH with their private key. This method is ideal because it doesn't require the consultant to have a Google account, and it follows the best security practices of using SSH key pairs for authentication purposes.

Option A, on the other hand, would require the external consultant to use the gcloud compute ssh command line tool with Identity-Aware Proxy (IAP). However, using IAP typically requires the user to have a Google account, which the external consultant does not have in this scenario. Therefore, this option is not viable.

Option C suggests using Google Cloud IAM to create a temporary service account and providing the consultant with the JSON key file. However, this method is less secure because it provides the consultant with broader access to resources, rather than the specific access required in this case.

Option D incorrectly suggests requesting the private key from the consultant and adding it to the instance yourself. This goes against SSH best practices, as private keys should never be shared. Additionally, this option would require the consultant to use their public key for authentication, which is not how SSH key pairs work.

In conclusion, the best option for granting the external consultant access to the Compute Engine instance is option B, as it adheres to recommended security practices and doesn't require the consultant to have a Google account.

Solution to Question 4: B

The correct answer is B. Use GCP Marketplace to launch the Jenkins solution.

Here's why:

Option A: Deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service is not the most suitable approach because IAP is primarily used for authentication and securing access to applications deployed on GCP rather than deployment itself. Setting up Jenkins with IAP would be an additional step after deploying Jenkins.

Option B: Using GCP Marketplace to launch the Jenkins solution is the most efficient and fastest approach. GCP Marketplace offers a pre-configured Jenkins solution that can be deployed with just a few clicks on the Google Cloud Platform infrastructure. This allows you to set up a new Jenkins server quickly and efficiently, meeting your manager's requirements.

Option C: Creating a Jenkins instance using Cloud Functions is an inappropriate choice as Jenkins is not a light-weight, stateless serverless application. Jenkins requires a fixed and continuous runtime environment, and it is not suitable for running on Cloud Functions, which are designed for stateless, event-driven applications.

Option D: Downloading and deploying the Jenkins Java WAR to App Engine Standard is not the most suitable approach. App Engine Standard is designed for scalable web applications and has several limitations making it suboptimal for hosting Jenkins. Some features required by Jenkins, such as write access to the local filesystem and dynamic scaling based on resources, are not supported on App Engine Standard.

In conclusion, B is the most suitable approach for quickly and efficiently deploying a new Jenkins server for your development team's upcoming project. GCP Marketplace provides a fast and easy way to deploy pre-configured solutions, saving time and effort.

Solution to Question 5: C

The correct answer is C: Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

Option A is not suitable as it suggests using Google Cloud Run instead of GKE, which is not the given requirement. Cloud Run is a serverless platform for running stateless containers, while GKE is a managed Kubernetes service that allows you to run, manage, and orchestrate containerized workloads. Cloud Run is more suited for individual stateless services rather than the deployment of an entire application consisting of various microservices.

Option B is impractical because you are trying to minimize manual intervention. Creating a custom GKE cluster without autoscaling would require manual monitoring and scaling efforts, which defeats the purpose of finding an automated solution.

Option C is the best choice for the given requirements, as it allows you to create a GKE cluster with autoscaling enabled on the node pool. This means the cluster will automatically scale up or down based on the workload demand and the specified scaling thresholds (minimum and maximum node pool sizes). With autoscaling enabled, you can ensure that your application can handle increasing workloads without requiring manual intervention every time.

Option D is incorrect because it suggests using both HorizontalPodAutoscaler (HPA) and VerticalPodAutoscaler (VPA) to scale the application. While it's true that HPA and VPA can help manage scaling in different ways, using both simultaneously can cause instability and unpredictable scaling behaviors. Furthermore, it's not guaranteed that adding both autoscalers will minimize manual intervention and is not required for the basic scenario presented in the question.

In conclusion, creating a GKE cluster with autoscaling enabled on the node pool (Option C) is the most appropriate choice, as it addresses the requirements of automatic scaling and minimizing manual intervention while deploying an application consisting of various microservices.

Solution to Question 6: C

The correct answer is C: Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

This is the best solution because when you set the proxy credentials using environment variables, they do not get logged by the gcloud CLI, thus maintaining the security of your proxy credentials. The environment variables are only available during the CLI session; once the session is closed, the credentials are no longer available, reducing the risk of being exposed in logs.

Option A: Creating a .gcloudignore file in your home directory and adding CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD property names to it will not help. The .gcloudignore file is used to specify files and directories that should not be uploaded to Google Cloud Storage during deployment, not to prevent specific values from being logged.

Option B: Encrypting your proxy credentials using asymmetric encryption might protect the credentials themselves. However, this method does not prevent the gcloud CLI from logging the encrypted version of the values, and it can be cumbersome to implement encryption and decryption on the user side during each session.

Option D: Using base64 encoding might obfuscate the username and password values. Still, base64 encoding is not a secure mechanism to protect credentials as it can be easily reversed, and it does not address the fundamental problem of preventing credentials from being logged by the gcloud CLI.

Solution to Question 7: D

The correct answer is D: Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

Explanation:

Option D is the most efficient and automated method to achieve the goal of uploading new medical images to Cloud Storage. The gsutil command line tool is designed specifically for such tasks, allowing you to synchronize data between local storage and Cloud Storage efficiently. By scheduling the script as a cron job, you ensure that the process runs automatically at a defined interval, thus meeting the clinic's requirements.

Why other options will not work:

Option A: Manually copying the medical images to Cloud Storage using a Compute Engine instance is inefficient, prone to human error, and does not meet the requirement of automation.

Option B: Cloud Functions with Cloud Storage triggers are typically used for responding to events within Cloud Storage, not for transferring data from on-premises storage. Additionally, this approach would require additional development and might not efficiently handle the large size of medical imaging data.

Option C: Creating a Data Fusion pipeline would involve unnecessary complexity for this task. Data Fusion is designed for data integration and transformation tasks, whereas the clinic's requirement is more straightforward - transferring medical images from on-premises storage to Cloud Storage. Moreover, Data Fusion might not be the most efficient or cost-effective solution in this scenario.

Solution to Question 8: C

The correct answer is C: Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

Explanation:

C: Creating a GKE Autopilot cluster ensures a high level of reliability, as it automatically manages the maintenance, scaling, and upgrading of nodes, making it more suitable for business-critical applications than standard clusters. Enrolling in the stable release channel provides access to well-tested, stable versions of Kubernetes to maintain system stability and avoid any potential issues encountered in less stable versions.

A: While creating a zonal GKE standard cluster and enrolling it in the stable release channel provides some degree of reliability, it does not offer the same benefits as an Autopilot cluster. A zonal cluster is limited to a single zone, which increases the chance of disruption due to outages or maintenance.

B: Creating a regional GKE standard cluster provides better availability compared to a zonal cluster. However, standard clusters still require manual management and maintenance. They do not optimize for reliability as well as GKE

Autopilot clusters, which automatically handle node management, scaling, and upgrading.

D: Although creating a GKE Autopilot cluster provides optimized reliability, enrolling it in the preview release channel is not a Google-recommended practice for mission-critical applications. Preview releases may contain experimental features and are not guaranteed to be as stable or reliable as those in the stable release channel. This option increases the risk of disruption and negatively impacts the reliability of the application.

Solution to Question 9: D

The best course of action is D. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization. This option is ideal for ensuring high availability, performance, and adhering to Google-recommended best practices for automating operations. An instance group with autoscaling based on CPU utilization ensures that the solution scales up or down automatically based on computing requirements and helps maintain maximum efficiency and performance.

Option A is not ideal because deploying your solution using Cloud Run services without autoscaling may limit your ability to handle a rapidly growing user base. Monitoring CPU utilization with Cloud Monitoring alone is not sufficient to maintain high availability, as you would need to manually intervene to adjust CPU resources.

Option B would work, but it might not be as efficient as D. While deploying your solution to an instance group allows for high availability, manually increasing the number of available instances in response to high CPU utilization, instead of using autoscaling, may lead to slower adjustments to resource needs, resulting in inconsistent user experience and inefficient resource allocation.

Option C is not recommended as it can lead to increased manual intervention and management overhead. Deploying your solution on multiple standalone Compute Engine instances makes it difficult to manage instance states, and replacing instances with high-CPU instances may lead to unnecessary downtime and manual maintenance.

In conclusion, option D, deploying your solution to an instance group and setting autoscaling based on CPU utilization, is the most efficient andGoogle-recommended way to ensure high availability and performance for your rapidly expanding user base while minimizing manual intervention for better resource allocation and user experience.

Solution to Question 10: B

The correct answer is B. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

Explanation:

Answer B is the best approach for handling both structured and unstructured data from IoT devices in a scalable and efficient way. Google Cloud Pub/Sub is a messaging service that allows you to send messages between independent systems. It's ideal for ingesting and delivering event-driven data generated by IoT devices. Dataflow is a fully managed, serverless service for deploying and managing data processing pipelines, making it suitable for transforming and processing the data. Cloud Storage is a highly durable, cost-effective, and versatile storage service that can store both structured and unstructured data, making it suitable for the data lake requirements.

In contrast, other options are not suitable for this scenario:

Option A: Using IoT Core and Cloud Functions to send data to Bigtable is not ideal, as Bigtable is primarily designed for handling structured data, not unstructured data. Therefore, it's not suitable for a data lake that requires storing varied data types.

Option C: Streaming data to Pub/Sub and using Storage Transfer Service to send data to Firestore is not suitable because Firestore is a NoSQL database designed for web and mobile applications. It's not optimized for large-scale analytics and is not the right choice for a data lake.

Option D: Streaming data to Cloud Pub/Sub and using Dataflow to send data to Cloud SQL is not the best choice, as Cloud SQL is a relational database service designed for structured data. It doesn't handle unstructured data efficiently, and it's not optimized for data lake storage.

Therefore, Option B (streaming data to Pub/Sub and using Dataflow to send data to Cloud Storage) is the best approach for a robust architecture aimed at handling structured and unstructured data from IoT devices.

Solution to Question 11: A

The correct answer is A. Use kubectl to delete the topic resource.

Explanation for A: As a software engineer using Google Cloud Platform, you will most likely be using Kubernetes for the management and deployment of containerized applications on your cloud infrastructure. Config Connector is a Kubernetes add-on that extends Kubernetes API to include Google Cloud Platform (GCP) resources, allowing you to manage GCP resources with the same Kubernetes tools and workflows. Therefore, using kubectl to delete the topic resource would be the recommended approach, as it removes the Pub/Sub topic managed by Config Connector within your company's Google Cloud project.

Reasons why other options will not work:

B. Use Firebase CLI to delete the topic resource: Firebase CLI is a tool designed for managing Firebase projects, which include services like real-time databases, HTTP requests, and storage. Although Firebase is a part of the Google Cloud Platform, it is not the correct tool for managing resources managed by Con-

fig Connector. Kubernetes kubectl tool should be used for managing Config Connector resources.

C. Use kubectl to create a new topic with the same name to replace the old one: This option will not permanently delete the existing Pub/Sub topic, instead, it would only create a new topic with the same name. Therefore, it does not address the requirement of permanently deleting the topic.

D. Use kubectl to rename the topic resource: Renaming a topic resource does not delete it, so this option also does not meet the requirement of permanently deleting the Pub/Sub topic managed by Config Connector within the company's Google Cloud project.

Solution to Question 12: C

The correct answer is C.

Option C is the most efficient method to transfer the IT systems of the acquired startup to your organization. The projects.move method allows you to move an entire Google Cloud project to another organization, including all the resources, configurations, and settings. After transferring the project using this method, you can then update the billing account of the project, ensuring that all the bills will be directed to your organization's account. This process is streamlined and ensures seamless integration of the startup's IT systems into your organization.

Option A is not an appropriate solution because VPC Network Peering simply connects the networks of the two projects, without actually transferring the resources from the startup's project to your organization's project. Additionally, configuring the Billing Export to send billing data from the startup's project to your organization's project does not make the startup project part of your organization.

Option B is also not a suitable solution because creating a Private Catalog for the Google Cloud Marketplace involves uploading the resources of the startup's production project to the Catalog and then sharing the Catalog with your organization. This process does not merge the IT systems but rather creates a copy of startup's resources, causing redundancy and increasing maintenance complexity.

Option D is not an appropriate solution because it involves creating Kubernetes manifests for all resources in the project and then deploying them to a Kubernetes cluster in your organization. This approach requires a significant amount of manual work to recreate and deploy the resources, and is not efficient for transferring a Google Cloud project between organizations. Furthermore, this process involves deleting the project from the startup's Google Cloud organization, which could cause a downtime for services and potential data loss.

In conclusion, the most efficient method to transfer the acquired startup's IT systems to your organization is by using the projects.move method (option C)

to move the project to your organization, and then updating the billing account of the project to that of your organization.

Solution to Question 13: A

The correct answer is A. Search for the CMS solution in Google Cloud Marketplace and deploy the solution directly from the Cloud Marketplace because this option provides a fast, simple, and efficient way to deploy and install the desired CMS. Google Cloud Marketplace offers ready-to-deploy solutions from third-party vendors, which are already optimized for integration with the Google Cloud ecosystem. This means that you don't have to worry about the technical details and manual configurations, resulting in a smooth and easy deployment experience.

Option B, deploying the CMS to a Firebase hosting environment and manually configuring it using the Cloud Functions, is not the fastest and simplest way to get a CMS up and running on Google Cloud. Firebase hosting is designed for hosting static websites and web applications. It would require additional effort to integrate with the CMS, which could be time-consuming and complex.

Option C, deploying the CMS solution using Kubernetes Engine and manually configuring the solution using the YAML files, is not the best choice for a fast and simple deployment process. It is a more complex method that requires a deep understanding of Kubernetes, which might not be necessary for a CMS deployment. Moreover, manual configurations increase the likelihood of potential mistakes and errors.

Option D, creating a custom VM image with the CMS pre-installed and then deploying the image to a new Compute Engine instance, is also not the most efficient way for deploying a CMS. This option could be suitable for more customized setups, but it adds a layer of complexity and additional steps to the process, making it less simple and more time-consuming than searching for the CMS solution in the Google Cloud Marketplace and deploying it directly.

Solution to Question 14: D

The correct approach for estimating the monthly total cost of a Google Cloud solution is option D: "For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product."

Option D is the most accurate and reliable way to estimate the costs as it considers each Google Cloud product's pricing details. The pricing calculator helps to combine the costs for all the products, providing a clear and comprehensive estimation of the monthly total cost.

Option A doesn't account for the specific architecture and usage patterns of your project. Costs might be different based on resource utilization, location, and other factors, making customer testimonials and case studies a poor benchmark to estimate your costs.

Option B lacks any basis in accurate data as it merely averages different team members' guesses. This method might result in highly inaccurate and unreliable cost estimations, as it doesn't consider actual prices or resource usage.

Option C only measures the costs of one week, which might not provide a complete representation of the monthly costs. It doesn't consider fluctuations in resource usage and won't provide a comprehensive understanding of long-term costs. Moreover, it won't factor in any discounts, sustained use, or other cost-saving measures that can impact monthly costs.

In conclusion, option D offers the most accurate and reliable cost estimation approach by considering the pricing details of each Google Cloud product in the solution and utilizing the pricing calculator to calculate the total monthly costs.

Solution to Question 15: C

The correct answer is C. To list the instances running on Google Cloud using the gcloud compute instances list command, you must ensure that you are authenticated and authorized to access your organization's resources. By running the gcloud auth login command, you are prompted to enter your Google Cloud login credentials in the dialog window. After successfully authenticating, you receive a login token which should be pasted into the gcloud CLI to grant access.

Option A is incorrect because creating a new instance is not related to viewing the existing instances. The command gcloud compute instances create is used to create new instances, not list them.

Option B is not correct because setting the GOOGLE_APPLICATION_CREDENTIALS environment variable is usually done when you need to authenticate using a service account. Although using a service account is a valid method of authentication, it is not the primary method for interactive authentication via the gcloud CLI.

Option D is incorrect because enabling the required APIs is not a prerequisite to listing instances using the gcloud compute instances list command. While API enablement is necessary for some tasks, this is not a required step before listing instances already running on the project.

Solution to Question 16: A

The best option is A. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

Explanation:

Option A provides the most precise and efficient way to grant the required permissions to the external team member, adhering to Google's recommended practices on the principle of least privilege. By creating a custom role with the needed permissions (compute.disks.list and compute.images.list) at the project

level, the external team member will have access to view the compute images and disks specifically in the ongoing project without granting additional unnecessary permissions.

Reasons why other options will not work:

Option B: Creating a custom role with only compute.disks.list permissions as includedPermissions will not cover the requirement of the external team member to view compute images. Also, granting it at the organization level is not recommended since it would give the external team member access to all projects within the organization, which is against the least privilege principle.

Option C: Granting the Project Viewer role without including the required compute.images.list and compute.disks.list permissions at the project level will not provide the necessary access for the external team member to view the compute images and disks as required.

Option D: Creating a custom role based on the Compute Storage Admin role would provide more permissions than needed by the external team member. Granting a role with unnecessary permissions goes against Google's recommended practices and the principle of least privilege. It can also pose a security risk, as it could allow the external team member to perform actions beyond their intended scope.

Solution to Question 17: A

The correct answer is A: Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

Explanation:

Option A is the correct choice because Cloud Run is a serverless technology offered by Google Cloud Platform that is designed to deploy and manage applications. It is built on top of containers, allowing flexibility in terms of the languages, frameworks, and dependencies you can use. One of the popular features of Cloud Run is gradual rollout, which enables you to split traffic between different versions of your application. This is perfect for testing a new version of an app with a small percentage of production traffic before rolling it out to all users.

Option B: Deploying the application to Google Kubernetes Engine (GKE) and using Anthos Service Mesh for traffic splitting isn't the best choice for two reasons. First, GKE is not serverless; it's a managed Kubernetes service that still requires infrastructure management, whereas the question specifically asks for a serverless option. Second, Anthos Service Mesh is more suited for managing traffic between microservices in a multi-cloud environment, not for traffic splitting between different versions of a single application, making it a less ideal choice in this scenario.

Option C: Deploying the application to Bigtable and using data replication for traffic splitting is incorrect because Bigtable is a NoSQL database solution

designed for storing large amounts of data, not for deploying applications. Additionally, data replication is not a method for splitting traffic between different versions of an application.

Option D: Deploying the application to Cloud Functions and specifying the version number in the function's name is also incorrect. Although Cloud Functions is a serverless technology, it does not provide a native feature for traffic splitting between different versions of an application. Simply specifying the version number in the function's name will not allow you to split traffic for testing purposes.

Solution to Question 18: C

The correct answer is C: Enable API, create a workspace under project A, and then add projects B and C.

Explanation:

Option A: Creating a custom Cloud Functions service to gather metrics data from projects A, B, and C, would add unnecessary complexity and maintenance overhead. Moreover, it would not take advantage of the built-in tools provided by Google Cloud for monitoring multiple projects.

Option B: Creating separate monitoring dashboards for each project would not fulfill the requirement of having a single overview for CPU, memory, and disk usage. This would only lead to multiple dashboards that need to be switched between to view the data, which can be cumbersome and inefficient.

Option C: Enabling API, creating a workspace under project A, and then adding projects B and C would be the proper approach. By creating a workspace, you can associate multiple projects to a single Google Cloud Monitoring dashboard. This will provide an integrated view of resource usage and monitoring data from all three projects, making it easier to monitor and manage the application's performance.

Option D: Setting up Google Kubernetes Engine for projects A, B, and C with a single dashboard will not directly help in monitoring application performance. While Google Kubernetes Engine is a powerful orchestration tool for containerized applications, it does not inherently provide the monitoring solution required in this scenario. The monitoring of CPU, memory, and disk usage needs to be addressed by Google Cloud Monitoring, and not by the Kubernetes Engine alone.

Therefore, the best action to accomplish the task of setting up application performance monitoring for the three projects on Google Cloud is option C: Enable API, create a workspace under project A, and then add projects B and C.

Solution to Question 19: D

The correct answer is D: "Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery

export."

This is the best approach because it automates the process of transferring billing data into a suitable data storage solution like BigQuery and enables the use of Looker Studio to create dynamic and customizable visualizations that meet the unique requirements of the company. BigQuery is a powerful and fully managed data warehouse that allows for fast and efficient querying, analysis, and management of data when coupled with Looker Studio for visualization.

Option A is not ideal because manually downloading billing data in JSON format and creating a custom visualization with Google Data Studio would require repetitive manual intervention and would be time-consuming. Google Data Studio is a good tool for creating visualizations but lacks the automated integration with billing data and advanced customization that is required in this scenario.

Option B is not suitable because Stackdriver Monitoring (now called Google Cloud Monitoring) is primarily focused on monitoring the performance of applications and infrastructure, but not billing details. Moreover, it cannot create custom cost metrics based on unique company criteria for multiple projects connected to a single billing account.

Option C is not the best choice because, even though Looker Studio is used for visualization, exporting the Cost table data as a CSV file in the Google Cloud console is a manual process. This approach doesn't offer the same level of automation, data integration, and advanced analysis capabilities provided by exporting the data to BigQuery.

In conclusion, the best approach for automating the process of monitoring multiple projects connected to a single billing account with custom metrics and dynamic calculations in an e-commerce company is to configure Cloud Billing data export to BigQuery and create a Looker Studio dashboard on top of the BigQuery export, which corresponds to option D.

Solution to Question 20: B

The correct answer is B because installing an RDP (Remote Desktop Protocol) client on your desktop allows you to establish a remote connection with the SQL Server 2017 instance running on the Compute Engine. Setting a Windows username and password in the Google Cloud Platform (GCP) Console ensures secure authentication, and using these credentials when logging into the instance will enable efficient and secure connection to the SQL Server.

Option A is incorrect because creating a VPN tunnel between your desktop and the GCP environment, although secure, is not related to efficiently connecting to the SQL Server instance. Additionally, verifying a firewall rule for port 3389 and using your existing RDP client with an internal IP address is not the most efficient and secure approach.

Option C is incorrect because enabling Windows authentication in the GCP Console doesn't provide a direct way to efficiently connect to the SQL Server.

Verifying a firewall rule for port 3389 is not directly related to connecting to the SQL Server instance, and the RDP button with "Connect using Windows Authentication" doesn't exist in the GCP Console.

Option D is incorrect because VNC (Virtual Network Computing) is not used for connecting to the SQL Server instances. Moreover, verifying a firewall rule for port 5900 provides no advantage since the port is not used by RDP.

Solution to Question 21: A

The correct answer is A. Create two separate BigQuery external tables on Cloud Storage and Cloud Bigtable. Use the BigQuery console to join these tables through user fields, and apply appropriate filters.

Here's why A is the best choice and the other options are not as efficient:

A. This option enables you to utilize the powerful querying and data joining capabilities of BigQuery to efficiently manage and retrieve data from Cloud Spanner and Cloud Bigtable. Both of these data sources can be read by BigQuery through external tables, allowing you to perform queries across both databases without the need for additional data preprocessing or manual data extraction.

B. Although Cloud Dataproc and Spark could potentially join data from Cloud Bigtable and Cloud Storage, this solution would require more setup and maintenance compared to using BigQuery. Additionally, it would not be as efficient because you would need to create a cluster and run complex Spark jobs to perform the required data processing.

C. This option focuses on copying data when backups occur, which may not be sufficient for real-time analysis or quick updates to user data. Furthermore, this could lead to redundant data storage in Cloud Bigtable, increasing storage costs. It also does not directly address how to join the data from Cloud Spanner and Cloud Bigtable in an efficient manner.

D. Creating a temporary table in Cloud Spanner to store Cloud Bigtable data might seem like a suitable solution at first, but it introduces unnecessary complexity and performance overhead. This method would involve copying data to a temporary table and running SQL queries on it, which would consume additional resources and might impact the performance of your existing Cloud Spanner database.

Therefore, option A is the most efficient and optimal solution to accomplish the task described in the question.

Solution to Question 22: D

The correct answer is option D, which states that you should grant the service account the IAM Role of Compute Storage Admin in the project called proj-vm. This is the appropriate action because it provides the service account from proj-sa with the required permissions to take snapshots of VMs in proj-vm, while

maintaining separation of roles and duties between the two projects.

Option A is incorrect because enabling Google Cloud Storage JSON API in proj-vm is not directly relevant to allowing a service account to take VM snapshots. Additionally, using the proj-sa service account JSON key for authentication does not automatically grant the required permissions.

Option B is incorrect because setting the service account's API scope for Compute Engine to read/write only affects the VM instances' access scope. This will not grant the necessary permissions for the service account from proj-sa to take snapshots of VMs in proj-vm.

Option C is incorrect because creating a service account key and adding it to the VM's boot disk does not give the service account the necessary permissions to take snapshots of VMs in proj-vm. Instead, it only allows you to use the service account key when accessing the Google Cloud SDK and APIs on the VM.

To summarize, by granting the service account the IAM Role of Compute Storage Admin in proj-vm (option D), you will ensure the service account has the necessary permissions to take snapshots of VMs without interfering with the projects' separation of roles and responsibilities.

Solution to Question 23: C

The correct answer is C. Enable node auto-provisioning on the GKE cluster.

Explanation: Enabling node auto-provisioning in the GKE cluster allows the cluster to automatically create and delete node pools as per the resource requests of the users' workloads. This ensures that the necessary resources, including GPUs, are available when required, without impacting the data scientists' work. Additionally, it minimizes expenses by not having under-utilized or idle resources.

Why other options will not work:

A. Create a node pool with preemptible VMs and GPUs attached to those VMs. While preemptible VMs with GPUs can offer cost savings, their nature of being terminated within 24 hours might affect the long-duration, non-restartable jobs that the data scientists require. In such cases, the solution would be unreliable and could disrupt their work.

B. Enable Cluster Autoscaler on the existing GKE cluster without adding GPU-enabled VMs. Enabling Cluster Autoscaler provides a way to automatically resize the number of nodes in a GKE cluster based on the workload requirements. However, if GPU-enabled VMs aren't added to the cluster, the data scientists' jobs requiring GPU resources will not be able to run optimally, or even at all.

D. Create a VerticalPodAutoscaler for those workloads. VerticalPodAutoscaler (VPA) is used for automatically adjusting the CPU and memory resources allocated to individual pod instances. Creating a VPA won't help in achieving

the purpose of minimizing expenses without impacting the data scientists' work because vertical scaling is not appropriate for changing the resources allocated to the nodes themselves, such as GPUs.

Solution to Question 24: D

The correct answer is D, and here's the explanation:

Option D: Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

This is the most efficient way to ensure that your SREs have the same project permissions in the acquired startup's organization, as this method will directly copy the permissions from your organization to the target organization. The gcloud iam roles copy command allows you to copy a custom role from a source organization to a destination organization, maintaining consistency in IAM roles across organizations.

Here's why other options will not work:

Option A: Use the gcloud iam roles copy command, and provide the project IDs of all projects in the startup company's organization as the destination.

This option is incorrect because providing only the project IDs would not ensure that the roles are copied to the entire organization. It would only copy the roles to specific projects, which is not the intended outcome.

Option B: In the Google Cloud console for the startup company, select Create role from selection and choose source as the startup company's Google Cloud organization.

This option is incorrect because it would require you to manually create the roles for each permission, which is time-consuming and error-prone. It does not provide an automated way to copy the roles from your organization to the startup company's organization.

Option C: In the Google Cloud console for the startup company, copy the roles and permissions, then manually create custom roles in your organization's console.

This option is incorrect because it suggests copying roles from the startup company's organization to your organization, which is the opposite of the intended outcome. The goal is to copy the roles from your organization to the startup company's organization. Moreover, this approach would involve manual role creation that may be prone to errors.

Solution to Question 25: D

The correct answer is D.

Option A is incorrect because Cloud SQL is a fully-managed database service, and Docker images are not stored in database services. Storing a Docker image in Cloud SQL would not be possible.

Option B is incorrect because the command `gcloud app deploy` is used to deploy applications on Google App Engine, which is a different service from Kubernetes Engine. Also, it does not deal with Dockerfiles directly.

Option C is incorrect because Bigtable is a NoSQL database service, not a platform for managing containerized applications. Similar to option A, storing a Docker image in Bigtable would not be possible.

Option D is the correct way to deploy the Dockerfile on the Kubernetes Engine. This is because:

1. Container Registry is a Google Cloud service for storing and managing Docker images, which is the purpose of the task.
2. Creating a Deployment YAML file is required to define the Kubernetes deployment object and its desired state, such as the Docker image and the number of replicas.
3. Using `kubectl` to create the deployment with the YAML file allows you to manage the entire lifecycle of the Kubernetes objects by interacting with the Kubernetes API.

Therefore, the correct approach is to create a Docker image from the Dockerfile, upload it to Container Registry, create a Deployment YAML file pointing to the stored image, and finally use `kubectl` to create the deployment based on the YAML file.

Solution to Question 26: D

The correct answer is D - to create a GKE Autopilot cluster and enroll the cluster in the stable release channel. Here's why:

A: Creating a GKE standard cluster without an availability preference doesn't fully ensure maximum reliability, as it might result in running everything in a single zone, which makes it vulnerable to zone outages. Enrolling in the stable release channel is appropriate, but the lack of availability preference makes this option suboptimal.

B: Creating a regional GKE standard cluster is a step in the right direction in terms of reliability because it spreads the cluster across multiple zones within a region. However, enrolling the cluster in the rapid release channel is not the best choice, as this channel typically includes newer features that may not be as stable, potentially introducing instability and reliability issues in a business-critical application.

C: Creating a GKE Autopilot cluster provides benefits like node management and auto-repair, thus increasing overall reliability. However, not enrolling in any specific release channel makes it difficult to guarantee stability, as it's unclear which features and updates are being used.

D: Creating a GKE Autopilot cluster and enrolling in the stable release channel is the most appropriate choice. GKE Autopilot simplifies cluster management by automating tasks like resizing, upgrading, and repairing nodes. The stable

release channel also provides access to well-tested and stable features, ensuring maximum reliability for a critical business application that is being deployed on Kubernetes.

Solution to Question 27: A

The correct answer is A: 1. Create a subnetwork in the same VPC, in europe-west1. 2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

This is the best solution because, according to Google-recommended practices, creating resources within the same VPC reduces latency, increases security, and simplifies management. By adding a subnetwork in the europe-west1 region within the same VPC, you ensure that both instances can communicate internally using their private IP addresses. This provides direct and secure access to the application without requiring additional services or configuration.

Reasons why other options will not work:

B. This option involves using Cloud VPN, which creates an unnecessary and costly overhead to connect two subnetworks within the same VPC. This complexity is not needed since VPC networks are already global, and communication can be achieved through internal IP addresses.

C. This option requires creating a new VPC and configuring VPC peering, which is not necessary when using the same VPC for the instances. Additionally, this option suggests using the first instance's public address as the endpoint, which exposes the internal application publicly, increasing security risks.

D. Cloud Interconnect is designed to connect a VPC to on-premises networks, not to connect subnetworks within the VPC. This would be an overly complex and expensive solution for the problem. In this scenario, simply using the instances' private addresses within the same VPC is a much easier and cost-effective solution.

Solution to Question 28: B

The correct answer is B. Enable Private Google Access on the subnet within the custom VPC.

Explanation:

Private Google Access allows VM instances with only internal IP addresses to access Google Cloud Storage without needing a public IP address or a route to the public internet. By enabling Private Google Access on the subnet within the custom VPC, you ensure that the VM instances can communicate with the Cloud Storage bucket using Google's private network, complying with the company's security policies.

Why other options will not work:

A. Deploy a Cloud NAT instance and route the traffic to the dedicated IP address of the Cloud Storage bucket: This option requires the use of external IP addresses and the internet to route the traffic to Cloud Storage. It's not compliant with the company's policy of prohibiting connecting to the internet.

C. Set up a Cloud Storage FUSE mount on the VM instances to access the Cloud Storage bucket: Although Cloud Storage FUSE allows VM instances to access the Cloud Storage bucket as a mounted file system, it still needs internet access to operate. Hence, it doesn't comply with the company's security policies.

D. Create a VPN tunnel between Compute Engine VMs and Cloud Storage bucket: Cloud Storage doesn't support setting up a VPN tunnel directly. VPN tunnels are designed for communication between VM instances or VPC networks, not directly with Cloud Storage. This option will not work for the given scenario.

Solution to Question 29: C

The correct answer is C. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

Explanation:

Option A is incorrect because assigning the IAM role roles/pubsub.editor is unnecessary. This role is meant for managing Pub/Sub resources, not for reviewing Audit Logs and Data Access logs. Exporting logs to Cloud Storage is also not required to provide access to the auditor.

Option B is incorrect because creating a custom role with a single permission (logging.logEntries.list) would not be sufficient for the auditor to review all necessary logs, especially when there is a predefined role (roles/logging.privateLogViewer) that perfectly fits the requirement.

Option C is the correct choice because it provides the auditor with the predefined role roles/logging.privateLogViewer, which grants the necessary permissions to view Private Logs. This would enable the auditor not only to view Audit Logs and Data Access logs but also to review the logs for changes to Cloud IAM policy. This approach simplifies the process and adheres to the principal of least privilege.

Option D is incorrect because the permission monitoring.logsWriter is not appropriate for the auditor. It grants write access to logs but does not provide read access, which is needed for the auditor to review the logs. Furthermore, exporting logs to Cloud Storage is not required in this scenario as the auditor can directly access the logs through IAM roles.

Solution to Question 30: D

The correct answer is D because it adheres to security best practices and follows the principle of least privilege, which minimizes the risk of unauthorized access to resources.

Option A suggests creating individual user accounts for each pipeline. This approach does not follow security best practices because it can lead to difficulties in managing and maintaining consistency in permissions, and might inadvertently permit unauthorized access due to manual errors in permission management.

Option B involves granting full project level permissions to the service account. This is a poor security practice as it violates the principle of least privilege because it provides unnecessary and excessive access to resources that may not be required for the continuous integration and delivery pipeline.

Option C recommends using Application Default Credentials without setting specific IAM permissions. This can lead to security vulnerabilities because it lacks adequate control over permissions and may provide unintended access to resources that should be restricted.

On the other hand, Option D adheres to security best practices by:

1. Creating multiple service accounts with the appropriate minimal IAM permissions. This follows the principle of least privilege, ensuring that each pipeline has access to only the necessary resources and actions.
2. Utilizing a secret manager service to securely store the key files of the service accounts. This prevents unauthorized access to the keys, reducing the risk of potential breaches.
3. Allowing the CI/CD pipeline to request the appropriate secrets during execution. This ensures that only the required permissions are utilized at the right time when needed, minimizing exposure and unauthorized access.

By following this approach, the IT professional maintains the security and integrity of the pipelines while also implementing the most secure solution for granting permissions.

Solution to Question 31: B

The most suitable course of action in this situation is option B: creating an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

Option B is the best choice because it aligns with Google's best practices for managing a Cloud Spanner instance and ensuring optimal query performance. Monitoring high priority CPU utilization is essential, and 65% is the recommended threshold for triggering an alert when performance might be impacted. By adding nodes once the threshold is exceeded, you will be enhancing your Cloud Spanner instance's performance to maintain efficient operations.

Option A is not suitable because a 55% threshold is not the recommended value according to Google's best practices. Setting the threshold lower than necessary would lead to unnecessary alerts and potential over-provisioning of nodes, which might lead to increased costs and suboptimal resource utilization.

Option C is not appropriate because increasing the percentage of high priority CPU utilization to 85% could result in performance degradation and might negatively impact the production environment. Monitoring for performance degradation alone is not sufficient to ensure optimal query performance and adhering to best practices.

Finally, Option D is not the most suitable course of action because migrating to a multi-region configuration may not be necessary in all cases and may require significant additional resources and associated costs. It is more efficient to first manage and improve performance within your current single-region Cloud Spanner instance by optimizing monitoring and alerting according to Google's recommended best practices.

Solution to Question 32: A

The correct answer is A. Storage Admin.

Explanation for A (Storage Admin): The Storage Admin role is the most suitable role for your team members because it grants them the necessary permissions to manage buckets and objects within Google Cloud Storage. This role aligns with the principle of least privilege, as it provides just the right amount of access required for the task, without granting excessive permissions. The Storage Admin role enables them to create, configure, and delete buckets, as well as manage object data (including uploading, downloading, and deleting files). By assigning this role, you ensure that your team can work efficiently with Cloud Storage while following Google-recommended practices.

Reasons why other options will not work:

B. Storage Object Admin: The Storage Object Admin role only provides permissions to manage object data within existing buckets, but it does not allow creating, modifying, or deleting buckets themselves. While team members can still manage files within the buckets with this role, they will not have the required flexibility and control for tasks that require bucket-level management, which limits their efficiency.

C. Bigtable Admin: The Bigtable Admin role is not relevant to managing Cloud Storage. This role provides full administrative access to Bigtable instances, tables, and data, which is a separate Google Cloud service focused on a managed NoSQL database. It does not grant any permissions related to managing buckets or object data in Google Cloud Storage.

D. API Gateway Admin: The API Gateway Admin role is also not relevant to managing Cloud Storage. This role grants full control over API Gateway resources and services, which is another separate Google Cloud service that helps you create, publish, and manage APIs for your applications. Assigning this role to your team members would not provide them with any access or permissions related to managing buckets or files in Cloud Storage.

Solution to Question 33: D

The correct answer is D, which is to add your SREs to a group and then add this group to roles/accessapproval.approver role. This approach aligns with the Google-recommended practices because it ensures that only authorized members, specifically SREs, can approve access requests to the resources in the Google Cloud projects. This access control is necessary when SREs open support cases and require the Google Cloud support team to access the resources in these projects.

Option A is incorrect because adding your SREs to the roles/storage.admin role would give them administrative access to Google Cloud Storage but would not give them the specific authorization needed to approve access requests from the Google Cloud support team.

Option B is incorrect because adding your SREs to a group and then adding this group to roles/iam.roleAdmin.role would give them the ability to create and manage custom IAM roles but would not enable them to approve access requests from the Google Cloud support team.

Option C is incorrect because adding your SREs to a group and then adding this group to roles/cloudfunctions.admin role would permit them to manage Google Cloud Functions but would not grant the necessary permissions to approve access requests from the Google Cloud support team.

In conclusion, option D is the most appropriate choice to maintain strict access control while empowering your Site Reliability Engineers to approve requests from the Google Cloud support team when needed. By adding SREs to a group and assigning them the roles/accessapproval.approver role, you ensure that only authorized personnel can grant access when required for the resolution of support cases.

Solution to Question 34: C

The correct answer should be C. Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.

Explanation: The requirement is to have a cost-effective solution for managing relational data on the Google Cloud Platform, support a small set of operational data, and support point-in-time recovery. Cloud SQL (MySQL) is designed to handle relational data, and it comes with point-in-time recovery using the binary logging feature, which can be enabled to ensure the safety of the data without adding significant cost.

Reasons why other options are not suitable:

A. Select Firestore (Native Mode). Set up your instance as multi-regional: Firestore (Native Mode) is not suitable for this scenario because it is designed for a system requiring high scalability, whereas the requirement here is for a small set of operational data. Additionally, setting it up as multi-regional would add unnecessary and avoidable costs as the startup company is only operating in one geographic location.

B. Select Cloud Datastore. Set up your instance with 2 nodes: Cloud Datastore is a NoSQL database, not a relational database, and may not suit the requirements to manage relational data as efficiently as Cloud SQL (MySQL). Furthermore, Cloud Datastore does not provide native point-in-time recovery, which is another requirement in this scenario.

D. Select Bigtable. Create a backup schedule for your operations: Bigtable is also a NoSQL database, which makes it unsuitable for managing relational data. Moreover, it is primarily designed for high-velocity, high-volume data, which is not needed for a small set of operational data. Besides, it does not have native point-in-time recovery support.

Solution to Question 35: B

The correct answer is B. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

Explanation: By assigning the IAM role of BigQuery User to a Google Group that contains the members of the BI team, you are granting the necessary permissions for each team member to run custom SQL queries on the most recent data ingested into BigQuery. This approach is practical because it manages access to resources and follows recommended best practices for managing Google Cloud Identity and Access Management (IAM) roles.

Here's why the other options will not work:

A. Creating a Data Studio dashboard that uses the related BigQuery tables as a source and giving the BI team view access to the Data Studio dashboard is not sufficient since Data Studio cannot directly run custom SQL queries. While it can visualize and report data, it does not provide the same level of flexibility that running SQL queries in BigQuery does.

C. Granting the BI team access to Cloud Pub/Sub to receive real-time data updates from the data pipeline does not allow them to run custom SQL queries against the ingested data. Cloud Pub/Sub is a messaging service used for sending and receiving real-time messages but does not support the ability to run complex SQL queries required for Business Intelligence analysis.

D. Configuring the BI team's API keys to have read and write access to BigQuery might allow them to query data, but API keys are not recommended for managing user access. It is not a secure practice because API keys can be easily misplaced or exposed, increasing the risk of unauthorized access. Instead, IAM roles should be used for managing access as they provide fine-grained control and follow best practices for security.

Solution to Question 36: C

The correct answer is C: Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image. This is because Artifact Registry is the recommended registry for storing and managing container images in Google Cloud. It provides an organized way to store and manage container images

in a way that's compatible with Kubernetes. Creating a Kubernetes Deployment ensures that the required number of instances (replicas) of the application are always running and can be managed effectively. It is suitable for stateless applications and provides simple updates, rolling back, and scaling capabilities.

Option A won't work because it suggests using a Kubernetes StatefulSet. StatefulSets are intended for stateful applications that require stable network identity and persistent storage, which is not necessarily the case for a typical application container. Therefore, using StatefulSet is unnecessary and might introduce unwanted complexity.

Option B won't work because it suggests using a Kubernetes DaemonSet. DaemonSets ensure that a specific instance of a container runs on every node in the cluster. It is suitable for deploying system-level services like log collectors and monitoring agents, not for general application workloads.

Option D won't work because it suggests uploading the image to Cloud Storage, which is not intended for storing container images. Cloud Storage is a general-purpose storage service and lacks the proper container image scanning, security, and versioning features provided by Artifact Registry, making it a less suitable choice for this use case. Additionally, Kubernetes won't be able to directly reference images that are stored in Cloud Storage.

Solution to Question 37: C

The correct answer is C: In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

To enable users to authenticate via your company's SSO provider, you need an option that supports the SAML integration your company uses. Setting up SSO with a third-party identity provider in Cloud Identity allows you to get SAML-based SSO working correctly because Google acts as a service provider to authenticate your users.

Option A and Option B are not valid as they are related to OAuth 2.0, which is an authorization framework, not an authentication protocol like SAML. Although OAuth 2.0 can be used for authentication in some cases, it requires an additional layer like OpenID Connect. In your case, the focus should be on SAML integration, which is not mentioned in these options.

Option D is also incorrect because Domain-Wide Delegation allows third-party applications to access Google Workspace data on behalf of your users, which is not related to setting up authentication via SSO. Enabling this feature will not achieve the required outcome of allowing users to authenticate via your company's SSO provider.

Therefore, the correct answer is to set up SSO with a third-party identity provider in Cloud Identity (Option C), which will enable users to authenticate using your company's SAML-compatible SSO provider.

Solution to Question 38: B

The correct answer is B: Select Compute Engine. Use preemptible VM instances of the appropriate standard machine type.

Explanation:

Option B works best for this scenario because preemptible VM instances in the Google Compute Engine offer a significant discount compared to regular VM instances. They are short-lived (up to 24 hours) and are well-suited for batch processing jobs that can tolerate interruptions, like the ones described in the question. Since the jobs take around 2 hours to complete and are run every night, the use of preemptible VM instances can effectively manage these jobs while minimizing service costs.

Reasons why other options will not work:

A. Select Compute Engine. Use VM instance types that support micro bursting. Micro bursting VM instances are designed for workloads that have occasional spikes in resource usage but are otherwise operating at low utilization levels. Since the batch processing jobs in this scenario run for 2 hours daily and require consistent resources throughout that period, micro bursting VM instances would not be suitable for this case.

C. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types. Using Google Kubernetes Engine (GKE) in this scenario can lead to higher costs and increased complexity, as GKE is designed for container orchestration and not specifically for batch processing jobs. Additionally, using micro instance types would not provide the necessary consistent resources needed for the 2-hour batch processing jobs.

D. Select Cloud Functions with maximum memory allocation. Cloud Functions are better suited for event-driven and lightweight tasks, not for long-running batch processing jobs. This option would likely result in significant timeliness issues or potential function timeouts due to the 2-hour job duration. In addition, using Cloud Functions for this case may lead to higher costs, as they are priced based on the function invocation count and resources consumed.

Solution to Question 39: A

The correct answer should be A. Coldline Storage for the following reasons:

1. Coldline Storage is a cost-effective storage class designed specifically for data recovery and disaster recovery scenarios. It offers low storage costs, durable storage solution, and quick retrieval capabilities - all important factors when it comes to effective disaster recovery management.

2. While Coldline Storage is not intended for frequently accessed data, it is perfect for data recovery specialists dealing with backup files. These files often need to be stored for extended periods and may only be actively accessed in the event of a disaster or data loss.

3. Coldline Storage ensures data durability by providing geo-redundant storage and automatic data integrity checks. This feature is critical for data recovery purposes, ensuring that your backup data will be available and intact when it is most needed.

On the other hand, the other options do not fit the requirements:

B. Persistent Disk - While persistent disks offer high storage capacity and performance, they are not designed specifically for disaster recovery management. They are more suitable for applications that require high IOPS and low latency. Additionally, they are not cost-effective for long-term storage of backup data.

C. Local SSD - Local SSDs offer high-performance and low-latency storage, but they are only suitable for temporary storage. Local SSDs have limited capacity and are not persistent, meaning data loss can occur if the instance is terminated or if there is a hardware failure, making them unsuitable for disaster recovery management.

D. Datastore - Datastore is a NoSQL database service that allows developers to easily store and retrieve data for applications. While Datastore is useful for application development, it is not designed for long-term backup data storage and disaster recovery management purposes.

In conclusion, Coldline Storage is the most appropriate storage option for a data recovery specialist working in a technology company, as it offers cost-effective, durable, and fast retrieval capabilities specifically designed to handle disaster recovery management scenarios. The other options are not aligned with these requirements, making them unsuitable choices for this use case.

Solution to Question 40: A

The correct answer is A. You should use the BigQuery interface to review the nightly job and look for any errors. Since the issue is related to the daily summary being recalculated by overwriting the table, it makes the most sense to investigate the job responsible for the data update. By reviewing the nightly job in the BigQuery interface, you can check for any errors, warnings, or inconsistencies that might be affecting the charts in Looker Studio.

Option B is not the best choice because the Data Transfer Service is used for data replication between sources and the data warehouse, not for handling the process of recalculating daily summaries. Delays in data replication would affect the appending of data during the day, not the nightly overwriting process.

Option C is also not ideal, as the issue seems to stem from the data warehouse itself and not Looker Studio. While using Stackdriver Monitoring to check for Looker Studio-specific issues might provide valuable information about the application, it won't help you determine the root cause of the problem related to the daily summary recalculations.

Lastly, option D is not the best choice because the issue is related to the overwriting process, not the schema of the data warehouse. While inspecting the

schema might provide insight into the overall structure of the data warehouse, it is unlikely to help identify the specific issue related to the nightly job and the daily summary recalculations.

Solution to Question 41: C

The correct answer is C: Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

Here's why the other options would not work and an explanation of why option C is the most suitable approach:

A. Using a third-party tool to provide remote access to the instances can introduce additional risks and dependencies. This option might be less secure and could increase costs. Relying on Google Cloud's native tools and methods is more secure and generally more cost-effective.

B. Using Google Cloud VPN to connect directly to instances has additional costs associated with setting up and maintaining a VPN infrastructure. Moreover, using SSH over VPN can introduce additional delays as the traffic will need to pass through the VPN tunnel. This might not be the most secure or cost-effective solution.

D. Creating a bastion host with public internet access presents an additional security risk. While the bastion host could be locked down and hardened, its very presence provides an additional attack surface for potential intruders. This approach also requires additional costs for maintaining this additional host.

C. Using the gcloud compute ssh command with the –tunnel-through-iap flag is the most suitable approach as it ensures secure and cost-effective access to Linux instances on Google Cloud. Google Cloud's Identity-Aware Proxy (IAP) allows context-aware access control and doesn't require setting up a VPN or a bastion host. Allowing ingress traffic only from the IP range 35.235.240.0/20 ensures that the SSH connection is made securely from Google Cloud resources, and only authorized SSH traffic is allowed on port 22. This approach provides a balance of security, ease of use, and cost-effectiveness.

Solution to Question 42: D

The correct answer is D.

Creating a separate node pool with compute-optimized machine type nodes for the image rendering microservice ensures that the resource usage is optimized for each workload. Compute-optimized machine types are specifically designed for tasks that require more CPU time than memory, which is the case for the image rendering microservice.

Option A is not the correct answer because assigning a higher pod priority to the image rendering microservice only affects the scheduling order of the pods, not the optimization of actual resources used.

Option B is not the correct answer because deploying on App Engine Flexible Environment rather than Kubernetes Engine would, in this case, introduce unnecessary complexity to the deployment process. This option does not address the specific needs of the image rendering microservice that requires more CPU time than memory.

Option C is not the correct answer because although it allows developers to configure resource requests, it still won't guarantee that the image rendering microservice will have enough CPU-intensive resources to run efficiently. With a separate node pool as in option D, it becomes more feasible to ensure that the required resources are properly allocated and optimized.

In conclusion, option D is the most effective way to optimize the resource usage for all microservices in the Kubernetes cluster by allocating the appropriate resources for each workload.

Solution to Question 43: B

The correct answer is B for the following reasons:

1. Creating a dedicated Google group in Cloud Identity is a good practice as it allows you to manage access more easily. By adding or removing users from the group, you can control their access to resources. This is especially relevant when dealing with a high turnover rate, as is the case with the data science team in the retail company.
2. Adding each data scientist's user account to the group ensures that all team members have the necessary permissions to access the BigQuery resources. As personnel changes occur, it's easy to modify the group's membership to grant or revoke access as needed.
3. Assigning the BigQuery jobUser role to the group is suitable for this situation, as this role has the necessary permissions to run and manage jobs (such as queries) but does not grant too much access that can put the data at risk. It effectively allows data scientists to perform their tasks without opening the door for unauthorized editing, deletion, or publishing of datasets.

The other options are not recommended due to the following reasons:

Option A: The BigQuery machineLearningDeveloper user role also enables running queries, but it explicitly gives access to machine learning capabilities within BigQuery, which is not mentioned as a requirement for the data science team in this retail company. It is generally better to assign the least privilege required to perform the job to minimize the risk of misuse or data breaches.

Option C: The BigQuery dataEditor user role is too permissive in this case, as it would allow data scientists to create, update, and delete datasets, tables, and views in their assigned projects. This is not suitable considering that only a few members require access to perform queries, not to edit the data. Further-

more, adhering to the principle of least privilege, it's better to avoid granting unnecessary permissions.

Option D: Creating individual IAM entries for each data scientist's user account is less efficient than using a cloud identity group, as it requires more administrative overhead to manage each user's access individually. It is also harder to track and maintain, particularly if there is a high turnover. Additionally, the BigQuery user role referenced in this option does not exist, making this option incorrect.

Solution to Question 44: A

The correct answer should be A. This is because exporting the billing data to BigQuery allows you to analyze and handle all the data associated with your Google Cloud project's costs more efficiently. By using a Cloud Function, you can create a specific function that will sum the egress network costs of the exported billing data for the Apache web server and send email notifications if costs surpass $100 for the current month. In addition, using Cloud Scheduler ensures that the Cloud Function is run hourly, automating the process of checking costs and sending notifications, without requiring any manual intervention.

On the other hand, option B requires manual review and action, which is not efficient for a network administrator, as they may have other important tasks to attend to, and the hourly manual review can be time-consuming.

Option C is not suitable because using the Cloud Logging Agent to parse HTTP response log data might not accurately reflect the actual egress network costs, which are based on data transfer, rather than HTTP response sizes. Additionally, multiplying by the current Google Cloud egress prices might lead to over- or under-estimations due to possible fluctuations in prices.

Option D, while seemingly automated, introduces unnecessary complexity by creating an App Engine application and cron job. Moreover, this method incurs additional costs associated with the App Engine application, which might not be required when the same task can be achieved using a much simpler and cost-effective approach like Option A.

Solution to Question 45: C

The correct answer is C because going to Cloud Shell and running gcloud config list will provide you with the current Google Cloud configuration used for deployment. This way, you can check if the project, account, and other settings are properly configured for your desired application deployment destination.

Option A is not correct because Deployment Manager is used for creating and managing resources on Google Cloud but not for deploying applications to App Engine. It wouldn't provide the necessary information to find out where the app was deployed.

Option B is not correct because checking the Google Cloud SDK installation is not sufficient to determine where the application was deployed. You need

to review the settings used by gcloud at the time of deployment, which can be accessed using the gcloud config list command (Option C).

Option D is not correct because reviewing logs in the App Engine dashboard would only provide information about deployment activities for the current project and may not indicate where an app was deployed if the wrong project was selected during deployment. To identify the exact project and settings used in deployment, you should run gcloud config list (Option C).

Solution to Question 46: B

The correct answer is B: Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

This is the best solution because it ensures that the partner company is able to access the specific data they need while maintaining a separation between your resources and theirs. By asking the partner to create a Service Account in their own project, you are ensuring they have control over the account that interacts with your data. Once the Service Account is created, you can grant the necessary BigQuery permissions for their Service Account to access your dataset. This approach maintains both security and control over access to your data.

Option A is incorrect because creating a Service Account in your own project and proposing to grant that account access to Cloud Functions in the partner's project would not provide the partner's company the access to your BigQuery dataset, which is the primary requirement.

Option C is incorrect because giving the partner's Service Account access to Compute Engine in their project would not directly provide access to your data. Compute Engine enables them to create VMs but does not, by itself, grant access to your BigQuery dataset.

Option D is incorrect because giving the partner's Service Account access to Cloud Storage in their project does not grant access to your BigQuery dataset. While Cloud Storage is a useful component for storing and accessing data, this scenario specifically requires access to your data warehouse, which is managed in the BigQuery dataset.

Solution to Question 47: A

The correct answer is A. Enable parallel composite uploads using gsutil on the file transfer.

Here's why answer A is the best choice:

Using parallel composite uploads allows you to split a large file into smaller components, which are then uploaded in parallel, leveraging the maximum possible capacity of the 1 Gbps WAN connection. By enabling parallel composite

uploads using gsutil, you can utilize the full potential of the WAN connection and expedite the entire file transfer process.

Here's why the other options are not suitable:

Option B: Uploading the file using Google Cloud Pub/Sub streaming is not ideal because Pub/Sub is primarily designed for messaging and real-time data streaming purposes. It is not designed for efficient file uploading, especially for a 32 GB single file. Moreover, it would not utilize the maximum capacity of the 1 Gbps connection, making the file upload slower.

Option C: Running multiple instances of gsutil in parallel without using composite uploads would not work in this scenario since there is only one 32 GB file to upload and not multiple independent files. Running multiple instances would not split the one large file and would not provide the expected benefit from the multiple instances.

Option D: Disabling resumable uploads in gsutil would not speed up the file transfer process. Resumable uploads provide a mechanism to resume file uploads if the process is interrupted, which is crucial for large file transfers. Disabling this feature would not utilize the maximum capacity of the 1 Gbps connection and may increase the risk of file transfer failure.

In conclusion, enabling parallel composite uploads using gsutil (Option A) is the most efficient and effective method to transfer a 32 GB single file by utilizing the maximum capacity of a 1 Gbps WAN connection, making it the correct choice.

Solution to Question 48: D

The correct answer is D. Go to Data Catalog and search for employee_ssn in the search box.

Explanation:

Option A: Write a shell script that uses the bq command line tool to loop through all the projects in your organization. While this approach might eventually give you the information needed, it would require significant time and effort to write a custom script that loops through every project, dataset, and table to find the employee_ssn column. This method does not minimize the effort required, as stated in the question.

Option B: Create a Pub/Sub topic and configure Data Catalog to send all the dataset metadata updates to this topic, then filter the messages to find those containing employee_ssn. This approach requires setting up an unnecessary infrastructure that does not directly solve the problem. Pub/Sub is a messaging service and does not inherently possess the ability to filter or search specific metadata criteria. The filtering step would still require additional scripting and may not minimize the effort needed.

Option C: Write a Cloud Run service that accepts dataset information, scans for the employee_ssn column, and automatically responds with the results to

find desired tables. This option is focused on creating a custom cloud service to solve the problem, which is not efficient in terms of resources and time. It is also not an optimal use of Google Cloud products to address the given situation.

Option D: Go to Data Catalog and search for employee_ssn in the search box. This is the most efficient and quickest way to locate the information required. Data Catalog is a fully managed and scalable metadata management service that allows users to search and discover data assets across their organization. By simply searching for employee_ssn in the search box, Data Catalog will identify any tables containing this column across all the datasets in your organization, minimizing the time and effort required to complete the task.

Solution to Question 49: C

The best approach for this situation is option C, creating an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket. Here's why this is the ideal solution and why the other options are not suitable:

C. Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket: This strategy is perfect for long-term, cost-effective storage of data that is not frequently accessed, such as audit log files for a 3-year retention period. Coldline Storage is designed for infrequent access and low cost. It offers a good balance between data retrievability and cost management for the financial firm.

A. Create an export to the sink that saves logs from Cloud Audit to BigQuery: While exporting logs to BigQuery would make them more easily searchable, this solution is not as cost-effective as using Coldline Storage, especially when considering the 3-year retention period. BigQuery is more focused on running large-scale analytics and is optimized for high-speed processing, which is not necessary in this case.

B. Export these logs to Cloud Pub/Sub and write a Cloud Dataflow pipeline to store logs to Cloud SQL: Exporting logs to Cloud Pub/Sub and using Cloud Dataflow pipelines to store logs in Cloud SQL adds an extra layer of complexity to the process, which is not required for storing audit logs. In addition, while Cloud SQL is an excellent managed database service, it is not designed to be a long-term and cost-effective storage solution like Coldline Storage.

D. Export logs to Cloud Pub/Sub and utilize Cloud Dataflow pipeline to store logs in Cloud Bigtable: Similar to option B, this solution involves unnecessary complexity by engaging Cloud Pub/Sub and Cloud Dataflow. Moreover, Cloud Bigtable is a high-performance NoSQL database designed to handle large amounts of data and heavy workloads, which is not needed for storing audit logs over a 3-year retention period.

In summary, the most cost-effective and efficient approach for storing the audit log files for a period of 3 years across hundreds of Google Cloud projects is option C, which involves creating an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket.

Solution to Question 50: C

The correct answer is C: Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

An explanation for why this option is the best choice is as follows:

In this scenario, we have three main requirements: dynamic routing, shared address space, and no overprovisioning of tunnels during a failover event.

Option C meets all the requirements. A custom mode VPC network allows you to define the IP address range and subnetting configuration, which will enable you to effectively share the 10.19.0.1/22 address space as required. Using Cloud Router with BGP establishes dynamic routing between the VPC and the remote site, ensuring that traffic is routed correctly between them. Active/passive routing helps achieve high availability in the Cloud VPN setup without overprovisioning tunnels during failover events because both primary and backup tunnels will be used, with the backup tunnel taking over automatically when the primary tunnel goes down.

Now, let's evaluate the other options and see why they are not the best choices:

Option A: This option suggests using active/active routing with Cloud NAT. However, this doesn't meet the requirement of no overprovisioning of tunnels during a failover event. It also involves additional complexity by using Cloud NAT, which is not necessary for the given scenario.

Option B: While this option proposes using BGP routes for dynamic routing, it relies on an automatic mode VPC network, which doesn't allow for granular control over the IP address range and subnetting configuration and might conflict with the given shared address space requirement. Additionally, active/passive routing (used in the correct answer) would provide better failover capabilities, preventing overprovisioning of tunnels during a failover event.

Option D: This option suggests using an automatic mode VPC network, which suffers from the same IP address range conflicts as Option B. It also recommends using static routes, which do not provide the dynamic routing capability needed for this scenario. Lastly, active/active routing could lead to overprovisioning of tunnels during a failover event, which is against the given requirement.

In conclusion, Option C best meets the requirements by utilizing a custom mode VPC network for shared address space, Cloud Router BGP for dynamic routing, and active/passive routing for high availability without overprovisioning tunnels during failover events.

Practice Exam 12

Question 1: As a data engineer working for an e-commerce company, you are dealing with large volumes of unstructured data in various file formats. In order to run ETL transformations on this data for analytics purposes, you need to make it accessible on Google Cloud for processing by a Dataflow job. What is the most appropriate action to take?

A. Upload the data into Cloud Spanner using the import function in the Google Cloud console.

B. Upload the data to Firestore using the gcloud firestore command.

C. Upload the data to Kubernetes Engine using the gcloud container clusters create command.

D. Upload the data to Cloud Storage using the gcloud storage command.

Question 2: You are an IT Specialist at a technology company, and your Dataproc cluster runs in a single Virtual Private Cloud (VPC) network in a single subnetwork with range 172.16.20.128/25. The subnetwork runs out of private IP addresses. Your manager asks you to find a way to add new VMs for communication with the cluster while minimizing the steps involved. What should you do?

A. Create a new subnetwork in the existing VPC with a range of 172.16.21.0/24 and configure the VMs to use that subnetwork.

B. Create a new VPC network for the VMs with a subnet of 172.32.0.0/16. Enable VPC network Peering between the Dataproc VPC network and the VMs VPC network. Configure a custom Route exchange.

C. Configure Shared VPC for the existing VPC and add the VMs to a new subnetwork in the Shared VPC.

D. Modify the existing subnet range to 172.16.20.0/24.

Question 3: As an IT professional working at a growing tech company, you've successfully created a new project in Google Cloud via the gcloud CLI and linked it to a billing account. Now, you need to set up a Compute Engine instance using CLI. What prerequisite steps should you take?

A. Enable the cloudresourcemanager.googleapis.com API.

B. Enable the compute.googleapis.com API.

C. Create a VPC network in the project.

D. Create an App Engine application in the project.

Question 4: As a data analyst at a tech company, you need to run a crucial query in BigQuery, anticipating a large number of records in the result. To

determine the cost of executing this query using on-demand pricing, what action should you take?

A. Export data to Cloud Storage to reduce costs and then run the query.

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

C. Use the command line to run a dry run query, then estimate the cost based on the overall data read.

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

Question 5: As a software engineer in a tech company, you are responsible for handling a nightly batch workload that utilizes a large quantity of virtual machines (VMs) and can withstand the termination of some VMs. However, the current cost of VMs is proving to be too expensive. What strategy should you implement to reduce these costs?

A. Run a test using App Engine Flex. If the test is successful, use N1 Standard VMs in the App Engine Flex environment when running future jobs.

B. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

C. Run a test using Google Dataproc. If the test is successful, use N1 Standard VMs in the Dataproc cluster when running future jobs.

D. Run a test using Google Compute Engine (GCE). If the test is successful, use preemptible N1 Highmem VMs when running future jobs.

Question 6: As a software engineer at a leading tech company, you are responsible for deploying production and test workloads on Compute Engine for a crucial project. The production VMs need to be in a separate subnet from the test VMs, but all VMs must be able to communicate with each other using Internal IPs without creating extra routes. How should you set up the VPC and two subnets to fulfill these requirements?

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

B. Create a single custom VPC with 3 subnets. Create 2 subnets for production and test in the same region with different CIDR ranges, and the third subnet as the communication link between the two.

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

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

Question 7: As a system administrator for a software development company, you need to configure an SSH connection to a single Compute Engine instance specifically for the members of the dev1 team. This instance is the sole resource in the Google Cloud Platform project that dev1 team members should have access to. How should you proceed?

A. Enable block project wide keys for the instance. Generate an SSH key for each user in the dev1 group. Distribute the keys to dev1 users and direct them to use their third-party tools to connect.

B. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.InstanceAdmin role. Direct them to use the Cloud Console to ssh to that instance.

C. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

D. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osAdminLogin role. Direct them to use third-party SSH tools to connect to the instance.

Question 8: You are working as a Cloud Operations Engineer at a multinational company. The sales team has a project named Sales Data Digest that has the ID acme-data-digest for their Google Cloud resources. You are tasked with setting up similar Google Cloud resources for the marketing team within the organization, but their resources must be organized independently of the sales team. What should you do?

A. Grant the Project Editor role to the Marketing team for acme-data-digest.

B. Create a new marketing folder under acme-data-digest project and grant the Marketing team folder editor access.

C. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

D. Utilize Cloud Composer to build a pipeline that transfers data from acme-data-digest to the Marketing team's resources.

Question 9: As a data management specialist in a healthcare company, you need to set up and configure a solution on Google Cloud Platform to store and archive patient data originating from a particular geographic location. For compliance purposes, the data must be archived after 30 days and accessed only once per year. How should you achieve this?

A. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Cloud Storage Archive.

B. Select Multi-Regional Storage. Add a bucket lifecycle rule that moves data to Cloud SQL after 30 days.

C. Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

D. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

Question 10: As a system administrator in a tech company, you are responsible for managing an application running on multiple virtual machines within a managed instance group with autoscaling enabled. The autoscaling policy is configured to add more instances if the CPU utilization goes above 80% until the maximum limit of five VMs or until CPU utilization lowers to 80%. The initial delay for HTTP health checks is set to 30 seconds, and the virtual machine instances take about three minutes to become available for users. However, you notice that the instance group adds more instances than necessary to support the levels of end-user traffic when autoscaling. What modification should you make to maintain proper instance group sizes when autoscaling?

A. Decrease the initial delay of the HTTP health check to 10 seconds.

B. Use an HTTP(S) load balancer instead of a TCP load balancer.

C. Decrease the autoscaling threshold to 50%.

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

Question 11: As a software engineer at a tech company, you've been tasked with setting up a Compute Engine instance in a new project that hasn't been created yet. What is the correct sequence of steps to achieve this?

A. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

B. Create a service account with permissions to create Compute Engine instances and then use it to create instances in the new project.

C. Create a Compute Engine instance in the default project and then move it to the new project using the Cloud Console.

D. Enable the Firestore API in the Cloud Console, create a new project, and then use the Cloud SDK to create a Compute Engine instance.

Question 12: As a software engineer at a growing tech company, you received a notification that your managed instance group raised an alert stating that new instance creation has failed. To resolve this issue and ensure the smooth functioning of your company's infrastructure, what action should you take?

A. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

B. Verify that the instance template being used by the instance group contains valid syntax. Increase the instance count of the managed instance group.

C. Delete the current instance template and create a new instance group using a template with valid syntax. Delete any persistent disks with the same name as instance names.

D. Delete the current instance template and create a new one with valid syntax. Set the disks.autoDelete property to false in the instance template.

Question 13: You work for a web development company that has been tasked with creating a secure website with autoscaling for a client based on the compute instance CPU load. Additionally, you need to enhance the performance by storing static content in Cloud Storage. Which resources are necessary to distribute user traffic effectively?

A. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

B. An internal TCP/UDP load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

C. An external HTTP(S) load balancer with managed SSL for the backend service and an additional Cloud Pub/Sub integration for distributing the requests for the static content to the Cloud Storage backend.

D. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load, and Google Cloud Storage FUSE to serve static content from the compute instances.

Question 14: You are working as an IT administrator at a company with strict security policies that prevent the servers hosting an application on bare-metal servers in your on-premises data center from having public IP addresses or access to the internet. You need to ensure that the application can connect to Google Cloud Storage without violating these security policies and following Google-recommended practices. How should you accomplish this?

A. 6. Deploy a Kubernetes cluster on your on-premises servers using Anthos, then configure the application to access Cloud Storage using the Anthos Service Mesh.

B. 1. Using Cloud VPN, create a VPN tunnel to a Virtual Private Cloud (VPC) in Google Cloud. 2. In this VPC, create a Compute Engine instance and install the Squid proxy server on this instance. 3. Configure your servers to use that instance as a proxy to access Cloud Storage.

C. 1. Use nslookup to get the IP address for storage.googleapis.com. 2. Negotiate with the security team to be able to give a public IP address to the servers. 3. Only allow egress traffic from those servers to the IP addresses for storage.googleapis.com.

D. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in Google

Cloud. 2. Use Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel. 3. In your on-premises network, configure your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com.

Question 15: As a leading construction equipment rental company, your business heavily relies on renting out large-scale machinery equipped with several sensors that continuously transmit event data. These sensors monitor various metrics such as engine status, distance covered, and fuel level, which are used to bill customers. Expecting a high traffic - with thousands of hourly events per device - you need a solution that ensures data consistency based on the event's time and allows atomic storage and retrieval of individual signals. What is the best course of action for your company?

A. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

B. Create a file in Cloud Filestore per device and append new data to that file.

C. Create a file in Cloud Storage per device and append new data to that file.

D. Create a file in Cloud SQL per device and append new data to that table.

Question 16: You are working as a system administrator for a technology company that utilizes multiple Linux instances on Compute Engine. The company plans to increase the number of instances in the near future. Your task is to enable access to these instances through an SSH client over the internet without configuring specific access for both existing and new instances, while keeping the Compute Engine instances without a public IP. What approach should you take?

A. Enable Cloud Armor with an SSH policy for the instances.

B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

C. Use Cloud Load Balancer with the TCP Proxy protocol for the instances.

D. Create an SSH keypair and store the public key as a project-wide SSH Key.

Question 17: As a lead developer in a major software company, you are required to create a custom IAM role for a GCP service that is suitable for production use. Your goal is to share the status of the custom role with the entire organization, emphasizing that this is only the first version. How should you proceed?

A. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to GA while testing the role permissions.

B. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to GA while testing the role permissions.

C. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to PRE-ALPHA while testing the role permissions.

D. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

Question 18: As an employee in a broadcasting company, you are tasked with extracting text from audio files using the Speech-to-Text API. The audio files are constantly being uploaded to a Cloud Storage bucket. Your goal is to implement a fully managed, serverless compute solution with authentication and adherence to Google-recommended practices. In order to automate the API calls, you must submit each file to the API as it arrives in the bucket. What is the best approach to achieve this?

A. Configure a Cloud Pub/Sub subscription to listen for events from the Cloud Storage bucket and submit the file URI to the Google Speech-to-Text API.

B. Run a Kubernetes job to scan the bucket regularly for incoming files, and call the Speech-to-Text API for each unprocessed file.

C. Deploy a Cloud Shell script on a regular schedule to scan the bucket regularly for incoming files and call the Speech-to-Text API for each unprocessed file.

D. Create a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

Question 19: As a data analyst at your company, you are tasked with setting up IAM access audit logging in BigQuery for external auditors while adhering to Google-recommended practices. How should you proceed?

A. Add the auditor user accounts to the 'bigQuery.jobUser' and 'bigQuery.dataOwner' predefined IAM roles.

B. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

C. Add the auditor user accounts to two new custom IAM roles.

D. Add the auditors group to the 'bigQuery.dataViewer' and 'logging.admin' predefined IAM roles.

Question 20: You are working as a Cloud Engineer in a tech company and need to access several resources in a Google Cloud project. Your team provided you with a JSON file containing the private key of a Service Account. After downloading and installing the Cloud SDK, how should you use this private key for authentication and authorization when executing gcloud commands?

A. Use the command gcloud auth activate-service-account and point it to the private key.

B. Use the command gcloud init and point it to the private key.

C. Place the private key file in the .config/gcloud folder in your home directory and rename it to active_credentials.json.

D. Place the private key file in the Cloud SDK installation directory and set the environment variable GOOGLE_APPLICATION_CREDENTIALS to its path.

Question 21: As an IT specialist working in a company that utilizes Google Cloud Platform, you are managing multiple VPC-native Google Kubernetes Engine clusters in the same subnet. The available IP addresses for the nodes have been exhausted, and you need to make sure the clusters can expand with more nodes when necessary. What should be your next course of action?

A. Expand the CIDR range of the relevant subnet for the cluster.

B. Create an additional node pool with a smaller node count within the same subnet.

C. Create a new region for the GKE clusters.

D. Add an alias IP range to the subnet used by the GKE clusters.

Question 22: You are working as a software engineer in a large company managing a web application on Compute Engine. Your manager has tasked you with ensuring that the support team receives automatic notifications if users face high latency for at least 5 minutes. You are required to implement a Google-recommended solution without any development costs involved. What approach should you take?

A. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

B. Export Cloud Monitoring metrics to Cloud Storage and use Data Studio to create a dashboard for monitoring latency.

C. Use Stackdriver Logging to monitor latency and send notifications when latency exceeds the specified threshold.

D. Use the Cloud Monitoring dashboard to observe latency and take the necessary actions when the response latency exceeds the specified threshold.

Question 23: You are working as a data engineer at a finance company and are tasked with building a pipeline to process time-series data. Which Google Cloud Platform services should you put in boxes 1, 2, 3, and 4?

A. Cloud Storage, Cloud Dataflow, Cloud Datastore, BigQuery

B. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery

C. Cloud Pub/Sub, Cloud Dataflow, Cloud Datastore, BigQuery

D. Cloud Pub/Sub, Cloud Dataproc, Cloud Storage, BigQuery

Question 24: You are working as a Data Analyst for a technology company that relies heavily on Google Cloud Platform (GCP) for their operations. Recently, the company asked you to investigate and analyze the logs of all

their GCP projects from the past 60 days. They want you to use Google-recommended practices to obtain the combined logs for all projects. How should you proceed?

A. Use Data Fusion to extract logs from Stackdriver, transform them and load them into BigQuery. Configure the table expiration to 60 days.

B. Navigate to Stackdriver Logging and select resource.labels.project_id="*"

C. Configure a Cloud Function to read from Stackdriver Logging and write the logs to Cloud Spanner. Set the retention policy to 60 days for the database.

D. Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

Question 25: You are working as a cloud engineer in a company that heavily relies on Google Cloud services. Your task is to configure service accounts for an application that spans multiple projects. Virtual machines (VMs) running in the web-applications project need access to BigQuery datasets in the crm-databases-proj. In order to follow Google-recommended practices, how should you grant access to the service account in the web-applications project?

A. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

B. Create a new dataset in web-applications project and replicate the crm-databases-proj main dataset.

C. Create a new service account in crm-databases-proj and give it a bigquery.dataViewer role in web-applications project.

D. Grant bigquery.dataViewer role to crm-databases-proj and bigquery.dataOwner role to web-applications project.

Question 26: As a software engineer in a retail company, you are tasked with migrating your firm's on-premises ecommerce application to a serverless Google Cloud solution. The application comprises a complicated network of Python-based microservices, each operating within Docker containers, with configurations implemented via environment variables. What would be the best approach to successfully deploy your current application to the serverless infrastructure?

A. Migrate the code to App Engine Flexible Environment and deploy each microservice as separate services. Update the configurations and the required endpoints.

B. Use Firestore as a serverless database and manually rewrite all microservices to store configurations in Firestore. Deploy microservices as separate Cloud Run instances.

C. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Build. Update the configurations and the required endpoints.

D. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

Question 27: As a database administrator in a growing technology company, you have a critical workload running on Compute Engine that is essential for company operations. To ensure the boot disk's data is backed up regularly and restore a backup quickly in case of disaster while following Google-recommended practices, you also want older backups to be cleaned automatically to save costs. What strategy should you implement?

A. Create a Cloud Task to create an image and export it to Cloud Storage.

B. Use Cloud Memorystore for Redis to keep regular copies of the boot disk data.

C. Use Cloud Filestore to store regular copies of the boot disk files.

D. Create a snapshot schedule for the disk using the desired interval.

Question 28: As an IT manager in a rapidly growing software development company, you have noticed that many employees have been using their personal credit cards to create projects on the Cloud Platform and later getting reimbursed by the company. To streamline and centralize billing for all these projects under one account, what action should you take?

A. In the Cloud Console, create a new billing account and manually transfer each employee's project to the root Organization.

B. Create a billing account in the Google Cloud Console with the company's GCP-related expenses only.

C. Contact the GCP sales team to request a new, centralized billing account for your company's projects.

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

Question 29: As a data storage specialist at a renowned analytics company in the United States, you are tasked with setting up optimal data storage for files in Cloud Storage while minimizing costs. These files are crucial for the company's analytics pipeline, which operates continuously, and the majority of users are located in Boston, MA. What is the best course of action?

A. Configure dual-regional storage for the region furthest from the users. Configure an Archive storage class.

B. Configure regional storage for the region closest to the users. Configure an Archive storage class.

C. Configure regional storage for the region closest to the users. Configure a Standard storage class.

D. Configure dual-regional storage for the dual region closest to the users. Configure a Standard storage class.

Question 30: You are working as a system administrator for a tech company in the healthcare industry and notice an increased number of user complaints about a specific error in one of your applications. Upon investigating, you find that the error is caused by a Service Account with insufficient permissions. After resolving the issue, you want to ensure that you are promptly notified if the problem arises again. What action should you take?

A. Create a sink to BigQuery to export all the logs. Create a Data Studio dashboard on the exported logs.

B. Grant Project Owner access to the Service Account.

C. Modify the error log severity level to Warning.

D. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

Question 31: As a security specialist working in a multinational corporation, you are asked to confirm that a new Google Cloud Platform service account was created at a specific point in time. How should you proceed?

A. Filter the Audit logs to view the Configuration category. Filter the Resource type to Compute Engine.

B. Filter the Activity log to view the Data Access category. Filter the Resource type to Networking.

C. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

D. Filter the Stackdriver logs to view the Configuration category. Filter the Resource type to Google Project.

Question 32: As a financial analyst in a rapidly growing tech company, you are responsible for consolidating the costs of your own company's GCP organization with hundreds of projects and a billing account, as well as those of a recently acquired company with a similar number of projects and its own billing account. You want to merge all GCP expenses from both organizations onto a single invoice starting from tomorrow. What is the most efficient approach to achieve this?

A. Enable cost aggregation in the Cloud Console for both billing accounts.

B. Link the acquired company's projects to your company's billing account.

C. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued.

D. Create a new GCP organization and a new billing account. Migrate the acquired company's projects and your company's projects into the new GCP

organization and link the projects to the new billing account.

Question 33: As a data analyst in a rapidly growing technology company, you need to set up an archiving solution for data stored in a Cloud Storage bucket. This solution should be cost-effective while allowing multiple versions of the data to be archived after 30 days. The previous versions are accessed once a month for generating reports and are occasionally updated at the end of the month. What action should you take to achieve this?

A. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Coldline Storage.

B. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

C. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Coldline Storage.

D. Add a bucket lifecycle rule that archives data with older versions after 60 days to Nearline Storage.

Question 34: You are working as a Cloud Engineer for a company in the e-commerce industry, and you have a single binary application that needs to run on Google Cloud Platform. The company wants to automatically scale the application based on underlying infrastructure CPU usage. The company's policy requires the use of virtual machines directly. Your task is to ensure that the application scaling is operationally efficient and completed as quickly as possible. What is the best approach to achieve this?

A. Create a Cloud Function to monitor CPU usage and trigger VM creation or deletion based on thresholds.

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

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

D. Use Cloud Dataflow to manage the scaling of the application based on CPU usage.

Question 35: You work for a large company that has recently implemented a complicated organizational structure on Google Cloud, which consists of numerous folders and projects. In order to maintain a specific level of security, you need to ensure that only a select few team members can view the entire hierarchy. Your goal is to grant them the least possible permissions while adhering to Google's recommended practices. What course of action should you take?

A. Add the users to roles/cloudtrace.agent role.

B. Add the users to a group, and add this group to roles/compute.admin.

C. Add the users to a group, and add this group to roles/browser.

D. Add the users to a group, and add this group to roles/bigquery.dataViewer.

Question 36: You are working at a software company and have developed an App Engine application for a client's development environment. After successful testing, you are required to create a new project for the production environment. What should you do?

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

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

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

D. Use Dataflow to copy the application code from one project to another for deployment.

Question 37: You recently joined a software development company that manages their infrastructure using Google Cloud. Your manager assigned you a Google Cloud project with an attached billing account and requested that you create instances, set firewalls, and store data in Cloud Storage. To ensure compliance with company policies and Google-recommended practices, what should you do?

A. Open the Google Cloud Console and manually create instances, set firewalls, and store data in Cloud Storage without enabling any APIs.

B. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

C. Deploy instances and set firewall rules using default settings without enabling any APIs in the Google Cloud console.

D. Manually enable individual APIs from the Google Cloud Console's API section only after an error message prompts these actions.

Question 38: As a system administrator for a company specializing in low-latency web services, you are responsible for setting up a single caching HTTP reverse proxy on GCP to optimize performance for a latency-sensitive website. The reverse proxy consumes minimal CPU, and you require a 30-GB in-memory cache along with an additional 2 GB of memory for other processes. Your goal is to minimize costs while achieving the desired outcome. What would be the best way to run this reverse proxy in GCP?

A. Create a Cloud Storage bucket with 32-GB capacity, and use it as the cache for the reverse proxy.

B. Create a Cloud Filestore with 32 GB of storage, and use it as the cache for the reverse proxy.

C. Package it in a container image, and run it on Kubernetes Engine, using n1-standard-32 instances as nodes.

D. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

Question 39: As an IT administrator at a large technology company, you are responsible for deploying a critical production application on Compute Engine. To avoid any accidental deletion of the instance by your colleagues, what measure should you take?

A. Create a custom image with a longer deletion protection period.

B. Enable autohealing on the instance group.

C. Enable delete protection on the instance.

D. Disable live migrations for the instance.

Question 40: You are working as a software engineer at a tech company and have just finished setting up a development environment for an application using Compute Engine and Cloud SQL. Your next task is to create a production environment while adhering to your company's security guidelines that prohibit network routes between development and production environments. Additionally, you are required to follow Google's recommended practices. What should be your approach to accomplish this task?

A. Create a production environment within the same project by setting up the necessary firewall rules to restrict traffic between development and production environments.

B. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

C. Enable Private Google Access and Private Service Access in the existing project to restrict traffic between the Compute Engine and Cloud SQL instances for both environments.

D. Implement a Virtual Private Network (VPN) between the development and production environments in the same project to meet the security requirements.

Question 41: You are working as a project manager in a company that uses G Suite for communication and collaboration. To streamline work processes, you need to grant certain G Suite users access to your company's Cloud Platform project. How should you proceed?

A. In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group.

B. Grant them the required IAM roles using their G Suite email address.

C. Create a GCP IAM user manually and configure G Suite accounts to sync with this user.

D. Create a CSV sheet with all users' email addresses. Use the gcloud command line tool to convert them into Google Cloud Platform accounts.

Question 42: As a project manager at a software development company, you are responsible for overseeing multiple Google Cloud Platform projects. You need to monitor resources across these projects and consolidate the reporting under a single Stackdriver Monitoring dashboard. What is the most effective approach to achieve this?

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

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

C. Enable BigQuery in each project to aggregate monitoring data and configure Stackdriver to pull data from BigQuery tables.

D. Create a single Google Cloud project with separate folders for each monitored project and link Stackdriver to the project.

Question 43: As a software developer working in a tech company, you are tasked with addressing an issue in your company's application that runs on a general-purpose Compute Engine instance. The application is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk while primarily reading large files from disk. The disk size is currently 350 GB. Your goal is to provide the maximum amount of throughput while minimizing costs. What should you do?

A. Increase the size of the disk to 1 TB.

B. Increase the allocated CPU to the instance.

C. Migrate to use a Local SSD on the instance.

D. Increase the size of the disk to 750 GB.

Question 44: As a Database Administrator at a software company, you are setting up a Linux VM that needs to connect to Cloud SQL. You have created a service account with the required access rights, but you want to ensure that the VM uses this service account instead of the default Compute Engine service account. What should you do?

A. Use the gcloud CLI to set the service account as the default Compute Engine service account for the project.

B. Create an external IP address for the VM and add it to the Authorized Networks of the Cloud SQL instance.

C. Create a separate VPC network for the VM and Cloud SQL, allowing only the service account to access it.

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

Question 45: As a software developer in a leading tech company, you are tasked with deploying a new version of your web application while ensuring that the available capacity does not decrease during the deployment, considering that your web application is currently receiving live web traffic and is deployed as a managed instance group. What action should you take?

A. Use Google Kubernetes Engine (GKE) to gradually deploy the new app version without using a managed instance group.

B. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

C. Use Google Cloud Build to push the new app version to all instances in the managed instance group simultaneously.

D. Create a new instance template with the new application version. Update the instances within the managed instance group one by one manually, without setting maxSurge or maxUnavailable values.

Question 46: As a system administrator at a tech company, you are tasked with granting access to a new operations partner who does not use Google Accounts. They need access to maintain the installed tooling on the Linux workloads running on Compute Engine instances. What is the best method for granting them access?

A. Set up Cloud VPN between your Google Cloud VPC and the internal network of the operations partner.

B. Configure a Google Cloud Pub/Sub topic that allows the operations partner to send and receive messages related to instance maintenance.

C. Configure Compute Engine instances to use an external metadata server and grant the operations partner access to that server.

D. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

Question 47: You are working at a financial organization that utilizes an internal application to handle transactional orders within a single office location. The application needs to ensure strong consistency, quick query response time, and ACID guarantees for multi-table transactional updates. The initial development of the application was done using PostgreSQL, and your goal is to migrate it to the cloud while making minimal modifications. Which database service would be the most suitable choice for this application?

A. Cloud SQL

B. Firestore

C. Cloud Bigtable

D. Datastream

Question 48: You are working as a network administrator at a software company. Your task is to set up load balancing for an instance group serving a public web application over HTTPS. You need to ensure the client SSL session is terminated at the load balancer while following Google-recommended practices. What is the best approach to achieve this goal?

A. Configure an HTTP(S) load balancer.

B. Configure a network endpoint group.

C. Configure an internal TCP load balancer.

D. Configure a regional external forwarding rule.

Question 49: You're working as a Cloud Engineer at a company that wants to migrate their on-premises workloads to Google Cloud. The current on-premises workloads consist of a Flask web application, a backend API, and a scheduled long-running background job for ETL and reporting. With a focus on keeping operational costs low and following Google-recommended practices, how should you migrate these workloads to serverless solutions on Google Cloud?

A. Migrate the web application to Cloud Functions and the backend API to Kubernetes Engine. Use Cloud Scheduler to run your background job on Compute Engine.

B. Migrate the web application to Cloud Functions and the backend API to Cloud Run. Use Cloud Pub/Sub to run your background job on Compute Engine.

C. Migrate the web application to Kubernetes Engine and the backend API to App Engine. Use Cloud Pub/Sub to run your background job on Cloud Run.

D. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

Question 50: You are working for a software development company and have just developed an application within a Docker container. Your task is to deploy this Docker image on Google Kubernetes Engine as a workload for the company's infrastructure. How should you proceed?

A. Upload the image to BigQuery and create a Kubernetes Deployment referencing the image.

B. Upload the image to Firestore and create a Kubernetes Service referencing the image.

C. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

D. Upload the image to Container Registry and create a Kubernetes StatefulSet referencing the image.

Practice Exam 12 Solutions

Solution to Question 1: D

The correct answer is D. Upload the data to Cloud Storage using the gcloud storage command.

Explanation:

When dealing with large volumes of unstructured data, it is important to find a storage solution that can provide the necessary scalability, durability, and accessibility. Google Cloud Storage is a highly scalable, durable, and available storage solution specifically designed for large scale data storage, making it the most suitable choice among the available options.

Reasons why other options will not work:

A. Cloud Spanner is a fully managed, global scale relational database service, designed to handle structured transactional data. Uploading unstructured data into Cloud Spanner is an inappropriate solution, as it is not designed for handling such data types and might lead to complexities in data processing with Dataflow jobs.

B. Firestore is a NoSQL document database designed for web, mobile, and server development from within the Google Cloud Console. Although it can handle both structured and unstructured data, it is not the ideal choice in this scenario due to its limitations on query capabilities and storage volume compared to Google Cloud Storage. Moreover, Firestore is more suitable for real-time data syncing in web and mobile applications rather than massive-scale data storage and access.

C. Kubernetes Engine is a managed environment for deploying, scaling, and managing containerized applications. It is not a storage solution, and using it to store unstructured data would not be efficient. Kubernetes Engine focuses on orchestrating and managing container deployments rather than providing a scalable storage service for data engineering purposes.

Solution to Question 2: D

The correct answer is D. Modify the existing subnet range to 172.16.20.0/24.

The reason why option D is the best choice is that it allows you to expand the available IP address pool within the same subnetwork without making any other network configuration changes. By modifying the existing subnet range to 172.16.20.0/24, you can double the number of available IP addresses and enable new VMs to communicate with the Dataproc cluster within the same VPC and subnetwork. It also minimizes the steps involved in setting up the environment.

Option A is not the best choice because creating a new subnetwork in the existing VPC would involve additional configuration and might require VMs in different subnetworks to communicate using VPC peering or routes. This would

result in more steps being involved compared to just modifying the existing subnet range.

Option B is also not the best solution because it involves creating a new VPC network, which would require VPC network peering and route configuration between the two VPCs to ensure proper communication between the Dataproc cluster and the new VMs. This would be more complex compared to expanding the subnet range in the existing VPC.

Option C is not the ideal solution either because Shared VPC is mainly used for sharing resources across multiple projects within the same organization. Configuring Shared VPC would involve creating a new subnetwork in the host project, which is an unnecessary complication for a task that can be easily solved by modifying the existing subnet range.

Solution to Question 3: B

The correct answer is B. Enable the compute.googleapis.com API.

Before setting up a Compute Engine instance using CLI, it is essential to enable the Compute Engine API. This is because Google Cloud APIs are made available under their respective APIs, which must be enabled before they can be used. Enabling the compute.googleapis.com API grants your project the necessary access to create and manage Compute Engine resources, ensuring smooth operations and preventing errors due to missing API access.

Option A, enabling the cloudresourcemanager.googleapis.com API, is not the correct choice because this API is used for managing Google Cloud resources like projects, folders, and organizations. While it's essential in creating a new project in Google Cloud, it doesn't directly relate to the management of Compute Engine instances.

Option C, creating a VPC network in the project, is not a prerequisite for setting up a Compute Engine instance using CLI. Although VPC networks are crucial for defining the networking structure and connectivity rules for your resources, you can still create a Compute Engine instance without specifying a VPC network during the creation process. Google Cloud automatically assigns the instance to the default VPC network.

Option D, creating an App Engine application in the project, is not appropriate as it deals with a different Google Cloud service, App Engine. App Engine is a fully managed platform for developing and hosting web applications, and it's entirely separate from Compute Engine. While both services might be used in the same project, they don't have any direct dependency on each other for initialization.

Therefore, the most appropriate prerequisite step to take before setting up a Compute Engine instance using CLI is option B, enabling the compute.googleapis.com API.

Solution to Question 4: D

The correct answer is D. By using the command line to run a dry run query, you can estimate the total bytes read, without actually executing the query. This allows you to check the magnitude of data usage without being charged for it. After obtaining the number of bytes read, you can use Google Cloud's Pricing Calculator to convert the bytes estimate into a cost in dollars. This will provide you with a clear cost estimate for executing the query, without having to switch pricing models or export data.

Option A is incorrect because exporting data to Cloud Storage may help in certain cases, but it does not allow you to estimate the cost of executing the BigQuery query itself. Moreover, you might incur additional costs for data storage and data retrieval.

Option B is not suitable because switching to Flat-Rate pricing only for one query and then switching back to on-demand might not be a cost-effective or practical solution. This method would also make it difficult for you to specifically determine the cost of the single query.

Option C is partially correct. While using a command line to run a dry run query can help you estimate the overall data read, it does not instruct you how to convert the data read into a cost estimate. Comparing with option D, it does not provide a complete solution for the problem.

Solution to Question 5: B

The correct answer is B. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

Explanation: Option B should be chosen because preemptible VMs offer a solution for batch workloads that can handle the termination of some VMs while also providing a significant cost reduction compared to regular VMs. Preemptible VMs are short-lived instances that can be terminated by Google Compute Engine with a 30-second notice and are up to 80% cheaper than regular instances. By testing the system using simulated maintenance events, you can ensure that your current workload can handle the termination of preemptible VMs without significant disruption to the process. If the test is successful, using preemptible N1 Standard VMs will help you save cost and maintain the desired workload in the future.

Option A is not a suitable solution because App Engine Flex is designed for applications that require custom deployment environments or additional administrative access. While App Engine Flex may provide some cost benefits, it is not specifically designed to handle nightly batch workloads that run on a large number of VMs with termination flexibility.

Option C is not the best choice because Google Dataproc is intended for running Apache Spark and Hadoop workloads. Although it offers efficient scaling and some cost reductions, it might not support the specific requirements of your nightly batch workload, especially when you need to handle the termination of some VMs.

Option D is not appropriate because preemptible N1 Highmem VMs focus on providing more memory per virtual CPU instead of focusing on providing a balance between processing power and memory like N1 Standard VMs. This may result in higher costs without offering significant benefits for your particular workload.

Solution to Question 6: C

The correct answer is C. Create a single custom VPC with 2 subnets. Create each subnet in a different region and with a different CIDR range.

Explanation:

A custom VPC enables you to create and configure the network according to your requirements. In this scenario, you need to deploy production and test workloads separately but still want them to communicate with each other using Internal IPs. Creating two subnets within the same custom VPC, each with a different CIDR range, will enable this. Placing the subnets in different regions allows for better isolation while still allowing VMs to communicate because they are within the same VPC.

Option A is incorrect because overlapping CIDR ranges will result in the inability to correctly route traffic between subnets.

Option B is incorrect because creating a separate third subnet for communication between production and test subnets is unnecessary. The VMs within the same VPC can communicate with each other using their Internal IPs, regardless of which subnet they are in.

Option D is incorrect because a Shared VPC is used to share network resources among multiple projects within an organization, rather than separating workloads as required in this scenario. Creating a custom VPC provides better isolation and control over network configurations.

Solution to Question 7: C

The correct answer is C. Here's why:

A. This option is incorrect because enabling 'block project wide keys' will block the project-wide public SSH keys from being added to the instance, but it doesn't address the requirement of providing access specifically to the dev1 team members.

B. This option is incorrect because granting the 'compute.InstanceAdmin' role to the dev1 group would unnecessarily give them administrative privileges over the entire Compute Engine instance. This goes beyond just providing SSH access and may result in unintended consequences and security risks.

C. This is the correct option because setting the metadata to 'enable-oslogin=true' for the instance ensures only authorized users can access the instance using their Google credentials. Granting the 'compute.osLogin' role to the dev1 group provides the necessary access to the instance without additional

unnecessary permissions. Directing the dev1 users to use the Cloud Shell to SSH into the instance ensures a secure and streamlined connection process.

D. This option is incorrect because the 'compute.osAdminLogin' role grants administrative access to the instance, which goes beyond the necessary SSH access permission required for dev1 team members. In addition, third-party SSH tools are not directly integrated with Google Cloud Platform's authentication and authorization mechanisms, which could lead to potential security risks.

Solution to Question 8: C

The correct answer is C because it addresses the requirement of setting up similar Google Cloud resources for the Marketing team that are organized independently of the Sales team. By creating a separate project with the ID acme-marketing-data-digest, you are establishing an independent and isolated environment for the Marketing team resources. This approach also simplifies management, and enhances security and access control.

Option A is incorrect because granting the Project Editor role for the Sales' project (acme-data-digest) to the Marketing team would not create an independent organization for Marketing's resources. It would only provide the Marketing team access to the Sales team's project, which could lead to security and data management issues.

Option B is incorrect because creating a folder within the acme-data-digest project would still keep the Marketing resources dependent on the Sales project, even if you grant them folder editor access. This does not achieve the desired independence between the two teams.

Option D is incorrect because using Cloud Composer to transfer data would, in most cases, only be useful in sharing and transferring data between teams. It does not provide a solution for creating isolated and independent environments for the Marketing team's resources.

Solution to Question 9: D

The correct answer is D. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

Explanation:

D is the correct answer because:

1. Regional Storage is the preferred choice when the data pertains to a particular geographic location. In this scenario, the patient data is originating from a specific region, making Regional Storage the appropriate choice.
2. Google Cloud Storage's Coldline storage class is designed for infrequently accessed data, with a minimum storage duration of 90 days, which is perfect for the requirement of accessing the data only once per year.

3. Adding a bucket lifecycle rule that archives data after 30 days to Coldline Storage meets the compliance requirement of archiving the data after 30 days.

Considering other options:

A. Select Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Cloud Storage Archive.

- This option is incorrect because there is no "Cloud Storage Archive" storage class in Google Cloud Platform. Coldline Storage is what's needed for long-term data archival.

B. Select Multi-Regional Storage. Add a bucket lifecycle rule that moves data to Cloud SQL after 30 days.

- This option is incorrect because Multi-Regional Storage is not required when the data is specific to a particular geographic location. Additionally, moving the data to Cloud SQL is not appropriate for data archival purposes.

C. Select Multi-Regional Storage. Add a bucket lifecycle rule that archives data after 30 days to Coldline Storage.

- This option is incorrect because Multi-Regional Storage is not necessary when the data is specific to a single geographic location. In this case, Regional Storage is the suitable option.

Hence, Option D is the most appropriate answer to meet the given requirements.

Solution to Question 10: D

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

Explanation:

The autoscaling policy is adding more instances than necessary because the policy evaluates the health of the newly added instances too early. The problem occurs because the virtual machine instances take about three minutes (180 seconds) to become available for users, while the initial delay for HTTP health checks is set to 30 seconds. This means that autoscaling is triggered when a new instance is not ready to handle traffic yet, leading to the creation of additional instances unnecessarily.

To maintain proper instance group sizes when autoscaling, you should:

D. Increase the initial delay of the HTTP health check to 200 seconds. This way, the autoscaling policy will wait until each newly added instance is ready to handle end-user traffic before evaluating if another instance is required. This will prevent the creation of unnecessary instances.

The other options are not correct as they do not resolve the issue properly:

A. Decreasing the initial delay to 10 seconds would only worsen the situation because the autoscaling policy would be triggered even earlier before the virtual machine instances are available for users.

B. Using an HTTP(S) load balancer instead of a TCP load balancer will not resolve the issue since the problem is with the initial delay for health checks. The type of load balancer is irrelevant to the current issue.

C. Decreasing the autoscaling threshold to 50% would trigger the creation of additional instances at a lower CPU utilization rate. This approach would make the instance group even more oversized and result in more unnecessary virtual machines in the group.

Solution to Question 11: A

The correct sequence of steps to set up a Compute Engine instance in a new project is Option A, which involves using the Cloud SDK to create a new project, enabling the Compute Engine API in that project, and then creating the instance specifying your new project. This sequence ensures that you create the new project first, enable the necessary API, and then proceed to create the instance within the properly-configured project.

Option B is not the correct choice, as it only describes the creation of a service account with permissions to create Compute Engine instances. It does not mention the process of creating a new project, enabling the Compute Engine API, and actually creating the instance.

Option C is incorrect because one cannot create a Compute Engine instance in the default project and then move it to the new project using the Cloud Console. Creating the instance in the correct project from the start is essential to properly organizing resources and managing access permissions.

Option D is also incorrect, as it misleadingly includes enabling the Firestore API, which is unrelated to creating a Compute Engine instance. Additionally, it does not mention enabling the Compute Engine API in the new project. The proper step is to enable the Compute Engine API to be able to create an instance.

Solution to Question 12: A

The answer should be A: Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

Explanation:

A managed instance group (MIG) requires an instance template that contains valid syntax for creating instances. The alert mentioned that new instance creation has failed, which suggests that there might be an issue with the instance template's syntax or naming conflicts with persistent disks. Therefore, creating a new instance template with valid syntax and ensuring there are no naming conflicts with persistent disks is the appropriate action.

Here's why the other options will not work:

B: Verifying the syntax of the instance template being used is a good step, but it does not address the issue of potentially conflicting persistent disks. Also, increasing the instance count will not resolve the problem if instance creations are failing due to errors or conflicts.

C: Deleting the current instance template and creating a new instance group might unnecessarily disrupt the functioning of the existing infrastructure. This option also does not mention updating the instance group to use the new template.

D: While creating a new instance template with valid syntax is a good step, setting the disks.autoDelete property to false might result in accumulating unused disks, which could lead to higher costs and management overhead. This option also does not mention updating the instance group to use the new template.

In summary, Option A is the best answer because it directly addresses the underlying issue (syntax errors in the instance template and potential conflicts with persistent disks) without causing unnecessary disruptions to the existing infrastructure or undesired side effects.

Solution to Question 13: A

The correct answer is A. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

Here's why the other options will not work:

Option B: An internal TCP/UDP load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend. This option doesn't work because an internal TCP/UDP load balancer cannot handle HTTP(S) requests. Additionally, it is designed for internal use within a Virtual Private Cloud (VPC) network and isn't well-suited for distributing external traffic.

Option C: An external HTTP(S) load balancer with managed SSL for the backend service and an additional Cloud Pub/Sub integration for distributing the requests for the static content to the Cloud Storage backend. While this option uses an external HTTP(S) load balancer, it needlessly complicates the setup with Cloud Pub/Sub integration. This isn't necessary for the distribution of requests for static content to the Cloud Storage backend as a URL map is more suited for this purpose.

Option D: An external HTTP(S) load balancer with a managed SSL certificate to distribute the load, and Google Cloud Storage FUSE to serve static content from the compute instances. Although this option uses an external HTTP(S) load balancer, it doesn't effectively handle distributing the static content. FUSE serves content from Cloud Storage on the local file system of the instances,

causing additional unnecessary overhead, and it doesn't use the URL map's capabilities.

In summary, option A is the best choice because it uses an external HTTP(S) load balancer to effectively distribute user traffic while leveraging a managed SSL certificate for security. The URL map allows for easy targeting of requests to Cloud Storage for optimally serving static content. This setup meets all the requirements for a secure, autoscaling website with enhanced performance for the client.

Solution to Question 14: D

The correct answer should be option D, and other options will not work for the following reasons:

A. Deploying a Kubernetes cluster on your on-premises servers using Anthos and configuring the application to access Cloud Storage using the Anthos Service Mesh does not address the actual requirement of not having public IP addresses or access to the internet for the servers in the on-premises data center.

B. While creating a VPN tunnel and using a Squid proxy server in Google Cloud VPC might seem like a possible solution, it does not follow Google-recommended practices for connecting on-premises resources securely to Google Cloud Storage. Furthermore, this option adds unnecessary complexity by introducing an additional proxy layer, leading to potential performance and maintenance concerns.

C. Negotiating with the security team to provide a public IP address to the servers and allowing egress traffic only to storage.googleapis.com contradicts the strict security policies the company has in place. Relying on IP addresses exclusively is not recommended since Google Cloud Storage may use different IPs or IP ranges, which could cause the application to lose access over time.

On the other hand, option D provides the best solution by fulfilling the requirements:

1. Using Cloud VPN or Interconnect, you can create a secure and private tunnel from your on-premises network to a Virtual Private Cloud (VPC) in Google Cloud. This helps maintain the strict security policies prohibiting public IP addresses and internet access for the on-premises servers while still allowing them to communicate with Google Cloud Storage.
2. Cloud Router allows creating a custom route advertisement for the reserved IP range (199.36.153.4/30) used by Google's restricted.googleapis.com domain. Announcing this network through the VPN tunnel enables restricted access to Google services only, keeping the servers compliant with the company's security policies.
3. Configuring the on-premises DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com ensures that the application communicates only with the restricted version of Google APIs and services, reducing the risk of security breaches or unauthorized access.

In summary, option D is the correct choice as it provides a secure and compliant way to connect the on-premises servers with Google Cloud Storage, while the other options either do not address the security requirements or involve unnecessary complexities.

Solution to Question 15: A

The best course of action for your company is option A: Ingest the data into Cloud Bigtable and create a row key based on the event timestamp.

Here's why option A is the most suitable choice:

1. Scalability: Cloud Bigtable is designed to handle billions of rows and terabytes of data, making it an ideal choice for handling large-scale machinery IoT data with thousands of hourly events per device.
2. Data Consistency: By using the event timestamp as the row key, you ensure that data is stored in a consistent and time-ordered manner, allowing for efficient queries and accurate billing.
3. Atomic Storage and Retrieval: Cloud Bigtable supports row-level atomic operations, enabling atomic storage and retrieval of individual signals.
4. Performance: Cloud Bigtable provides low-latency and high-throughput performance, ensuring that real-time data processing and analysis can be carried out effectively even in high-traffic scenarios.

Reasons why other options will not work:

B. Cloud Filestore: While it can store the data, it does not provide the required level of scalability, data consistency, and atomic operations needed for this use case.

C. Cloud Storage: Although Cloud Storage is highly scalable, it does not provide atomic append operations, which could lead to incorrect data and billing inconsistencies. Additionally, event data stored in Cloud Storage may not be easily queriable, making it inefficient for processing and analysis.

D. Cloud SQL: While Cloud SQL is suitable for transactional processing, it is not designed to handle the high volume of time-series data generated by large-scale machinery with thousands of hourly events per device. Moreover, its performance may not be optimal for this scenario.

Solution to Question 16: B

The correct answer is B. Configure Cloud Identity-Aware Proxy for SSH and TCP resources.

Explanation:

Option B allows you to set up Cloud Identity-Aware Proxy (IAP) to access instances securely over SSH without needing public IPs. IAP enables context-aware access control for SSH and TCP resources based on user identity, group,

and project membership. Hence, it fulfills the requirement of accessing instances via SSH without specifying access for each instance.

Reasons why other options will not work:

Option A: Enabling Cloud Armor with an SSH policy for the instances would provide protection against Distributed Denial of Service (DDoS) attacks and traffic filtering. However, it does not address the requirement of enabling access to instances without configuring specific access and without public IP addresses.

Option C: Using Cloud Load Balancer with the TCP Proxy protocol for the instances would help distribute traffic among multiple instances, but it does not fulfill the requirement of accessing instances without public IP addresses. Moreover, it does not provide a secure way to enable SSH access without configuring specific access for both existing and new instances.

Option D: Creating an SSH keypair and storing the public key as a project-wide SSH Key would allow access to all instances within the project. However, it does not address the requirement of accessing the instances without a public IP, as the instances would still need public IP addresses for SSH access over the internet.

Solution to Question 17: D

The correct answer is D. The reason for choosing D and not the other options is as follows:

A. Using the 'testing' support level for role permissions is not suitable for a production environment. This is because permissions labeled as 'testing' are not guaranteed to be stable and may change or be removed without notice. Setting the role stage to GA (General Availability) while testing the role permissions doesn't communicate the role's first-version status, which may mislead users regarding its stability and reliability.

B. Setting the role stage to GA (General Availability) while testing the role permissions is not recommended as it may lead to confusion about the stability and the version of the custom role. GA stage should be reserved for stable, production-ready roles. Thus, this option is not suitable.

C. Although using the 'testing' support level for role permissions and setting the role stage to PRE-ALPHA conveys that the role is in its preliminary stage, it is unsuitable for a production environment. Permissions labeled as 'testing' may change or be removed without notice, creating instability in production use cases.

D. This option uses the 'supported' support level for role permissions, ensuring that the custom IAM role being developed is stable and suitable for production use. Setting the role stage to ALPHA effectively communicates that the custom role is in its first version and not its final state. This allows the entire organization to be aware of its current status and proceed accordingly. Hence, this option is the most appropriate for achieving the lead developer's goal.

Solution to Question 18: D

The correct answer is D. This is because Cloud Functions provide a fully managed, serverless compute solution that will automatically respond to specific triggers, like the storage events from a Cloud Storage bucket. By creating a Cloud Function that triggers on Cloud Storage events, you can ensure that each uploaded file is submitted to the Speech-to-Text API as soon as it's uploaded. This approach aligns with Google-recommended practices such as event-driven architecture and authentication using the built-in features of Cloud Functions.

Option A is incorrect because Cloud Pub/Sub is a messaging service designed for asynchronous communications between applications and components. While it is useful for many use cases, it does not directly handle processing or calling APIs, and thus, would require additional components to achieve the desired result.

Option B is also incorrect because deploying a Kubernetes job for regularly scanning the bucket adds complexity to the architecture and does not align with the requirement of a serverless solution, as Kubernetes requires management of clusters and resources.

Option C is not a suitable solution because Cloud Shell is designed for interactive administration and development, not for deploying scheduled scripts. Furthermore, using Cloud Shell in this manner would not be a serverless solution, as it does not provide the required automation and management capabilities.

In summary, option D is the best approach because it meets all requirements, including a fully managed serverless compute solution, automatic triggering on storage events, and adherence to Google-recommended practices.

Solution to Question 19: B

The correct answer is B. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles. The reason this is the best approach is because it adheres to Google's recommended practices for providing the least amount of privileges necessary for the auditors to perform their tasks, which are to view logs and data in BigQuery.

Option A is wrong because adding the auditor user accounts to the 'bigQuery.jobUser' and 'bigQuery.dataOwner' predefined IAM roles would grant the auditors unnecessary permissions beyond their auditing tasks. The 'bigQuery.jobUser' role would allow the auditors to run jobs, while the 'bigQuery.dataOwner' role would grant full control over data and metadata, leading to potential issues with data integrity and security.

Option C is wrong because creating custom IAM roles for this purpose is unnecessary. The predefined IAM roles provided by Google ('logging.viewer' and 'bigQuery.dataViewer') already include the necessary permissions for the auditors to efficiently complete their tasks.

Option D is wrong because adding the auditors group to the 'bigQuery.dataViewer' role is correct, but the 'logging.admin' role provides excessive permissions. The 'logging.admin' role grants full control over logs, including the ability to modify and delete logs, which isn't necessary for audit logging. The 'logging.viewer' role is more appropriate, as it only allows the auditors to view existing logs without making changes.

Solution to Question 20: A

The correct answer is A: Use the command gcloud auth activate-service-account and point it to the private key. The reason behind this is that this command is specifically designed to let you authenticate using the Service Account credentials JSON file. It registers the service account with the gcloud tool, making it the active account for future gcloud commands. This way, you can use the correct authentication and authorization for accessing the required resources in the Google Cloud project.

Option B is not correct because the gcloud init command is used to initialize the Cloud SDK on your local machine, setting up the default user account and project. The gcloud init command initializes the SDK configurations and doesn't relate to service account authentication.

Option C is not correct because there is no active_credentials.json file involved in the authentication process. Placing the private key file and renaming it inside the .config/gcloud folder in your home directory will not work for proper authentication.

Option D is not correct because setting the environment variable GOOGLE_APPLICATION_CREDENTIALS with the private key's path is a method to authenticate with application default credentials. This is used to set the default Service Account for applications running on the local machine or a Google Cloud Platform service but not for the gcloud commands.

In conclusion, the best way to use a Service Account private key for authentication and authorization when executing gcloud commands is to use the gcloud auth activate-service-account command and provide the private key's path.

Solution to Question 21: A

The correct answer is A: Expand the CIDR range of the relevant subnet for the cluster.

Explanation:

A. Expanding the CIDR range of the relevant subnet for the cluster is the best solution in this scenario. By expanding the CIDR range, you can accommodate more IP addresses, providing the necessary IP space for the Kubernetes Engine clusters to expand with more nodes when required. This action directly addresses the core issue of exhausted IP addresses.

B. Creating an additional node pool with a smaller node count within the same

subnet does not resolve the issue of exhausted IP addresses. It may temporarily alleviate the problem by providing a little more headroom for cluster expansion, but it still utilizes the same CIDR range with limited IP addresses and the problem could reoccur in the future.

C. Creating a new region for the GKE clusters is not a suitable solution in this case. The issue is not related to the regions but rather to the exhausted IP addresses in the subnet. A new region will not guarantee sufficient IP space for the clusters to expand with more nodes when necessary.

D. Adding an alias IP range to the subnet used by the GKE clusters might help with allocating more IP addresses to the subnet. However, it does not directly increase the IP address capacity of the subnet itself. Even if you add an alias IP range, there might still be a shortage of IP addresses for the nodes. Expanding the CIDR range of the subnet (Option A) is a direct and more effective solution to the problem.

Solution to Question 22: A

The correct answer is A. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold. This is because it is the Google-recommended solution that helps in creating automatic notifications for high latency, without any additional development costs involved. Setting up an alert policy based on latency thresholds allows support teams to quickly react to issues as they happen, ensuring a better user experience.

Option B is not ideal because exporting Cloud Monitoring metrics to Cloud Storage and using Data Studio would create an additional overhead of managing storage and creating custom dashboards, which can lead to more costs and would not provide real-time notifications as required by the support team.

Option C is not a good choice because Stackdriver Logging is primarily used for analyzing logs and not for monitoring metric thresholds like latency. It would involve custom implementation to convert logs into latency metrics, which may incur development costs and may not provide real-time alerts as needed.

Option D is not recommended because it involves manual monitoring using the Cloud Monitoring dashboard, which is not automated and might not allow the support team to immediately react to instances of high latency. This approach would not meet the requirement of sending automatic notifications when latency is crossed.

Solution to Question 23: B

The correct answer is B. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, and BigQuery.

Explanation: In processing time-series data for a finance company, you need services to handle streaming data, transform and process the data, store the processed data, and analyze it.

1. Cloud Pub/Sub: It's a messaging service to handle streaming data and data ingestion in real-time. It allows you to decouple data producers and data consumers. So in this case, it helps in ingesting real-time time-series data.
2. Cloud Dataflow: It's a fully-managed service for executing Apache Beam pipelines. Cloud Dataflow is used to perform transformations and process the data, including cleaning, aggregating, and windowing the time-series data.
3. Cloud Bigtable: It's a highly-scalable, low-latency NoSQL database suited for time-series data. It provides good performance in handling sequential writes or reads and can store large amounts of data. It is useful in storing processed time-series data in a well-structured form for further analysis.
4. BigQuery: It's a fully-managed, serverless data warehouse for large-scale data analytics. It enables you to analyze the time-series data and derive insights, generate reports, and visualize the data using SQL-like queries.

Why other options will not work:

A. Cloud Storage is an object storage service, not suitable for streaming data ingestion or real-time processing. Cloud Datastore is a NoSQL database designed for web and mobile applications, not for time-series data.

C. Cloud Datastore, while a NoSQL database, is not optimized for time-series data. It is designed for web and mobile applications and does not deliver the performance required for time-series data processing.

D. Cloud Dataproc is a managed Hadoop and Spark service, which can be used for batch processing but does not fit the real-time processing needs of time-series data. Cloud Storage, while useful for storing large amounts of data, is not optimized for the real-time processing requirements of time-series data pipelines.

Solution to Question 24: D

The correct answer is D: "Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days."

Explanation:

Option A uses Data Fusion, which is a data integration tool, not a logging analytics solution. Even though you could potentially extract logs from Stackdriver and load them into a BigQuery table with a 60-day expiration, it does not follow Google-recommended practices for aggregating logs. Data Fusion is not the best tool for this task.

Option B talks about navigating to Stackdriver Logging and selecting resource.labels.project_id="*". However, this approach is inefficient and won't give you a complete analysis of all the logs for all projects. It may help you view logs in the console, but it won't provide an aggregate dataset needed for further analysis.

Option C uses a Cloud Function to read logs from Stackdriver Logging and writes them to Cloud Spanner, with a retention policy of 60 days. While the Cloud Function could potentially ingest logs from Stackdriver Logging, using Cloud Spanner for log analysis is not a Google-recommended practice, and it might not be cost-effective compared to using BigQuery for large-scale log storage and analysis.

Option D is the correct and recommended approach. By creating a Stackdriver Logging Export with a Sink destination to a BigQuery dataset, you can easily aggregate logs from all your GCP projects in one place, following Google's recommended best practices. Configuring the table expiration for 60 days ensures that the company's requirement of having 60 days of log history is also satisfied. BigQuery is an excellent choice for analyzing large-scale log data, and this method is in line with Google's recommendations for working with logs in GCP.

Solution to Question 25: A

The correct answer is A: Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

This is the correct choice because granting the bigquery.dataViewer role to the service account in the crm-databases-proj project will give it access to view the data in the BigQuery datasets within that project. Additionally, providing the appropriate roles to the web-applications project will allow the VMs running in that project to use the service account effectively.

Reasons why other options will not work:

B. Creating a new dataset in the web-applications project and replicating the crm-databases-proj main dataset will consume unnecessary additional storage and doesn't allow for real-time data access between projects. Additionally, this approach doesn't follow the Google-recommended practices for service account access.

C. Creating a new service account in the crm-databases-proj and giving it a bigquery.dataViewer role in the web-applications project is not a correct approach because the service account should be created in the web-applications project, not in the crm-databases-proj project. This way, a single service account is used to manage all resources running in the web-applications project, following Google's best practices.

D. Granting both bigquery.dataViewer role to crm-databases-proj and bigquery.dataOwner role to the web-applications project is unnecessary since the dataOwner role includes dataViewer permissions, among others that might not be needed to read the data. In addition, it is important to follow the Principle of Least Privilege (PoLP), and giving excess privileges can lead to potential data breaches or misuse.

Solution to Question 26: D

The best approach to successfully deploy the current application to a serverless Google Cloud solution is D: Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

Option D is the most suitable because it allows you to leverage the existing CI/CD pipeline and Docker-based infrastructure that you are already familiar with. Cloud Run is designed to easily support containerized applications with minimal changes, making it an ideal choice for Python-based microservices. Furthermore, it fully manages the underlying infrastructure, ensuring the serverless characteristics of the deployment. Additionally, updating the configurations and required endpoints is consistent with your current setup.

Option A – While the App Engine Flexible Environment can support Python-based microservices, it requires you to re-architect and potentially rewrite some parts of your application. Also, it does not natively support the Docker containers that your current application is using. This approach involves more effort compared to deploying the existing Docker containers to Cloud Run.

Option B – Using Firestore as a serverless database and rewriting all microservices to store configurations in Firestore seems unnecessary and time-consuming. It would also require additional efforts for a complete transition from environment variables to Firestore. Besides, Firestore focuses on database services, while Cloud Run is better suited for containerized applications like yours.

Option C – Cloud Build is inappropriate for deploying the application since it is more focused on building, testing, and packaging the code rather than managing and running the infrastructure required for the application. Using Cloud Build would result in missing the serverless benefits and running the actual services with proper scaling, which Cloud Run provides.

In summary, Option D is the most appropriate approach since it supports your existing Docker-based infrastructure, leverages the existing CI/CD pipeline, and provides a serverless deployment without requiring significant changes to your application's architecture.

Solution to Question 27: D

The correct answer is D. Create a snapshot schedule for the disk using the desired interval.

Explanation: As a database administrator, your primary concern is to ensure that the boot disk's data is backed up regularly and that backups can be restored quickly in the case of disaster. In addition, you want to follow Google-recommended practices and have older backups cleaned automatically to save costs.

Option D, creating a snapshot schedule for the disk using the desired interval, aligns with your needs as a database administrator. Snapshot schedules allow you to automate the process of taking snapshots of your persistent disks at

regular intervals, ensuring that you have the latest copies of your boot disk data to restore quickly if needed. Furthermore, Google Cloud Platform automatically manages snapshot retention and deletes older snapshots based on the defined retention policy, helping you save costs.

Option A, creating a Cloud Task to create an image and export it to Cloud Storage, is not the ideal strategy. While it would create backups of the boot disk, this method is not as efficient or cost-effective as creating a snapshot schedule. Exporting images to Cloud Storage would not be suitable for a database that needs to be restored quickly since it is time-consuming to recreate disk volumes from the exported images.

Option B, using Cloud Memorystore for Redis to keep regular copies of the boot disk data, is not suitable for this use case. Cloud Memorystore is intended to work as a cache, and it doesn't provide backup functionality for boot disks.

Option C, using Cloud Filestore to store regular copies of the boot disk files, is not the right solution for this scenario. Although Cloud Filestore provides cloud-based file storage, it does not offer the same automated backup scheduling and seamless retention management as snapshot schedules. Manually copying the boot disk files to Cloud Filestore also introduces a greater chance of human error or inconsistency in the backup process.

In conclusion, the best strategy for ensuring the boot disk's data is backed up, quickly restorable, and cost-effective, while following Google-recommended practices, is option D: Create a snapshot schedule for the disk using the desired interval.

Solution to Question 28: D

The correct answer to this question is option D: In the Google Cloud Platform Console, create a new billing account and set up a payment method.

Explanation: As an IT manager, the main concern is to centralize and streamline all the billing processes to the company's account for better expense management and accountability. Creating a new billing account in the Google Cloud Platform Console and setting up a payment method linked to the company's financial resources, such as a corporate credit card, can address this issue effectively. This will allow for easy tracking of expenses and central management of all projects.

Why other options will not work:

A. In the Cloud Console, create a new billing account and manually transfer each employee's project to the root Organization. This option is not the best solution because creating a new billing account alone does not centrally manage the billing. Transferring projects to the root Organization may organize projects but does not address the issue of creating a centralized billing account with the company's financial resources.

B. Create a billing account in the Google Cloud Console with the company's GCP-related expenses only. This option is vague and does not exactly specify how to create a centralized billing account with the company's financial resources. It also does not mention connecting a payment method, which is essential for the IT manager's goal to streamline and centralize billing.

C. Contact the GCP sales team to request a new, centralized billing account for your company's projects. While contacting the GCP sales team may provide guidance, it is not an action that directly creates a centralized billing account. The IT manager should take action within the Google Cloud Platform Console by creating a new billing account and setting up a payment method to efficiently centralize and streamline billing for all projects.

Solution to Question 29: C

The answer should be C. Configure regional storage for the region closest to the users. Configure a Standard storage class. Here's why:

A. Configure dual-regional storage for the region furthest from the users. Configure an Archive storage class. – This option would not work because configuring dual-regional storage for the region furthest from the users would introduce higher latency for the majority of users in Boston, MA. Additionally, Archive storage class is designed for long-term, infrequently accessed data, and it wouldn't suit the needs of a continuous analytics pipeline.

B. Configure regional storage for the region closest to the users. Configure an Archive storage class. – This option would not work because, although configuring regional storage for the region closest to the users would be appropriate, Archive storage class is not suitable for a continuous analytics pipeline that requires frequent data access.

C. Configure regional storage for the region closest to the users. Configure a Standard storage class. – This is the best course of action. Regional storage ensures low-latency access for the majority of users in Boston, MA, while the Standard storage class provides low-cost storage with performance suitable for continuous analytics pipelines.

D. Configure dual-regional storage for the dual region closest to the users. Configure a Standard storage class. – This option would not work because the dual-regional storage would increase the costs compared to the regional storage without providing significant benefits for the majority of users that are already located in Boston, MA. Regional storage provides lower costs and optimal data storage performance for the given situation.

Solution to Question 30: D

The correct answer is D, "Create a custom log-based metric for the specific error to be used in an Alerting Policy". This is because creating a custom log-based metric focused on the specific error will allow you to monitor the occurrence of the error in real-time and to implement an Alerting Policy based on this metric.

The Alerting Policy will notify you promptly if the problem arises again, aiding in the quick resolution of the issue and providing better user experience.

Other options are not suitable for the following reasons:

A. "Create a sink to BigQuery to export all the logs. Create a Data Studio dashboard on the exported logs." This option, while providing a visual representation of the log data, does not provide real-time alerting capabilities. It requires manual monitoring of the dashboard to detect the occurrence of the specific error, which is not as timely and efficient as setting up an Alerting Policy based on a log-based metric.

B. "Grant Project Owner access to the Service Account." This option is not recommended because it grants excessive permissions to the Service Account which may pose security risks. Also, it does not address the need for prompt notifications when the problem arises again.

C. "Modify the error log severity level to Warning." Changing the severity level of the error logs will not help in promptly notifying you if the problem arises again. It only alters the log severity classification, and does not contribute to real-time monitoring or alerting of the specific error occurrences.

Solution to Question 31: C

The correct answer is C because it directly addresses the requirements of the task, which is to confirm the creation of a new Google Cloud Platform service account at a specific point in time.

Option C instructs you to filter the Activity log to view the Configuration category, which records changes to the Google Cloud Platform's service accounts. Additionally, filtering the Resource type to Service Account ensures that you are specifically looking at service account-related log entries, making it the most appropriate option.

Option A is incorrect because it refers to the Compute Engine resource type, which is related to virtual machines and not service accounts.

Option B is incorrect as it suggests filtering the Data Access category, which tracks access to user-provided data and not configuration changes like service account creation. Additionally, the Resource type mentioned (Networking) is not related to service accounts either.

Option D is incorrect for two reasons. First, it refers to Stackdriver logs, which have now been incorporated into Google Cloud Logging and Monitoring; thus, the answer is outdated. Second, it asks to filter by Google Project as a resource type, which is irrelevant to the task of determining a specific service account's creation.

Solution to Question 32: B

The correct answer should be B. Link the acquired company's projects to your company's billing account. This approach allows you both to consolidate all

costs from both companies onto a single invoice and to achieve this starting from tomorrow. It is the most efficient way since you only need to link the projects of the acquired company to your existing billing account, which would combine all costs without any additional setup or configuration.

Option A, enabling cost aggregation, would not help in consolidating the costs onto a single invoice as it only summarizes and organizes the cost data within a billing account. It does not merge the costs from two separate billing accounts into one.

Option C, configuring both billing accounts to send email notifications whenever a new invoice is issued, would only help in tracking the invoices for both companies but would not merge the expenses onto a single invoice.

Option D, creating a new GCP organization and a new billing account, might seem like a reasonable choice, but it is not an efficient approach. This option involves extra steps like creating a new organization and billing account, then migrating all the projects for both companies into the organization. In addition, the question asks for the most efficient approach with a start date of tomorrow, which makes this option less suitable due to the significant time and effort required to execute these migration steps compared to simply linking the acquired company's projects to your company's billing account.

Solution to Question 33: B

The correct answer is B: Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

Explanation:

Option A is not suitable because it archives the data to Coldline Storage after 30 days. Coldline Storage is more suitable for long-term storage and infrequent access. In this case, the previous versions are accessed once a month, which means that Nearline Storage would be a more cost-effective solution.

Option B is the best choice because it meets the requirements by archiving newer versions of the data after 30 days to Nearline Storage. Nearline Storage is designed for infrequently accessed data, making it a cost-effective solution. Additionally, it allows for multiple versions of the data to be archived and will enable easy data retrieval for generating monthly reports and any necessary updates.

Option C is not suitable because it archives the data with newer versions to Coldline Storage. As mentioned earlier, Coldline Storage is suitable for long-term storage with infrequent access, making it less cost-effective for data that is accessed monthly.

Option D is not suitable because it archives older versions of the data after 60 days to Nearline Storage. In this case, the data must be archived after 30 days, so this option does not meet the requirements.

In conclusion, option B is the best choice for a cost-effective archiving solution that allows multiple versions of the data to be archived after 30 days and supports the required monthly access and update frequency.

Solution to Question 34: C

The correct answer is C, as the best approach to achieve an operationally efficient and quick scaling of the application on Google Cloud Platform is to create an instance template and use the template in a managed instance group with autoscaling configured. This method allows the infrastructure to automatically scale based on underlying CPU usage without any manual intervention. It also follows the company's policy of using virtual machines directly.

Option A does not work because Cloud Functions are serverless and not meant to manage virtual machines directly. Moreover, using Cloud Functions would add additional complexity to the setup and might cause latency in scaling.

Option B is not ideal because it relies on third-party tools when Google Cloud Platform natively supports automatic scaling of Virtual Machines using managed instance groups. Relying on third-party tools introduces potential issues like higher costs, compatibility problems, and additional maintenance work.

Option D is unsuitable because Cloud Dataflow is used for processing data pipelines and is not meant for managing the scaling of virtual machines or applications directly. Using Cloud Dataflow for the described scenario would be an incorrect way to handle scaling in Google Cloud Platform.

Hence, the best approach to meet the company's requirements, quickly scale the application, and maintain operational efficiency is to use an instance template and create a managed instance group with autoscaling configured (Option C).

Solution to Question 35: C

The correct answer is C: Add the users to a group, and add this group to roles/browser.

Explanation:

Option A is incorrect because the roles/cloudtrace.agent role is used for granting permission for tracing applications and managing traces. This role doesn't provide the ability to view the entire Google Cloud hierarchy.

Option B is incorrect because the roles/compute.admin role grants admins all the permissions to manage every resource within the Compute Engine. This role grants more permissions than necessary for simply viewing the Google Cloud hierarchy.

Option C is correct because adding the users to a group and assigning this group to roles/browser is the best course of action in this scenario. The roles/browser role provides the least privilege, enabling users to view the hierarchy in Google Cloud, which fulfills the given security requirement. Roles/browser allows read

access to browse Google Cloud resources metadata, without granting permission to modify any resources.

Option D is incorrect because the roles/bigquery.dataViewer role is meant for providing read-only access to BigQuery datasets. This role is specific to BigQuery and would not grant the necessary permissions to view the Google Cloud organizational hierarchy.

In summary, adding users to a group and assigning this group to roles/browser follows the least privilege principle and Google's recommended practices, ensuring that only selected team members can view the entire hierarchy without granting them unnecessary permissions.

Solution to Question 36: B

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

Explanation: When you need to create a new project for the production environment, you should use the gcloud command-line tool to create the new project. gcloud is a part of the Google Cloud SDK, which is a set of tools and libraries for interacting with Google Cloud Platform services.

After creating the new project, you should deploy your App Engine application to this project using the appropriate gcloud command. This way, you are ensuring that your application is correctly set up and configured for the production environment.

Here's why the other options will not work:

A. Create a Deployment Manager configuration file that copies the current App Engine deployment into a new project. - Deployment Manager is used for infrastructure deployment and management, but it doesn't support copying an existing App Engine deployment into a new project.

C. Use gcloud to create the new project and to copy the deployed application to the new project. - While gcloud can be used to create a new project, it cannot directly copy a deployed application from one project to another. You need to deploy the application code to the new project instead.

D. Use Dataflow to copy the application code from one project to another for deployment. - Google Cloud Dataflow is designed specifically for large-scale data processing and analytics, not for deploying or copying App Engine applications between projects.

Solution to Question 37: B

The correct answer is B which involves enabling the Compute Engine and Cloud Storage APIs using the gcloud services enable commands. This is because API services are essential in providing the necessary tools for interacting with Google Cloud Services programmatically, and it's a Google-recommended practice to enable the necessary APIs before creating any infrastructure components.

Option A is not suitable as it suggests manually creating instances, firewalls, and storing data without enabling any APIs. This approach may not be compatible with company policies and Google-recommended practices, as it lacks the required API enablement for proper interaction.

Option C is not a good choice either, as it entails deploying instances and setting firewall rules without enabling the required APIs. This may lead to compatibility issues and doesn't follow the best practices recommended by Google.

Option D is not ideal since it recommends enabling individual APIs only after an error message prompts you. This is not a proactive approach and may slow down infrastructure management and development, leading to potential issues and delays that could have been avoided had the APIs been enabled beforehand.

Solution to Question 38: D

The best way to run this reverse proxy in GCP is by using option D: creating a Cloud Memorystore for Redis instance with a 32-GB capacity.

Cloud Memorystore is a managed in-memory datastore that provides a fast and scalable caching solution, particularly suitable for low-latency and latency-sensitive applications like the one in question here. By setting up a 32-GB Redis instance, you allocate the required 30 GB for the in-memory cache and the additional 2 GB for other processes, effectively meeting the requirements while minimizing costs.

Options A and B are not appropriate solutions because they rely on storage services (Cloud Storage and Cloud Filestore) for caching, which introduce higher latency and are not designed for caching purposes. These services are better suited for storing data, not optimizing low-latency web services.

Option C suggests using a container image and deploying it on Kubernetes Engine, utilizing n1-standard-32 instances as nodes. While running a reverse proxy as a container in a Kubernetes cluster is a viable option, it would likely result in higher costs and complexity than using Cloud Memorystore. The n1-standard-32 instances are quite resource-heavy, and your use case does not require a lot of CPU, making this an inefficient and expensive option. Thus, option D is the most suitable and cost-effective solution for running the reverse proxy in GCP.

Solution to Question 39: C

The correct answer is C. Enable delete protection on the instance.

Explanation:

A. Create a custom image with a longer deletion protection period:

Creating a custom image with a longer deletion protection period will not prevent accidental deletion of the instance by your colleagues. Deletion protection is a property of instances and not of custom images. Therefore, this option will not be effective in addressing the issue at hand.

B. Enable autohealing on the instance group:

Autohealing is a feature that monitors the instances in a managed instance group and automatically recreates them when they become unresponsive or unhealthy. While this feature ensures high availability and maintains a specific number of healthy instances, it does not prevent accidental deletion of instances by your colleagues. Hence, this option is irrelevant to the problem.

C. Enable delete protection on the instance:

Delete protection is a feature provided by Google Compute Engine specifically to prevent instances from being accidentally deleted. When enabled, this feature blocks the deletion of an instance until the delete protection is disabled. This measure ensures that instances cannot be deleted by mistake, preserving your critical production application. Therefore, this is the most appropriate and effective solution.

D. Disable live migrations for the instance:

Disabling live migrations does not protect the instance from accidental deletion by your colleagues. Live migrations are used to relocate running instances to another host for maintenance or other reasons without any downtime to the instances. Disabling this feature would only prevent automatic migrations for the instance but would not add any protection against accidental deletion. Thus, this option does not address the main concern.

In conclusion, the best measure to avoid accidental deletion of the critical production application on Compute Engine is to enable delete protection on the instance, as described in option C.

Solution to Question 40: B

The correct answer is B: Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

The rationale behind the answer:

- The primary reason behind our choice is that Google's best practices recommend separating different environments, like development and production, into separate projects. Doing so helps to maintain isolation and minimize the risk of unwanted interactions between these environments, which aligns with the company's security guidelines.
- By creating a new project, we can apply specific Identity and Access Management (IAM) permissions, quotas, and policies without affecting the development environment, providing a greater level of control and security.
- Additionally, it is easier to manage billing and resources for each environment by keeping them in separate projects.

Why other options will not work:

A. The issue with this option is that it does not adhere to Google's recommended practices of separating environments into different projects. While using firewall rules can restrict traffic, it does not provide the same level of isolation and control compared to different projects. Moreover, firewall rules may not guarantee complete isolation, and errors in rule configuration could lead to unintended routes between environments.

C. Enabling Private Google Access and Private Service Access in the existing project might help restrict some traffic between the Compute Engine and Cloud SQL instances. However, it does not meet Google's recommended practices for separating environments into different projects, and it would be challenging to maintain complete isolation between development and production environments within the same project.

D. Implementing a VPN between the development and production environments only addresses network security but does not provide the level of isolation and control needed to meet the company's security guidelines. Additionally, using a VPN within the same project goes against Google's recommended practices for separating environments into different projects.

Solution to Question 41: B

Option B is the correct choice because it allows you to grant the required Identity and Access Management (IAM) roles to specific G Suite users based on their email addresses. This direct assignment of roles ensures that the users have the appropriate level of access and permissions within your company's Cloud Platform project. This method is reliable and follows best practices in terms of security and access management.

Option A doesn't work because there is no default behavior in Google Cloud Platform (GCP) that grants users access based on their membership in a specific group. Creating a special group would not achieve the desired outcome of granting access to GCP.

Option C is not suitable because creating a GCP IAM user manually and configuring G Suite accounts to sync with this user is an unnecessary and complex approach. GCP and G Suite are designed to work together seamlessly, and you can directly assign IAM roles using the user's G Suite email address as mentioned in Option B.

Option D involves converting the users' email addresses into GCP accounts using the gcloud command-line tool. However, this method is time-consuming, tedious, and less accurate compared to assigning IAM roles directly using their G Suite email addresses (Option B).

Solution to Question 42: B

The most effective approach to achieve consolidated reporting under a single Stackdriver Monitoring dashboard is option B, to configure a single Stackdriver account and link all projects to the same account. This will enable centralized

reporting and monitoring, making it easier for you as a project manager to oversee multiple projects under one dashboard.

Option A is not the best choice because even though it creates a Group in Stackdriver, it still references only the resources of one project. This would not provide a complete overview of all resources across the different projects.

Option C focuses on enabling BigQuery in each project and having Stackdriver pull data from BigQuery tables. However, this method can be more complex and time-consuming as it involves configuring data aggregation in each project and handling data transfers between BigQuery and Stackdriver. It's not the most effective way to achieve consolidated monitoring.

Finally, option D is not an ideal solution because it suggests creating a single Google Cloud project with separate folders for each monitored project. This would not only result in an unnecessary restructuring of the existing projects, but it would also not provide the desired consolidated view within Stackdriver Monitoring since it still treats the projects as separate entities.

In conclusion, the most effective approach is option B, which simplifies the process of consolidating monitoring data across multiple Google Cloud Platform projects by linking them all to a single Stackdriver account.

Solution to Question 43: C

The correct answer is C: Migrate to use a Local SSD on the instance.

Explanation:

Option A: Increasing the size of the disk to 1 TB will indeed increase the throughput, as the larger the size of the SSD Persistent Disk, the more IOPS and throughput it can achieve. However, this will also increase the cost, and it's not the most optimized solution for the requirement of maximizing throughput while minimizing costs.

Option B: Increasing the allocated CPU to the instance will not directly impact the disk read throttling on the application. Disk read throttling is primarily related to the disk type and its size, not the CPU.

Option C: Migrating to a Local SSD on the instance is the best solution because it provides higher IOPS and throughput compared to Persistent Disk SSDs. Local SSDs are designed for workloads that require high IOPS and low latency. This makes them ideal for handling large files and avoiding disk read throttling while maintaining reasonable costs.

Option D: Increasing the size of the disk to 750 GB will also increase the throughput, but it still won't be as efficient a solution as using a Local SSD. Additionally, increasing the size would still increase costs, which is not the goal in this case.

In conclusion, to achieve maximum throughput while minimizing costs, migrating to a Local SSD (Option C) is the best choice, as it addresses the disk read

throttling issue and is more cost-effective than simply increasing the size of the Zonal SSD Persistent Disk.

Solution to Question 44: D

The correct answer is D. When creating the VM via the web console, specify the service account under the 'Identity and API Access' section. This ensures that the VM uses the specified service account instead of the default Compute Engine service account, providing the VM with the necessary access rights to connect to the Cloud SQL.

Option A is incorrect because setting the service account as the default Compute Engine service account for the entire project would affect all VMs within the project, not just the specific Linux VM you want to connect to the Cloud SQL. This approach may inadvertently grant unnecessary access rights to other VMs or services within the project.

Option B is incorrect because creating an external IP address for the VM and adding it to the Authorized Networks of the Cloud SQL instance doesn't change the service account used by the VM. It may allow traffic to flow between the VM and the Cloud SQL instance, but it does not ensure that the correct service account is used by the VM to access Cloud SQL.

Option C is incorrect because creating a separate VPC network for the VM and Cloud SQL would only isolate these resources within a dedicated network, but it won't change the service account the VM uses for accessing Cloud SQL. The correct service account needs to be assigned directly to the VM, which is accomplished in Option D.

Solution to Question 45: B

The correct answer is B - Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

Here's why the other options will not work:

Option A: Using Google Kubernetes Engine (GKE) to deploy the new app version without using a managed instance group would deviate from the current deployment architecture. Managed instance groups have specific features that allow for easier management and scaling of the application. While GKE is a great tool for orchestrating containerized applications, it does not directly address the problem at hand and would require a complete change in the setup and possible downtime during the transition.

Option C: Using Google Cloud Build to push the new app version to all instances in the managed instance group simultaneously may result in decreased capacity during deployment. Since all instances are being updated at the same time, there will be some temporary downtime for each instance, leading to possible adverse effects on the live web traffic.

Option D: Creating a new instance template with the new application version

and manually updating the instances within the managed instance group without setting maxSurge or maxUnavailable values would make the deployment process more time-consuming and prone to errors. Additionally, manual updates could result in temporary drops in available capacity during the individual update processes, impacting live web traffic.

On the other hand, Option B - performing a rolling start-update with maxSurge set to 1 and maxUnavailable set to 0 - ensures that the available capacity does not decrease during the deployment. By setting maxSurge to 1, the system adds an extra instance during the rolling updates, ensuring that there is always sufficient capacity to handle the incoming web traffic. With maxUnavailable set to 0, the system does not allow any instances to become unavailable during the update process, ensuring that the available capacity remains unaffected. This approach enables you to deploy the new version of your web application seamlessly and efficiently without affecting the user experience or the performance of your application.

Solution to Question 46: D

The correct answer is D, enabling Cloud IAP for the Compute Engine instances and adding the operations partner as a Cloud IAP Tunnel User. This is because Cloud IAP (Identity-Aware Proxy) provides secure, granular access to applications and resources without requiring users to have a Google Account or traditional VPN access. By using Cloud IAP, system administrators can restrict access to specific users and groups, ensuring the operations partner has the appropriate level of access while maintaining the overall security of the environment.

Option A, setting up a Cloud VPN between the Google Cloud VPC and the internal network of the operations partner, is not ideal because it would provide broad access to the Google Cloud VPC. This might not be the desired level of access given to the operations partner. Additionally, this method still requires the partner to have a Google Account to access the Compute Engine instances.

Option B, configuring a Google Cloud Pub/Sub topic that allows the operations partner to send and receive messages related to instance maintenance, is not sufficient because it only provides a messaging system. It does not actually grant access to the instances to perform the required maintenance tasks. Pub/Sub does not allow remote administrative access to Compute Engine instances.

Option C, configuring Compute Engine instances to use an external metadata server and granting the operations partner access to that server, is not recommended because it can introduce security risks. This approach might expose sensitive metadata to the operations partner and potentially lead to unauthorized access. Furthermore, merely providing access to metadata does not guarantee the ability to perform maintenance on the instances themselves.

Therefore, the best option for granting the operations partner access to maintain the Linux workloads running on Compute Engine instances is D, enabling Cloud

IAP for the instances and adding the operations partner as a Cloud IAP Tunnel User.

Solution to Question 47: A

The most suitable choice for this application is A. Cloud SQL.

Explanation for why the answer should be A (Cloud SQL):

1. Compatibility: Cloud SQL is a managed SQL database service that supports MySQL, PostgreSQL, and SQL Server. Since the initial development of the application was done using PostgreSQL, migrating to Cloud SQL would require minimal modifications.
2. Strong consistency: Cloud SQL provides strong consistency for SQL transactions, which is a key requirement for the financial organization's transactional orders application.
3. Quick query response time: Cloud SQL is optimized for OLTP (Online Transaction Processing) workloads, which demand fast query responses, making it suitable for the application.
4. ACID guarantees: As a fully managed relational database service, Cloud SQL offers ACID (Atomicity, Consistency, Isolation, Durability) guarantees for multi-table transactional updates, ensuring data integrity and improving the reliability of the application.

Explanation for why other options will not work:

B. Firestore: Firestore is a NoSQL database primarily designed for mobile and web applications. It does not support the same SQL-based relational structure as PostgreSQL and would require significant modifications to the application. Additionally, Firestore is document-based and does not fully support multi-table transactional updates, which are needed for the financial organization's application.

C. Cloud Bigtable: Cloud Bigtable is a NoSQL wide-column store that is designed mainly for high-throughput, large-scale workloads. It does not inherently support ACID transactions across multiple rows like a relational database. Migrating from PostgreSQL to Cloud Bigtable would require major changes to the application and would not meet the application's strong consistency and multi-table transactional update requirements.

D. Datastream: Datastream is a serverless, fault-tolerant, change data capture, and real-time data replication service in the Google Cloud. It is not a suitable database service for handling transactional orders as its primary purpose is to stream changes from source to destination systems. It does not offer the consistency, quick query response, or ACID guarantees required for the application.

Solution to Question 48: A

The correct answer is A, configuring an HTTP(S) load balancer.

Explanation for A: An HTTP(S) load balancer is designed to handle HTTP and HTTPS traffic, thus enabling it to manage SSL termination at the load balancer level. This adheres to Google's recommended practices for ensuring secure and efficient load balancing. The HTTP(S) load balancer can offload SSL decryption and encryption from the backends, reducing the CPU overhead and enabling better performance. Additionally, it can cater to a global audience as it supports cross-regional load balancing.

Reasons why other options will not work:

B. Configure a network endpoint group: A Network Endpoint Group (NEG) is a grouping of backend instances that can be attached to a load balancer. While NEGs can be an essential component of a load-balancing solution, they do not handle SSL termination directly. Therefore, this option will not achieve the goal of terminating the client SSL session at the load balancer.

C. Configure an internal TCP load balancer: An internal TCP load balancer deals with non-HTTP(S) traffic in a regional or global scope within a Virtual Private Cloud (VPC) network, thus it does not support SSL termination. This option is more suitable for internal services that do not require SSL termination or traffic processing at the application layer.

D. Configure a regional external forwarding rule: A regional external forwarding rule is used to direct traffic to a specific regional resource or a global resource based on IP protocol, port number, and other attributes. However, this option does not specifically terminate SSL sessions at the load balancer and focuses on forwarding rules rather than providing the required HTTPS load balancing.

In conclusion, the best approach to achieve the goal of setting up load balancing for a public web application over HTTPS and terminating the client SSL session at the load balancer while following Google-recommended practices is to configure an HTTP(S) load balancer (Option A).

Solution to Question 49: D

The correct answer is D. Here's why:

D. Migrate the web application to App Engine and the backend API to Cloud Run. Use Cloud Tasks to run your background job on Cloud Run.

- Migrating the web application to App Engine allows you to take full advantage of its managed infrastructure, including auto scaling and automatic updates, which helps in keeping operational costs low. It also aligns with Google-recommended practices for running web applications.
- Migrating the backend API to Cloud Run ensures it runs in a serverless environment, which means you only pay for what you use, and it automatically scales based on demand. This is ideal for APIs and microservices, and adheres to Google-recommended practices.
- Using Cloud Tasks with Cloud Run to handle the scheduled long-running background job allows you to fully leverage serverless technologies, thus

reducing operational costs. Cloud Tasks supports automatic retries and flexible scheduling, making it a suitable choice for executing long-running background jobs.

Now let's evaluate the other options:

A. Migrate the web application to Cloud Functions and the backend API to Kubernetes Engine. Use Cloud Scheduler to run your background job on Compute Engine.

- Cloud Functions is a suitable choice for event-driven serverless computing but not ideal for web applications. Using Kubernetes Engine for the backend API does not fully utilize serverless pricing models and requires additional management, increasing operational costs. Running background jobs on Compute Engine also goes against the serverless approach aimed at reducing costs.

B. Migrate the web application to Cloud Functions and the backend API to Cloud Run. Use Cloud Pub/Sub to run your background job on Compute Engine.

- As mentioned earlier, Cloud Functions is not the best choice for web applications. Additionally, using Cloud Pub/Sub to trigger background jobs on Compute Engine does not leverage the full advantages of the serverless approach and can result in higher operational costs.

C. Migrate the web application to Kubernetes Engine and the backend API to App Engine. Use Cloud Pub/Sub to run your background job on Cloud Run.

- Using Kubernetes Engine for the web application goes against the serverless approach and results in increased management and costs. Although using Cloud Pub/Sub with Cloud Run for background jobs is a better option, it's not as well-suited for scheduled tasks and long-running jobs as Cloud Tasks.

In summary, option D provides the most cost-effective and Google-recommended approach to migrating the on-premises workloads to serverless solutions on Google Cloud.

Solution to Question 50: C

The correct answer is C: Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Explanation:

A Kubernetes Deployment is the best option for deploying a Docker container image within a Google Kubernetes Engine (GKE) cluster. Deployments help in managing the desired state of the application, scale up or down based on demand, and perform rolling updates.

Here's why the other options are not suitable:

A: BigQuery is a Google Cloud Platform service used for analyzing large datasets using SQL-like queries. It is not designed for storing Docker container images or managing Kubernetes Deployments. Thus, uploading the image to BigQuery is irrelevant to the task at hand.

B: Firestore is a NoSQL database provided by Google Cloud Platform. It is used to store and sync data for applications, but it is not intended for storing Docker container images or managing Kubernetes Deployments. Uploading the image to Firestore would not help deploy it on GKE.

D: A Kubernetes StatefulSet is used for applications that require stable network identities and persistent storage. While StatefulSets can be used with GKE, they are not the best fit for deploying typical containerized applications that do not have specific stateful requirements. In this scenario, a Kubernetes Deployment is a better choice for managing the Docker container.

In conclusion, the best approach to deploy the Docker container image on GKE is to upload the image to Google Container Registry and create a Kubernetes Deployment referencing the image. This ensures proper management of the application's desired state, smart scaling options, and efficient update processes.

Practice Exam 13

Question 1: As a DevOps engineer working for a software company, you are tasked with setting up a Google Kubernetes Engine (GKE) cluster with autoscaling capabilities. To ensure that each node in the cluster runs a monitoring pod for reporting container metrics to a third-party monitoring solution, what course of action should be taken?

A. Deploy the monitoring pod in a ConfigMap object.

B. Enable binary authorization at the cluster level to deploy monitoring pods.

C. Deploy the monitoring pod in a StatefulSet object.

D. Deploy the monitoring pod in a DaemonSet object.

Question 2: As a leading IT specialist working in a multinational corporation, you have recently noticed several users with email addresses outside of your company's Google Workspace domain during a routine audit of your firm's Google Cloud resources. To ensure that your resources are only shared with users from your domain, you must remove any mismatched users without having to continuously audit your resources. What course of action should you take?

A. Configure a Pub/Sub topic to monitor resource sharing and notify you if a mismatched user is detected.

B. Create a Cloud Scheduler task to regularly scan your projects and delete mismatched users.

C. Write a custom script that uses the Google Cloud SDK to identify and remove mismatched users.

D. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

Question 3: As a software engineer in a rapidly growing tech company, you've been tasked with streamlining the process for creating and managing multiple Google Cloud resources using Infrastructure as Code, with a focus on reducing repetitive code. How should you approach this task?

A. Manually use the gcloud command-line tool to manage all resources interactively.

B. Use Google Cloud Pub/Sub to implement message-based asynchronous resource management.

C. Develop templates for the environment using Cloud Deployment Manager.

D. Use curl in a terminal to send a REST request to the relevant Google API for each individual resource.

Question 4: You are working as a cloud engineer for a company utilizing Google Cloud Platform (GCP), and you have been tasked with generating a list of enabled GCP APIs for a specific project called "my-project" using the gcloud command line in the Cloud Shell. What should you do?

A. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

B. Run gcloud auth login to authenticate, and then run gcloud services list –project my-project.

C. Run gcloud config list –filter "core.project=" *to verify the project value, and then run gcloud services list –filter=.*

D. Run gcloud projects describe my-project to verify the project value, and then run gcloud services list-apis.

Question 5: As a security manager in a software development company, you need to add a new auditor to a Google Cloud Platform project. They should have the ability to read all project items but not modify them. How would you configure the auditor's permissions?

A. Assign the user to the IAM project Editor role with view-only permissions. Add the user's account to the Editor role.

B. Select the built-in IAM project Viewer role. Add the user's account to this role.

C. Assign the user to the IAM BigQuery Data Viewer role with project-wide permissions. Add the user's account to this role.

D. Add the user to the IAM Billing Account Viewer role with project-wide permissions. Add the user's account to this role.

Question 6: While working at a tech company in the software development department, you have developed a code snippet that should be triggered when a new file is uploaded to a Cloud Storage bucket. To properly deploy this code snippet, what approach should you take?

A. Use Cloud Run and configure the bucket as an event source using Cloud Pub/Sub.

B. Use Cloud Data Fusion and create a pipeline triggered by the bucket.

C. Use Cloud Functions and configure the bucket as a trigger resource.

D. Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub.

Question 7: You are working at a tech company and your role involves managing cloud infrastructure. Your responsibility is to enable the development team to deploy new features to an existing Cloud Run service in production. It is

crucial to minimize the risk associated with a new revision and reduce the number of customers who might be affected by an outage while not introducing any development or operational costs for your customers. You are required to follow Google-recommended practices for managing revisions to a service. What is the best course of action to achieve this?

A. Configure a Cloud Function to automatically roll back the service if a certain number of errors are detected in Stackdriver Monitoring.

B. Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

C. Create multiple Cloud Run staging environments for testing before deploying to production, but maintain the same traffic allocation.

D. Enable Google Cloud Logging on the new revision and closely monitor logs to identify issues and perform rollbacks when necessary.

Question 8: As a software engineer in a large technology company, you manage an on-premises server running a monthly batch process that takes approximately 30 hours to complete. The task can be performed offline and must be restarted if interrupted. You are looking to transition this workload to the cloud while keeping costs as low as possible. What is the most appropriate course of action?

A. Use App Engine standard environment to run the workload.

B. Use Cloud Dataflow with autoscaling enabled for running the workload.

C. Migrate the workload to a Google Kubernetes Engine cluster with Preemptible nodes.

D. Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

Question 9: As a network administrator in a software development company, you are managing an on-premises infrastructure where all machines are running at maximum capacity. You decide to burst to Google Cloud to handle the additional workload, and you need the workloads on Google Cloud to directly communicate with the on-premises workloads using a private IP range. What would be the best solution to achieve this?

A. Create Cloud NAT both in your on-premises environment and on Google Cloud and set up IP forwarding instead of VPN.

B. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

C. Configure Firewall rules only on the on-premises environment to allow all traffic between both networks.

D. In Google Cloud, configure the VPC for Organization-wide authorized networks.

Question 10: You are working as a software engineer in a tech company that has a website hosted on App Engine standard environment. Your team decides to test a new version of the website on 1% of the users while minimizing complexity. What should you do?

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

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

C. Deploy the new version using the same application and enable traffic splitting in App Engine by assigning 1% traffic to the new version using the Console.

D. Deploy the new version using Firebase Hosting and use Cloud Functions to redirect 1% of the traffic to the new version.

Question 11: As an employee in a financial company, you are responsible for a legacy on-premises data analytics system that processes transactional data files in memory every midnight, taking approximately 45 minutes. The file sizes range from 1 gigabyte to 16 gigabytes. Your company wants to migrate this application to Google Cloud with minimal effort and cost. What would be the most appropriate solution?

A. Create a Pub/Sub topic to trigger the set of binaries. Use Cloud Scheduler to publish a message to the topic.

B. Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

C. Upload the code to Cloud Run and use Cloud Scheduler to trigger the execution every midnight.

D. Create a container for the set of binaries and deploy it to Cloud Functions, scheduled to run every midnight.

Question 12: As a cloud engineer working in a software company, you have recently made significant changes to a complex Deployment Manager template. You want to ensure that the dependencies of all defined resources are properly met before committing it to the project, and you want to receive the fastest feedback possible. What should you do?

A. Modify the Deployment Manager template to include real-time monitoring using Firebase and identify any discrepancies in the resources.

B. Manually inspect the interdependent resources within the GCP Console, comparing them to the revised Deployment Manager template.

C. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

D. Simulate the Deployment Manager template changes in the Cloud Shell before applying it to the project.

Question 13: As a DevOps engineer working for a fintech company, you are tasked with setting up a new Google Kubernetes Engine (GKE) cluster to ensure it always runs a supported and stable version of Kubernetes. What action should you take?

A. Use "Windows Server" as a node image for your GKE cluster.

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

C. Use "Ubuntu" as a node image for your GKE cluster.

D. Enable the "Stackdriver Monitoring" for your GKE cluster.

Question 14: You are working as a data engineer for a media company planning to migrate your on-premises data to Google Cloud. The company's data includes 200 TB of video files in SAN storage, Data warehouse data stored on Amazon Redshift, and 20 GB of PNG files stored on an S3 bucket. Your task is to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud Storage bucket. You are expected to follow Google-recommended practices and avoid writing any code for the migration. What should you do?

A. Use Cloud Data Fusion for the video files, Dataflow for the data warehouse data, and Dataproc for the PNG files.

B. Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

C. Use Storage Transfer Service for the video files, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

D. Use Dataproc for the video files, BigQuery Data Transfer Service for the data warehouse data, and Cloud Pub/Sub for the PNG files.

Question 15: As a software engineer at a tech company, you are tasked with configuring a Windows VM on Compute Engine to ensure seamless access to the virtual machine via RDP. What is the appropriate procedure to follow?

A. After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM.

B. After the VM has been created, use the SSH keys for your VM to log in via RDP.

C. After the VM has been created, use your Google Account credentials to log in into the VM.

D. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

Question 16: As an IT administrator for a large e-commerce company, you oversee a batch workload that runs every night, utilizing numerous virtual machines (VMs). This process is fault-tolerant and can withstand some VM terminations. However, the current cost of VMs is becoming an issue for the company. What should you do to reduce costs?

A. Run a test using simulated maintenance events. If the test is successful, use N2 Standard VMs when running future jobs.

B. Run a test using Cloud Dataproc with preemptible VMs enabled. If the test is successful, use Cloud Dataproc with N2 Standard VMs for future jobs.

C. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

D. Run a test using Kubernetes Engine with Committed Use Discounts. If the test is successful, use Kubernetes Engine with N2 Standard VMs for future jobs.

Question 17: As a manager at a software development company, you have assigned 10 developers for an in-house project. To explore and experiment with Google Cloud solutions, each of your developers has been given an individual Google Cloud Project to use as their personal sandbox. You want to be alerted if any of your developers spend more than $500 per month on their sandbox environment. What should you do?

A. Use Cloud Pub/Sub to notify you when developers are creating new resources in their sandbox projects.

B. Create a separate billing account per sandbox project and enable BigQuery billing exports. Create a Data Studio dashboard to plot the spending per billing account.

C. Create a budget per project and configure budget alerts on all of these budgets.

D. Create a single budget for all projects and configure budget alerts on this budget.

Question 18: You are working as a software developer in an IT company, and one of your tasks is to deploy a containerized application for a client. This application has an HTTP endpoint and receives only a limited number of requests daily. Knowing that your client wants to minimize costs, what deployment method should you choose?

A. Deploy the container on Cloud Functions with HTTP trigger.

B. Deploy the container on Kubernetes Engine with Vertical Pod Autoscaler.

C. Deploy the container on GKE with cluster autoscaling and horizontal pod autoscaling enabled.

D. Deploy the container on Cloud Run.

Question 19: You are working as a database architect in a rapidly growing tech company that is building a sophisticated application catering to users worldwide. Your company is unsure about the size of its global user base, and your CTO wants you to design a database solution capable of scaling alongside user growth with minimal configuration changes. Which storage solution should you implement?

A. Cloud Spanner

B. Cloud SQL

C. Cloud Datastore

D. Cloud Data Fusion

Question 20: As an IT specialist working in a company with a hybrid cloud infrastructure, you are tasked with deploying a new Compute Engine instance while ensuring that public Internet traffic cannot reach it. The company's Google Cloud Virtual Private Cloud (VPC) is connected to your WAN through a Virtual Private Network (VPN). What should you do to accomplish this?

A. Create a firewall rule to only allow traffic from Google Cloud VPC.

B. Create the instance with Private Google Access enabled.

C. Restrict the instance to only allow traffic from on-premises WAN IP addresses.

D. Create the instance without a public IP address.

Question 21: As a software engineer in a global e-commerce company, you've been assigned to develop a new project for a worldwide application deployment, utilizing Cloud Spanner for data storage. Before creating the Cloud Spanner instance as the initial step, what action should be taken first?

A. Create a new Google Cloud Firestore instance for global data storage.

B. Enable the Cloud Spanner API.

C. Create a new VPC network with subnetworks in all desired regions.

D. Enable Cloud Storage API for the project.

Question 22: As a financial analyst in a multinational corporation, you have been tasked with managing expenses across various departments using various Google Cloud projects. Each project is linked to different billing accounts. In order to provide a comprehensive overview of all costs incurred and to include new cost data as quickly as possible for projections, what would be the most appropriate course of action?

A. Use the Cloud Billing API to fetch the costs from each project and compile them into a single file for visualization in Excel.

B. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

C. Export cost data from each billing account to a Google Sheet, and use the Google Sheets API to combine them for visualization

D. Use Google Cloud Monitoring to track costs of each project and create dashboards.

Question 23: You are working as an IT administrator for a company that utilizes Active Directory for user identities management. The company wants to maintain Active Directory as their primary source for user identity information while also having full control over Google accounts used by employees for Google services, including the company's Google Cloud Platform (GCP) organization. What action should you take to achieve this?

A. Use Google Workspace to create and manage users instead of synchronizing with Active Directory.

B. Use the GCP Console to migrate users from Active Directory to Cloud Identity.

C. Create user accounts manually in Cloud Identity for each employee and assign them roles.

D. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

Question 24: You are working as a cloud engineer at a software development company, and your team needs to deploy multiple applications on different Compute Engine instances within the same project. To ensure proper access control when interacting with Google Cloud APIs, you must assign service accounts to these instances accordingly. How can you achieve this at a granular level?

A. When creating the instances, specify a Service Account for each instance.

B. When creating the instances, assign the name of each Service Account as instance metadata.

C. Assign the IAM role for each Service Account to their respective instance's metadata.

D. Create individual user accounts for each instance and use them as Service Accounts.

Question 25: As a software engineer working in a company that follows Google-recommended practices, you need to refactor the app configuration to ensure the database password is no longer stored in plain text. How should you proceed?

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

B. Store the database password inside a Cloud Storage bucket and use a Cloud Function to retrieve it during runtime.

C. Store the database password in a separate YAML file and use kubectl to apply the updated configuration.

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

Question 26: As a software engineer working for an e-commerce company, you need to create an autoscaling managed instance group for the HTTPS web application used by your customers. Your goal is to ensure that unhealthy VMs are automatically replaced. What action should you take to achieve this?

A. Use the default health check for network load balancing when creating the Managed Instance Group.

B. In the Instance Template, add the label 'health-check'.

C. Create a health check on port 443 and use that when creating the Managed Instance Group.

D. Enable automatic rolling updates for the Managed Instance Group with a minimal action time.

Question 27: You are working in a software company, developing an application to be deployed on Google Kubernetes Engine for a client in the finance industry. The team has decided to use MongoDB as the database system for this application, and needs to ensure a managed MongoDB environment with a support SLA. What should you do?

A. Use Cloud Datastore with the MongoDB API enabled.

B. Deploy MongoDB Atlas from the Google Cloud Marketplace.

C. Set up a VPN connection between your Google Kubernetes Engine cluster and a self-managed MongoDB instance hosted on another cloud provider.

D. Deploy a MongoDB container on Cloud Functions and trigger it with an event.

Question 28: As a software engineer in a rapidly growing tech company, your development team requires a new Jenkins server for their upcoming project. To deploy the server with minimum steps, what should you do?

A. Try deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service.

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

C. Deploy Jenkins on Cloud Run using a custom Docker image.

D. Use GCP Marketplace to launch the Jenkins solution.

Question 29: You are working as a network administrator for a company that has adopted a hybrid cloud strategy, utilizing Google Cloud for some of its applications. Your company's Virtual Private Cloud (VPC) in Google Cloud is connected to the on-premises network via a Virtual Private Network (VPN) tunnel. In this setup, multiple applications in Google Cloud require access to an on-premises database server. To prevent the need for adjusting the IP configuration in all applications when the database IP changes, what action should you take?

A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances.

B. Configure Firebase Realtime Database as a middle layer for the applications and the on-premises database.

C. Utilize Google Cloud Endpoints to create an API proxy for your database and avoid changing the IP configuration in the applications.

D. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

Question 30: As a data security analyst in a financial company, you are handling sensitive customer information that is stored in a Cloud Storage bucket. Due to industry regulations, you are required to record all requests that access any of the stored data. What measure should you take to ensure compliance with these regulatory requirements?

A. Deploy a Google Cloud Armor security policy.

B. Enable Data Access audit logs for the Cloud Storage API.

C. Configure a Cloud Pub/Sub Notification for the bucket.

D. Enable the Cloud Storage Uniform Access Control.

Question 31: You are working as a Data Analyst in a global corporation and need to share an object containing sensitive information, stored in a Cloud Storage bucket, with a client company for a limited time. The client company lacks a Google account for assigning specific user-based access privileges. You need to utilize the most secure method with the least steps while ensuring content access gets removed after four hours. What is the best course of action?

A. Create a new custom role with read access to the object in Cloud Storage and use a service account to grant the external company temporary access. Revoke the role after four hours.

B. Use Cloud Functions to create an endpoint that provides temporary read access to the object. The external company will be allowed access for only four hours before the endpoint stops working.

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

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

Question 32: You are working as a cloud administrator in a software development company, and your manager has recently assigned you to maintain a Google Cloud Platform project previously handled by another colleague. To ensure the project's security, you need to verify the individuals granted the Project Owner role. What step should you take?

A. Use the command gcloud projects get-iam-policy to view the current role assignments.

B. Enable Stackdriver Monitoring for the project and review the logs for role changes.

C. Go to the IAM & admin page in the console and review the Service Accounts permissions.

D. Go to the Firebase Console and check the Authentication section for users who have been granted the Project Owner role.

Question 33: As a data engineer working in a marketing analytics company, you have a large 5-TB AVRO file stored in a Cloud Storage bucket. The company's data analysts are proficient only in SQL and require access to the information contained within this file. Your objective is to find a cost-effective solution to complete their request as quickly as possible. What should you do?

A. Configure Cloud Dataflow to read the AVRO file and write the data into Cloud Firestore for SQL querying.

B. Create a Memorystore instance and use Cloud Functions to process the AVRO file, storing the data in the Memorystore for SQL querying.

C. Create a Datastore-based App Engine Application to process the AVRO file and expose the data through an API for SQL querying.

D. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

Question 34: As a security engineer at a software development company, you need to ensure that unauthorized users do not have access to view sensitive data stored in your company's Google Cloud Project during your monthly security audit. What is the most appropriate action to take in this situation?

A. Apply the Binary Authorization settings on the resources.

B. Create and apply a VPC Service Controls perimeter.<

C. Review the Bucket Policy Only settings for your storage buckets.

D. Review the IAM permissions for any role that allows for data access.

Question 35: You are an IT administrator for a company that relies heavily on cloud computing. Your company has assigned you the task of configuring 10 Compute Engine instances for high availability when maintenance occurs. The instances should automatically restart if they crash and remain highly available even during system maintenance. How should you achieve this?

A. Create an instance group for the instances. Set the 'Autohealing' health check to healthy (HTTP).

B. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

C. Create a regional managed instance group for the instances. Set the 'Availability policies' to configure the instances to automatically restart during maintenance.

D. Create an instance group for the instances. Configure the instances to use an instance template with an attached Persistent Disk. Set 'On-host maintenance' to Migrate VM instance.

Question 36: In your software development company, your manager has assigned you a task to deploy a workload to a Kubernetes cluster for one of your clients. However, you are uncertain about the workload's resource requirements, as they might vary with usage patterns, external dependencies, or other factors. To satisfy your client's needs, you want to implement a cost-effective solution that recommends appropriate CPU and memory requirements while maintaining a consistent workload performance in any situation. Additionally, you aim to follow Google-recommended best practices. What should you do?

A. Configure the Cluster autoscaler for cost optimization, and configure the Vertical Pod Autoscaler recommendations for latency optimization.

B. Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

C. Configure the Horizontal Pod Autoscaler for availability, and configure the cluster autoscaler for suggestions.

D. Configure the Vertical Pod Autoscaler recommendations for cost optimization, and configure the Node Auto Provisioning for suggestions.

Question 37: As a cloud architect in a tech company, you are tasked with finding a dynamic method for provisioning virtual machines on Compute Engine, with their specifications stored in a dedicated configuration file while adhering to Google's recommended practices. Which method should you use?

A. App Engine

B. Deployment Manager

C. Cloud Dataflow

D. Cloud SQL

Question 38: You are working at a tech company that forayed into the cloud services industry 6 months ago. As more clients sign up for your services and your reliance on Google Cloud intensifies, you want to streamline the process of project creation for your engineers without requiring their credit card details. What is the most effective approach to achieve this?

A. Require engineers to submit reimbursement requests for their personal credit card expenses related to Google Cloud usage.

B. Create separate billing accounts for each engineer and associate their individual credit cards.

C. Request Google Cloud to provide a corporate credit card for the entire engineering team.

D. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

Question 39: You work in a company that uses Cloud Storage to host a static website for the marketing team. They've recently started including links to PDF files in their promotional materials, but when users click on these links, the browser prompts them to save the file locally instead of displaying the PDF directly in the browser. What should you do to resolve this issue?

A. Configure the website's caching policy to show application/pdf content.

B. Add a label to the storage bucket with a key of Content-Type and value of application/pdf.

C. Set Content-Type metadata to application/pdf on the PDF file objects.

D. Enable multi-regional storage class for the bucket containing PDF files.

Question 40: You're working as a Cloud Engineer at a tech company and are tasked with deploying a new Enterprise Resource Planning (ERP) system on Google Cloud. The application operates with the full database in-memory for optimal data access speeds. What is the most suitable resource configuration on Google Cloud for this particular application?

A. Provision preemptible Compute Engine instances.

B. Use a Cloud Spanner instance for in-memory database handling.

C. Provision Compute Engine instances with M1 machine type.

D. Deploy the application on Kubernetes Engine with memory optimized nodes.

Question 41: You're working for a software development company and recently deployed an application on a managed instance group in Compute Engine within your organization's infrastructure. The application needs to accept TCP traffic on port 389 while preserving the IP address of the client making a request. To

make the application accessible via the internet using a load balancer, what is the most appropriate solution?

A. Expose the application by using an external UDP Network Load Balancer.

B. Expose the application by using an internal Serverless Network Endpoint Group Load Balancer.

C. Expose the application by using an internal HTTP(S) Load Balancer.

D. Expose the application by using an external TCP Network Load Balancer.

Question 42: After experiencing a security breach in your tech company, your team has decided to look for better ways to monitor activities within your Google Cloud environment, such as unexpected firewall adjustments and instance creations. Your company values simple and efficient solutions. What action should you take?

A. Enable Object Lifecycle Management on Cloud Storage to store the logs and use Stackdriver Monitoring to analyze them.

B. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

C. Set up a cron job on a compute instance to periodically check for changes in firewall rules and instances, and send email notifications if any discrepancies are found.

D. Create a log sink to forward Cloud Audit Logs filtered for firewalls and compute instances to Cloud Storage. Use BigQuery to periodically analyze log events in the storage bucket.

Question 43: You are working as a DevOps engineer in a tech company that relies heavily on using Google Cloud Platform. Your task is to utilize Deployment Manager for creating a Google Kubernetes Engine cluster. Simultaneously, you are required to create a DaemonSet in the kube-system namespace of the cluster within the same Deployment Manager deployment while minimizing the number of services used. How should you proceed?

A. In the cluster's definition in Deployment Manager, add a metadata that has kube-system as key and the DaemonSet manifest as value.

B. Use the Deployment Manager to create a Cloud Run service that deploys the DaemonSet to the kube-system namespace when triggered by an HTTP request.

C. Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

D. Update the Deployment Manager configuration to include a Cloud Logging sink that deploys the DaemonSet to the kube-system namespace whenever a log entry is created.

Question 44: You are working as a cloud architect for a financial services company and are in charge of migrating a mission-critical application from the company's local data center to Google Cloud. To guarantee high availability and prevent data loss in case of a zonal failure, what should be your approach to store the application data?

A. Use Cloud Datastore to store the application data and configure inter-zone replication for high availability.

B. Store the application data in a Cloud SQL instance and enable automatic cross-zone failover.

C. Store the application data on a zonal persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

D. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

Question 45: As an IT manager for a finance company, your web application has been running smoothly on Cloud Run for Anthos. Now, you want to assess an updated version of the application with a specific percentage of your production users (canary deployment). What approach should you take to achieve this?

A. Create a new Cloud Storage bucket with the new version of the application. Use Cloud CDN to direct traffic to both buckets.

B. Create a new Compute Engine instance with the new version of the application. Configure the instance group to direct traffic to both instances.

C. Create a new revision with the new version of the application. Add an HTTP Load Balancer in front of both revisions.

D. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

Question 46: You are working as a cloud engineer for a tech company using Google Cloud for hosting their applications. Your company's application is running on a managed instance group (MIG). You notice errors in Cloud Logging for one virtual machine (VM) indicating that one of the processes is not responsive. To quickly replace this VM in the MIG, what should you do?

A. Use the gcloud compute instance-groups managed resize command to resize the MIG.

B. Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

C. Set the autohealing policy for the MIG to replace unhealthy instances automatically.

D. Use the gcloud compute instance-groups managed delete-instances command followed by gcloud compute instance-groups managed add-instances to replace

the VM.

Question 47: You are working as a cloud engineer in a software development company and are tasked with updating a deployment in Deployment Manager without causing any downtime for the resources in the deployment. Which command should you use?

A. gcloud deployment-manager resources update –config

B. gcloud deployment-manager deployments delete –config

C. gcloud deployment-manager deployments update –config

D. gcloud deployment-manager deployments list –config

Question 48: You are working in a software development company, and you have been assigned the task of deploying an application on Cloud Run for a project involving message processing from a Cloud Pub/Sub topic, adhering to the Google-recommended practices. What steps should you follow to achieve this goal?

A. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

B. 1. Create a Cloud Dataflow pipeline that reads messages from the Pub/Sub topic and then calls your Cloud Run application with each message.

C. 1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run. 2. Create a Cloud Pub/Sub subscription for that topic. 3. Make your application pull messages from that subscription.

D. 2. Use Cloud Scheduler to periodically trigger your Cloud Run application, which then reads and processes messages from the Pub/Sub topic.

Question 49: As a leading software developer for a rapidly growing e-commerce company, you are tasked with deploying a crucial application to App Engine. To accommodate the high request rate of the booming business, you must scale the number of instances accordingly, while also ensuring there are always 3 unoccupied instances available. Which scaling type would be the most appropriate to meet these requirements?

A. Automatic Scaling with min_idle_instances set to 3.

B. Manual Scaling with 5 instances.

C. Basic Scaling with target_latency set to 3 seconds.

D. Automatic Scaling with cool_down_period_sec set to 3.

Question 50: As a software engineer at a rapidly growing tech company, you've been assigned to develop a new application and need to find a Jenkins installa-

tion to build and deploy your source code. To streamline the process and ensure efficiency, you want to automate the installation. What should you do?

A. Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image.

B. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application.

C. Use Cloud Build to create an instance of Jenkins and deploy the application.

D. Deploy Jenkins through the Google Cloud Marketplace.

Practice Exam 13 Solutions

Solution to Question 1: D

The correct answer is D. Deploy the monitoring pod in a DaemonSet object.

Explanation:

A DaemonSet is an object in Kubernetes that ensures that each node in the cluster runs a copy of a specified pod. When a new node joins the cluster, the DaemonSet automatically deploys the required pod to that node, making it an ideal solution for deploying monitoring pods that need to be present on each node for continuous reporting of container metrics.

Now let's discuss why the other options are incorrect:

A. Deploy the monitoring pod in a ConfigMap object: ConfigMap is an object in Kubernetes that allows you to store and manage configuration data as key-value pairs. It has nothing to do with deploying or managing monitoring pods. ConfigMaps are used to separate configuration data from container images, making it easier to maintain and update.

B. Enable binary authorization at the cluster level to deploy monitoring pods: Binary authorization is a deploy-time security feature that ensures only verified images are deployed on your GKE cluster by enforcing signature validation policy. This feature only provides additional security and control over what images can be deployed but doesn't help in distributing the monitoring pod across all nodes.

C. Deploy the monitoring pod in a StatefulSet object: StatefulSet is used for deploying and managing stateful applications in Kubernetes, which require unique identities and persistent storage. Unlike DaemonSet, StatefulSet doesn't ensure that each node runs a copy of the specified pod. Monitoring pods do not typically require persistence or unique identities, so StatefulSet is not the ideal choice.

In conclusion, the best course of action for deploying a monitoring pod on every node in a Google Kubernetes Engine (GKE) cluster with autoscaling capabilities is to use a DaemonSet object, as it ensures that each node in the cluster runs a copy of the specified monitoring pod.

Solution to Question 2: D

The correct answer is D. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

Explanation: The main goal is to ensure that the resources are shared only with users from your domain and remove mismatched users without having to continuously audit the resources. By setting an organizational policy constraint, you can impose restrictions on identities by limiting them to your domain. This policy will automatically prevent users from outside your domain from accessing

your resources in the future, thus eliminating the need for constant monitoring. After implementing this constraint, you can retroactively remove the existing mismatched users to ensure the security and privacy of your resources.

Reasons why other options will not work:

A. Configuring a Pub/Sub topic to monitor resource sharing and notify you if a mismatched user is detected would mean you still need to continuously audit your resources. Moreover, this would only notify you about any mismatched users but would not prevent them from accessing your resources.

B. Creating a Cloud Scheduler task to regularly scan your projects and delete mismatched users is another way to continuously audit your company's resources, which is not an efficient solution. Also, it may not prevent new outside users from being added and accessing your resources between the scheduled scans.

C. Writing a custom script that uses the Google Cloud SDK to identify and remove mismatched users could be a useful approach, but it may not prevent newly added users with mismatched email addresses from accessing the resources. Additionally, this option implies that you will need to keep running the script to maintain the security of your resources, which is inefficient in the long run.

Solution to Question 3: C

The correct answer is C: Develop templates for the environment using Cloud Deployment Manager.

Explanation: Infrastructure as Code (IaC) refers to the management and provisioning of infrastructure using code and templates, rather than manually configuring resources through individual processes. Cloud Deployment Manager is a service provided by Google Cloud that enables users to define their infrastructure as code. By using this, you can create reusable templates in YAML, Python, or Jinja2 format, which can be parameterized to reduce repetitive code and streamline the process of creating and managing multiple Google Cloud resources.

Reasons why the other options will not work:

A. Manually use the gcloud command-line tool to manage all resources interactively: This option would not meet the requirement of reducing repetitive code because manually using gcloud to manage resources is an interactive process, and not a template-based approach. It could also be time-consuming and error-prone.

B. Use Google Cloud Pub/Sub to implement message-based asynchronous resource management: Google Cloud Pub/Sub is a messaging service, and although it helps in exchanging messages between applications, it doesn't offer a way to manage Google Cloud resources or implement Infrastructure as Code. This would not satisfy the requirement.

D. Use curl in a terminal to send a REST request to the relevant Google API for each individual resource: This option would involve manually sending requests for each resource, which would not help in streamlining the process or reducing repetitive code as required. It could be time-consuming and error-prone as compared to using templating solutions provided by Cloud Deployment Manager.

Solution to Question 4: A

The correct answer is A. You should first run the command 'gcloud projects list' to get the project ID for "my-project". After obtaining the project ID, you should run the command 'gcloud services list –project ' to generate the list of enabled GCP APIs for "my-project". This approach ensures that you are targeting the correct project and lists only the enabled APIs for that specific project.

Here's why the other options will not work:

Option B: This option will not work because 'gcloud auth login' is used for authenticating the user, not for listing enabled APIs in a project. Moreover, using the project name instead of the project ID may result in a wrong or incomplete list of enabled APIs as the 'gcloud services list' command requires project ID, not project name.

Option C: This is not the correct option because 'gcloud config list' is used for listing the gcloud configurations and not for listing the enabled APIs within a project. Additionally, the use of –filter "*" does not restrict the output to only the enabled APIs of the "my-project".

Option D: This option will not work since 'gcloud projects describe my-project' is used for describing the properties of a project and not for listing the enabled APIs. Also, the command 'gcloud services list-apis' is incorrect and not a valid gcloud command.

Solution to Question 5: B

The correct answer is B, which is to select the built-in IAM project Viewer role and add the user's account to this role. The reason for this is that the Viewer role will provide the auditor with the necessary permissions to read all project items, without having the ability to modify them. This is the perfect role for an auditor who should only have access to view the project components and not make any changes.

Option A is incorrect because assigning the user to the IAM project Editor role with view-only permissions still adds the user's account to the Editor role. This could unintentionally allow them with more access than just viewing project items, and might allow for modifications.

Option C is not suitable because the IAM BigQuery Data Viewer role is specific to BigQuery data. This would not provide the auditor with access to read all project items. Instead, it would limit their access to BigQuery-related resources.

Finally, Option D is incorrect because the IAM Billing Account Viewer role focuses on providing visibility into the billing account. Adding the user to this role would not grant them access to read all the project items because it is largely centered around billing information.

In conclusion, Option B is the best choice, as it gives the auditor the correct permissions to view all project items without granting them any additional or unnecessary capabilities.

Solution to Question 6: C

The correct answer is C: "Use Cloud Functions and configure the bucket as a trigger resource."

Explanation:

Option A (Use Cloud Run and configure the bucket as an event source using Cloud Pub/Sub) is not the best approach because Cloud Run is primarily designed for running stateless containers, and it requires extra configuration with Cloud Pub/Sub to manage bucket events. This option adds unnecessary complexity when there's a more straightforward solution available with Cloud Functions.

Option B (Use Cloud Data Fusion and create a pipeline triggered by the bucket) is not suitable for this scenario because Cloud Data Fusion is mainly used for building data integration pipelines with pre-built connectors and transformations. It's more focused on data ingestion and processing tasks rather than event-driven solutions like running code snippets in response to bucket events.

Option C (Use Cloud Functions and configure the bucket as a trigger resource) is the most fitting solution for this use case. Cloud Functions is designed for building event-driven, serverless applications. By setting the Cloud Storage bucket as a trigger resource, the code snippet will be automatically executed when new files are uploaded to the bucket. This is exactly what the question asked for.

Option D (Use Google Kubernetes Engine and configure a CronJob to trigger the application using Pub/Sub) is not ideal because it adds complexity to the deployment process. Kubernetes Engine and a scheduled CronJob may be overkill for the simple requirement of running a code snippet when a file is uploaded to a bucket. Moreover, CronJobs run on a fixed schedule and are not natively event-driven based on bucket events.

In conclusion, option C is the most suitable approach for this particular scenario since it directly matches the requirements of deploying a code snippet that is triggered when a new file is uploaded to a Cloud Storage bucket. Deploying the code snippet using Cloud Functions and configuring the bucket as a trigger resource fits the requirements best and keeps the solution event-driven and straightforward.

Solution to Question 7: B

The best course of action to achieve your requirement is option B - Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs. This is the most effective way to minimize the risk and impact of possible outages on your customers while following Google-recommended practices for managing revisions.

Option A - Configuring a Cloud Function to automatically roll back the service if a certain number of errors are detected in Stackdriver Monitoring is not recommended because it can introduce complexity and additional cost. Moreover, this approach will not minimize the impact on users since the rollback only happens after errors have occurred.

Option C - Creating multiple Cloud Run staging environments for testing before deploying to production, but maintaining the same traffic allocation, does not address the core issue of minimizing the impact on users in the production environment. Staging environments are useful for testing, but they cannot guarantee that no issues will arise once the new revision is deployed to production.

Option D - Enabling Google Cloud Logging on the new revision and closely monitoring logs to identify issues and perform rollbacks when necessary is a reactive approach that can be useful in troubleshooting, but it does not prevent the impact on users. Moreover, relying solely on log monitoring can be time-consuming and may not provide real-time visibility into the system performance.

In conclusion, gradually rolling out the new revision and splitting customer traffic between the revisions (option B) is the best way to minimize the risk and impact on users while enabling the development team to deploy new features to an existing Cloud Run service in production. This approach allows for a smooth transition and enables a quick rollback in case any problems occur during deployment.

Solution to Question 8: D

The correct answer is D, migrate the workload to a Compute Engine VM and start and stop the instance as needed.

Here's why:

A. Using the App Engine standard environment to run the workload is not the most appropriate option because it is designed for applications that require rapid scaling and can handle requests within seconds. A 30-hour long monthly batch process does not need rapid scaling and seamless handling of incoming requests. Additionally, App Engine might be more expensive than Compute Engine for long-running tasks.

B. Cloud Dataflow with autoscaling enabled is not the most suitable option as it is primarily designed for real-time data processing and continuous streaming pipelines, not for offline, batch processing jobs. Furthermore, autoscaling may lead to extra costs when the instance scales up according to the workload demand.

C. Migrating the workload to a Google Kubernetes Engine (GKE) cluster with Preemptible nodes is not ideal because Preemptible nodes are short-lived and can be terminated within 24 hours. This might not be suitable for a 30-hour long monthly batch process that needs to be restarted if interrupted, leading to increased costs and inefficiencies.

D. Migrating the workload to a Compute Engine VM is the most appropriate course of action as it allows you to start and stop the instance as needed. This will enable you to run your offline, long-duration batch process without interruption while keeping the costs as low as possible. Compute Engine VMs can be customized according to the workload's resource requirements, and you would only pay for the resources you use while the VM is running, making it a cost-effective solution for your use case.

Solution to Question 9: B

The correct answer is B. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Explanation:

A network administrator managing an on-premises infrastructure needs to handle the additional workload by bursting to Google Cloud. The goal is to allow direct communication between workloads on Google Cloud and the on-premises workloads using a private IP range.

Option B is the most effective solution for creating a secure connection between the on-premises environment and the Google Cloud infrastructure. Cloud VPN establishes a secure tunnel and encrypts data traveling between the two networks. This ensures that the company's private IP range is maintained between the on-premises environment and the Google Cloud resources.

The other options are not suitable for handling this scenario because:

Option A suggests creating Cloud NAT in both on-premises and Google Cloud environments and using IP forwarding instead of a VPN. This would not provide the required private IP range between both networks, as Cloud NAT is used to map private IP addresses to public IP addresses rather than creating a secure connection between on-premises and Google Cloud.

Option C focuses on configuring firewall rules only on the on-premises environment, which is insufficient for the desired outcome. The primary concern is to create a secure connection between the networks, and only modifying the on-premises firewall rules does not achieve that. Moreover, it doesn't address the need for a private IP range.

Option D proposes configuring the VPC in Google Cloud for Organization-wide authorized networks. This suggests allowing traffic from all authorized networks across the organization, which is likely too broad of an approach. The primary goal is to enable direct communication between on-premises and Google Cloud

workloads using a private IP range, and this option does not directly address that requirement.

In conclusion, Option B best meets the needs of the scenario by setting up a secure and private connection between on-premises and Google Cloud infrastructures via Cloud VPN. The other options do not adequately address the specific requirements of the situation.

Solution to Question 10: A

The correct answer is A: Deploy the new version in the same application and use the –splits option to give a weight of 99 to the current version and a weight of 1 to the new version. This is because the App Engine standard environment allows you to perform traffic splitting based on the weight you allocate for each version. By using the –splits option, you can gradually roll out the new version to a percentage of users while keeping the complexity minimal.

Option B is not suitable because the –migrate option is used for routing 100% traffic to the newly deployed version, which doesn't serve the purpose of testing the new version on just 1% of the users.

Option C is incorrect because, although it suggests using traffic splitting in App Engine, it recommends doing so using the Console. This approach does not minimize complexity as it would require manual intervention for configuration and management, compared to using the –splits option on deployment.

Option D is not suitable because deploying the new version using Firebase Hosting and using Cloud Functions to redirect traffic is more complex and adds unnecessary overhead to the process. This approach also adds external dependencies and deviates from the App Engine standard environment, which is not required for this purpose.

Solution to Question 11: B

The most appropriate solution for migrating this legacy on-premises data analytics system with minimal effort and cost would be option B: Lift and shift to a VM on Compute Engine and use an instance schedule to start and stop the instance.

Explanation for option B: Lifting-and-shifting the application to a VM on Compute Engine maintains the existing architecture and requires minimal adjustments. Compute Engine allows you to run and manage your VM instances easily, making it a cost-effective and simple solution. You can create an instance schedule that starts and stops the instance according to your needs, such as running it every midnight to process the transactional data files efficiently.

Reasons why other options will not work:

Option A: Pub/Sub and Cloud Scheduler are more suited to event-driven architectures and message-based communication between components. However, the current scenario describes a data processing application rather than

a microservices-based or event-driven one. Implementing Pub/Sub and Cloud Scheduler would require significant changes to the existing architecture and may not align well with the company's requirement for minimal effort and cost.

Option C: Cloud Run is a serverless platform designed for deploying, scaling, and managing containerized applications. Although Cloud Run supports instances with a maximum of 2 gigabytes of memory, the legacy system processes files up to 16 gigabytes, which would pose a problem. Additionally, rewriting the application or adapting it to a containerized environment might require more effort than a straightforward lift-and-shift to Compute Engine.

Option D: Cloud Functions is a serverless computing environment intended for the deployment of single-purpose, lightweight functions. It imposes a maximum execution limit of 540 seconds, which is not enough for the system that takes about 45 minutes for processing. Furthermore, creating a containerized solution is not suitable in this scenario due to the potential for additional effort, and using Cloud Functions might not provide the desired level of control and memory for the analytics system.

In conclusion, option B is the most suitable choice because it enables minimal effort and cost while properly addressing the requirements and constraints of migrating this legacy on-premises data analytics system to Google Cloud.

Solution to Question 12: C

The correct answer is C: Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

Explanation:

Option A is incorrect because Firebase is used for developing mobile and web apps, not verifying dependencies in Deployment Manager templates. It would not provide the desired feedback for this use case.

Option B is incorrect because manually inspecting interdependent resources can be time-consuming and error-prone, especially with complex Deployment Manager templates. This method would not provide the fastest feedback possible, as required in the question.

Option C is the correct choice because executing the Deployment Manager template using the "-preview" option allows for a quick assessment of whether the resources are properly provisioned before committing it to the project. This enables the cloud engineer to receive fast feedback on the dependencies of all defined resources in the template.

Option D is incorrect because simulating the template changes in the Cloud Shell only helps verify the syntax of the deployment configurations, but it would not help in providing feedback on the dependencies between resources as the template is not getting executed in the project environment.

Solution to Question 13: B

The correct answer is B. Enable the Node Auto-Upgrades feature for your GKE cluster.

Explanation:

As a DevOps engineer working for a fintech company, your primary concern is to ensure that your GKE cluster always runs a supported and stable version of Kubernetes. To achieve this, enabling the Node Auto-Upgrades feature for your GKE cluster is the most suitable choice. This feature automatically keeps the nodes in your cluster up-to-date with the latest stable version of Kubernetes. It ensures that your cluster has the latest security patches, bug fixes, and features, minimizing the risk of vulnerabilities and maintaining stability in your environment.

Why other options will not work:

A. Use "Windows Server" as a node image for your GKE cluster: While GKE supports running Windows Server containers, this option does not directly cater to the requirement of ensuring a supported and stable version of Kubernetes. The node image choice is related to the operating system your workloads are running on instead of maintaining the Kubernetes version.

C. Use "Ubuntu" as a node image for your GKE cluster: Similar to option A, the choice of "Ubuntu" as a node image is focused on the operating system of your workloads but does not directly ensure the stability and the supported version of Kubernetes.

D. Enable the "Stackdriver Monitoring" for your GKE cluster: Enabling Stackdriver Monitoring provides you with essential monitoring and logging features necessary to track the performance and health of your GKE cluster. Although it is an essential part of managing and maintaining the cluster, it does not inherently ensure that your cluster runs a supported and stable version of Kubernetes.

Solution to Question 14: B

The correct answer is B. Here's why:

Option B: Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

- Transfer Appliance is a Google-recommended, non-programmatic method for transferring large quantities (100s of TB) of data to Google Cloud Storage. In this scenario, 200 TB of video files are best suited for Transfer Appliance.
- BigQuery Data Transfer Service is designed to automatically transfer data from external data sources like Amazon Redshift to BigQuery. It can

handle data warehouse migration without any custom code, which aligns with the task's requirements.
- Storage Transfer Service is ideal for transferring data from Amazon S3 to Google Cloud Storage, like the 20 GB of PNG files mentioned in the problem statement. It also does not require any coding.

Options A, C, and D are incorrect for these reasons:

Option A: Cloud Data Fusion is not ideally suited for transferring large volumes of binary files like videos. Dataflow is a stream and batch processing platform, not a tool for migrating data warehouse data. Dataproc is a managed Hadoop and Spark service for big data processing, which is not appropriate for transferring PNG files.

Option C: Although Storage Transfer Service is suitable for the PNG files stored in S3, it's not designed for transferring on-premises data, such as the 200 TB of video files stored in SAN storage.

Option D: Dataproc is not suitable for transferring data to Cloud Storage, as it primarily focuses on data processing. Similarly, Cloud Pub/Sub itself is not designed for transferring data to Cloud Storage; it is a messaging service between applications that can't be used for transferring PNG files directly between two storage services.

Solution to Question 15: D

The correct answer is D. The explanation for why the answer should be D and why other options will not work is as follows:

Option D: "After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM." This is the correct procedure for configuring a Windows VM on Compute Engine for seamless RDP access. The `gcloud compute reset-windows-password` command generates a new random password for the default admin user of the Windows VM. When executed, the command also displays the information required to establish an RDP session, such as the username and the new password. This option ensures a secure and automated way to access the VM via RDP.

Option A: "After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM." This option will not work because JSON private keys are used for authenticating service accounts to interact with Google Cloud APIs. They are not intended for accessing VMs directly via RDP.

Option B: "After the VM has been created, use the SSH keys for your VM to log in via RDP." This option is incorrect because SSH keys are used for authentication in Secure Shell (SSH) connections, which is a different protocol than Remote Desktop Protocol (RDP). RDP requires its own authentication method, such as usernames and passwords, rather than SSH keys.

Option C: "After the VM has been created, use your Google Account credentials to log in into the VM." Using Google Account credentials for accessing Windows VMs via RDP is not a supported method in Compute Engine. In fact, Google Account credentials are primarily used for accessing Google Cloud Console and managing cloud services, not for logging into VMs.

Solution to Question 16: C

The correct answer is C, as it provides the most cost-effective solution for a fault-tolerant batch workload without compromising efficiency.

C. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs. The main advantage of using Spot N2 Standard VMs is their discounted pricing when compared to standard VMs. Spot VMs are offered at a lower cost since they utilize spare capacity within the data center. The use of simulated maintenance events tests the resilience of the batch workloads to ensure there is no significant impact if VM terminations occur. Implementing Spot VMs is a suitable strategy for fault-tolerant workloads since it ensures cost optimization while continuing to meet operational requirements.

A. Run a test using simulated maintenance events. If the test is successful, use N2 Standard VMs when running future jobs. Although testing the fault-tolerance with simulated maintenance events is an appropriate approach, this option proposes the use of N2 Standard VMs instead of Spot N2 Standard VMs. This choice does not reduce costs effectively, as Spot VMs provide better cost savings without compromising performance.

B. Run a test using Cloud Dataproc with preemptible VMs enabled. If the test is successful, use Cloud Dataproc with N2 Standard VMs for future jobs. Cloud Dataproc is a managed service for Apache Hadoop and Apache Spark, but it is not well-suited for general virtual machine management, which is required in the given scenario. Although preemptible VMs can lower costs, they are less efficient than Spot VMs when optimizing expenses for fault-tolerant batch workloads.

D. Run a test using Kubernetes Engine with Committed Use Discounts. If the test is successful, use Kubernetes Engine with N2 Standard VMs for future jobs. While Kubernetes Engine is an excellent choice for container orchestration, it is not the ideal solution for managing VMs solely for batch workloads. Furthermore, Committed Use Discounts require long-term commitments, thus limiting the company's flexibility in VM management. This option does not offer the most cost-effective solution when compared to Spot VMs.

Solution to Question 17: C

The correct answer is C: Create a budget per project and configure budget alerts on all of these budgets.

Explanation:

Option A is not the right choice because Cloud Pub/Sub is used for messaging and streaming data between services and applications. It does not provide any functionality to monitor or manage the costs of Google Cloud resources.

Option B is not the most efficient solution. While creating a separate billing account and using BigQuery billing exports along with Data Studio can help you visualize the costs, it does not provide an automatic alert system to notify you when a developer spends more than $500 per month.

Option C is the best option because it allows you to create individual budgets for each of the sandbox projects and set budget alerts. This way, you'll be automatically notified when a developer's spending on their sandbox environment surpasses the $500 threshold you've set.

Option D is not ideal because creating a single budget for all projects would not allow you to monitor the spending of your developers individually. You could potentially miss essential alerts if one developer spends more than $500 while the total costs remain within the shared budget. This also reduces the granularity of tracking each sandbox project's cost.

Solution to Question 18: D

The correct answer should be D. Deploy the container on Cloud Run, and here's the explanation for why this option is the best among all others and why other options will not work efficiently:

A. Deploy the container on Cloud Functions with HTTP trigger: This is not an ideal choice because Cloud Functions is designed for running event-driven serverless applications and not for deploying containerized applications. It would require significant rework and would not utilize the container efficiently.

B. Deploy the container on Kubernetes Engine with Vertical Pod Autoscaler: While Kubernetes Engine provides a solid platform for deploying containerized applications, using a Vertical Pod Autoscaler could become costly for a client who has limited requests and wants to minimize costs. It might also require manual management of the environment, which can be time-consuming.

C. Deploy the container on GKE with cluster autoscaling and horizontal pod autoscaling enabled: While this option is great for scaling, it is not necessary in this scenario, given that the application receives a limited number of requests daily. It could be overkill and might introduce unnecessary complexity and costs to the client.

D. Deploy the container on Cloud Run: This is the best option for the given situation. Cloud Run is a managed compute platform that enables you to run containers with ease. It automatically scales with the number of requests, has built-in support for HTTP endpoints, and you only pay for the actual usage. It perfectly meets the client's requirements for a cost-efficient and hassle-free deployment method.

Solution to Question 19: A

The ideal storage solution in this scenario would be option A: Cloud Spanner.

Cloud Spanner is a fully managed, horizontally-scalable relational database that offers strong consistency and high availability. It is designed to handle globally-distributed applications with ease, automatically scaling as needed to accommodate large user bases and workloads while maintaining low latencies. Furthermore, it requires minimal configuration changes as it grows, which aligns perfectly with the primary requirement mentioned by the CTO.

Here's why the other options are not ideal for this situation:

B. Cloud SQL is a fully managed relational database service for MySQL, PostgreSQL, and SQL Server. While it does provide some level of scalability through the ability to add read replicas and scale the underlying infrastructure, it does not offer the level of horizontal scalability or global distribution that Cloud Spanner does. As a result, it may not be sufficient for an application with an uncertain, potentially large global user base.

C. Cloud Datastore is a fully managed, highly-scalable NoSQL database specifically designed for web and mobile applications. Although it provides some level of scalability similar to Cloud Spanner, it lacks the strong consistency offered by a relational database like Cloud Spanner. The application being developed in this scenario is described as "sophisticated", which may imply a need for the kind of relational integrity and complex querying that Cloud Spanner is more suited to handle.

D. Cloud Data Fusion is a data integration and ETL (Extract, Transform, Load) service that allows users to create, schedule, and manage data pipelines. It is not a database solution itself; instead, it is focused on processing and preparing data for analytics and machine learning through integration with other storage systems. Thus, it does not meet the storage and scalability requirements outlined by the CTO.

In conclusion, implementing Cloud Spanner would be the most suitable option in this case, as it provides a scalable, globally-ready solution with strong consistency and low-latency performance that can adapt to the application's user growth with minimal configuration changes.

Solution to Question 20: D

The correct answer is D, create the instance without a public IP address. When a Compute Engine instance is created without a public IP address, it only has a private IP address, which means it can only be accessed within the same VPC or over the connected VPN. This ensures that public Internet traffic cannot reach the instance, fulfilling the task requirement.

Option A is incorrect because creating a firewall rule to only allow traffic from Google Cloud VPC does not prevent public Internet traffic from reaching the instance. The instance would still have a public IP address, and a determined attacker could potentially bypass the firewall rules.

Option B is also incorrect. While enabling Private Google Access allows traffic to pass between Google Cloud services and the instance, it does not prevent Internet traffic from accessing the instance if it still has a public IP address.

Option C is not a suitable solution because restricting the instance to only allow traffic from on-premises WAN IP addresses still exposes the instance to public Internet traffic, even if it is limited to the company's WAN IP range. This does not entirely ensure that the instance is inaccessible to the public Internet.

In conclusion, the answer should be D, create the instance without a public IP address, as this will effectively prevent public Internet traffic from accessing the instance and ensure that it can only be reached over the VPN connection.

Solution to Question 21: B

The correct answer is B - Enable the Cloud Spanner API.

Here's why:

A. Create a new Google Cloud Firestore instance for global data storage. This option is incorrect because the question explicitly states that Cloud Spanner will be used for data storage. Google Cloud Firestore is an alternative choice for data storage and not the required technology in this scenario. It is essential to focus on the Cloud Spanner instance rather than creating another instance type.

B. Enable the Cloud Spanner API. This is the correct option. Before you can create a Cloud Spanner instance, you must enable the Cloud Spanner API for your project. This action allows your project to communicate with the Cloud Spanner service, ensuring that it's available and accessible during the development phase. Enabling the API is a prerequisite for effectively utilizing Cloud Spanner.

C. Create a new VPC network with subnetworks in all desired regions. While creating a VPC network with subnetworks is crucial for deploying resources in various regions, it is not the initial step needed for creating a Cloud Spanner instance. The question explicitly concerns the first action needed in starting a Cloud Spanner instance. In this case, enabling the Cloud Spanner API precedes creating the VPC network.

D. Enable Cloud Storage API for the project. This option is incorrect because it doesn't relate to Cloud Spanner directly. The Cloud Storage API pertains to Google Cloud Storage, which is a different service from Cloud Spanner. There is no requirement to enable the Cloud Storage API in this specific context, as the goal is to create a Cloud Spanner instance.

In conclusion, the first action taken before creating a Cloud Spanner instance should be to enable the Cloud Spanner API. Enabling the API will allow your project to interface with the Cloud Spanner service as needed throughout the development process. Other options, like creating new instances, networks, or en-

abling unrelated APIs, can be implemented as needed during subsequent phases, but they should not precede enabling the Cloud Spanner API.

Solution to Question 22: B

The most appropriate course of action for managing expenses across various departments using Google Cloud projects and providing a comprehensive overview of all costs incurred is option B: Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

Option B is the best choice because it allows you to automate the process of collecting cost data from various billing accounts and consolidating it into a single, scalable environment (BigQuery) for further analysis and reporting. BigQuery is designed to handle large datasets, and Looker Studio is a powerful visualization tool that can help you create comprehensive, dynamic, and interactive reports for better cost management and projections.

Option A: Using the Cloud Billing API to fetch the costs from each project and compile them into a single file for visualization in Excel is not ideal because it involves manually fetching and compiling data from multiple projects, which can be time-consuming and error-prone. Moreover, this approach may not scale well if the number of projects or expenses grows significantly. Also, Excel may not be the best tool for handling large datasets and creating complex visualizations compared to Looker Studio.

Option C: Exporting cost data from each billing account to a Google Sheet and using the Google Sheets API to combine them for visualization is not the most efficient solution. Google Sheets has limitations in terms of the volume of data it can handle, which might cause slow performance or crashes if the dataset becomes too large. Additionally, this process does not update cost data as quickly as BigQuery and Looker Studio, which can hinder real-time analysis and projections.

Option D: Using Google Cloud Monitoring to track costs of each project and create dashboards is not focused on comprehensive cost analysis and visualization across multiple billing accounts. While it can provide some insights into individual project costs, it does not offer the same level of depth and flexibility in cost management and analysis as exporting data to BigQuery and visualizing it via Looker Studio.

Solution to Question 23: D

The answer is D, to use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity. This is because using GCDS allows you to sync your Active Directory with Google Cloud services, ensuring that your company can maintain Active Directory as the primary source for user identity information while also having full control over Google accounts used by employees for various Google services, including Google Cloud Platform (GCP).

Option A, using Google Workspace to create and manage users, would not work

because it doesn't involve Active Directory as the primary source for user identity information. This approach would mean maintaining separate user management systems, potentially leading to inconsistencies between Active Directory and Google Workspace user profiles.

Option B, using the GCP Console to migrate users from Active Directory to Cloud Identity, would not meet the company's requirement of maintaining Active Directory as their primary source for user identity information. Migrating users from Active Directory to Cloud Identity would make Cloud Identity the main source of user information, instead of letting the company continue using Active Directory.

Option C, manually creating user accounts in Cloud Identity for each employee and assigning them roles, is not a feasible option because it could lead to significant administrative overhead. In addition, it does not utilize Active Directory, which the company specifically wants to maintain as their primary source of user information.

Hence, using Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity (Option D) would be the most suitable choice as it allows the company to maintain access control and user management in a unified and organized manner while meeting their requirements for Active Directory integration.

Solution to Question 24: A

The correct answer is A. When creating the instances, specify a Service Account for each instance.

Explanation: Option A is the right choice because it allows you to set proper access control for different Compute Engine instances by assigning a specific service account to each instance during its creation. This ensures that every instance will have the necessary permissions to interact with Google Cloud APIs according to the assigned service account's roles.

Option B is incorrect because assigning the name of each Service Account as instance metadata doesn't actually give the instances permissions to interact with Google Cloud APIs. Metadata is just key-value pairs associated with the instance; it doesn't have any direct impact on the instance's access control.

Option C is incorrect because IAM roles should be assigned to service accounts, not to instance metadata. Assigning IAM roles to instance metadata wouldn't establish the permissions necessary for proper access control when interacting with Google Cloud APIs.

Option D is incorrect because creating individual user accounts for each instance and using them as Service Accounts is not a recommended practice. User accounts are meant for individual users, whereas service accounts are specifically designed for managing access control for applications and services running on Google Cloud instances. Using user accounts instead of service accounts would

defeat the purpose of having well-defined access control mechanisms in Google Cloud.

Solution to Question 25: A

The correct answer is option A: Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.

Explanation for why option A is correct:

Using the Secret object is the recommended approach because it allows you to securely store sensitive information like database passwords, API keys, etc., separate from the application code and configurations. By modifying the YAML file to populate the DB_PASSWORD environment variable from the Secret, you can easily provide the necessary credentials to the application while ensuring that the password is not stored in plain text or directly in your YAML file. This complies with best practices recommended by Google for managing sensitive data in Kubernetes.

Why other options will not work:

Option B: Storing the database password in a Cloud Storage bucket adds complexity to the setup and requires a separate Cloud Function to retrieve it during runtime. This increases the overall latency and potential failure points in the system when compared to using a Secret object, which is more straightforward and specifically designed for this purpose.

Option C: Storing the database password in a separate YAML file and using kubectl to apply the updated configuration might protect the sensitive data from being accidentally exposed in the core configuration file. However, it still stores the password as plain text somewhere and does not provide the same level of security, encryption, or access control as a Secret object.

Option D: Storing the database password inside the Docker image of the container would not be a secure approach. Anyone with access to the container image can extract the sensitive information. Also, it would require rebuilding and redeploying the image every time there is a change in the password. Using a Secret object is a more secure and flexible approach.

Solution to Question 26: C

The correct answer is C. Create a health check on port 443 and use that when creating the Managed Instance Group.

Explanation:

Since the goal is to ensure that unhealthy VMs are automatically replaced for an HTTPS web application, we need to use a health check that monitors the VMs based on the expected behavior of the HTTPS web application. HTTPS primarily listens on port 443, so creating a health check for that port will ensure the health check is specific to the HTTPS application. Using this health check

when creating a Managed Instance Group (MIG) guarantees that it will only flag instances as unhealthy if they're not responding correctly on port 443, leading to their automatic replacement.

Option A is incorrect because using the default health check for network load balancing is not suitable for HTTPS web applications. Network load balancing health checks are focused on the overall availability of a VM instance, not of a specific service like the HTTPS web application.

Option B is incorrect because adding the label 'health-check' in the Instance Template is just a way to label instances. Adding this label doesn't actually configure or enable any real health checks. It's more of a way to organize and identify instances.

Option D is incorrect because enabling automatic rolling updates with a minimal action time only helps in keeping the MIG up-to-date with the latest instance template versions and does not address the issue of monitoring and replacing unhealthy VMs. Rolling updates help to incrementally update instances in an MIG, but they don't evaluate the health of specific instances.

Solution to Question 27: B

The correct answer is B. Deploy MongoDB Atlas from the Google Cloud Marketplace.

Explanation:

Option B is the best choice because MongoDB Atlas is a managed database service provided by MongoDB, Inc., and it comes with a support SLA. By deploying it from the Google Cloud Marketplace, you can easily integrate it with your Google Kubernetes Engine (GKE) cluster, ensuring a seamless deployment and high availability. This option allows the team to focus on application development and not worry about managing the MongoDB environment.

Option A is incorrect because Cloud Datastore is a NoSQL database service provided by Google Cloud Platform (GCP) that automatically scales with the application and doesn't require management. Although it has a MongoDB API, it cannot guarantee all MongoDB specific functionalities and does not come with a specific MongoDB support SLA. Therefore, it is not the right fit for the finance client's requirements for a managed MongoDB environment.

Option C is incorrect because setting up a VPN connection between the GKE cluster and a self-managed MongoDB instance hosted on another cloud provider adds complexity to the deployment, requires additional maintenance, and can introduce latency and security concerns. Furthermore, it would not provide a managed MongoDB environment with a support SLA, since the team would still be responsible for managing the MongoDB instance.

Option D is incorrect because Cloud Functions are designed for serverless, event-driven applications, not for deploying and hosting databases like MongoDB.

Deploying a MongoDB container on Cloud Functions would not provide a managed MongoDB environment nor a support SLA. Additionally, using a database within Cloud Functions would introduce significant limitations, such as higher latencies and limited container resources.

Solution to Question 28: D

The correct answer is D. Use GCP Marketplace to launch the Jenkins solution. This option minimizes the steps involved in deployment since GCP Marketplace offers pre-built solutions that are quick and easy to configure. By using the Jenkins solution from the GCP Marketplace, you can leverage an already optimized deployment template, ensuring a smooth and hassle-free setup.

Let's examine why the other options are not as efficient:

A. Deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service is not ideal because Cloud IAP is primarily used to provide secure access to web applications running on Google Cloud without the need for a VPN. While it can help to secure access to Jenkins, it does not aid in deploying the Jenkins server itself.

B. Creating a Kubernetes cluster on Compute Engine and using a deployment with the Jenkins Docker image requires more steps and a deeper understanding of Kubernetes configurations. This approach may be more complex and time-consuming, particularly for users who are not experienced with Kubernetes. Furthermore, the question's objective is to deploy the server with minimum steps, making this option less suitable.

C. Deploying Jenkins on Cloud Run using a custom Docker image poses several challenges. First, Cloud Run is designed for stateless, short-lived processes, whereas Jenkins stateful and long-running by nature. Cloud Run's time-limited executions might not be appropriate for Jenkins, which could result in an inadequate solution for the development team. Additionally, configuring and deploying a custom Docker image can be time-consuming and complex, in contrast to the objective of a quick, minimal-steps deployment.

In conclusion, using GCP Marketplace to launch the Jenkins solution (Option D) is the best choice to deploy the Jenkins server with minimum steps while ensuring an efficient and reliable setup for the development team in a rapidly growing tech company.

Solution to Question 29: D

The correct answer is D: Create a private zone on Cloud DNS, and configure the applications with the DNS name.

Explanation: In a hybrid cloud setup with multiple applications that require access to an on-premises database server, you want to avoid having to change the IP configuration in all of the applications when the database IP changes. To achieve this, you can use Cloud DNS to create a private zone, then configure the applications with a DNS name that resolves to the on-premises database server.

Why other options will not work: A. Configure Cloud NAT for all subnets of your VPC to be used when egressing from the VM instances: Cloud NAT is used for outbound connections of private VM instances, allowing them to access public IPs without being directly connected to the internet. This option doesn't provide a solution for the database IP change problem, and it doesn't provide a way to access the on-premises database through a domain name.

B. Configure Firebase Realtime Database as a middle layer for the applications and the on-premises database: Firebase Realtime Database is a managed NoSQL database for web and mobile applications. While it could be used as a middle layer for data synchronization, it would add unnecessary complexity to the system, and it still wouldn't provide a solution for the database IP change problem.

C. Utilize Google Cloud Endpoints to create an API proxy for your database and avoid changing the IP configuration in the applications: Google Cloud Endpoints is used to develop, deploy, protect, and monitor APIs. While this might provide a proxy for the database, it's an overly complex solution not designed for database access, and implementing it might require significant changes to the applications.

Solution to Question 30: B

The correct answer is B. Enable Data Access audit logs for the Cloud Storage API.

Explanation:

As a data security analyst in a financial company, it is essential to maintain a record of all requests concerning the storage, access, and manipulation of sensitive customer information. Enabling Data Access audit logs for the Cloud Storage API ensures that all actions performed on the stored data are logged and available for auditing purposes in compliance with regulatory requirements.

Why other options will not work:

A. Deploy a Google Cloud Armor security policy: Although Google Cloud Armor is a security tool that helps protect applications from web-based threats, it doesn't provide logging or auditing capabilities for data access. Its primary function is to protect against Distributed Denial of Service (DDoS) attacks and other malicious web activities.

C. Configure a Cloud Pub/Sub Notification for the bucket: Cloud Pub/Sub Notifications allow real-time notifications about changes to objects stored in a Cloud Storage bucket. While this feature can be useful for triggering events based on changes in the bucket, it does not provide a complete and detailed record of data access requests necessary for regulatory compliance.

D. Enable the Cloud Storage Uniform Access Control: Uniform Access Control is an access control system for Cloud Storage that allows a consistent way to manage permissions on objects and buckets. Although it helps manage access

to stored data, it does not automatically log data access requests or actions needed for ensuring regulatory compliance.

Solution to Question 31: C

The correct answer is C: Create a signed URL with a four-hour expiration and share the URL with the company.

Explanation:

Option C is the most suitable choice because it meets the requirements stated in the question while involving the least steps and ensuring a secure exchange of information. A signed URL provides temporary access to the object in the Cloud Storage bucket, and by setting a four-hour expiration, you ensure that the content access is removed after the desired timeframe. Sharing the URL with the company allows them to access the data without needing a Google account.

Reasons why other options will not work:

Option A: Creating a new custom role and using a service account would require the client company to have a Google account for assigning user-based access privileges. This is not a feasible option as the company lacks a Google account.

Option B: Although using Cloud Functions to create an endpoint with temporary read access is a possible solution, it is more complex compared to a signed URL, requiring more steps and resources to set up. Besides, the endpoint would need to be securely shared.

Option D: Creating a new Cloud Storage bucket and copying the object adds unnecessary duplicity of data, expanding extra resources. Additionally, deleting the bucket after four hours may not instantly revoke access to cached or in-transit versions of the object.

Solution to Question 32: A

The correct answer is A. The reason you should use the command "gcloud projects get-iam-policy" to view the current role assignments is that it allows you to directly retrieve and examine the IAM policy for your project. By doing this, you can easily identify the individuals who are granted the Project Owner role. This tool efficiently helps you to maintain the security of your Google Cloud Platform project as required.

Option B is incorrect because enabling Stackdriver Monitoring and reviewing logs for role changes only provides information about historical changes. It doesn't give a clear representation of the current role assignments, which is what you need to verify the individuals with the Project Owner role.

Option C might sound tempting, but it is incorrect because by reviewing the Service Accounts permissions on the IAM & admin page, you only get information about the permissions assigned to service accounts, not to individual users.

Your goal is to identify individuals with the Project Owner role, which is not covered in this part of the console.

Option D is not appropriate because the Firebase Console is mainly designed to manage the authentication and database aspects of a Firebase-based application. It is not the right place to check for a Google Cloud Platform project's IAM roles, particularly the Project Owner role.

Solution to Question 33: D

The correct answer is D. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

Explanation:

D is the best solution because it leverages BigQuery's ability to create external tables linked to Cloud Storage buckets, which allows analysts to query the data directly using SQL without needing to move or process the underlying 5-TB AVRO file. BigQuery is designed to handle large datasets and is cost-effective, which makes it an ideal solution for this scenario.

A. Configure Cloud Dataflow to read the AVRO file and write the data into Cloud Firestore for SQL querying. This option is not cost-effective, and it is slower because it involves reading the AVRO file using Cloud Dataflow and writing the data into Cloud Firestore. Additionally, Cloud Firestore is a NoSQL database that might be challenging for analysts proficient only in SQL to work with.

B. Create a Memorystore instance and use Cloud Functions to process the AVRO file, storing the data in the Memorystore for SQL querying. This option is not suitable because Memorystore is an in-memory data store, which is expensive and not designed to handle large 5-TB datasets. Additionally, using Cloud Functions to process such a large file can be slow and inefficient.

C. Create a Datastore-based App Engine Application to process the AVRO file and expose the data through an API for SQL querying. This option is not ideal because creating a Datastore-based App Engine Application and processing the AVRO file adds unnecessary complexity and is less efficient than directly querying the data through BigQuery. Datastore is also a NoSQL database, which might be challenging for analysts proficient only in SQL to work with.

In conclusion, the best solution for providing SQL access to the data contained within the 5-TB AVRO file stored in a Cloud Storage bucket is to create external tables in BigQuery and point them to the Cloud Storage buckets (option D). This approach is cost-effective and provides quick SQL access to the data requested by the data analysts.

Solution to Question 34: D

The correct answer is D. Review the IAM permissions for any role that allows for data access.

An explanation for why D is the correct answer:

As a security engineer, the main goal is to prevent unauthorized users from accessing sensitive data, which is achievable through efficient and effective Identity and Access Management (IAM) practices. Reviewing the IAM permissions for any role with data access privileges will help to identify and rectify any deficiencies in users' access controls. By auditing and refining the IAM policies for data access roles, the security engineer ensures that only authorized personnel within the organization have access to sensitive information.

Why the other options are not suitable:

A. Apply the Binary Authorization settings on the resources - Binary Authorization is a deploy-time security control that enforces signature validation when deploying container images. Although this is a valuable security measure, it doesn't directly address the specific need to manage access to sensitive data during the monthly security audit.

B. Create and apply a VPC Service Controls perimeter - VPC Service Controls provide a security perimeter around Google Cloud Platform resources, preventing data exfiltration. While this is a useful security feature, it doesn't directly target unauthorized access to sensitive data within the organization. The question focuses on controlling access to sensitive data, which is better addressed by managing IAM permissions.

C. Review the Bucket Policy Only settings for your storage buckets - Bucket Policy Only settings are relevant for managing access to Cloud Storage buckets at the bucket-level instead of the individual object-level. Although this is a useful access control feature, it is not enough to ensure that unauthorized users do not have access to sensitive data throughout the entire Google Cloud Project during the security audit. Instead, a broader IAM review should be the main focus in this situation.

Solution to Question 35: B

The correct answer is option B. The reasons why option B is the most suitable option and why the other options are not as appropriate are explained below:

Option B: This option involves creating an instance template for the instances and configuring it with the necessary settings, such as enabling 'Automatic Restart' and setting 'On-host maintenance' to Migrate VM instance. The instances are added to an instance group, which ensures that the instances are collectively managed for high availability. This approach not only takes care of automatically restarting the instances in case of a crash but also involves active management of instances during system maintenance, meeting the requirements of the task.

Option A: While creating an instance group with autohealing enabled can help instances recover from certain types of failures (e.g., those related to instance health), it does not address the specific requirement of remaining highly available during system maintenance. The autohealing health check only monitors the instance's health but does not cover maintenance requirements.

Option C: Although a regional managed instance group can offer higher availability by distributing instances across multiple zones, this option only covers the automatic restart of instances during maintenance. It does not address the requirement of maintaining high availability during system maintenance since it does not specify how the maintenance should be handled (e.g., migrating VM instances).

Option D: This option mentions configuring instances to use an instance template with an attached Persistent Disk, which is useful for preserving the data during system maintenance. However, it does not specify enabling 'Automatic Restart' and setting 'On-host maintenance' to Migrate VM instance, which are required settings for achieving high availability during maintenance.

In summary, option B is the most appropriate solution, as it meets both requirements of automatically restarting instances and ensuring high availability during system maintenance.

Solution to Question 36: B

The correct answer is B: Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

Explanation:

A. This option is not suitable because configuring the Cluster Autoscaler for cost optimization may not guarantee consistent workload performance in various situations. The Vertical Pod Autoscaler recommendations for latency optimization may help, but it only addresses one aspect of the varying resource requirements.

B. This is the best option because configuring the Horizontal Pod Autoscaler (HPA) for availability ensures that the application scales out properly to handle the increased load, maintaining workload performance in different situations. At the same time, configuring the Vertical Pod Autoscaler (VPA) recommendations for suggestions allows you to receive valuable CPU and memory recommendations, supporting a cost-effective solution without compromising performance.

C. While configuring the Horizontal Pod Autoscaler for availability is a valid approach, it does not address the main objective of estimating and recommending appropriate CPU and memory requirements. The cluster autoscaler serves to adjust the number of nodes in a cluster, but it does not provide suggestions for the workload's resource requirements.

D. Configuring the Vertical Pod Autoscaler recommendations for cost optimization might lead to an aggressive solution that prioritizes cost over performance,

which could lead to inconsistent workload performance across different situations. Configuring the Node Auto Provisioning for suggestions, like the cluster autoscaler, does not directly address the workload's resource requirements recommendation.

Therefore, following Google-recommended best practices, you should configure the Horizontal Pod Autoscaler for availability to maintain consistent workload performance and the Vertical Pod Autoscaler recommendations for suggestions to receive appropriate CPU and memory recommendations (option B).

Solution to Question 37: B

The correct answer is B: Deployment Manager.

Explanation for why the answer should be B: Deployment Manager is a scalable cloud infrastructure management service offered by Google that allows you to create and manage resources, such as virtual machines, in a programmatic and dynamic way. When using Deployment Manager, you can write templates in popular languages like Python or Jinja2 that define the resources needed for your application. Deployment Manager uses a dedicated configuration file (YAML) which includes details like the virtual machine's specifications, storage configurations, and network settings, all while adhering to Google's recommended practices. This approach helps in managing and provisioning virtual machines on Compute Engine in a more efficient and error-free manner.

Why other options will not work:

A. App Engine: App Engine is a fully managed platform as a service (PaaS) for building and deploying applications, not specifically designed to provision virtual machines and manage their specifications. It automatically scales depending on application traffic and takes care of the underlying infrastructure, which means you don't have direct control over VM provisioning.

C. Cloud Dataflow: Cloud Dataflow is a data processing service primarily used for executing big data processing pipelines. It is not designed for provisioning or managing virtual machines and their specifications on Compute Engine. Instead, its main purpose is to help with data processing tasks like ETL, batch, and stream data processing in a fully managed environment.

D. Cloud SQL: Cloud SQL is a fully-managed database service providing traditional relational SQL databases like MySQL, PostgreSQL, and SQL Server. It is not intended for provisioning or managing virtual machines on Compute Engine. Cloud SQL is focused on database management, maintenance, and scaling, while Compute Engine is meant for running general-purpose computing workloads within virtual machines.

Solution to Question 38: D

The most effective approach to achieve a streamlined process of project creation without requiring engineers' credit card details is option D: Create a Billing

account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

Here's why the other options won't work: Option A: Require engineers to submit reimbursement requests for their personal credit card expenses related to Google Cloud usage. This option contradicts the given requirement of not involving the engineers' personal credit card details in the process. Moreover, this approach is time-consuming, adds extra administrative workload for processing reimbursements, and may cause uncertainty for employees regarding their repayment.

Option B: Create separate billing accounts for each engineer and associate their individual credit cards. This option still involves using the engineers' personal credit cards, which is against the goal of the question. Additionally, it creates unnecessary complications by separating billing accounts for each engineer, making the billing management more complex.

Option C: Request Google Cloud to provide a corporate credit card for the entire engineering team. This is an unrealistic and infeasible option, as cloud service providers like Google Cloud do not issue corporate credit cards to clients. Companies are responsible for managing their own payment methods.

Option D solves the given problem by setting up a single billing account, linking it to an appropriate payment method, and granting the necessary permissions to project creators. This approach keeps the engineers' personal credit card information off the table, centralizes billing management across all projects, and simplifies the process for the engineering team, making it the most effective solution.

Solution to Question 39: C

The correct answer is C. Set Content-Type metadata to application/pdf on the PDF file objects.

Explanation:

In Cloud Storage, the Content-Type metadata determines how the object should be treated when it is accessed by a client. By setting the Content-Type metadata to application/pdf, you ensure that when users click on the link to access the PDF files, the browser recognizes the type of file and directly displays the PDF in the browser window instead of prompting the user to download the file.

Why other options will not work:

A. Configure the website's caching policy to show application/pdf content: Caching policy determines how the content is cached and served by the browser and does not affect how the browser treats the Content-Type of the file. Updating the caching policy will not change the way the browser handles the PDF file.

B. Add a label to the storage bucket with a key of Content-Type and value

of application/pdf: Labels are used for organizing resources, not for storing metadata associated with the files. Adding a label to the bucket will not change how the browser treats the PDF files.

D. Enable multi-regional storage class for the bucket containing PDF files: Multi-regional storage classes determine the geographical distribution of data but do not affect the Content-Type metadata or how the content is displayed. Enabling multi-regional storage will not resolve the issue of the browser prompting users to download the PDF files.

Solution to Question 40: C

The correct answer is C, provisioning Compute Engine instances with M1 machine type:

The major reason is that M1 machine type instances are memory-optimized, which means they provide more memory per virtual CPU than other machine types. This is crucial for an ERP system that requires its full database to be in-memory for fast data access speeds.

Here's why the other options are not suitable for this particular application:

A. Provision preemptible Compute Engine instances: Preemptible instances are short-lived, with a maximum of 24 hours, and can be terminated at any time by Google. This characteristic makes them unsuitable for a mission-critical ERP system that relies on in-memory databases, as database consistency and availability cannot be ensured with preemptible instances.

B. Use a Cloud Spanner instance for in-memory database handling: While Cloud Spanner is a highly scalable, managed relational database that supports global transactions and is designed for high-performance workloads, it is not specifically optimized for in-memory operations. Therefore, it might not provide the optimal data access speeds needed for this particular ERP system.

D. Deploy the application on Kubernetes Engine with memory optimized nodes: Kubernetes is a powerful platform for container orchestration, but using Kubernetes Engine for this particular requirement could be an unnecessary complexity, especially if the ERP system does not benefit from containerization or does not require the whole set of features provided by Kubernetes. Additionally, performance characteristics on Kubernetes Engine might differ from the performance obtained on Compute Engine instances specifically configured for in-memory workloads. Thus, relying on Compute Engine instances with M1 machine type would be a more straightforward and suitable solution.

Solution to Question 41: D

The most appropriate solution in this case is to expose the application by using an external TCP Network Load Balancer (Option D). This is because the application needs to accept TCP traffic on port 389 and preserve the client's IP address. The TCP Network Load Balancer works on the Transport Layer (Layer 4) of the OSI model and can accommodate such requirements.

Here's why the other options will not work:

Option A: Expose the application by using an external UDP Network Load Balancer. This option is not suitable because the application needs to accept TCP traffic, not UDP traffic. UDP Network Load Balancers are not designed to handle TCP traffic.

Option B: Expose the application by using an internal Serverless Network Endpoint Group Load Balancer. The Serverless Network Endpoint Group (NEG) Load Balancer is for serverless applications on Google Cloud Functions or Cloud Run. Since the application is deployed on a managed instance group in Compute Engine, this option is not suitable. Additionally, this works internally within your organization's infrastructure, not exposing the application via the internet.

Option C: Expose the application by using an internal HTTP(S) Load Balancer. The HTTP(S) Load Balancer operates on the Application Layer (Layer 7) of the OSI model, mainly handling HTTP and HTTPS traffic. It is not suitable for the application's requirement to accept TCP traffic on port 389. Moreover, the internal HTTP(S) Load Balancer would not expose the application via the internet, as it works internally within your organization's infrastructure.

In conclusion, the most appropriate solution is Option D - using an external TCP Network Load Balancer to expose the application, as it will accommodate the application's requirement to accept TCP traffic on port 389 while preserving the client's IP address.

Solution to Question 42: B

The correct answer is B: Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

Option B should be chosen because it is a simple and efficient solution to monitor activities within your Google Cloud environment. By creating log-based metrics for firewall and instance actions, you can easily track any unexpected changes or creations in real-time. Furthermore, setting up reasonable alerts will notify relevant team members when any suspicious activities are detected, effectively addressing potential security threats and staying within the company's value of simple and efficient solutions.

Option A is not optimal because Object Lifecycle Management is designed for controlling the lifecycle of storage objects in Google Cloud Storage, not for monitoring activities or analyzing logs. Stackdriver Monitoring, which is now called Google Cloud Monitoring, can be used to monitor and analyze logs, but it is not directly integrated with Object Lifecycle Management.

Option C is inefficient and does not provide real-time monitoring. Cron jobs will only check for firewall rules and instances changes periodically, which means there could be a considerable delay in identifying potential issues. Additionally,

this method would require manual reviews of email notifications, rather than automating the process with alerts and monitoring tools.

Option D is not optimal because it involves combining multiple services, making the process more complex while still being less efficient for real-time monitoring. Using a log sink to forward Cloud Audit Logs to Cloud Storage and then analyzing the logs with BigQuery would require a significant amount of manual effort, leading to a more complex, less efficient solution that does not align with the company's values.

Solution to Question 43: C

The correct answer is C. Here's why:

Option A: Adding metadata with kube-system as the key and the DaemonSet manifest as the value in the cluster's definition in Deployment Manager is not a suitable method for creating the DaemonSet within the Deployment Manager deployment. Metadata in a cluster definition is meant for storing name-value pairs, not for direct deployment of resources into the Kubernetes cluster.

Option B: Using Deployment Manager to create a Cloud Run service that deploys the DaemonSet to the kube-system namespace is not recommended, as it adds an extra unnecessary service into the process (Cloud Run) and does not minimize the number of services used.

Option C: Adding the cluster's API as a new Type Provider in Deployment Manager allows you to create a custom type provider to communicate with the Kubernetes API directly. By creating the DaemonSet using the new type, you can create the required DaemonSet in Google Kubernetes Engine (GKE) cluster within the same Deployment Manager deployment. This method minimizes the number of services involved, meeting the requirement.

Option D: Updating the Deployment Manager configuration to include a Cloud Logging sink is not suitable for this purpose. Cloud Logging sinks' primary intent is to route log entries to specific outputs, not to deploy resources like DaemonSets into Kubernetes clusters. This option would introduce unnecessary complexity and does not minimize the number of services used.

In conclusion, Option C is the best choice as it allows creating a DaemonSet in the kube-system namespace of the cluster within a single Deployment Manager deployment, minimizing the number of services used.

Solution to Question 44: D

The correct answer is D. Store the application data on a regional persistent disk. If an outage occurs, create an instance in another zone with this disk attached.

In a financial services company, it is crucial to maintain high availability and prevent data loss. Storing the data on a regional persistent disk ensures that the data is automatically replicated across two zones within the region, providing higher durability and lower latency compared to replicating data manually.

This allows you to create instances in another zone during an outage, ensuring continuity of service without manual intervention.

Here's why the other options are not suitable:

A. Cloud Datastore is a NoSQL database service, and while it does offer high availability, it is designed for applications that need a more scalable and flexible storage solution. It is not the most suitable option for a typical mission-critical financial services application that may require a more traditional relational database and various consistency and durability guarantees. Additionally, Cloud Datastore no longer supports inter-zone replication, as it is now replaced with multi-region replication by default.

B. Cloud SQL is a managed relational database service, and while it can be a good choice for a financial services application, it should be noted that only the failover replicas provide high availability. Enabling automatic cross-zone failover does not guarantee data durability in the case of a zonal failure, as live migrations are limited to the same zone. This option would not be enough to meet the high availability requirements for this use case.

C. Storing the application data on a zonal persistent disk has a single point of failure, as it is limited to only one zone. In case of a zonal failure, manual intervention would be required to create an instance in another zone and attach the disk, which could lead to data loss and unavailability during that process. This option does not satisfy the high availability needs of a mission-critical application in a financial services company.

Solution to Question 45: D

The correct answer is D. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

Explanation:

In a canary deployment, a small percentage of users are directed towards a new version of an application, allowing you to assess its performance and stability without fully rolling it out to all users. Cloud Run for Anthos supports traffic splitting between revisions, which makes it an ideal platform for canary deployments.

Answer D is the best approach because creating a new revision with the new version of the application and splitting the traffic between the current and new revisions allows you to gradually assess its performance with a subset of users. Additionally, this approach leverages the existing Cloud Run for Anthos infrastructure, making it simple to implement and manage.

Option A is not a suitable choice because Cloud Storage buckets are used to store static assets and do not host web applications. Cloud CDN is used for caching and serving static content from Cloud Storage buckets or HTTP(S) Load Balancers, and it would not help evaluate a new version of the application.

Option B involves using Compute Engine instances, which do not take advantage of the serverless nature of Cloud Run for Anthos. Furthermore, configuring an instance group may be more complex than simply using traffic splitting as suggested in option D.

Option C would only partially achieve the desired outcome, as creating a new revision is a step in the right direction. However, using an HTTP Load Balancer to distribute traffic between multiple Cloud Run for Anthos revisions is unnecessary when Cloud Run for Anthos natively supports traffic splitting functionality.

Thus, answer D - creating a new revision and splitting the traffic is the most efficient and effective method for canary deployment on Cloud Run for Anthos.

Solution to Question 46: B

The correct answer is B: Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

Explanation: When you see that one of the virtual machines in your managed instance group is having issues, the quickest way to replace the problematic VM with a new one is to utilize the 'gcloud compute instance-groups managed recreate-instances' command. This command will allow you to specify the problematic instance and request a recreation, ensuring that a new VM with an updated configuration will be created in its place.

Here is why the other options are not suitable:

A. Use the gcloud compute instance-groups managed resize command to resize the MIG. - This option is not ideal because resizing the managed instance group only changes the overall number of instances within the group. It does not address the issue with the specific VM exhibiting errors.

C. Set the autohealing policy for the MIG to replace unhealthy instances automatically. - While setting up an autohealing policy can be helpful in addressing problematic instances automatically, it is a more long-term solution. If you need to replace the problematic VM quickly in the current situation, this option would not be the most efficient method.

D. Use the gcloud compute instance-groups managed delete-instances command followed by gcloud compute instance-groups managed add-instances to replace the VM. - This option could work, but it consists of multiple steps and is not as efficient as using the 'recreate-instances' command. Additionally, deleting the instance and adding a new one may cause unintended downtime, while the 'recreate-instances' command ensures smooth transition by only removing the instance after the new one is created.

Solution to Question 47: C

The correct answer is C: gcloud deployment-manager deployments update –config

Explanation:

A. gcloud deployment-manager resources update –config This option is incorrect because there is no "resources update" command in the gcloud deployment-manager. Besides, updating resources directly could potentially cause downtime.

B. gcloud deployment-manager deployments delete –config This option is incorrect because the "deployments delete" command will delete the entire deployment, thus causing downtime as the resources will be removed from the project.

C. gcloud deployment-manager deployments update –config This is the correct answer. The "deployments update" command will update the deployment with the specified configuration file while keeping the resources intact and running. It ensures there is no downtime during the update process.

D. gcloud deployment-manager deployments list –config This option is incorrect because the "deployments list" command only lists the deployments available in the project and will not have any effect on updating the deployment or avoiding downtime.

Solution to Question 48: A

The correct answer is A, and here's the reasoning behind it:

A. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

This is the correct approach because it follows the Google-recommended practices for integrating Cloud Run with Cloud Pub/Sub. By creating a dedicated service account, you ensure least privilege access and enhance your application's security. Assigning the Cloud Run Invoker role to the service account enables it to call your Cloud Run application. Lastly, creating a Cloud Pub/Sub subscription with the service account allows for efficient and seamless message processing.

B. 1. Create a Cloud Dataflow pipeline that reads messages from the Pub/Sub topic and then calls your Cloud Run application with each message.

This option is not ideal because it adds an unnecessary layer of complexity with the use of Cloud Dataflow. In this scenario, Cloud Run can be directly subscribed to the Pub/Sub topic, and there is no need for an additional service like Dataflow.

C. 1. Grant the Pub/Sub Subscriber role to the service account used by Cloud Run. 2. Create a Cloud Pub/Sub subscription for that topic. 3. Make your application pull messages from that subscription.

This approach is not recommended as it involves manual pulling of messages, which may lead to inefficient processing and increased latency. Instead, using

the 'push' mechanism, as described in option A, allows for greater scalability and better resource usage.

D. 2. Use Cloud Scheduler to periodically trigger your Cloud Run application, which then reads and processes messages from the Pub/Sub topic.

This option is not recommended because it introduces an unnecessary dependency on Cloud Scheduler. The Cloud Pub/Sub push mechanism automatically and efficiently processes messages as they are published to the topic. Moreover, the numbering should start with 1, not 2.

In conclusion, option A is the best solution as it provides a direct, efficient, and secure integration between Cloud Run and Cloud Pub/Sub, following the recommended Google practices.

Solution to Question 49: A

The correct answer to this question is A. Automatic Scaling with min_idle_instances set to 3.

Explanation for choosing Answer A: Automatic Scaling is the most appropriate scaling type to meet the requirements because it automatically adjusts the number of instances based on the incoming request rate. By setting the min_idle_instances to 3, the App Engine ensures that there are always three unoccupied instances available. This setup helps accommodate the high request rate by scaling the instances seamlessly according to the demand and meets the specified requirements.

Reasons why other options will not work:

Option B: Manual Scaling with 5 instances With Manual Scaling, the number of instances is fixed and will not change according to traffic demand. By choosing this option, the growing e-commerce company could potentially face challenges when the request rate increases. The five instances may not be enough to handle the higher request rates or maintain three unoccupied instances at all times.

Option C: Basic Scaling with target_latency set to 3 seconds Basic Scaling is more suitable for applications that have occasional or low traffic. In this case, the request rate is high due to the rapid growth of the e-commerce company. Also, setting target_latency does not guarantee that there will be 3 unoccupied instances, as it only manages the latency of the user's request, rather than the number of instances needed.

Option D: Automatic Scaling with cool_down_period_sec set to 3 Although Automatic Scaling is the right choice for the given requirements, the cool_down_period_sec parameter does not ensure that there will always be 3 unoccupied instances. This parameter only configures the frequency at which additional instances can be scaled, but this does not ensure that the three idle instances will be maintained all the time.

Solution to Question 50: D

The correct answer is D. Deploy Jenkins through the Google Cloud Marketplace.

The reason for this is that Google Cloud Marketplace provides a variety of pre-built and pre-configured solutions, including Jenkins. By deploying Jenkins through the Marketplace, you can ensure a smooth installation and have it up and running with just a few clicks. This process is well suited for a rapidly growing tech company because it streamlines the setup, allowing you to focus on the development of the application rather than configuring Jenkins.

Now, let's discuss why the other options will not work as efficiently:

A. Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image. While this option would allow you to automate Jenkins installation on Kubernetes, it would require additional work in managing and maintaining the Kubernetes cluster. This approach is more complex, time-consuming, and might be overkill for the task of installing Jenkins when compared to using the Google Cloud Marketplace.

B. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application. Uploading the Jenkins executable to a Cloud Storage bucket does not automate the installation process. It would still require the manual installation of Jenkins on your infrastructure and would not streamline the deployment process. Moreover, Cloud Storage is mainly for storage purposes and using it for deployment would not be the most efficient way to implement Jenkins.

C. Use Cloud Build to create an instance of Jenkins and deploy the application. Although Cloud Build is designed to streamline the build and deployment process, it is not intended for deploying instances of Jenkins. Using Cloud Build for this purpose would be an improper use of the tool. Cloud Build is more suitable for building and deploying containerized applications rather than installing third-party software like Jenkins.

In conclusion, option D—deploying Jenkins through the Google Cloud Marketplace—provides a quick and efficient way to automate the installation of Jenkins for a software engineer at a rapidly growing tech company.

Practice Exam 14

Question 1: As an IT manager in a finance company, how can you grant external auditor access to only view but not modify resources in a project where Domain Restricted Sharing is enabled?

A. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

B. Ask the auditor for their Google account and give them the Security Admin role on the project.

C. Give the auditor Compute Viewer role on the project.

D. Create a temporary account for the auditor in Cloud Identity, and give that account the Security Reviewer role on the project.

Question 2: As a network engineer in a growing tech company, you've noticed that the primary internal IP addresses in a custom mode VPC subnet are running out. The current subnet, with an IP range of 10.0.0.0/20, is primarily occupied by virtual machines within the company. In order to provide more IP addresses for these virtual machines, what action should you take?

A. Allocate external IP addresses for the virtual machines.

B. Implement Cloud VPN for additional address space.

C. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

D. Add a secondary IP range 10.2.0.0/20 to the subnet.

Question 3: As a Cloud Storage Manager at a leading tech company, you have been asked to create a policy that moves videos stored in a specific Regional Cloud Storage bucket to Coldline after 90 days, and then deletes them one year from their creation date. How should you set up this policy?

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

B. Use Cloud Pub/Sub and Cloud Functions to trigger the SetStorageClass and Delete actions after 90 and 275 days respectively.

C. Use Cloud Scheduler to execute a script that moves objects to Coldline after 90 days and deletes them after 275 days.

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

Question 4: As an IT administrator working in a large tech company collaborating with various teams, you must host an application on a Compute Engine instance in a shared project and need to ensure that other teams don't unintentionally cause downtime for the application. Which feature should you utilize?

A. Enable autoscaling for the instance

B. Enable deletion protection on the instance.

C. Use a Shielded VM.

D. Implement instance tags and labels

Question 5: You are working as a cloud engineer at a tech company, and your manager has assigned you the task of setting up the billing configuration for a new Google Cloud client. The client wants to group resources that share common IAM policies. What is the best approach to achieve this?

A. Create dedicated load balancers for resources sharing common IAM policies.

B. Set up separate billing exports for resources with common IAM policies.

C. Use folders to group resources that share common IAM policies.

D. Set up separate Cloud SQL instances for resources with common IAM policies.

Question 6: As a software engineer at a fast-paced technology company, you have developed a containerized web application to assist your internal colleagues during business hours. To avoid incurring any costs outside of the hours the application is in use, you need to deploy the application in your newly created Google Cloud project. What is the most suitable approach for deployment?

A. Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero.

B. Create a cloud monitoring alert to notify you when the application is used outside of business hours, and manually stop it.

C. Deploy the container on Google Kubernetes Engine (GKE), and set the minimum number of instances to zero.

D. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

Question 7: You are an IT specialist working in a tech company that relies on Compute Engine instances running in multiple zones for a critical project. Your manager asks you to configure autohealing for network load balancing whilst minimizing the number of steps involved. Additionally, you must ensure that VMs are re-created if they remain unresponsive after three attempts, each with a duration of 10 seconds. What is the most appropriate course of action?

A. Create an HTTP load balancer with a backend configuration that references an existing instance group. Define a balancing mode and set the maximum RPS to 10.

B. Create an HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP)

C. Create a managed instance group. Set the Autohealing health check to healthy (HTTP)

D. Create a managed instance group with an Instance Template without health checks

Question 8: As a financial analyst in a tech company, you need to analyze the Google Cloud Platform service costs from three different departments within the organization. You are tasked with creating service cost estimates, categorized by service type, for daily and monthly expenses over the next six months using standard query syntax. How should you proceed?

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

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

C. Use Stackdriver Monitoring to analyze service costs from three separate projects.

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

Question 9: You work as a Cloud Engineer for a company that heavily relies on Google Cloud Platform and you have access to both production and development projects. The management requires you to create an automated process that provides a daily list of all compute instances in development and production projects. What method should you implement?

A. Create two separate folders in Google Cloud Storage for production and development projects, then write a script to export the list of compute instances daily using Google Cloud Storage Transfer Service.

B. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

C. Create a Firestore database for each project and store all compute instances information in it, then use Firestore Export to backup the data daily.

D. Create two Service Accounts for each project and use them in a script to access the Google Compute Engine API for listing all compute instances.

Question 10: As a database administrator at a financial services firm, you are tasked with ensuring the long-term storage of a Cloud SQL MySQL database's month-end copies for audit purposes over a period of three years. What strategy should you implement to achieve this goal?

A. Convert the automatic first-of-the-month backup to an export file. Write the export file to a Coldline class Cloud Storage bucket.

B. Save the automatic first-of-the-month backup for three years. Store the backup file in an Archive class Cloud Storage bucket.

C. Configure an on-demand backup for the first of the month. Store the backup file directly within the Cloud SQL MySQL database. Create a snapshot of the first-of-the-month database, and store it in an Archive class Cloud Storage bucket. Set up a scheduled Cloud Scheduler job that will trigger a Cloud Function to extract the month-end database data and store it in a Firestore. Set up a Data Transfer Service to copy the database to Bigtable and retain the month-end copy in an Archive class Cloud Storage bucket. Create a BigQuery scheduled query to transfer a copy of the database into a new dataset on the first of the month and store it in an Archive class Cloud Storage bucket. Configure a serverless export solution using Cloud Run to export the database first-of-the-month to Cloud Spanner, and store in an Archive class Cloud Storage bucket. Configure automated daily export of the entire database, and only store the first of the month copies in a Coldline class Cloud Storage bucket. Create a continuous Dataflow synchronization for the month-end database copy, and store the replicated data into an Archive class Cloud Storage bucket.

D. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

Question 11: As a Project Manager at a tech company working with multiple development teams across the United States, you are in charge of ensuring that each team can only create cloud resources within the US using their individual Google Cloud projects. How should you go about implementing this restriction?

A. Create an Identity and Access Management (IAM) policy to restrict the resources locations in the US. Apply the policy to all dev projects.

B. Create a folder to contain all the dev projects and use an IAM policy to restrict the resources to US regions.

C. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations. Most Voted

D. Create a VPC network in US regions and restrict all dev projects to use only that network.

Question 12: As a financial analyst working at a tech company, you are responsible for monitoring the expenses on various services, including Compute Engine services on three Google Cloud Platform projects under the company's account. In order to set a budget alert for one of these projects, what is the appropriate course of action to take?

A. Verify that you are the project administrator. Select the associated billing account and set a quota for the appropriate project.

B. Verify that you are project administrator. Select the associated billing account and create a budget and a custom alert.

C. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

D. Verify that you have owner role at the organization level. Select the associated billing account and create a budget and alert for the appropriate project.

Question 13: As a DevOps engineer in a software company, you recently deployed a new application within your Google Kubernetes Engine cluster following the YAML file specified. After checking the status of the deployed pods, you notice one remains in PENDING status. To determine the cause of the pending status, what should you do?

A. Review details of the myapp-deployment Deployment object and check for warning messages.

B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

C. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for error messages.

D. View logs of the myapp-deployment Deployment object and check for warning messages.

Question 14: You have been assigned to manage the IT infrastructure of a renowned e-commerce company, and one of your primary tasks is to reduce GCP service costs for a specific division. Your goal is to turn off all configured services in an existing GCP project in the fewest possible steps. What should you do?

A. 1. Verify that you are assigned the Compute Network Admin IAM role for this project. 2. Locate the project in the GCP console, click on compute and disable any connected services.

B. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Switch to the project in the GCP console, locate the resources and delete them.

C. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID.

D. 1. Verify that you are assigned the Cloud Engineering IAM role for this project. 2. Switch to the project in the GCP console, locate the resources, and disable their APIs.

Question 15: As an IT professional in a software development company, you notice that the continuous integration and delivery (CI/CD) server is unable to execute Google Cloud actions in a specific project due to permission issues. To validate if the service account used has the necessary roles in the project, what should you do?

A. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

B. Visit the CI/CD server logs and look for any configuration errors.

C. Check the firewall settings in the VPC network configuration to ensure proper access.

D. Verify if the billing account associated with the project is in good standing.

Question 16: You have recently joined a software development company that specializes in cloud-based applications, and have been tasked with hosting a new application on Google Kubernetes Engine with autoscaling enabled. The company wants this application to be publicly available using HTTPS on a public IP address. What step should you take to achieve this goal?

A. Deploy your application on Google Cloud Functions and use API Gateway to expose the HTTPS endpoint.

B. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

C. Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluster. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing.

D. Configure a Google Compute Engine instance with Nginx as a reverse proxy, and expose the application on HTTPS. Connect this instance to your GKE cluster.

Question 17: You are working as a cloud engineer in a software company that develops an application spanning multiple projects. Your task is to configure service accounts for virtual machines (VMs) running in the web-applications project to access BigQuery datasets in the crm-databases project, following Google-recommended practices. How should you grant access to the service account in the web-applications project?

A. Grant "project owner" role to crm-databases and the web-applications project.

B. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

C. Grant roles/iam.serviceAccountAdmin role to crm-databases and roles/bigquery.admin role to web-applications.

D. Grant roles/bigquery.user role to crm-databases and "project owner" role to web-applications.

Question 18: As a cloud architect in a growing e-commerce company, you need to prepare for an anticipated upsurge in user traffic following the acquisition of

another online retailer. You are tasked with replicating a custom Compute Engine virtual machine (VM) to handle the increased workload. What steps should you take?

A. Create a custom Compute Engine image from a snapshot. Create your instances from that image.

B. Create a custom Compute Engine image from a snapshot. Create your instances from a Cloud Storage bucket.

C. Create a custom Compute Engine image from your base VM. Create your instances from that image.

D. Use Cloud Dataflow to create a copy of your base VM. Create your instances from that copy.

Question 19: As a cybersecurity expert in the financial industry, your company's security vulnerability management policy demands that a member of the security team has clear visibility into vulnerabilities and other OS metadata for a crucial Compute Engine instance running an essential application in your Google Cloud project. How can you effectively implement this policy in line with company guidelines?

A. Install the Cloud Logging agent on the Compute Engine instance.

B. Enable the VPC Service Controls for the Google Cloud project.

C. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.vulnerabilityReportViewer permission.

D. Provide the security team member with roles/compute.instanceAdmin permission.

Question 20: As an IT professional in a software development company, you have been tasked with managing a third-party application that will operate on a Compute Engine instance. Other instances are already running using the default configuration. The application's installation files are stored on Cloud Storage, and it's crucial to ensure that only the new instance can access these files without providing access to other virtual machines (VMs). What course of action should you take?

A. Create the instance with the default Compute Engine service account. Create a Cloud Function that copies files from Cloud Storage to Compute Engine.

B. Create the instance with the default Compute Engine service account. Add metadata to the objects on Cloud Storage that matches the metadata on the new instance.

C. Create an instance with a custom IAM role and grant it permissions on Cloud Storage. Assign that IAM role to the new instance and restrict access to other VMs.

D. Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

Question 21: As a software engineer at a major tech company, you are responsible for managing and maintaining a Google Kubernetes Engine (GKE) cluster named 'dev' for your company's development projects on Google Cloud. You need to ensure that all CLI commands by default target this specific GKE cluster after you have successfully downloaded and installed the Cloud SDK. What should be your next step?

A. Use the command gcloud compute instances update dev.

B. Use the command gcloud config set container/cluster dev.

C. Use the command gcloud config set project/cluster dev.

D. Create a file called config.json in the ~/.gcloud folder that contains the cluster name.

Question 22: As a part of a leading software development company working with numerous clients, you maintain an application backed by Cloud Spanner as the primary database. The application experiences a consistent and predictable traffic pattern. To optimize resource usage, you need to automatically scale the number of Spanner nodes based on the traffic demands. How can you achieve this?

A. Create an instance group in Cloud Spanner to handle autoscaling based on traffic patterns.

B. Create a Cloud Run service that listens to Cloud Monitoring alerts and resizes the Spanner nodes accordingly.

C. Create a Cloud Monitoring alerting policy to send an alert to Google Cloud Support email when Cloud Spanner CPU exceeds your threshold. Google support would scale resources up or down accordingly.

D. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

Question 23: You are an IT administrator at a company that heavily utilizes data analysis and processing. Your current Google Cloud Dataproc cluster is set up within a single Virtual Private Cloud (VPC) network in a single subnet with the range 172.16.20.128/25. Unfortunately, there are no private IP addresses available in the VPC network. Your task is to integrate new VMs into the infrastructure to communicate with your cluster using the minimum number of steps. What is the most efficient approach to achieve this?

A. Create a new GCP project with an additional VPC network and set up Shared VPC for the Dataproc cluster.

B. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

C. Create a new VM with multiple NICs and add a secondary subnet for communication with Dataproc Cluster.

D. Create a new VPC network for VMs, set up VPC peering, and configure DNS peering between the Dataproc cluster and VMs VPC networks.

Question 24: As a software engineer working for a company that focuses on developing apps, your team has developed Docker images for an application which will be hosted on Google Cloud. The team prefers not to handle the infrastructure management for this application, and it's crucial for the application to scale automatically as its user base starts to grow. What would be the best approach to achieve this?

A. Deploy the application on App Engine standard environment with a custom runtime.

B. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

C. Upload Docker images to Artifact Registry, and deploy the application on Google Kubernetes Engine using Standard mode.

D. Create an instance template with the container image, and deploy a Managed Instance Group with Autoscaling.

Question 25: As a data analyst at a tech company, you are tasked with sending all logs from your Compute Engine instances to a BigQuery dataset called platform-logs for analysis purposes. The Cloud Logging agent has already been installed on all instances, and your goal is to minimize cost. What steps should you take to accomplish this?

A. 1. In Cloud Logging, create a logs export with a Cloud Pub/Sub topic called logs as a sink. 2. Create a Cloud Function that is triggered by messages in the logs topic. 3. Configure that Cloud Function to drop logs that are not from Compute Engine and to insert Compute Engine logs in the platform-logs dataset.

B. 7. Modify your instances' startup scripts to send the logs directly to the BigQuery dataset (platform-logs) using the bq command-line tool. 8. Grant BigQuery Data Editor role on the dataset to the service accounts used by your instances.

C. 1. In Cloud Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the platform-logs dataset as Sink Destination.

D. 8. Use Logstash to generate a pipeline that pulls logs from Compute Engine instances and sends them to the platform-logs dataset in BigQuery. 9. Grant BigQuery Data Editor role to the service account used by Logstash.

Question 26: As a project manager for a software development company, you are in charge of granting permissions to the DevOps team. They require full control over Compute Engine resources in the development project, but you don't want them to have permission to create or update any other resources. To enforce this while following Google's recommendations for setting permissions, what should you do?

A. Create a custom role at the folder level and grant all compute.instanceAdmin.* permissions to the role. Grant the custom role to the DevOps group.

B. Grant the basic role roles/compute.admin and the predefined role roles/bigquery.admin to the DevOps group.

C. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

D. Grant the basic role roles/owner and the predefined role roles/compute.admin to the DevOps group.

Question 27: As an IT specialist working for a marketing agency, you manage the company's application that stores files on Cloud Storage using the Standard Storage class. The application only requires access to files created within the last 30 days. To reduce storage costs for files that are no longer accessed, which solution should you implement?

A. Create a retention policy on the storage bucket of 30 days, and lock the bucket by using a retention policy lock.

B. Create a BigQuery table to identify files older than 30 days and delete them using a scheduled query.

C. Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

D. Set a custom metadata key on the objects in the storage bucket to mark them for deletion after 30 days.

Question 28: You work for a software company that utilizes Cloud Run to handle their web application services for clients with hundreds of users. Some clients have reported that the main webpage takes a significant amount of time to load compared to subsequent pages. To resolve this issue while adhering to Google's recommendations, which action should you take?

A. Set the minimum number of instances for your Cloud Run service to 3.

B. Change the Cloud Run memory allocation to a larger value.

C. Decrease the request timeout for your Cloud Run service.

D. Enable autoscaling on the Cloud Run service.

Question 29: As a network administrator in a software company that recently set up an LDAP server on Compute Engine, you need to ensure clients can

access it through TLS on port 636 using UDP. What is the appropriate action to take for establishing the desired connectivity?

A. Create a VPC peering connection to allow access to the LDAP server on port 636 using UDP. Enable the 'Allow Secure LDAP access over the Internet' option in the Compute Engine settings. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow ingress on TCP port 636 for that network tag. Create a Cloud VPN tunnel and configure the LDAP server to be reachable only through the VPN. Create a firewall rule to allow ingress on UDP port 636 without specifying any specific network tags. Set the VM instance to use a shared VPC and enable ingress on UDP port 636 in the Shared VPC settings. Deploy an Identity-Aware Proxy for the LDAP server and allow access on UDP port 636 only for authorized users. Create a Cloud NAT gateway and configure it to allow access to the LDAP server on port 636 using UDP.

B. Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

C. Add the network tag allow-udp-636 to the VM instance running the LDAP server.

D. Create a route called allow-udp-636 and set the next hop to be the VM instance running the LDAP server.

Question 30: As a security analyst at a large financial institution, you are responsible for monitoring and securing the company's infrastructure, which includes a Bigtable instance consisting of three nodes that store personally identifiable information (PII) data. You are required to log all read or write operations, as well as any metadata or configuration reads of this database table, in the organization's Security Information and Event Management (SIEM) system. What should you do to accomplish this task?

A. • Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.

B. Enable VPC Flow Logs for the network containing the Bigtable instance and stream logs to your SIEM system.

C. Use Stackdriver to create a custom dashboard to monitor the Bigtable instance and send alerts to your SIEM system.

D. Create a custom log-based metric in Cloud Monitoring to track Bigtable operations and export it to your SIEM system.

Question 31: You are working as a network administrator for a company that uses a 3-tier solution running on Compute Engine. The current infrastructure configuration consists of each tier having a service account associated with all

its instances. To ensure smooth operations, your task is to enable communication on TCP port 8080 between tiers as follows: * Instances in tier #1 must communicate with tier #2. * Instances in tier #2 must communicate with tier #3.

What steps should you take to achieve this?

A. 1. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow TCP: 8080 2. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow TCP: 8080

B. 1. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow all 2. Create an ingress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow all

C. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow all 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow all

D. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP: 8080

Question 32: As a cloud infrastructure engineer at a leading software company, you are responsible for maintaining and updating the organization's cloud infrastructure. You've recently designed an update to the infrastructure and want to share your proposed changes with the rest of your team, following Google's recommended best practices. How should you proceed?

A. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

B. Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket.

C. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.

D. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

Question 33: You are working as a software engineer at a technology company focused on developing innovative applications with multiple microservices. The company plans to deploy a new application to Google Kubernetes Engine (GKE) and ensure its scalability for future applications without requiring manual intervention with each deployment. What approach should you take?

A. Create a GKE cluster and manually increase or decrease the number of nodes based on load prediction.

B. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

C. Deploy the application on multiple VM instances in Compute Engine with an instance group and configure autoscaling.

D. Create a custom GKE cluster without autoscaling and manually add nodes when needed.

Question 34: As a database administrator in a tech company, you are trying to help a client who has implemented a solution using Cloud Spanner and is experiencing read latency-related performance problems on a specific table. This table is accessed only by the client's users through a primary key. The table schema is provided to you. In order to address the issue, what should be your recommended course of action?

A. Change the primary key to not have monotonically increasing values.

B. Implement pagination to limit the number of rows returned in each read query.

C. Enable interleaved tables to improve read performance.

D. Change the primary key to a composite key consisting of person_id and created_at.

Question 35: As a project manager in a software development company, you need to grant your finance team access to view the billing report for ongoing projects without giving them any additional permissions. What should you do?

A. Add the group for the finance team to roles/storage admin role.

B. Add the group for the finance team to roles/container admin role.

C. Add the group for the finance team to roles/billing viewer role.

D. Add the group for the finance team to roles/appengine admin role.

Question 36: You are working as a cloud architect at a tech company and responsible for hosting an application from Compute Engine virtual machines (VMs) in us-central1-a. To improve the infrastructure resilience against a single Compute Engine zone failure, eliminate downtime, and minimize cost, what is the best approach to adjust your design?

A. Create a Cloud Datastore instance in us-central1-b and set up replication between the two instances.

B. Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

C. Create a Managed Instance Group and specify us-central1-a as the zone. Configure the Health Check with a short Health Interval.

D. Configure VMs in us-central1-a to run as serverless instances using Google App Engine standard environment, and distribute traffic between the two zones using App Engine Traffic Splitting.

Question 37: As a software engineer at a leading tech company, you have developed an application that will be deployed on Google Kubernetes Engine. Portions of the application can tolerate downtime, but some critical components must always be available. Your goal is to configure a cost-efficient Google Kubernetes Engine cluster while maintaining the necessary availability. How should you proceed?

A. Create a cluster with a single node-pool by using standard VMs. Label the fault-tolerant Deployments as spot_true.

B. Create a cluster with a single node-pool by using Balanced Persistent Disks. Label the critical Deployments as disk_balanced_false.

C. Create a cluster with both a Preemptible VM node pool and a Shielded VM node pool. Deploy the critical deployments on the Preemptible VM node pool and the fault-tolerant deployments on the Shielded VM node pool.

D. Create a cluster with both a Spot VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Spot VM node pool.

Question 38: As a rapidly growing tech company, you are currently using Google Workspace to manage 100 employee accounts. Within the next 2 years, the number of employees is expected to increase tenfold, reaching 1,000. Your company will require most employees to have access to the Google Cloud account, and you must ensure that the systems and processes can accommodate this growth without causing performance issues, unnecessary complexity, or security breaches. What is the best course of action to take in this situation?

A. Turn on identity federation between Cloud Identity and Google Workspace. Enforce multi-factor authentication for domain wide delegation.

B. Connect Google Workspace directly to an on-prem LDAP server for authentication and user management.

C. Use a third-party identity provider service through federation. Synchronize the users from Google Workplace to the third-party provider in real time.

D. Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

Question 39: You are working as a software engineer in a company that specializes in container orchestration solutions. You are tasked with managing a Google Kubernetes Engine cluster which has a single preemptible node pool. You have created a Deployment with 2 replicas and after a few minutes, you check the Pod status using kubectl. You notice that one of the Pods is still in Pending status. What is the most likely cause for this situation?

A. A firewall rule is blocking communication between the control plane and the node, preventing the Pod from being scheduled.

B. Google Kubernetes Engine is experiencing an internal error that prevents the Pod from being scheduled.

C. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

D. The GKE autoscaler is not set up correctly, causing the cluster to not scale out.

Question 40: You are working as a data manager in a financial company and are responsible for developing an archival system for the data warehouse using Cloud Storage. Your colleagues need to access the archived data once every quarter to fulfill regulatory obligations. Which cost-effective storage option should you choose for this purpose?

A. Cold Storage

B. One Zone-Infrequent Access Storage

C. Partner Interconnect

D. Firestore

Question 41: As a system administrator for a company using Google Cloud Platform, you are responsible for monitoring a Compute Engine instance that hosts a critical production application. The management team requires you to set up email notifications if the instance consumes over 90% of its CPU resources for more than 15 minutes. How would you achieve this using Google services?

A. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Write a script that monitors the CPU usage and sends it as a custom metric to Cloud Monitoring. 3. Create an uptime check for the instance in Cloud Monitoring.

B. 1. Create a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it. 2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

C. 1. In Cloud Logging, create a logs-based metric to extract the CPU usage by using this regular expression: CPU Usage: ([0-9] {1,3})% 2. In Cloud Monitoring, create an Alerting Policy based on this metric. 3. Configure your email address in the notification channel.

D. 1. Create a consumer Gmail account. 2. Write a script that monitors the CPU usage. 3. When the CPU usage exceeds the threshold, have that script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.

Question 42: As a software developer at a tech company, you recently developed an application on your personal laptop that utilizes Google Cloud services. The app uses Application Default Credentials for authentication and runs smoothly on your laptop. Your task is to migrate this application to a Compute Engine virtual machine (VM) within the company's infrastructure and ensure authentication adheres to Google's recommended practices with minimal modifications. What should be your next step?

A. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

B. Create an OAuth2.0 client ID for the application running on the Compute Engine VM and store the client secret in a secure file.

C. Use your personal account credentials to authenticate the applications running on the Compute Engine VM.

D. Create a new Google account with appropriate access for Google services and use its credentials in a Compute Engine VM.

Question 43: As a cloud engineer at a growing technology company, you encountered an issue where your managed instance group sent an alert notifying you that new instance creation failed. To efficiently handle the expected application traffic, you must maintain the number of running instances according to the template. How should you resolve this issue?

A. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

B. Enable Shielded VMs on the instances and create an instance template that contains valid syntax which will be used by the instance group.

C. Set the minimum CPU platform for the instances, then create an instance template that contains valid syntax which will be used by the instance group.

D. Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

Question 44: You are working in a tech company and just deployed an application on a single Compute Engine instance within the company's infrastructure.

The application is responsible for writing logs to disk. However, users have recently started reporting errors with the application. In order to diagnose the issue, what should you do?

A. Create a new Google Kubernetes Engine cluster and migrate the application there.

B. Install and configure the Ops agent and view the logs from Cloud Logging.

C. Use Cloud Pub/Sub to push error logs from the application to a subscriber.

D. Use Stackdriver Monitoring to view the application logs.

Question 45: You have recently joined a software development company as a Project Manager, and your first task is to create a new billing account and then link it with an existing Google Cloud Platform project. What should be your course of action?

A. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

B. Verify that you are Billing Administrator for the billing account. Update the existing project to link it to the existing billing account.

C. Verify that you are Billing Account Viewer for the GCP project. Create a new billing account and link the new billing account to the existing project.

D. Verify that you are Project Billing Manager for the GCP project. Create a new GCP project and link the new project to the existing billing account.

Question 46: You are a lead engineer at a software development company, and you have been tasked with migrating the company's on-premises data management solutions to Google Cloud. Currently, the company uses a MySQL cluster for its main database, Apache Kafka for event streaming, and Cloud SQL for PostgreSQL for analytical and reporting needs. Your goal is to implement the Google-recommended solutions for the migration while ensuring global scalability and minimal operational and infrastructure management. What steps should you take?

A. Migrate from MySQL to Cloud Spanner, from Kafka to Cloud Data Fusion, and from Cloud SQL for PostgreSQL to Cloud SQL.

B. Migrate from MySQL to Cloud Spanner, from Kafka to Memorystore, and from Cloud SQL for PostgreSQL to Cloud SQL.

C. Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery.

D. Migrate from MySQL to Firestore, from Kafka to Cloud Tasks, and from Cloud SQL for PostgreSQL to BigQuery.

Question 47: As a software engineer working at a company in the e-commerce industry, you have created an application with multiple microservices, each in

its own Docker container image. To ensure scalability for each microservice, you are tasked with deploying the application on Google Kubernetes Engine. What is the best approach to achieve this?

A. Create and deploy a Deployment per microservice.

B. Create and deploy an Instance Group per microservice.

C. Create and deploy a Bundle per microservice.

D. Create and deploy a Dataproc Cluster per microservice.

Question 48: As an engineer at a software development company, you are building a product utilizing Google Kubernetes Engine (GKE) for your clients. Each client's Pod runs within a single GKE cluster and is capable of executing arbitrary code. To maximize the isolation between clients' Pods, what strategy should you implement?

A. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

B. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

C. Use Cloud Run for Anthos to deploy and manage your customers' Pods.

D. Use Cloud Armor to configure security policies for each customer's Pod.

Question 49: You are working as a data management specialist at a company that relies heavily on data storage. Your task is to set up Object Lifecycle Management for items stored in storage buckets. These items are written once and frequently accessed for 30 days. After the initial 30-day period, the items are not read again unless there's a special requirement. The company needs to keep these objects for three years while minimizing costs. What is the best approach to set up the Object Lifecycle Management policy?

A. Set up a policy that uses Nearline storage for 30 days, then moves the Coldline for one year, and then moves to Archive storage for two years.

B. Set up a policy that uses Nearline storage for 30 days, then moves to Coldline for two years, and then moves to Archive storage for one year.

C. Set up a policy that uses Standard storage for 30 days, then moves to Nearline storage for one year, and then moves to Archive storage for two years.

D. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

Question 50: You are working as a developer at a software company and recently deployed a new version of an application to App Engine. After deployment, you realized there is a bug in this release and need to revert to the

previous version of the application urgently. What action should you take to accomplish this?

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

B. Create a new App Engine instance and deploy the prior version, then route traffic to the new instance. Utilize storage service backups to restore the prior version to the App Engine. Revert the faulty code changes through Git, then deploy the resulting version to App Engine. On the GCP Console, choose GCP Datastore and rollback to an earlier snapshot to restore the application before the bug was released.

C. Run gcloud app restore.

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

Practice Exam 14 Solutions

Solution to Question 1: A

The correct answer is A: Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

Explanation: As an IT manager in a finance company, you'd want to provide external auditors with the ability to only view the resources in the project, without modifying them. Option A achieves this because it involves creating a temporary account for the auditor within your organization's Cloud Identity, ensuring that the Domain Restricted Sharing rule is respected. The Viewer role is a predefined role in Google Cloud, providing read-only access to project resources. This allows the external auditor to assess the project without causing any unwanted changes.

Why other options will not work: B. Asking the auditor for their Google account and giving them the Security Admin role on the project is not advisable because it will grant them more permissions than needed. Furthermore, this method would go against the Domain Restricted Sharing rule since the auditor won't be part of the organization's domain.

C. Giving the auditor Compute Viewer role on the project would only provide them read-only access to Compute Engine resources, not the entire project resources, which may not be sufficient for a comprehensive audit.

D. Creating a temporary account for the auditor in Cloud Identity and giving that account the Security Reviewer role on the project is incorrect because there is no such predefined role as "Security Reviewer" in Google Cloud.

Solution to Question 2: C

The answer should be C, changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

The reason for choosing this option is because when you change the subnet IP range to 10.0.0.0/18, the available IP addresses will increase from 4,096 (in a /20 subnet) to 16,384 (in a /18 subnet). This significant increase in IP addresses will accommodate the growing number of virtual machines within the company's network.

Let's analyze why the other options will not work:

Option A (Allocate external IP addresses for the virtual machines) is not suitable because external IP addresses are primarily used for external communication and do not solve the problem of running out of internal IP addresses. Additionally, relying on external IP addresses may increase security risks and costs.

Option B (Implement Cloud VPN for additional address space) is not applicable in this scenario, as Cloud VPN is used to connect on-premises networks to GCP

VPC networks through an IPsec VPN connection. This does not directly provide additional IP addresses for the network in the company's custom mode VPC subnet.

Option D (Add a secondary IP range 10.2.0.0/20 to the subnet) could work temporarily, but it might lead to the same issue in the future as the company grows. Moreover, managing multiple IP ranges can introduce complexity, as some Google Cloud Platform services do not support secondary IP ranges.

In conclusion, Option C is the most appropriate solution for providing more IP addresses to the virtual machines in the company's custom mode VPC subnet. Changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 increases the available IP addresses and meets the company's growing demand without significantly increasing complexity or cost.

Solution to Question 3: D

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

The reason why option D should be used is because Cloud Storage Object Lifecycle Management allows you to create policies based on specific conditions (in this case, the Age conditions). These policies can automatically perform actions such as changing the storage class or deleting objects after a certain number of days. This is both easy to implement and cost-effective, meeting the requirement to move objects to Coldline storage after 90 days and then to delete them after 365 days from their creation date.

Option A is incorrect because using gsutil rewrite might cause data inconsistency as it affects only the specified objects. Furthermore, setting the Delete action to 275 days (365-90) would result in deletion of the object 275 days after its creation rather than one year later, as required.

Option B is incorrect because using Cloud Pub/Sub and Cloud Functions would require additional processing and event management, which could be more complex and resource-intensive compared to using Cloud Storage Object Lifecycle Management built-in policies.

Option C is incorrect because relying on Cloud Scheduler to execute a script is not an efficient way to manage the lifecycle of storage objects, as it would require running the script at specified intervals rather than allowing the policy to handle transitions automatically based on the lifecycle management rules. Moreover, using a scheduled script might be less reliable and more prone to errors compared to the built-in policies.

Solution to Question 4: B

The correct answer is B. Enable deletion protection on the instance.

Explanation:

Enabling deletion protection on the Compute Engine instance ensures that other teams working within the shared project cannot accidentally delete the instance. Once this feature is enabled for the instance, it prevents unauthorized or unintentional deletion. To delete the instance, deletion protection must be manually removed by an authorized person.

Why other options will not work:

A. Enable autoscaling for the instance: Autoscaling helps in managing the number of instances according to the load and demand on the application. This feature is useful for handling changes in resource requirements and does not protect the instance from accidental deletion by other teams.

C. Use a Shielded VM: Shielded VMs provide security against threats like boot malware attacks and unauthorized access to VM data. This feature focuses on securing the VM and its data against potential threats, but it does not prevent the instance from accidental deletion by other teams.

D. Implement instance tags and labels: Instance tags and labels are used for organizing and managing Compute Engine instances. While tags are used for grouping instances for applying firewall rules or network routing, labels are used for annotating instances and identifying their purpose. Neither of these features is aimed at protecting the instance from accidental deletion by other teams.

Solution to Question 5: C

The correct answer is C. Use folders to group resources that share common IAM policies.

Explanation:

Option C is the best approach because folders in Google Cloud allow you to organize and manage resources that share common IAM policies. Folders help you group and hierarchically organize resources according to the principles of your organization.

Option A is not suitable because creating dedicated load balancers is not relevant to grouping resources based on their IAM policies. Load balancers are used for distributing network traffic among multiple resources and are not designed for this purpose.

Option B is not appropriate as it involves setting up separate billing exports for resources with common IAM policies. Billing exports are used for tracking costs and do not directly impact the organization or management of resources based on IAM policies.

Option D is not applicable because setting up separate Cloud SQL instances for resources sharing common IAM policies is not the right approach. Cloud SQL instances are focused on managing databases and are not suited for organizing and managing resources based on IAM policies.

Solution to Question 6: D

The correct answer is D. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

Explanation:

Option A - Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero: Cloud Run for Anthos provides some advantages like cluster-level customizations, but it incurs additional cost and complex management compared to a fully-managed Cloud Run service. In this scenario, you want to avoid incurring unnecessary costs and complexity when the application is not in use.

Option B - Create a cloud monitoring alert to notify you when the application is used outside of business hours, and manually stop it: This is not an efficient way as it still requires manual intervention from a user to stop the application when it is not in use. Also, it does not guarantee the application will always be stopped outside of working hours as it relies on manual handling.

Option C - Deploy the container on Google Kubernetes Engine (GKE), and set the minimum number of instances to zero: While GKE is a powerful platform for managing containerized applications, it is not the most cost-effective solution in this case. GKE requires you to manage a cluster of virtual machines, and even if the number of instances is set to zero, there are still costs for running the control plane and additional cluster management.

Option D - Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero: This is the most suitable approach in this case. Cloud Run (fully managed) is designed to handle containerized applications at scale and automatically manages resources for you. By setting the minimum number of instances to zero, you ensure that no instances are running when the application is not in use, and you won't incur unnecessary costs outside business hours. Additionally, Cloud Run (fully managed) provides a simpler management experience compared to other options in this list, which is ideal for a fast-paced technology company.

Solution to Question 7: C

The correct answer is C: Create a managed instance group and set the Autohealing health check to healthy (HTTP).

Explanation: To configure autohealing for network load balancing, the infrastructure needs to be set up using a managed instance group (MIG). This allows you to achieve the desired outcome of recreating VMs when they are unresponsive after three attempts, each with a duration of 10 seconds.

A: This option is incorrect because creating an HTTP load balancer with a backend configuration that references an existing instance group and setting the maximum RPS to 10 as the balancing mode does not enable autohealing, which was a requirement given by your manager.

B: This option is incorrect because creating an HTTP load balancer with a backend configuration that references an existing instance group and setting the health check to healthy (HTTP) does not enable autohealing for unresponsive VMs as required.

D: This option is incorrect because creating a managed instance group with an Instance Template without health checks won't enable autohealing as required. Health checks are necessary to determine whether a VM is responsive or not, and in this scenario, the health check should be set to healthy (HTTP).

Solution to Question 8: D

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

Here's why D is the best option, and why the other options aren't suitable in this scenario:

Option A: Export your bill to a Cloud Storage bucket, and then import into Google Sheets for analysis. While Google Sheets is a useful tool for smaller datasets and basic analysis, it lacks the advanced features and efficiency needed for larger datasets like the one in this scenario. It would be difficult to manage and analyze multiple large datasets covering daily and monthly expenses from three different departments. Additionally, Google Sheets is not ideal for standard query syntax, which is required in this task.

Option B: Export your bill to a Cloud Storage bucket, and then import into Cloud Datastore for analysis. Cloud Datastore is a NoSQL database service designed for scalability and web applications, not for analyzing costs and querying data with standard SQL syntax. It does not offer the necessary features for querying and categorization of costs as required by the task.

Option C: Use Stackdriver Monitoring to analyze service costs from three separate projects. Stackdriver Monitoring (now known as Google Cloud Monitoring) is a valuable tool for monitoring and managing the performance and availability of applications and infrastructure. However, it is not designed for analyzing cost data. Analyzing Google Cloud Platform service costs using Stackdriver would be inefficient and tedious compared to using BigQuery for the same purpose.

Option D (Correct): Export your bill to a BigQuery dataset, and then write time window-based SQL queries for analysis. BigQuery is a fully-managed data warehousing and analytics service that scales easily and supports advanced features like time window-based SQL queries. By exporting the bills to a BigQuery dataset, you will be able to leverage the power of standard SQL syntax and the service's advanced querying capabilities to analyze the service costs efficiently. This will allow you to fulfill the task requirements: creating service cost estimates categorized by service type for daily and monthly expenses over the next six months.

Solution to Question 9: B

The correct answer is B. Here's why:

Option B proposes to create two configurations using gcloud config, one for each project (development and production). A script can then be written to switch between these configurations using the `gcloud config set` command. This enables the script to obtain the project-specific context and list the compute instances using `gcloud compute instances list`. This approach is efficient, flexible, and appropriate for daily data extraction for both development and production projects.

Now let's discuss why the other options will not work:

Option A is not suitable because it suggests using Google Cloud Storage Transfer Service to export the list of compute instances. However, Cloud Storage Transfer Service is primarily used for transferring data between Cloud Storage buckets or from an online data source to a Cloud Storage bucket. It cannot directly access the list of compute instances.

Option C suggests storing compute instance information in separate Firestore databases for each project and then using Firestore Export to back up the data daily. While this might work, it is more complex and unnecessary since the required information can be directly obtained from the gcloud tool without needing to set up databases or manual storage of instances' data.

Option D involves creating two Service Accounts for each project and using them in a script to access the Google Compute Engine API for listing all compute instances. This approach may work but it is unnecessary to create separate Service Accounts for each project. Also to authenticate and authorize the required action, gcloud configuration is more straightforward than the manual manipulation of API keys. Option B, which uses gcloud configurations, is a simpler and more efficient solution.

Overall, Option B is the best choice as it effectively utilizes gcloud config to manage project-specific contexts and directly list compute instances without the need for additional databases, service accounts, or storage solutions.

Solution to Question 10: D

The correct answer is D, setting up an export job for the first of the month and writing the export file to an Archive class Cloud Storage bucket. This strategy ensures the long-term storage of the Cloud SQL MySQL database's month-end copies for three years while keeping the costs low.

Option A would not be suitable because it suggests converting the automatic first-of-the-month backup to an export file and storing it in a Coldline class Cloud Storage bucket. Coldline storage is designed for infrequently accessed data and would be more expensive than Archive storage for long-term storage.

Option B is incorrect because it suggests saving the automatic first-of-the-month backup for three years and storing it in an Archive class Cloud Storage bucket.

However, Cloud SQL doesn't support automatic monthly backups, so this option is invalid.

Option C is also incorrect as it suggests configuring an on-demand backup for the first of the month and storing the backup file directly within the Cloud SQL MySQL database. This would consume valuable database storage and is not a cost-effective or efficient solution for long-term storage.

All the other options mentioned involve complex setups and solutions that are unnecessary for the given task. These involve using Firestore, Bigtable, BigQuery, Cloud Spanner, Cloud Run, Dataflow, or daily exports, which would be overkill for the simple task of storing month-end backups efficiently and cost-effectively.

Thus, option D is the best strategy because it simplifies the process of storing month-end database copies by scheduling an export job on the first of each month and storing them in an Archive class Cloud Storage bucket, which is specifically designed for long-term storage, keeping storage costs and complexity minimal.

Solution to Question 11: C

The correct answer is C because creating a folder to hold all the development projects, followed by establishing an organization policy to limit resources exclusive to US locations, will effectively ensure that each team can only create cloud resources within the United States. This method offers a centralized approach for controlling and managing the restrictions on all dev projects.

Option A is incorrect because creating an IAM policy to restrict resource locations in the US, and applying it to all dev projects, will only address access control for users and roles within the projects. This would not be the most efficient way to limit the creation of resources to the specified locations.

Option B is also incorrect since using an IAM policy on a folder would not help restrict resources to US regions. As mentioned earlier, IAM policies control access for users and roles, but they do not place location-based restrictions on available GCP resources.

Lastly, option D is not ideal because creating a VPC network in US regions and restricting all dev projects to use that network only tackles the location limitations for networking components. It does not provide a comprehensive solution for restricting the location of other types of cloud resources like storage, databases, or compute instances.

Solution to Question 12: C

The correct answer is C. Here's why:

As a financial analyst responsible for monitoring expenses, your primary concern is setting budget alerts to ensure appropriate spending on Compute Engine services for the projects under the company's account.

Option A suggests setting a quota which, although can help control expenses, does not provide the required budget alerts. Quotas are different from budgets alerts as they set a limitation on resource usage while budget alerts provide timely notifications when approaching or exceeding the set budget.

Option B says to verify if you are the project administrator, but being a financial analyst, you need to be a billing administrator to manage budgets. Additionally, this option doesn't mention specifying the appropriate project for the budget and alert.

Option C is the correct choice as it covers all the necessary steps: 1. Verify that you are the project billing administrator - This role gives you the necessary permissions to manage and set budgets for the projects. 2. Select the associated billing account - You must choose the correct billing account for the project you want to set a budget alert for. 3. Create a budget and alert for the appropriate project - This step ensures you set a budget limit and receive notifications in case of approaching or crossing the budget threshold.

Option D may seem reasonable, but having owner role at the organization level is not required for this specific task. Being a billing administrator is sufficient for setting budgets and alerts, and ensuring the right permissions are granted.

Solution to Question 13: B

The correct answer should be B. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

The reason for choosing option B is that when a pod remains in PENDING status within a Google Kubernetes Engine cluster, it is typically due to a problem related to the resources or configuration of that specific pod. By reviewing the details of the affected pod (in this case, "myapp-deployment-58ddbbb995-lp86m") and checking for warning messages, you can understand the cause of the pending status and address any issues accordingly.

On the other hand, the other options will not help in resolving this issue:

Option A: Reviewing details of the "myapp-deployment" Deployment object might provide some insights into the general configuration of the application, but it will not give you specific information about the pending pod. Moreover, warning messages on the deployment level are not typically related to pod-level issues.

Option C: Checking for error messages on the pod is similar to option B, but warning messages are usually more helpful for uncovering issues that prevent a pod from starting. Error messages might give you information about problems that occurred after the pod has started running, rather than why it's stuck in the PENDING status.

Option D: Viewing logs of the "myapp-deployment" Deployment object will not be useful in this case, as logs will be available for pods that are running or have run in the past. Moreover, logs of the Deployment object usually don't

provide information about the specific pod-level issues that could be preventing the successful start of a pod.

Solution to Question 14: C

The correct answer is C, and here's the explanation for why and why the other options won't work:

Option C is correct because it requires the fewest steps to disable all configured services in an existing GCP project. First, you verify that you are assigned the Project Owners IAM role, which grants you the necessary permissions to manage the project and its services. Next, you simply locate the project in the GCP console, click Shut down, and then enter the project ID. This step will efficiently turn off all configured services in the project.

Option A is incorrect because the Compute Network Admin IAM role primarily focuses on managing network resources and will not provide you the needed permissions to shut down all configured services in the project. Also, by only disabling connected services under the compute section, you may miss other running services in the project.

Option B is incorrect because, though verifying the Project Owners IAM role grants you the necessary permissions, deleting resources will not effectively shut down the services in the least number of steps. Deleting resources can also lead to data loss and other unintended consequences.

Option D is incorrect because the Cloud Engineering IAM role may not provide you with sufficient permissions to turn off all configured services in the project. Additionally, disabling APIs will not be an efficient method of shutting down all services, as it only removes access to APIs and may not stop the associated instances that are consuming resources.

Solution to Question 15: A

The correct answer is A, as it focuses on directly checking and validating the permissions of the service account in the Google Cloud Console. In this scenario, permission issues are causing the CI/CD server to be unable to execute Google Cloud actions in the project. The best way to address this is to verify the roles assigned to the service account at the project, folder, or organization levels, which can be done through the Identity and Access Management (IAM) in the Google Cloud Console.

Option B is incorrect because the problem is related to permission issues in the Google Cloud and not configuration errors on the CI/CD server itself. While logs can provide useful information, they will not directly point to the roles and permissions in the Google Cloud Console.

Option C is also incorrect, as it deals with checking firewall settings within the VPC network configuration. This is not relevant to the permission issue at hand, which pertains to the service account's assigned IAM roles and not the VPC network configuration or firewall rules.

Lastly, option D is incorrect because verifying the billing account's standing does not relate to the permission issues being experienced. The billing account status may impact the availability of certain resources and services, but it would not directly affect the CI/CD server's ability to execute Google Cloud actions within a specific project due to service account permissions.

Solution to Question 16: B

The correct answer is B: Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer. This option is suitable because you are using Google Kubernetes Engine, and you require autoscaling, HTTPS support, and a public IP for your application. The NodePort service type will expose your application on a specified port on each node of the cluster. Then, by creating a Kubernetes Ingress to expose this NodePort service, the Cloud Load Balancer will provide load balancing and HTTPS support, addressing the company's requirements.

The other options are invalid for the following reasons:

A: Deploy your application on Google Cloud Functions and use API Gateway to expose the HTTPS endpoint. This option doesn't involve Google Kubernetes Engine at all, which is stated as a requirement in the question. Instead, it suggests using serverless architecture, which isn't suitable for this scenario.

C: Create a Kubernetes Service of type NodePort to expose the application on port 443 of each node of the Kubernetes cluster. Configure the public DNS name of your application with the IP of every node of the cluster to achieve load-balancing. This option doesn't involve using a Kubernetes Ingress or a Cloud Load Balancer, which are needed for properly managed load balancing and HTTPS support. It also suggests manually configuring the DNS, which is error-prone and not suitable for autoscaling.

D: Configure a Google Compute Engine instance with Nginx as a reverse proxy, and expose the application on HTTPS. Connect this instance to your GKE cluster. This option involves additional complexity with a reverse proxy and manual management of HTTPS certificates. Moreover, it may not provide proper autoscaling and managed load balancing like a Cloud Load Balancer would.

Solution to Question 17: B

The correct answer is B. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

The reasons why B is the right choice are as follows:

1. Using the Principle of Least Privilege: Google recommended practice advises using the principle of least privilege when configuring access to resources. This means granting the minimum permissions required for the VMs in the web-applications project to access BigQuery datasets in the crm-databases project. In this case, the roles/bigquery.dataViewer role

would be the most suitable as it enables read-only access to dataset metadata and data.

2. Separating Projects: Assigning the roles/bigquery.dataViewer role to the crm-databases project ensures that the service account from the web-applications project only has access to the necessary dataset in the crm-databases project, and not to the other resources within the same project.
3. Appropriate Roles: By granting appropriate roles to the web-applications project, you ensure that the service account has the necessary permissions to perform its tasks within the project limit, without excessive privileges.

The reasons why other options will NOT work:

A. Granting the "project owner" role to both projects would give excessive permissions and violates the principle of least privilege. This level of access would also introduce a higher security risk, as the service account would have full control over both projects.

C. Granting the roles/iam.serviceAccountAdmin role to crm-databases is not necessary for the given requirement, as it allows creating and managing service accounts, whereas the need is to provide access to BigQuery datasets. The roles/bigquery.admin role to web-applications is an excessive level of access, going beyond the requirement and violating the principle of least privilege.

D. The roles/bigquery.user role is not the most appropriate role for crm-databases, as it allows more than just read-only access, which is the requirement. Granting the "project owner" role to web-applications would also provide excessive privileges, violating the principle of least privilege.

Solution to Question 18: A

The correct answer to this question is A: Create a custom Compute Engine image from a snapshot. Create your instances from that image.

An explanation for why A is the correct answer:

Creating a custom Compute Engine image from a snapshot ensures that you have an exact replica of your original VM with all the necessary configurations, dependencies, and data required to handle the increased workload. By using the custom image to create new instances, you ensure that the replicated VMs will have the same configuration as the original, allowing them to seamlessly handle the additional traffic.

Reasons why other options will not work:

B. Create a custom Compute Engine image from a snapshot. Create your instances from a Cloud Storage bucket.

While creating a custom Compute Engine image from a snapshot is a good step, storing the instance data in a Cloud Storage bucket doesn't help in replicating

the VMs with the same configuration. The instances should be created using the custom image directly rather than referencing a Cloud Storage bucket.

C. Create a custom Compute Engine image from your base VM. Create your instances from that image.

Creating a custom image directly from the base VM won't include the current state and data of your VM, which means that the replicated VMs would likely not have the required dependencies and configurations needed for the anticipated workload. Creating an image from a snapshot ensures that the current state of the VM is preserved.

D. Use Cloud Dataflow to create a copy of your base VM. Create your instances from that copy.

Cloud Dataflow is not the appropriate service for VM replication; it is designed for processing and transforming large datasets in real-time. It doesn't have the functionality needed to replicate VMs and create instances with the same configuration as the original VM. Compute Engine and custom images should be used instead.

Solution to Question 19: C

The correct answer is C, and here's why:

A cybersecurity expert in the financial industry is required to manage the security vulnerability of a crucial Compute Engine instance in a Google Cloud project. To accomplish this, the expert needs clear visibility into vulnerabilities and other OS metadata.

Option C is the correct approach for the following reasons:

1. The OS Config agent is specifically designed for managing operating system metadata, patching, and software configuration for Google Cloud VM instances. By installing the OS Config agent on the Compute Engine instance, it ensures that vulnerabilities and other OS metadata can be properly managed.
2. Providing the security team member the roles/osconfig.vulnerabilityReportViewer permission grants the required visibility to see vulnerability reports generated by the OS Config agent. This level of access allows the team member to view the necessary data without compromising the system's security.

The other options are not suitable because:

Option A: Installing the Cloud Logging agent on the Compute Engine instance focuses on logging activities and monitoring the system events but does not provide clear visibility into vulnerabilities or OS metadata specifically required in this scenario.

Option B: Enabling VPC Service Controls for the Google Cloud project is a security measure for limiting unauthorized access to the project's resources but does not address the specific need for visibility into OS vulnerabilities and metadata.

Option D: Providing the security team member with roles/compute.instanceAdmin permission grants extensive privileges to manage Compute Engine instances, including starting, stopping, and deleting instances. It does not specifically target visibility into OS vulnerabilities and metadata and is also excessive in terms of granting unnecessary permissions.

Solution to Question 20: D

The correct answer is D, "Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage," and here is why:

Option A is not a suitable solution because even though you can use Google Cloud Function to copy files from Cloud Storage to Compute Engine, it doesn't ensure exclusive access for the new instance. Moreover, the default Compute Engine service account has access to all resources, including other virtual machines (VMs), making it insecure for the specified requirement.

Option B does not fulfill the requirement, as adding metadata to the objects on Cloud Storage that matches the metadata on the new instance is not enough to restrict access only to the new instance. Other virtual machines with the default Compute Engine service account would still be able to access the files.

Option C proposes creating an instance with a custom IAM role and granting it permissions on Cloud Storage. Though this method can restrict access to other VMs, assigning an IAM role directly to a virtual machine is not a recommended approach, as it could lead to inadequate control of permissions.

Option D is the best course of action to fulfill the requirement. By creating a new service account and assigning it to the new instance, you can set unique and specific permissions for that account, ensuring only the new instance can access files stored in Cloud Storage. This approach provides flexibility and fine-grained access control while adhering to the principle of least privilege.

Solution to Question 21: B

The correct answer is B: Use the command gcloud config set container/cluster dev.

Explanation for answer B: Using the command `gcloud config set container/cluster dev` sets the default Kubernetes cluster for the 'gcloud' command-line tool to the 'dev' cluster. This means that whenever you issue a command from the Cloud SDK, it knows which cluster to target by default, saving you the need to specify the cluster each time. This is an efficient way to ensure that all CLI commands target the 'dev' GKE cluster by default.

Why other options will not work:

Option A: Using the command `gcloud compute instances update dev` will not work because this command is used to update the settings of a virtual machine instance in Google Compute Engine, not to configure the default cluster for the Cloud SDK. This will not make all CLI commands target the dev GKE cluster by default.

Option C: Using the command `gcloud config set project/cluster dev` will not work because there is no setting "project/cluster" in 'gcloud' configuration. The correct setting for specifying the default Kubernetes cluster is "container/cluster", which makes option B the correct answer.

Option D: Creating a file called config.json in the ~/.gcloud folder containing the cluster name will not work because the gcloud tool does not use a config.json file for its default configurations. Instead, it relies on the command `gcloud config set` to update the default settings in the config file stored in the .config/gcloud folder. The format of the gcloud configuration file is also different, and it does not use a JSON format.

Solution to Question 22: D

The correct answer is D, and here's why:

Option A is not valid because Cloud Spanner does not provide native support for instance groups or autoscaling based on traffic patterns. While instance groups can be used for autoscaling in Compute Engine, this feature is not available in Cloud Spanner.

Option B is not an efficient solution because Cloud Run is designed for containerized applications and not specifically for managing databases like Cloud Spanner. It's not the appropriate service for optimizing resource usage and scaling Spanner nodes.

Option C is not practical because it involves relying on Google Cloud Support to handle capacity adjustments. This can introduce delays in responding to traffic fluctuations and increases the risk of not meeting the application's performance requirements.

Option D is the ideal solution as it leverages the combination of Cloud Monitoring and Cloud Functions. By creating an alerting policy in Cloud Monitoring, you can send an alert to a webhook when the Cloud Spanner CPU usage is over or under your threshold. This webhook can be linked to a Cloud Function that listens on HTTP and resizes Spanner resources accordingly. This setup provides a more efficient, automated, and real-time response to traffic demands, optimizing resource usage in your Cloud Spanner database.

Solution to Question 23: B

The correct answer is B. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

The reason why B is the best answer is that creating a new VPC network for the VMs and enabling VPC peering between the two networks will allow the VMs to communicate with the DataProc cluster using their private IPs. VPC peering establishes a low-latency, high-bandwidth connection between the VPC networks without the need for gateway devices, thus minimizing configuration complexities and costs.

Option A is not efficient since creating a new GCP project and setting up a Shared VPC for the Dataproc cluster requires more management and configuration than VPC Peering, as well as possible overhead due to IAM and firewall settings.

Option C is not an optimal solution because adding multiple NICs and a secondary subnet to VMs may lead to increased complexity and additional management tasks, particularly when working with a large number of VMs. VPC Peering simplifies the network configuration.

Option D is not necessary because configuring DNS peering between the Dataproc cluster and VMs VPC networks adds an additional layer of complexity that isn't needed for the VMs to communicate with the cluster. Simply enabling VPC peering between the two networks is sufficient for the required communication.

Solution to Question 24: B

The best approach to achieve the desired goal is B. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Reasons why option B is the best choice:

1. Cloud Run is a fully managed platform that automatically scales your application based on incoming traffic, which fits the requirement of not handling infrastructure management and allowing the app to scale as the user base grows.
2. Cloud Run natively supports Docker images, which means the Docker images your team has developed can be easily deployed to the platform.
3. Uploading the Docker images to Artifact Registry helps manage and keep track of your images in a secure and reliable manner.

Reasons why other options will not work as effectively:

A. Deploy the application on App Engine standard environment with a custom runtime: Although App Engine standard environment provides automatic scaling, it does not natively support Docker containers. This option would require additional configuration to work with the existing Docker images, making option B a more straightforward choice.

C. Upload Docker images to Artifact Registry, and deploy the application on Google Kubernetes Engine using Standard mode: Google Kubernetes Engine

(GKE) is a powerful option for managing containerized applications, but it requires more infrastructure management and maintenance as compared to Cloud Run. Because the team prefers not to handle infrastructure management, Cloud Run is a better choice in this case.

D. Create an instance template with the container image, and deploy a Managed Instance Group with Autoscaling: While Managed Instance Groups (MIG) with Autoscaling can also automatically scale based on incoming traffic, they are designed for Compute Engine instances rather than containerized applications. Using MIG would require additional work to manage and configure the instances to run your containers, making it less efficient and more complex compared to Cloud Run, which is specifically designed for containerized apps.

Solution to Question 25: C

The correct answer is C.

Here's why C is the correct answer and why other options will not work:

Option A: This option involves using Cloud Pub/Sub and Cloud Functions, adding unnecessary complexity and potential performance overhead to the task. You can accomplish the same goal by exporting the logs directly to BigQuery, as described in option C, which would be more cost-effective and less convoluted.

Option B: Modifying the instances' startup scripts to send logs directly to BigQuery using the bq command-line tool doesn't make sense because it would require manual intervention to configure each instance and manage the log sending process. This method could lead to inconsistencies in data management and would not be efficient for minimizing costs. In contrast, option C allows exporting logs directly from Cloud Logging to BigQuery, making it a simpler and more cost-effective solution.

Option C: By creating a filter in Cloud Logging to view only the Compute Engine logs and then exporting them to the BigQuery dataset, you can accomplish the task efficiently and minimize cost. This method does not involve any extra third-party tools, like in other options, and ensures that logs are consistently managed, providing a straightforward solution to the problem.

Option D: Using Logstash to generate a pipeline would introduce additional infrastructure and costs that are not necessary to achieve the goal. Granting BigQuery Data Editor roles to service accounts used by Logstash would add complexity to the configuration and increase the risk of unauthorized access. Option C does not require any additional tools and provides a secure and cost-effective solution.

In conclusion, option C is the most cost-effective and straightforward solution for sending Compute Engine logs to the BigQuery dataset, making it the best choice among the given options.

Solution to Question 26: C

The correct answer is C. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group. Here's why C is the right choice and why the other options will not work:

A. Creating a custom role at the folder level and granting all compute.instanceAdmin.* permissions to the role is not a recommended approach by Google. Custom roles, while more granular, can be harder to manage and maintain in the long run. Instead, Google recommends using predefined roles whenever possible to ensure consistent access controls.

B. Granting the basic role roles/compute.admin and the predefined role roles/bigquery.admin to the DevOps group is not the correct method. The DevOps team requires full control over Compute Engine resources but not BigQuery resources access, as they do not have to create or update any other resources. Providing additional access to BigQuery resources would be unnecessarily broadening their permissions.

C. (Correct answer) Granting the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group is the right choice. The roles/viewer role ensures that the DevOps team has the necessary read access to all resources in the project, while the roles/compute.admin role provides them with the specific permissions needed for full control over Compute Engine resources without being overly permissive for other resources. This follows Google's recommendations for using predefined roles while ensuring that the team only has permission to work on the relevant resources.

D. Granting the basic role roles/owner and the predefined role roles/compute.admin to the DevOps group is not a good solution. The roles/owner role is very broad and provides access to virtually all resources within the project, including modifying other resources beyond the scope of Compute Engine. This would not adhere to the requirement of limiting the DevOps team's permissions to Compute Engine resources only, and would violate the principle of least privilege.

Solution to Question 27: C

The correct answer is C. This is because creating an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days is the most appropriate and cost-effective solution. This will automatically move the files to a more affordable storage class (Archive Storage) after they are no longer needed by the application, reducing storage costs without having to take any manual action.

Option A is not suitable since applying a retention policy of 30 days and locking the bucket will prevent deletion or overwriting of objects within that time frame, without regard to managing storage costs. It is mainly used for regulatory and compliance uses, where the focus is on ensuring data is retained for a certain period without being altered.

Option B is not the best choice because, while it could be used to find and

delete files older than 30 days, BigQuery is primarily designed for big data analytics and not specifically for managing Cloud Storage costs. Additionally, using BigQuery for this purpose would require additional operations, such as scheduling queries and maintaining a table, which would introduce unnecessary complexity.

Option D is not effective because custom metadata keys are not automatically processed by Google Cloud Storage. It would require building a separate system that periodically checks and processes the custom metadata, which adds unnecessary complexity and manual intervention. Furthermore, it does not offer a straightforward solution to reducing storage costs for older files.

Solution to Question 28: A

The answer should be A. Set the minimum number of instances for your Cloud Run service to 3.

Explanation:

A. Setting the minimum number of instances for your Cloud Run service to 3 ensures that there are always at least three instances running, which can help distribute the incoming traffic and reduce the load time for the clients' main webpage. As a result, this will decrease the startup latency, provide better load balancing, and enhance performance. This approach adheres to Google's recommendations and directly addresses the clients' issue.

B. Changing the Cloud Run memory allocation to a larger value could improve performance in some scenarios but would not necessarily address the issue of the main webpage taking a significant amount of time to load. Additionally, increasing the memory allocation could lead to the overuse of resources, especially when multiple instances may not be needed for other pages on the website.

C. Decreasing the request timeout for your Cloud Run service would not solve the issue of the main webpage taking a significant amount of time to load. In fact, it may exacerbate the problem by causing requests to time out before the page has had a chance to load fully, leading to a poor user experience and increased frustration for clients' users.

D. Enabling autoscaling on the Cloud Run service might seem like a plausible solution; however, autoscaling is already enabled by default on Cloud Run. Thus, enabling it again would not bring about any changes or improvements to the current situation. Setting the minimum number of instances to 3 is a more effective solution to address clients' concerns about the web page load time.

Solution to Question 29: B

The correct answer is B because it specifically addresses the requirements of the question by allowing clients to access the LDAP server through TLS on port 636 using UDP. By adding a network tag to the instance and creating a firewall rule for ingress on UDP port 636 for that network tag, the desired connectivity is achieved.

Option A is incorrect because it includes several unrelated actions that have nothing to do with the requirement of establishing connectivity on UDP port 636. VPC peering, VPN tunneling, Secure LDAP over the Internet, Identity-Aware Proxy, and Cloud NAT gateway are all unnecessary for this particular objective. Additionally, this option creates a firewall rule on TCP port 636, while the requirement is for UDP port 636.

Option C is incorrect because it simply adds a network tag to the VM instance, but it does not create a firewall rule allowing ingress on UDP port 636. Without the firewall rule, clients won't be able to access the LDAP server on the specified port and protocol.

Option D is incorrect because creating a route called "allow-udp-636" does not actually enable firewall rules to allow ingress on UDP port 636. Routes in GCP are used to direct network traffic between instances, subnets, and external IP addresses, whereas firewall rules are used to control access and permissions.

Solution to Question 30: A

The correct answer is A. To accomplish the task of logging all read or write operations, as well as any metadata or configuration reads of the database table, in the organization's SIEM system, you need to perform the following steps:

1. Navigate to the Audit Logs page in the Google Cloud Console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. This will ensure that all necessary operations are logged.
2. Create a Pub/Sub topic as a Cloud Logging sink destination. This will allow you to export the logs from the Bigtable instance to a centralized location.
3. Add your SIEM as a subscriber to the Pub/Sub topic. This will enable the SIEM system to ingest and analyze the logs from the Bigtable instance.

In contrast, the other options will not work for the specific requirements of the task:

B. Enabling VPC Flow Logs for the network containing the Bigtable instance and streaming logs to your SIEM system will only provide information about the network traffic and not all the required read, write and admin operations for the database table.

C. Using Stackdriver to create a custom dashboard to monitor the Bigtable instance and send alerts to your SIEM system might be a good practice in general, but it will not log all the necessary information for complying with the requirement of logging all read, write, metadata, and configuration operations.

D. Creating a custom log-based metric in Cloud Monitoring to track Bigtable operations and exporting it to your SIEM system might provide some insights into database operations, but it will not provide the comprehensive logging details required for the scenario, such as metadata or configuration reads.

Therefore, the best solution for this task is to follow the steps provided in option A, which will ensure that all necessary read, write, metadata, and configuration operations are logged and properly sent to the SIEM system.

Solution to Question 31: D

The correct answer is D, as it addresses the requirement to enable communication on TCP port 8080 between the specific tiers. Let's examine why the other options will not work and why option D is the best choice.

Option A is incorrect because it involves creating egress firewall rules instead of ingress firewall rules. Egress rules control outbound traffic from instances, while in this scenario, we need to control inbound traffic to instances in tier #2 and tier #3.

Option B is incorrect because it allows all protocols instead of just allowing communication on TCP port 8080. This would create a security risk by allowing unnecessary and potentially harmful traffic between instances.

Option C is incorrect because, like option B, it allows all protocols instead of specifically allowing communication on TCP port 8080. This poses a security risk.

Option D is the correct choice because it meets the requirements:

1. It creates ingress firewall rules, which control inbound traffic to instances in the designated tiers.
2. It associates the instances with their respective service accounts for tier #1, tier #2, and tier #3, which is necessary for maintaining the 3-tier solution's structure.
3. It specifically allows communication on TCP port 8080, ensuring that only the required traffic is permitted between instances across tiers, maintaining a secure environment.

In conclusion, option D is the most suitable choice as it addresses the requirements correctly and maintains a secure network infrastructure.

Solution to Question 32: D

The correct answer is D: Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

Explanation:

Option A is not ideal because it involves applying the changes in a development environment and then running gcloud compute instances list. This only gives you a list of instances; it does not contain the actual infrastructure changes you made, which is what you want to share with your team.

Option B is closer to the correct answer, as it suggests using Deployment Manager templates to describe the changes. However, storing them in a Cloud Storage bucket is not the best practice for storing code-related artifacts. This

is because Cloud Storage is not a version-controlled system, and it lacks important code management features like collaboration, code review, and rollback capabilities.

Option C has similar issues as Option A. It involves applying changes in a development environment and saving the output in a shared Storage bucket, which does not accurately describe nor present your proposed infrastructure changes.

Option D is the correct answer because it follows Google's recommended best practices for managing infrastructure as code. By using Deployment Manager templates, you can accurately describe your proposed changes in a version-controlled manner. Storing these templates in Cloud Source Repositories enables your team to collaborate, review, and effectively manage the infrastructure changes. This approach ensures that your team can understand and evaluate the proposed updates before applying them to the production environment.

Solution to Question 33: B

The correct answer is B, and here's the explanation:

B) Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

Explanation: When working with multiple microservices in a technology company, the primary aim is to minimize manual intervention in the deployment process while ensuring scalability. GKE Autoscaling is a great feature to achieve this goal, as it automatically adjusts the number of nodes in a node pool based on the workload demand. By setting a minimum and maximum for the size of the node pool, you can maintain control over the scaling limits and optimize resource usage as the cluster scales up and down. With this approach, you don't need to predict the load beforehand or manually intervene during deployments.

A) Create a GKE cluster and manually increase or decrease the number of nodes based on load prediction.

This option is not recommended because it involves manual intervention when changing the number of nodes. It also relies on the ability to predict the load, which might not always be accurate. The objective is to minimize manual intervention and enable efficient scaling without relying on load prediction.

C) Deploy the application on multiple VM instances in Compute Engine with an instance group and configure autoscaling.

Although this option involves using autoscaling, it does not utilize Google Kubernetes Engine (GKE), which is designed to handle the deployment and management of containerized applications using Kubernetes. The question specifies deploying a new application to GKE and ensuring its future scalability; therefore, this option does not directly answer the question.

D) Create a custom GKE cluster without autoscaling and manually add nodes when needed.

This option is not suitable because it requires manual intervention for adding nodes when needed. As mentioned earlier, the goal is to ensure the scalability of the application without manual interventions during each deployment. Furthermore, this approach does not take advantage of GKE's autoscaling feature.

Solution to Question 34: A

The answer should be A, "Change the primary key to not have monotonically increasing values." The explanation for why this is the correct answer and the other options will not work is as follows:

A. When the primary key has monotonically increasing values, it leads to a "hotspot" issue in the database, which is a common cause of read latency-related performance problems. Cloud Spanner divides its data into splits, and if the data is not distributed evenly, reads and writes will be concentrated on specific splits, causing performance problems. By changing the primary key to not have monotonically increasing values, the data will be distributed more evenly across the splits, reducing read latency and eliminating hotspots.

B. Implementing pagination to limit the number of rows returned in each read query might help alleviate some of the client's performance issues, but it would not address the root cause of the problem, which is the hotspot caused by monotonically increasing primary key values. Additionally, pagination can sometimes hide issues with query performance, leading to incomplete solutions and greater problems down the line.

C. Enabling interleaved tables to improve read performance is not an appropriate solution for this problem. Interleaved tables can provide performance improvements in specific situations, such as when accessing related data in parent-child table relationships, but it would not address the hotspot issue caused by primary keys with monotonically increasing values.

D. Changing the primary key to a composite key consisting of person_id and created_at might seem like a solution to distribute the data more evenly, but it's not guaranteed to work. If the person_id values are still monotonically increasing, the hotspot issue could persist. Instead, the primary key should be designed in a way that it distributes the data evenly across the splits, which is the primary objective of changing the primary key as stated in option A.

Solution to Question 35: C

The correct answer should be C: Add the group for the finance team to roles/billing viewer role.

Explanation: The main task mentioned in the question is to grant the finance team access to view the billing reports for ongoing projects without giving them any additional permissions.

Option C is the most suitable choice as the roles/billing viewer role in a software development company focuses solely on providing access to view the billing-related information and reports, without granting any other unrelated permissions or access. This role exactly matches the given requirement.

Here's why the other options will not work:

A. Add the group for the finance team to roles/storage admin role. - The roles/storage admin role provides access to manage various storage resources, such as buckets and objects in a storage system. This role has nothing to do with accessing billing reports, thus making it an incorrect option.

B. Add the group for the finance team to roles/container admin role. - The roles/container admin role manages Kubernetes Engine resources, particularly the container clusters and deployments. This role is more related to application deployments and their configurations and does not provide any access to view billing reports, making it an irrelevant choice.

D. Add the group for the finance team to roles/appengine admin role. - The roles/appengine admin role allows a user to administer the App Engine environment and applications. It includes creating, updating, deleting, and viewing App Engine applications. This role is not relevant to accessing billing reports and can lead to granting unrelated permissions.

In summary, option C is the appropriate choice to fulfill the requirement of granting the finance team access to view the billing reports without providing any additional permissions.

Solution to Question 36: B

The best approach to adjust the infrastructure design is option B, which is to create Compute Engine resources in us-central1-b and balance the load across both us-central1-a and us-central1-b.

Here's why other options will not work:

Option A: Creating a Cloud Datastore instance in us-central1-b and setting up replication between the two instances only addresses data replication and redundancy. This solution does not address Compute Engine VMs' resilience or eliminating downtime related to Compute Engine instances.

Option C: Creating a Managed Instance Group and specifying us-central1-a as the zone does not improve resilience against a single Compute Engine zone failure because the instances remain in the same zone. The Health Check configuration will not help in case of zone failure.

Option D: Configuring the VMs to run as serverless instances using Google App Engine standard environment and distributing traffic between the two zones using App Engine Traffic Splitting is a misuse of App Engine. This option assumes that your application can be adapted for Google App Engine, which

is not always possible, and it fails to address resilience in Compute Engine instances.

Option B is the best choice because it balances the load across two separate zones (us-central1-a and us-central1-b), ensuring that if one zone goes down, the other zone will still be available to handle the load. This approach effectively improves the infrastructure's resilience against a single zone failure, eliminates downtime, and helps in cost minimization compared to creating instances in multiple regions.

Solution to Question 37: D

The correct answer is D. This is because the option D balances both cost-efficiency and the necessary availability for the application. By creating a cluster with both a Spot VM node pool and a node pool using standard VMs, it allows deploying critical components on the more reliable standard VMs, ensuring their availability. At the same time, fault-tolerant components can be deployed on the more cost-effective Spot VMs, which have the trade-off of being potentially interrupted (since they use unused resources at a lower cost). This structure also ensures that the application's fault-tolerant and critical components are logically separated, allowing for easier management and monitoring.

Option A will not work because it suggests deploying all components on a single node pool using standard VMs, labeling the fault-tolerant deployments as spot_true. This approach does not address the cost-efficiency requirements, as all components would be running on standard VMs, regardless of their fault tolerance. Additionally, simply labeling the deployments as spot_true doesn't automatically make them take advantage of the lower cost associated with Spot VMs.

Option B focuses on Balanced Persistent Disks, which are not directly related to the cost-efficiency and availability objectives mentioned in the problem. Labeling the critical deployments with disk_balanced_false does not affect the cost-efficiency or stability of the node pool or the deployed components.

Option C will not work because it suggests deploying critical deployments on Preemptible VMs and fault-tolerant deployments on Shielded VMs. This contradicts the requirement to maintain necessary availability for the critical components, as Preemptible VMs have a limited lifetime (up to 24 hours) and can be terminated with little notice. Thus, deploying critical components on Preemptible VMs would not ensure their availability. On the other hand, Shielded VMs provide security at the instance level but do not contribute to cost-efficiency or provide additional availability guarantees.

In summary, the best option is D, as it balances cost-efficiency and availability for the application by creating a cluster with both a Spot VM node pool and a node pool using standard VMs to deploy critical and fault-tolerant components accordingly.

Solution to Question 38: D

The best course of action in this situation is option D: Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity. Here's why this option is the most suitable, and why other options won't work:

Option A: Turning on identity federation between Cloud Identity and Google Workplace and enforcing multi-factor authentication for domain-wide delegation is not the ideal solution because it does not address the organization and management of a large number of users. Further, it does not help to scale the system and processes as the company grows.

Option B: Connecting Google Workspace directly to an on-prem LDAP server for authentication and user management is not the optimal choice, as it increases complexity and dependency on an on-premises infrastructure. As a growing tech company, relying on a cloud-based solution can offer better scalability, flexibility, and easier management.

Option C: Using a third-party identity provider service through federation and synchronizing users from Google Workspace to the third-party provider in real-time is not the most efficient solution. This would add an extra layer of complexity by introducing a new system, rather than utilizing the existing Google Cloud Identity. This also increases the potential risk of data breaches and performance issues due to the involvement of an additional external party.

Option D: Organizing users in Cloud Identity into groups and enforcing multi-factor authentication in Cloud Identity is the best course of action because it simplifies user management and enhances the security of the expanding workforce. By organizing users into groups, it becomes easier to manage a large number of users and their permissions. Multi-factor authentication ensures strong security by adding an extra level of protection to prevent unauthorized access.

Thus, option D provides a scalable, secure, and manageable solution that caters to the expected growth of employees in the company without causing performance issues or unnecessary complexity.

Solution to Question 39: C

The most likely cause for this situation is option C: Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

Explanation:

In this scenario, you are using a single preemptible node pool in your Google Kubernetes Engine (GKE) cluster. Preemptible nodes are short-lived instances, and because of their limited lifecycle, they offer fewer resources compared to regular nodes. When you have a Deployment with two replicas, GKE needs to find resources to host both Pods. If one is still in the Pending status, it's likely that there are not enough resources available for both Pods to run simultaneously.

Option A is not the most likely cause because a firewall rule blocking communication would not result in a Pod being in Pending status. Instead, communication problems would manifest as errors or timeouts when trying to communicate with the control plane or other nodes, rather than an inability to schedule the Pod altogether.

Option B is not the most likely cause as, although Google Kubernetes Engine might experience internal errors, GKE is a highly resilient and robust managed service, and it is far more likely that the cause lies in cluster resource limitations than in an internal GKE error.

Option D is not the most likely cause because the GKE autoscaler is not directly related to scheduling pods. The autoscaler is responsible for adjusting the size of the cluster based on workload requirements and available resources, not distributing Pods across nodes. Even if the autoscaler is not configured correctly, the Pods should be scheduled on the available resources, provided there is enough capacity. In this case, since the issue is a Pod stuck in Pending status which implies a lack of available resources, the autoscaler is not the main factor.

Solution to Question 40: A

The correct answer for this purpose is A. Cold Storage. An explanation for why each option should or should not be chosen is as follows:

A. Cold Storage: Cold Storage is the most cost-effective storage solution designed for data that is accessed infrequently, which makes it a perfect choice for the given scenario. As your colleagues only need to access the archived data once every quarter, Cold Storage will ensure lower costs, while still maintaining the availability and retrieval speed required for fulfilling regulatory obligations.

B. One Zone-Infrequent Access Storage: One Zone-Infrequent Access Storage is designed for infrequently accessed data, but it stores data in only a single availability zone, which makes it less durable than Cold Storage. In the context of a financial company, data durability and integrity are crucial. Therefore, despite being cost-effective, this option may pose a risk to the company's data, and hence, it is not the best option.

C. Partner Interconnect: Partner Interconnect provides a connection between your on-premises network and Google Cloud through a service provider. While it might provide a faster connection and low latency for data transfer, it is not a storage option that addresses the needs of developing an archival system for the data warehouse. Therefore, it is not appropriate for the given scenario.

D. Firestore: Firestore is a NoSQL database for mobile, web, and server development purposes. It is designed for real-time data synchronization, and while it may be suitable for other data processing needs, it is not a cost-effective option for storing infrequently accessed data, like the archived financial data in this case.

In conclusion, Cold Storage offers the best cost-effective solution for the infre-

quent access requirements of the archival system for a financial company's data warehouse. It provides the necessary durability and retrieval speed without incurring unnecessary costs compared to the other available options.

Solution to Question 41: B

The correct answer is B, and here's why:

Option B allows you to efficiently monitor the CPU usage of your Compute Engine instance using Google Cloud Platform's (GCP) built-in services. By following these steps, you can achieve the desired outcome:

1. Creating a Cloud Monitoring Workspace and associating it with your GCP project enables you to monitor and track your Compute Engine instance's performance.
2. Creating an Alerting Policy in Cloud Monitoring with the threshold trigger condition is vital for receiving notifications when the CPU usage exceeds 90% for more than 15 minutes. This ensures that you stay informed when CPU resources are heavily consumed.
3. Configuring your email address in the notification channel will send alerts to the specified email when the trigger condition is met. This allows your team to take immediate action regarding resource consumption in the Compute Engine instance.

Now let's examine why the other options are not suitable:

Option A is not viable because it requires you to create a custom script that monitors the CPU usage and sends it as a custom metric to Cloud Monitoring. This method is unnecessary as Cloud Monitoring can directly monitor Compute Engine instances' metrics. Additionally, this option does not specify setting up email notifications.

Option C is incorrect because creating a logs-based metric in Cloud Logging is redundant and provides less granularity compared to directly using Cloud Monitoring. Moreover, using regular expressions for extracting CPU usage information can result in inefficiencies and potential inaccuracies in the monitoring process.

Option D is not suitable due to its lack of integration with GCP services and reliance on a consumer Gmail account. This approach lacks the necessary security and scalability for a critical production application, and it does not make use of GCP's monitoring capabilities.

Solution to Question 42: A

The correct answer is A: Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Explanation for A: As a best practice for authentication, Google recommends using the Compute Engine VM's default service account to authenticate the application running on it. By assigning appropriate access to the service account,

you are ensuring that it adheres to the recommended practices, while minimizing the adjustments needed to your app. This method is the most secure, as it relies on the built-in security features provided by the Google Cloud Platform.

Reasons why other options are not suitable:

B: Creating an OAuth2.0 client ID for the app and storing its secret in a secure file is not the best choice in this scenario. OAuth2.0 authentication flow is suited for external users' access to applications, which is unnecessary in this context. Moreover, it would require significant changes to the application code, which goes against the goal of minimal modifications.

C: Using your personal account credentials to authenticate applications running on the Compute Engine VM is not recommended. This practice violates security best practices and could lead to unauthorized access or data breaches. Personal account credentials should never be used to authenticate applications, particularly in enterprise settings.

D: Creating a new Google account with appropriate access for Google services is not the optimal solution. This approach would require additional management and increase complexity. Additionally, it would not adhere to Google's recommended authentication practices, as you should be utilizing a service account for this purpose, rather than an individual user account.

Solution to Question 43: A

The answer should be A. "Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names."

The reason for choosing option A is that the primary issue mentioned in the question is the failure of new instance creation. This failure could be due to an invalid instance template causing conflicts. Therefore, ensuring a valid syntax in the instance template is crucial. Furthermore, deleting any persistent disks with the same name as instance names is essential as it would prevent conflicts during the creation process.

Option B, "Enable Shielded VMs on the instances and create an instance template that contains valid syntax which will be used by the instance group," is not the most appropriate answer. Although having a valid instance template is essential, enabling Shielded VMs is not directly related to the issue of new instance creation failure and maintaining the traffic efficiently.

Option C, "Set the minimum CPU platform for the instances, then create an instance template that contains valid syntax which will be used by the instance group," will not resolve the core issue. While providing a valid syntax in the instance template is essential, setting the minimum CPU platform for the instances is not necessarily related to solving the problem.

Option D, "Create an instance template that contains valid syntax that will be used by the instance group. Verify that the instance name and persistent

disk name values are not the same in the template," suggests verifying and comparing instance name and persistent disk name values rather than actually deleting the persistent disks. This may only help to identify the issue but will not resolve it, making option A a more effective solution.

Solution to Question 44: B

The correct answer is B: Install and configure the Ops agent and view the logs from Cloud Logging.

Here's the explanation for why B is the correct answer and why other options will not work:

B. Installing and configuring the Ops agent allows you to collect and send log and metric data from the Compute Engine instance to Cloud Logging. Cloud Logging is a Google Cloud service that allows you to securely ingest, store, analyze, and view log data, helping you diagnose and fix issues in your application. This is the most direct and efficient way to access the logs needed to diagnose the issue that users are experiencing with the application.

Now, let's explain why the other options will not work:

A. Creating a new Google Kubernetes Engine (GKE) cluster and migrating the application there may not be an immediate solution to the problem. GKE is mainly used for managing and deploying containerized applications, and it might not be necessary for the current single Compute Engine instance setup. The main issue at hand is to diagnose the reported errors in the application, which may not require migrating to an entirely new platform.

C. Cloud Pub/Sub is a messaging service designed for asynchronous communication between applications and services. Although pushing error logs to a subscriber might help in certain scenarios, it would require additional configuration and resources to set up the message pushing mechanism within the application. Using Cloud Logging is a more direct and efficient way to diagnose the errors reported by users.

D. Stackdriver Monitoring was rebranded to Cloud Monitoring in 2019, so it is an outdated term. Even then, Cloud Monitoring focuses mainly on collecting and visualizing performance metrics for cloud infrastructure and applications. While it would be helpful in identifying any performance-related issues in the application, it is not specifically designed to view and analyze log data. Cloud Logging would be the more appropriate tool for diagnosing issues by analyzing log data.

Solution to Question 45: A

The correct answer is A. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

Explanation:

Option A is the right course of action because, as a Project Manager, you need to have the Project Billing Manager role for the Google Cloud Platform (GCP) project. This role allows you to manage billing and create a new billing account for the project. After creating the new billing account, you can link it to the existing project to ensure proper billing management.

Option B is not correct because the task at hand is to create a new billing account, not link the existing project to an existing billing account. Furthermore, the Billing Administrator role is associated with billing accounts, not GCP projects.

Option C is not correct because having the Billing Account Viewer role only allows you to view billing information for a GCP project and not manage or create new billing accounts. The role lacks the necessary permissions to create a new billing account and link it to the existing project.

Option D is not correct because it suggests creating a new GCP project, which is not the objective. The goal is to create a new billing account and link it to the existing GCP project. Moreover, a new GCP project would require additional setup and configuration unrelated to the task at hand.

Solution to Question 46: C

The correct answer is C, to migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery. Here's why the other options will not work and why option C is the best choice for the given scenario.

A. Migrate from MySQL to Cloud Spanner, from Kafka to Cloud Data Fusion, and from Cloud SQL for PostgreSQL to Cloud SQL. - While migrating MySQL to Cloud Spanner and Cloud SQL for PostgreSQL to Cloud SQL are reasonable choices, migrating from Kafka to Cloud Data Fusion is not ideal. Cloud Data Fusion is primarily used for data integration, not event streaming.

B. Migrate from MySQL to Cloud Spanner, from Kafka to Memorystore, and from Cloud SQL for PostgreSQL to Cloud SQL. - While migrating MySQL to Cloud Spanner and Cloud SQL for PostgreSQL to Cloud SQL are appropriate, migrating from Kafka to Memorystore is not suitable. Memorystore is an in-memory storage system used for caching purposes, not for event streaming.

C. Migrate from MySQL to Cloud Spanner, from Kafka to Pub/Sub, and from Cloud SQL for PostgreSQL to BigQuery. - This is the best option because Cloud Spanner provides global scalability as well as strong consistency for the main database requirement. Google Cloud Pub/Sub is a fully-managed messaging service that is designed for event streaming, making it a direct replacement for Apache Kafka. Moreover, migrating from Cloud SQL for PostgreSQL to BigQuery targets analytical and reporting needs, offering a serverless, scalable data warehouse solution with minimal operational and infrastructure management.

D. Migrate from MySQL to Firestore, from Kafka to Cloud Tasks, and from

Cloud SQL for PostgreSQL to BigQuery. - Although Firestore is a NoSQL database that can scale globally, it's not the best solution for relational data management, making Cloud Spanner a better choice to replace MySQL. Moreover, migrating from Kafka to Cloud Tasks is not suitable because Cloud Tasks is a task queue service focused on asynchronous workloads rather than event streaming. However, migrating from Cloud SQL for PostgreSQL to BigQuery is reasonable for analytical and reporting needs.

In conclusion, option C is the most suitable answer to achieve global scalability and minimal operational and infrastructure management while migrating from existing on-premises data management solutions to Google Cloud.

Solution to Question 47: A

The best approach in this scenario is A: Create and deploy a Deployment per microservice. This is because Kubernetes Deployments are designed specifically for managing scalable and stateless applications in a container orchestration environment like Google Kubernetes Engine.

Here's why the other options are not suitable:

Option B: Create and deploy an Instance Group per microservice. Instance Groups are a Google Cloud feature used for managing groups of virtual machine instances. While they provide some level of scalability and load balancing, they are not designed to manage containerized applications. Kubernetes handles scalability and load balancing more effectively for containerized applications, making Deployments a better choice for this scenario.

Option C: Create and deploy a Bundle per microservice. The term "Bundle" in this context is not a well-defined concept in Google Cloud or Kubernetes. It is possible that this option refers to some sort of package or collection of resources, but it does not provide any inherent scalability or management features for containerized applications. Deployments are the standard method for managing scalable containerized applications in Kubernetes.

Option D: Create and deploy a Dataproc Cluster per microservice. Dataproc Clusters are a Google Cloud feature specifically designed for running and managing Apache Hadoop and Apache Spark workloads. These clusters are not meant for deploying containerized applications or managing microservices. Kubernetes Deployments are the appropriate choice for managing scalable containerized microservices.

In summary, the best approach to ensure scalability for each microservice is to use Kubernetes Deployments, which are designed specifically for managing containerized applications in a Google Kubernetes Engine environment.

Solution to Question 48: A

The correct answer is A.

A. Create a GKE node pool with a sandbox type configured to gvisor. Add

the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

Creating a GKE node pool with a sandbox type configured to gvisor provides a strong security boundary between clients' Pods. gVisor is an open-source sandbox runtime that provides an additional layer of isolation between the client's Pods and the underlying GKE infrastructure. By configuring each client's Pod with the parameter runtimeClassName set to gvisor, you ensure that their code runs in a secure, isolated environment, minimizing the risks associated with executing arbitrary code from multiple clients within a single GKE cluster.

B. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

Binary Authorization is a tool for controlling which container images can run in a certain environment, like a GKE cluster. While it's important for security, it doesn't provide the desired level of isolation between clients' Pods that are running arbitrary code, which is the main objective stated in the question.

C. Use Cloud Run for Anthos to deploy and manage your customers' Pods.

Cloud Run for Anthos is a platform for deploying serverless applications on a GKE cluster. While it's a useful service for easing the deployment of containerized applications, it doesn't specifically address the goal of maximizing the isolation between clients' Pods.

D. Use Cloud Armor to configure security policies for each customer's Pod.

Cloud Armor is a service that protects applications from Distributed Denial of Service (DDoS) and Application Layer attacks by providing customizable security rules and policies. Although it offers essential security measures for web applications, it doesn't directly address the challenge of isolating arbitrary code execution within clients' Pods, as required in the question.

Thus, the best strategy to maximize the isolation between clients' Pods is A. Create a GKE node pool with a sandbox type configured to gvisor and add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

Solution to Question 49: D

The correct answer should be D: Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

Explanation:

Option D is the best approach because of the cost optimization and the data access requirements mentioned in the question. As the items are frequently accessed for the initial 30 days, using Standard storage ensures high availability and performance. After the 30-day window, moving the objects to Archive storage minimizes storage costs over the next three years. Archive storage is

designed for long-term storage and infrequent access, which aligns with the company's needs.

Reasons why other options are not the best approach:

Option A: Nearline storage is more expensive for short-term storage as compared to Standard storage. Also, using Coldline for one year before moving to Archive storage for the next two years does not optimize costs, as Archive storage would still be cheaper over that time period given the infrequent access.

Option B: Similar to Option A, using Nearline storage for the first 30 days is not cost-effective compared to Standard storage, and storing data in Coldline for two years before moving to Archive storage doesn't optimize costs as effectively as moving directly to Archive storage after the initial 30 days.

Option C: Though using Standard storage for 30 days is the right approach, moving to Nearline storage for one year and then Archive storage for two years isn't the best cost optimization plan, especially given the access patterns. Storing objects in Archive storage for the entire three years is a more efficient and cost-effective option.

Solution to Question 50: D

The correct answer is D, and here's the explanation why:

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

By routing 100% of the traffic to the previous version, you'll be able to revert back to the previous state, which was presumably working fine, without the newly introduced bugs. Google Cloud Platform provides this functionality for a quick and easy rollback process in case of errors in newer deployments.

Now let's take a look at the other options and why they're not ideal:

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

There is no "Revert" button on the App Engine page of the GCP Console. The correct method for reverting to a previous version is by routing the traffic to that version, as mentioned in option D.

B. Create a new App Engine instance and deploy the prior version, then route traffic to the new instance. Utilize storage service backups to restore the prior version to the App Engine. Revert the faulty code changes through Git, then deploy the resulting version to App Engine. On the GCP Console, choose GCP Datastore and rollback to an earlier snapshot to restore the application before the bug was released.

This option consists of multiple actions that are not the most efficient way to address the issue. Creating a new App Engine instance and deploying the prior version would take more time and resources than simply routing the traffic to the

existing previous version. Storage service backups and datastore rollbacks don't directly address the issue of reverting the working version of the application.

C. Run gcloud app restore.

There's no "gcloud app restore" command for reverting to a previous version of the application on App Engine. The correct command would be "gcloud app services set-traffic" to route traffic to a different version, but using the GCP Console as described in option D is more user-friendly and less prone to errors.

Practice Exam 15

Question 1: As a DevOps engineer at a growing tech company, you need to review the configured Kubernetes Engine cluster of an inactive configuration in your gcloud account with the least number of steps. What should you do?

A. Use gcloud config set compute/zone and gcloud config set compute/region to review the output.

B. Use kubectl get nodes to review the output.

C. Use gcloud container clusters get-credentials and gcloud container clusters describe to review the output.

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

Question 2: You are working as a developer for a tech firm that is creating a global application to manage customer relationships. The company's management team is unsure about the future growth of the user base and wants the application to be able to scale accordingly with minimal changes to the database configuration. Which storage solution is the best fit for this requirement?

A. Datastore

B. Bigtable

C. Cloud Spanner

D. Cloud Storage

Question 3: As the network administrator of a leading tech company, you need to configure Cloud DNS to create DNS records that will direct home.mydomain.com, mydomain.com, and www.mydomain.com to the IP address of your Google Cloud load balancer. What is the most effective approach to achieve this?

A. Create one SOA record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

B. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively. Most Voted

C. Create one PTR record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

D. Create one A record to point mydomain.com to the load balancer, and create two NS records to point WWW and HOME to mydomain.com respectively.

Question 4: As a software engineer at a leading tech company, you have an application running in Google Kubernetes Engine (GKE) within your company's

infrastructure, and cluster autoscaling is enabled. This application exposes a TCP endpoint and runs multiple replicas. In the same region, there is a Compute Engine instance on another Virtual Private Cloud (VPC) called gce-network that doesn't have an overlapping IP range with the first VPC. For one of your projects, this instance is required to connect to the GKE application, and you want to achieve this with minimal effort. How should you proceed?

A. 1. In GKE, create a Service of type ClusterIP that uses the application's Pods as backend. 2. Peer the two VPCs together. 3. Configure the Compute Engine instance to use the address of the ClusterIP that has been created.

B. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add a Cloud Armor Security Policy to the load balancer that whitelists the internal IPs of the MIG's instances. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Set the service's externalTrafficPolicy to Cluster. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

D. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal 3. Peer the two VPCs together. 4. Configure the Compute Engine instance to use the address of the load balancer that has been created.

Question 5: As a data analyst working for a healthcare organization, you need to grant your fellow team members access to analyze datasets in BigQuery without running the risk of them accidentally deleting the datasets. To ensure a secure and effective solution in accordance with Google-recommended practices, what should you do?

A. Create a custom role by removing delete permissions, and add users to that role only.

B. Create a custom role by removing delete permissions. Add users to the group, and then.add the group to the custom role.

C. Add users to roles/bigquery dataEditor role only, instead of roles/bigquery dataOwner.

D. Add users to roles/bigquery.viewer role only, instead of roles/bigquery dataOwner.

Question 6: As a team lead in a software company, you have been assigned the responsibility to delegate the task of creating and managing all service accounts for Google Cloud projects to a dedicated team member. What role should you assign this person to fulfill this requirement with minimal permissions?

A. Add the user to roles/iam.serviceAccountAdmin role.

B. Add the user to roles/iam.serviceAccountAuditor role.

C. Add the user to roles/iam.serviceAccountOperator role.

D. Add the user to roles/iam.serviceAccountMaintenanceManager role.

Question 7: As a developer in a software development company, last month you noticed that your GKE container projects incurred higher costs than anticipated. Upon investigation, you discover that one of the development GKE containers generated numerous logs, which led to the increased expenses. In order to disable the logs swiftly and efficiently, what should be your approach?

A. 1. Go to the IAM console, and remove permissions for the GKE container to write logs to Stackdriver Logging.

B. 6. Go to the Monitoring console, and set log-based metrics to zero for the GKE container.

C. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

D. 4. Use the gcloud command-line tool to set the GKE container's logging level to "none."

Question 8: You are working as an organization and billing administrator at a software development company. The engineering team has been granted the Project Creator role within the organization. Your goal is to restrict the engineering team from linking projects to billing accounts, while allowing the finance team to do so without granting them additional permissions to change project settings. What action should be taken to achieve this?

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

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

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

D. Give the finance team only the Compute Network User role on the organization.

Question 9: You are an IT specialist working for a company in the radiology industry that stores its medical images in an on-premises data room. The company wants to use Cloud Storage for archival storage of these medical images and requires an automated process for uploading any new images to Cloud Storage. How would you design and implement this solution?

A. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

B. Deploy an App Engine service to sync the medical images from the on-premises storage to Cloud Storage using Cloud Endpoints.

C. Use the Cloud Vision API to process and store the medical images as JSON objects in Cloud Storage.

D. Create a Data Fusion pipeline to transfer medical images from the on-premises storage to Cloud Storage on a scheduled interval.

Question 10: As a data engineer working for a major retail corporation, you are tasked with managing a vast amount of unstructured data in various file formats. Your goal is to perform ETL transformations on this data and make it available on Google Cloud so that a Dataflow job can process it efficiently. What is the best approach to achieve this?

A. Upload the data to Cloud Firestore using the Firestore module in the Google Cloud Client Libraries.

B. Upload the data into Cloud SQL using the import function in the console.

C. Upload the data to Cloud Storage using the gsutil command line tool.

D. Upload the data to Cloud Datastore using the gcloud command line tool.

Question 11: You are a cybersecurity analyst working for a large financial services company. A former employee was terminated two weeks ago, and you've just discovered that their access to the company's Google Cloud was not immediately removed. You are tasked with determining if this employee accessed any sensitive customer data during this period. How should you proceed?

A. View Admin Activity logs in Cloud Auditing. Search for the IP address associated with the user.

B. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

C. View System Event Logs in Cloud Logging. Search for the service account associated with the user.

D. View Data Access audit logs in Cloud Logging. Search for the service account associated with the user.

Question 12: You are working as a cloud administrator at a company which relies on a Compute Engine instance to host an application, predominantly used between 9 AM and 6 PM on weekdays. To ensure disaster recovery, you need to establish a daily backup for this instance and retain the backups for 30 days. The company prefers a Google-recommended solution with minimal management overhead and the least number of services involved. What approach should you take?

A. 1. Create a Dataflow job that backs up the instance's disk to BigQuery daily.
2. Configure the Dataflow job to delete the backups older than 30 days.

B. 5. Update your instances' metadata to add the following value: backup-frequency: daily backup-retention: 30

C. 1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk. 2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM - 2:00 AM - Autodelete snapshots after: 30 days

D. 1. Update your instances' metadata to add the following value: snapshot-schedule: 0 1 * * * 2. Update your instances' metadata to add the following value: snapshot-retention: 30

Question 13: As a database engineer at a large software company, you are tasked with migrating a crucial on-premises application to Google Cloud Platform (GCP). This application requires 96 vCPUs to function efficiently. How should you ensure the application operates smoothly in a similar environment on GCP?

A. When creating the VM, use machine type n1-standard-96.

B. When creating the VM, use machine type custom with 48 vCPUs and increase the number of VM instances to 2.

C. Create the VM using Compute Engine default settings. Use gcloud to modify the running instance to have 96 vCPUs.

D. Use Cloud Functions to split the workload into smaller tasks and deploy to a serverless environment.

Question 14: As an IT specialist working in a healthcare company, you are responsible for managing sensitive data stored in three Cloud Storage buckets and have enabled data access logging. To ensure data security, you need to audit a specific employee's activities related to the addition of metadata labels and viewing files in these buckets, while taking the fewest possible steps. What should you do?

A. Use Cloud Pub/Sub to access the logs and filter the activity you need to verify.

B. Using the GCP Console, filter the Activity log to view the information.

C. Create a trace in Cloud Monitoring to view the information.

D. Create a trace in Stackdriver to view the information.

Question 15: You are working at a software company that has recently deployed an application on a single Compute Engine instance in the cloud. The application writes logs to disk, and users have started reporting errors with the application. In order to diagnose the issue, what should you do?

A. Configure Cloud Pub/Sub to receive logs and analyze them externally.

B. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

C. Create a Google Cloud Function to process and analyze the application logs.

D. Use the command `gcloud beta logging read` to connect to the instance and read the application logs.

Question 16: As a part of an IT team in a growing tech company, you have been tasked with adding a group of new employees to Cloud Identity. Some of these employees already have existing Google accounts. In order to adhere to Google's best practices and avoid account conflicts, what approach should you take?

A. Invite the user to use an email alias to resolve the conflict.

B. Invite the user to transfer their existing account.

C. Create a new Google account for each user.

D. Ask the user to create a separate Google Workspace account and migrate their data.

Question 17: As a database administrator in a technology company, you need to determine when users were added to Cloud Spanner Identity Access Management (IAM) roles in your team's Google Cloud Platform (GCP) project. Which action should you take in the GCP Console?

A. Open the BigQuery console, and check audit logs for Cloud Spanner IAM roles.

B. Open the Cloud Spanner console to review configurations.

C. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

D. Go to the Stackdriver Monitoring console and review information for Cloud Spanner.

Question 18: As a software engineer in a tech company, you are currently developing an application to be deployed in your organization's data center, which will utilize Google Cloud Platform (GCP) services like AutoML. You have already created a service account with proper access to AutoML. To enable authentication to the APIs from your on-premises environment, what should be your next step?

A. Configure a Compute Engine instance with appropriate permissions and connect your on-premises application to it

B. Use gcloud to create a key file for the service account that has appropriate permissions.

C. Create a user-managed service account with no permissions and use it for on-premises authentication

D. Use service account credentials in your on-premises application.

Question 19: As a software engineer working in a gaming company that has recently developed a mobile multiplayer game hosted on Google Cloud, you notice that gamers connect to the game via their personal phones over the Internet, and the game sends UDP packets to update the servers about the players' actions. The game backend is designed to scale across multiple virtual machines (VMs), and you have been tasked with exposing these VMs through a single IP address. What solution should you implement?

A. Utilize Cloud Armor with the application servers to distribute traffic.

B. Configure an External Network load balancer in front of the application servers.

C. Configure an Internal TCP/UDP load balancer in front of the application servers.

D. Configure an Internal UDP load balancer in front of the application servers.

Question 20: As a part of the IT department in a growing company, you have been tasked to manage the company's GCP accounts. One account is running in the default region and zone, while the other is in a non-default region and zone. You need to start new Compute Engine instances in both accounts using the command line interface. How should you proceed?

A. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

B. Create one configuration using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

C. Create a configuration file for each account and use the –configuration flag when running gcloud command to start Compute Engine instances.

D. Activate two configurations using gcloud configurations activate [NAME]. Run gcloud configurations list to start the Compute Engine instances.

Question 21: As a software engineer working for a large enterprise, you need to deploy additional pods to an existing application running in Google Kubernetes Engine (GKE) comprising multiple pods on four GKE n1-standard-2 nodes. These new pods require n2-highmem-16 nodes, and you must ensure there is no downtime during the deployment process. What is the most appropriate course of action?

A. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

B. Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

C. Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster.

D. Use Deployment Manager to change node type to n2-highmem-16 and redeploy the services.

Question 22: As a software developer at a leading fintech company, you need to create a financial trading platform accessible worldwide. The data must be stored and queried using a relational structure, ensuring that clients globally receive the exact identical state of data. To provide low latency for end users, the application will be deployed in multiple regions. Which storage option should you choose for the application data to minimize latency?

A. Use Cloud Spanner for data storage.

B. Use Firestore for data storage.

C. Use Cloud Filestore for data storage.

D. Use Cloud Storage for data storage.

Question 23: You are working as an IT administrator at a software company, and your manager has asked you to grant editing and viewing permissions for three team members on a Cloud Spanner instance. How should you proceed?

A. Run gcloud projects add-iam-policy-binding my-project –member group:group@example.com –role roles/spanner.databaseUser.

B. Run gcloud projects add-iam-policy-binding my-project –member user:email@example.com –role roles/spanner.databaseUser.

C. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

D. Run gcloud projects add-iam-policy-binding my-project –member user:email@example.com –role roles/spanner.databaseAdmin.

Question 24: As a software developer at a rapidly growing tech company, you are responsible for managing multiple Google Cloud projects efficiently. You want to configure the Google Cloud SDK command line interface (CLI) in a way that allows you to effectively manage multiple projects. What is the best approach to achieve this?

A. 1. Create a separate terminal session for each project you need to manage. 2. In each session, update the active project by changing the environment variable for the project ID.

B. 1. Use the default configuration for one project you need to manage. 2. Use gcloud init to update the configuration values when you need to work with a non-default project.

C. 1. Create an App Engine application for each project you need to manage. 2. Use gcloud app commands to deploy and manage resources in each different

project.

D. 1. Create a configuration for each project you need to manage. 2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

Question 25: You are an IT specialist working for a global company whose application receives SSL-encrypted TCP traffic on port 443 from clients worldwide. In order to minimize latency for these clients, which load balancing option would be best suited for this situation?

A. NAT Gateway Load Balancer

B. Cloud VPN Load Balancer

C. Internal HTTP(S) Load Balancer

D. SSL Proxy Load Balancer

Question 26: As a software engineer working at a tech company, you are tasked with setting up permissions for a group of Compute Engine instances, allowing them to write data into a specific Cloud Storage bucket while adhering to Google-recommended practices. What should you do?

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

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

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

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

Question 27: As a software engineer in a tech company, you have a development project with appropriate IAM roles defined. Now, you are creating a production project within the same company and wish to have the same IAM roles on the new project, using the fewest possible steps. What should you do?

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

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

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

D. Use gsutil iam setaclexamples for multiple projects with a single command.

Question 28: As a project manager at a software development company, you are leading the transition from an on-premises environment to Google Cloud.

Your company has multiple development teams using Cassandra environments as backend databases, and each team requires a separate, isolated development environment. The goal is to move to Google Cloud as swiftly as possible and minimize the support effort required. What course of action should you take?

A. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

B. 1. Set up a managed instance group for each development team with a custom Cassandra image. 2. Configure VPC Network Peering to isolate each team's network traffic.

C. 1. Deploy multiple Cassandra instances on Cloud Run using Docker containers. 2. Control access to each instance via Identity and Access Management (IAM) policies.

D. 1. Use Cloud Datastore as a replacement for Cassandra. 2. Set up separate projects for each development team to isolate their data.

Question 29: You are working as a software engineer in a gaming company that is developing a multi-player gaming application. The company's goal is to store game data in a database and maintain consistent performance as the game gains popularity. In order to avoid increasing management complexity, what should you do to ensure optimal gaming performance for users all over the world?

A. Use Cloud Spanner to store user data mapped to the game statistics.

B. Use Cloud Redis to store game statistics with regional replication in the EU, US, and APAC regions.

C. Store game statistics in a Bigtable database partitioned by username.

D. Use BigQuery to store game statistics with a Redis on Memorystore instance in the front to provide global consistency.

Question 30: As a software engineer at a tech company, you have developed an app using Google Cloud Platform and deployed it on an App Engine application within a GCP project. The application is currently served from the us-central region, but you now need to serve it from the asia-northeast1 region instead. What is the appropriate course of action to achieve this?

A. Create a new GCP project and add a Compute Engine instance in the asia-northeast1 region, then migrate the App Engine application to it.

B. Use a custom domain and map it to the asia-northeast1 region for the existing App Engine application.

C. Change the region property setting in the existing App Engine application from us-central to asia-northeast1.

D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

Question 31: As a software engineer at a leading tech company, you are working on a new web application that will be hosted on Google Cloud Platform. Your team's release cycle requires testing application updates on a small subset of real user traffic while the majority of users access a stable version of the app. How should you execute this process?

A. Deploy the application on App Engine. For each update, create a new service. Configure traffic splitting to send a small percentage of traffic to the new service.

B. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

C. Deploy the application on Compute Engine. For each update, create a new custom image. Use a Managed Instance Group and configure traffic splitting by adjusting the instance group's target size.

D. Deploy the application on Kubernetes Engine and use a StatefulSet for each update. Configure traffic splitting through a Kubernetes Ingress to direct a small percentage of traffic to the new StatefulSet.

Question 32: As a team lead in a software development company, you are in charge of deploying a licensing server for an application to the Compute Engine. The application should be able to access the licensing server using the IP 10.0.3.21 without requiring any configuration changes. What is the most suitable method to achieve this?

A. Configure the licensing server to listen on all IP addresses in the 10.0.3.0/24 subnet and assign a different static internal IP address to the server.

B. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

C. Configure the application to use a different IP address, then reserve that IP as a static internal IP address using gcloud and assign it to the licensing server.

D. Create a custom routing rule to route traffic destined for 10.0.3.21 to the licensing server's actual IP address.

Question 33: As a finance manager in a software development company, you are responsible for monitoring the costs associated with multiple Google Cloud projects. These projects are connected to separate billing accounts, making it essential for you to consolidate and visualize cost data for efficient forecasting. To achieve this, while also ensuring new cost data is included promptly, what approach should you adopt?

A. Use the Reports view in the Cloud Billing Console to view the desired cost information.

B. Create individual billing report alerts using Cloud Monitoring in each project.

C. Use Stackdriver Monitoring to display the costs of all projects on a single dashboard.

D. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

Question 34: As a network engineer for a rapidly growing tech company, you're tasked with creating a custom VPC containing a single subnet. The company requires the subnet's range to be as large as possible. Which IP address range should you use?

A. 203.0.113.0/24

B. 192.168.0.0/16

C. 169.254.0.0/16

D. 10.0.0.0/8

Question 35: As a DevOps engineer at a software development company, you are responsible for managing a Google Kubernetes Engine (GKE) cluster used by various teams for non-production workloads. The Machine Learning (ML) team requires access to Nvidia Tesla P100 GPUs for training purposes. In order to minimize both effort and cost, which action should you take?

A. Ask your ML team to use TPUs instead of GPUs for their training.

B. Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

C. Create your own Kubernetes cluster on top of Compute Engine with nodes that have GPUs. Dedicate this cluster to your ML team.

D. Recreate all the nodes of the GKE cluster to enable GPUs on all of them.

Question 36: As an IT manager in a tech company, you have three existing Google Cloud projects in your organization, and you are required to bill the Marketing department for their Google Cloud services used in a new initiative within their team. What steps should you take to accomplish this task?

A. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud account. 2. Create a separate Google Cloud project for each service used by the Marketing department without linking a Billing Account.

B. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud account. 2. Create a budget for the Marketing department, but don't create a separate project or billing account.

C. 1. Verify that you are assigned the Project Creator IAM role for your organization's Google Cloud account. 2. Create a new Marketing project and share the billing account with other projects.

D. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud Project for the Marketing department. 2. Link the new project to a Marketing Billing Account.

Question 37: You are working for a renowned pharmaceutical company that stores its research documents in an on-premises data room. The company wants to utilize Cloud Storage for archival storage of these documents and requires an automated process to upload any new research documents to Cloud Storage. How should you design and implement this solution?

A. Enable Cloud Spanner to store the medical images and create a script that transfers the images from on-premises storage to Cloud Spanner. Schedule the script as a cron job.

B. Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

C. Configure a Cloud Storage Transfer Service to sync the on-premises storage with Cloud Storage daily, without using a cron job or script.

D. Create a Cloud SQL instance and develop a script to import the image files into the database. Schedule the script as a cron job.

Question 38: As a software developer working in a tech company, you have been tasked with creating a new version of an application currently hosted in an App Engine environment. You are required to test the new version with 1% of users before fully transitioning the application to the new version. What should you do?

A. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

B. Deploy the new version of your application in a separate project within App Engine and then use GCP Console to split traffic.

C. Use Cloud Pub/Sub to distribute 1% of your application's traffic to the new version deployed in App Engine.

D. Deploy a new version of your application in a Compute Engine instance instead of App Engine and then use GCP Console to split traffic.

Question 39: You are working as a Project Manager in a software development company that extensively utilizes Google Cloud services centralized in a single project. The company has dedicated projects for testing and development, specific to each team. The DevOps team is responsible for managing production services, and you want to ensure their access rights remain consistent without being affected by future updates in Google Cloud products. In order to adhere to Google-recommended practices, how should you configure the access permissions for the DevOps team?

A. Create a custom role that combines the required permissions, but grant the DevOps team the Project Viewer role on the production project.

B. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

C. Grant all members of the DevOps team the role of Project Editor on the organization level.

D. Grant all members of the DevOps team the role of Project Viewer on the production project.

Question 40: As a DevOps engineer in your company, you have been asked to check and verify the IAM users and roles assigned within a GCP project named my-project. How should you proceed?

A. Use Stackdriver Logging to review IAM logs for my-project.

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

C. Run the command: gcloud projects get-iam-policy my-project. Review the output section.

D. Use Cloud Audit Logs to review IAM activity for my-project.

Question 41: As a data manager in a prominent tech company, your auditor has requested to review the usage of data stored in Google Cloud, specifically focusing on who accessed data in Cloud Storage buckets. In order to assist them in accessing the required information, what should be your course of action?

A. Turn on Cloud Asset Inventory for the organization to track asset metadata.

B. Set up Stackdriver Error Reporting to capture data access errors.

C. Configure a Cloud Pub/Sub topic to stream logs related to Cloud Storage access.

D. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

Question 42: You are a DevOps engineer working in a software company that heavily relies on containerization. Your team has decided to implement Google Kubernetes Engine for better container orchestration. To fulfill the necessary security requirements, you need to set up a cluster with verifiable node identity and integrity, ensuring that nodes cannot be accessed from the internet. Additionally, you'd like to minimize the operational cost of managing the cluster while adhering to Google-recommended best practices. What approach should you take?

A. Deploy a public autopilot cluster.

B. Deploy a public regional cluster and enable shielded nodes.

C. Deploy a private zonal cluster and enable shielded nodes.

D. Deploy a private autopilot cluster.

Question 43: As a manager in a tech company, you have been tasked with estimating the total cost of transitioning your three-tier web application from virtual machines that use a MySQL database to Google Cloud instances and Cloud SQL. What is the most effective method for determining this estimate?

A. Implement a similar architecture on Google Cloud, and run a reasonable load test on a smaller scale. Check the billing information, and calculate the estimated costs based on the real load your system usually handles.

B. Use Google BigQuery to analyze the data from your current on-premises infrastructure and use these insights to predict the costs of running your application on Google Cloud Platform.

C. Use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource you expect to use. Use similar size instances for the web server, and use your current on-premises machines as a comparison for Cloud SQL.

D. Use the GCP Marketplace to estimate the cost of deploying a pre-built web application similar to your existing application.

Question 44: As a software engineer working in a tech company, you are responsible for using Container Registry to store your organization's container images in a designated project. You are tasked with creating a Google Kubernetes Engine (GKE) cluster in a separate project, and you need to ensure that Kubernetes can properly access and download images from the Container Registry. What action should you perform to achieve this?

A. Enable the Kubernetes Engine API in the project where the GKE cluster is being created.

B. Choose the Allow full access to all Cloud APIs option under 'Access scopes' when you create the GKE cluster.

C. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

D. Use Workload Identity Federation to provide access to the images stored in the Container Registry.

Question 45: As a software engineer at a tech company, you're using a developer laptop with the Cloud SDK installed on Ubuntu from the Google Cloud Ubuntu package repository. You want to test your application locally on your laptop with Cloud Datastore. What should you do?

A. Use the gcloud datastore emulator start command to launch the emulator without installing it.

B. Set up a Firebase Realtime Database and use it instead of Cloud Datastore for your application.

C. Create a Cloud Datastore index using gcloud datastore indexes create.

D. Install the cloud-datastore-emulator component using the gcloud components install command.

Question 46: You are working as a cloud engineer in a tech company and have recently installed the Google Cloud CLI on your workstation, setting up the proxy configuration. You are concerned about the potential recording of your proxy credentials in the gcloud CLI logs and want to ensure that they remain secure. How can you prevent your proxy credentials from being logged while using the Google Cloud CLI?

A. Encrypt your proxy credentials using asymmetric encryption and set them in the gcloud CLI by using gcloud config set proxy/username and gcloud config set proxy/password commands.

B. Store your proxy credentials in a JSON file and use the gcloud auth activate-service-account command to enable them in the gcloud CLI.

C. Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

D. Disable logging for the entire gcloud CLI by issuing the command gcloud config set logging/verbosity none.

Question 47: As an IT manager at a rapidly growing software development company, all employees have a Google account and your operations team is responsible for managing numerous instances on Compute Engine. To allow team members only to have administrative access to the servers, your security team wants an efficient deployment of credentials, while also being able to track who accessed each instance. What approach should you adopt?

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

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

C. Generate a new SSH key pair. Give the private key to each member of your team. Restrict the access using firewall rules and grant 'compute.osAdminLogin' role to the Google group corresponding to this team.

D. Use Cloud Identity-Aware Proxy to authenticate and provide administrative access to the servers. Grant the 'compute.osAdminLogin' role to the Google group corresponding to this team.

Question 48: As an accountant at a corporation, you have been assigned the task of migrating invoice documents from on-premises storage to cloud storage. The company has outlined the following requirements for storing these documents:

• Documents must be kept for five years. • Up to five revisions of the same invoice document must be stored, to allow for corrections. • Documents older than 365 days should be moved to lower cost storage tiers.

You have been tasked with adhering to Google-recommended practices in order to minimize operational and development costs. What is the best approach?

A. Enable retention policies on the bucket, use Cloud Functions to manage storage classes of the objects, and utilize Firestore for handling document revisions.

B. Enable retention policies on the bucket, and use Cloud Scheduler to invoke a Cloud Function to move or delete your documents based on their metadata.

C. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

D. Enable lifecycle rules on the bucket and use Cloud Data Transfer Service to move your documents based on their metadata.

Question 49: As a network engineer in a tech company, you are collaborating with a client to set up their software application within a new VPC behind a firewall. The client is particularly concerned about data egress and wants to minimize open egress ports. What should be your approach to achieve this?

A. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

B. Configure a NetworkPeering policy to limit egress traffic to specific subnets.

C. Configure custom routes to block egress traffic on undesired ports.

D. Use a shared VPC to limit egress ports without configuring firewall rules.

Question 50: As a network administrator at a software company, you are responsible for configuring the firewall for the company's infrastructure, which includes two subnets (subnet-a and subnet-b) in the default VPC. The database servers are running in subnet-a, while the application servers and web servers are running in subnet-b. In order to securely set up the firewall and allow only database traffic from application servers to database servers, what should you do?

A. Create a service account sa-app and a network tag app-server. • Add the service account sa-app to the application servers and the network tag app-server to the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-b IP addresses.

B. • Create service accounts sa-app and sa-db. • Associate service account sa-app with the application servers and the service account sa-db with the database

servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

C. • Create a service account sa-app and a network tag db-server. • Associate the service account sa-app with the application servers and the network tag db-server with the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-a IP addresses.

D. Create service accounts sa-app and sa-db. • Associate service account sa-db with the application servers and the service account sa-app with the database servers. • Create an egress firewall rule to allow network traffic from source service account sa-db to target service account sa-app.

Practice Exam 15 Solutions

Solution to Question 1: D

The correct answer is D. Use kubectl config use-context and kubectl config view to review the output.

Explanation:

Option A is incorrect because `gcloud config set compute/zone` and `gcloud config set compute/region` are used to set the default compute zone and region, not review a specific Kubernetes Engine cluster configuration.

Option B is incorrect because `kubectl get nodes` only shows the status of the nodes in the cluster, not the entire configured Kubernetes Engine cluster of an inactive configuration in your gcloud account.

Option C is incorrect because `gcloud container clusters get-credentials` and `gcloud container clusters describe` would first require getting the credentials of the Kubernetes Engine cluster and then describing it. This requires more steps than the desired least number of steps.

Option D is the correct answer because it allows you to switch to the context of the inactive Kubernetes Engine cluster in your gcloud account with `kubectl config use-context` and then view the entire configuration with `kubectl config view`. This achieves the objective of reviewing the configured Kubernetes Engine cluster of an inactive configuration in your gcloud account with the least number of steps.

Solution to Question 2: C

The correct answer is C. Cloud Spanner.

The reason Cloud Spanner is the best fit for this requirement is due to its ability to scale horizontally while maintaining strong consistency, high performance, and broad application usage. Cloud Spanner is a fully managed, relational database service designed for scalability, and it easily accommodates the needs of a growing user base without significant changes to database configuration. It provides high availability, global consistency, and multi-version concurrency control, making it an ideal choice for a global application like the one described in the question.

Option A, Datastore, is a NoSQL document database suited for a specific type of application, but it may not offer the same flexibility and scalability, especially for relational data, as Cloud Spanner. While it can scale horizontally, it is better suited for applications with simpler data models and is not designed specifically to handle global applications. It also does not provide strong consistency.

Option B, Bigtable, is a high-performance NoSQL database built for large analytical and operational workloads. While Bigtable does offer horizontal scalability, it is mostly used for analytical and batch processing workloads and may

not be well-suited for transactional processing typically used in customer relationship management applications. Additionally, it doesn't guarantee strong consistency across multiple regions.

Option D, Cloud Storage, is an object storage solution designed for the storage and retrieval of large, unstructured data like files, rather than structured relational data typically needed for a customer relationship management application. Cloud Storage is a completely different type of database, more oriented towards storing blobs (e.g. images, documents, or backups), and is not ideal for this requirement.

In conclusion, Cloud Spanner is the most appropriate storage solution for the given requirement due to its ability to scale horizontally and accommodate a growing user base while maintaining strong consistency and high performance for a global customer relationship management application.

Solution to Question 3: B

The correct answer is B: Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

The reason why option B is the most effective approach is because it directly addresses the requirements mentioned in the question. An A (address) record is used to map a domain name to an IP address, in this case, the Google Cloud load balancer's IP address. By creating an A record that points mydomain.com to the load balancer's IP address, it ensures that any requests to mydomain.com will be directed to the load balancer.

Next, using CNAME (Canonical Name) records for the subdomains www.mydomain.com and home.mydomain.com allows these subdomains to reference the main domain's A record, so any requests to these subdomains will also be directed to the load balancer. This approach is streamlined and centralizes the management of the load balancer IP address, which is a single point of change in case it needs updating.

Option A is not the correct answer because it suggests creating an SOA (Start of Authority) record, which does not point a domain to an IP address. Instead, the SOA record defines the authoritative DNS server for a domain and contains essential information related to DNS zone administration.

Option C is not the right choice because it proposes creating a PTR (Pointer) record. PTR records are used for reverse DNS lookup, where they help in finding the domain name based on the given IP address. In this case, we want to bind a domain name to an IP address, not the other way around.

Finally, option D is incorrect as it suggests using NS (Name Server) records to point the WWW and HOME subdomains to mydomain.com. NS records are used to define the name servers responsible for handling DNS queries for a

domain or subdomain. They don't direct traffic to an IP address in the same way that A records and CNAME records do.

Therefore, option B is the most effective and appropriate choice to achieve the goal mentioned in the question.

Solution to Question 4: D

The answer is D, and here is the explanation for each option:

A. This option suggests creating a ClusterIP service, which only exposes the application internally within the GKE cluster. Although VPC peering is performed to connect the two VPCs, the Compute Engine instance will not be able to access the GKE application because ClusterIP is not reachable from outside the GKE cluster.

B. This option proposes creating a LoadBalancer service and configuring a Cloud Armor Security Policy. While this configuration would create a load balancer to distribute traffic to the GKE application, relying on Cloud Armor would be excessive and unnecessary, as Cloud Armor is designed for external traffic protection. Also, this setup does not connect the two VPCs, which is needed for communication between the separate networks.

C. Creating a LoadBalancer service and setting the externalTrafficPolicy to Cluster does allow the Compute Engine instance to access the GKE application. However, this configuration exposes the load balancer publicly, posing a security risk and not fulfilling the requirement of minimal effort.

D. This is the correct answer. Creating a LoadBalancer service with the "cloud.google.com/load-balancer-type: Internal" annotation will make an internal load balancer that distributes traffic to the GKE application. Peering the two VPCs will enable the Compute Engine instance in another VPC to access the GKE application. This setup meets both the connectivity and minimal effort requirements, making it the optimal solution.

Solution to Question 5: B

The correct answer is B: Create a custom role by removing delete permissions. Add users to the group, and then add the group to the custom role.

Explanation: - Option B is the best solution as it follows Google-recommended practices for managing permissions. Creating a custom role and specifically removing delete permissions helps prevent accidental deletion of datasets. By adding the users to a group and then assigning the custom role to that group, you can easily manage users and their permissions, thereby ensuring security and ease of maintainability.

Why other options will not work:

- Option A: Creating a custom role and adding users directly is feasible, but it is less flexible and not considered a best practice for managing permissions. Adding and removing users to/from the role would become

cumbersome, making it harder for administrators to manage access to the organization's resources.

- Option C: The roles/bigquery.dataEditor role allows users to create, update, and delete datasets and tables. Adding users to this role without any modification will still allow them to delete datasets, which is not the intended outcome in this scenario.
- Option D: Adding users to the roles/bigquery.viewer role would grant them read-only access to datasets, which is too restrictive for data analysts. They would not have the ability to create and edit datasets and tables, which is necessary for their job functions. Therefore, this option does not meet the requirements of the question.

Solution to Question 6: A

The correct answer is A. Add the user to roles/iam.serviceAccountAdmin role.

Explanation:

A. Add the user to roles/iam.serviceAccountAdmin role - This role is the most appropriate choice for the given requirement as it provides permissions to create, manage, and delete service accounts. The role's permissions enable the dedicated team member to fulfill their responsibilities without being granted any unnecessary permissions that could pose a security risk or violate the principle of least privilege.

B. Add the user to roles/iam.serviceAccountAuditor role - This role is not suitable for the given requirement as it only provides permissions to view service account properties and details, but not to create, manage, or delete service accounts. Assigning this role would not enable the team member to fulfill their responsibilities.

C. Add the user to roles/iam.serviceAccountOperator role - Although this role provides permissions to act as a service account, it does not grant the necessary permissions to create, manage, or delete service accounts. This role would be inadequate for the team member to complete their assigned task.

D. Add the user to roles/iam.serviceAccountMaintenanceManager role - This role does not exist within the Google Cloud Platform role list. As a result, assigning this role to the team member would not be possible or fulfill the given requirement.

In conclusion, option A (roles/iam.serviceAccountAdmin) is the best choice to enable the team member to adequately create and manage service accounts for Google Cloud projects with minimal permissions. The other options either provide insufficient permissions or do not exist.

Solution to Question 7: C

The correct answer is C: 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

Here's why the other options will not work and why C is the best choice:

Option A: Removing permissions for the GKE container to write logs to Stackdriver Logging only restricts the container's access. However, it doesn't disable the logs efficiently, and it might cause issues with other services that require the container to have logging permissions.

Option B: Setting log-based metrics to zero for the GKE container will not disable the logs. Log-based metrics are used to create custom metrics that are derived from the logs, but modifying them will not impact the logging process itself.

Option D: Setting the GKE container's logging level to "none" using gcloud command-line tool could have been a viable option, but it requires more work compared to Option C. Using the command-line tool requires the execution of specific commands and possibly dealing with various parameters. This makes Option C a more efficient and swift solution.

Option C is the correct answer because disabling the log source for the GKE container resource in Stackdriver Logging stops logging for the specified container, which will reduce costs and logging volume efficiently. It's a more direct approach compared to other options.

Solution to Question 8: B

The correct answer is B. Assign the finance team the Billing Account User role on the billing account and the Project Billing Manager role on the organization. By doing so, the finance team will have the required access to link projects to billing accounts without having additional permissions to change project settings. The Billing Account User role will let them view and manage billing accounts, while the Project Billing Manager role will enable them to link and unlink billing accounts to projects within the organization.

Reasons why other options will not work:

A. Assign the engineering team only the Billing Account User role on the billing account. - This option does not fulfill the requirement of restricting the engineering team from linking projects to billing accounts, as it grants them access to view and manage billing accounts. Additionally, it does not mention any action taken for the finance team.

C. Assign the finance team the Project Viewer role on the organization and the Billing Account User role on the billing account. - Although the finance team can view projects within the organization with the Project Viewer role, it does not provide them with the necessary permissions to link and unlink billing accounts to projects. The Billing Account User role alone will not be sufficient, as it does not grant them the ability to manage project billing settings.

D. Give the finance team only the Compute Network User role on the organization. - This option is not relevant to the problem, as the Compute Network User role is focused on managing Compute Networks and not billing accounts

or project billing settings. It does not provide the finance team with the needed permissions to link projects to billing accounts.

Solution to Question 9: A

The correct answer is A: Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

The reason this is the best solution is that gsutil, a command line tool provided by Google, natively supports synchronizing data between local storage and Cloud Storage. By creating a script with the gsutil command, you can ensure that new and modified files are automatically uploaded to Cloud Storage, keeping both storage locations in sync. Scheduling the script as a cron job allows you to automate the process, thereby ensuring continuous and efficient synchronization of the medical images to the Cloud Storage.

The other options are not suitable for the given requirements:

B. Deploying an App Engine service to sync the medical images from the on-premises storage to Cloud Storage using Cloud Endpoints.

This option is not suitable because App Engine services generally run in the cloud, and configuring such services to access on-premises systems involves complex networking and security configurations. Additionally, creating an App Engine service adds an unnecessary layer of complexity, while gsutil can directly interact with Cloud Storage.

C. Use the Cloud Vision API to process and store the medical images as JSON objects in Cloud Storage.

This option is not relevant to the requirements because Cloud Vision API focuses on image analysis and processing, not on transferring and archiving files. Moreover, storing medical images as JSON objects is an inefficient and unconventional format for archival purposes and might not meet storage and retrieval requirements.

D. Create a Data Fusion pipeline to transfer medical images from the on-premises storage to Cloud Storage on a scheduled interval.

Data Fusion is intended for large-scale data integration and transformation, specifically for Big Data processes. It is not designed for the requirements of transferring medical images from on-premises storage to Cloud Storage. Using Data Fusion for this purpose would be overkill and inefficient, incurring additional cost and maintenance concerns, while gsutil provides a simple and direct solution.

Solution to Question 10: C

The correct answer is C. Upload the data to Cloud Storage using the gsutil command line tool. Here's why the other options are not suitable:

Option A: Cloud Firestore is a NoSQL database mainly focused on structured data. Although it is part of the Google Cloud Platform, it is not suitable for handling the vast amount of unstructured data that needs to be processed with ETL transformations. The Firestore module provided in the Google Cloud Client Libraries is also geared towards application development, and not ETL use cases.

Option B: Cloud SQL is a fully managed relational database service, which is not ideal for handling the unstructured data required for this scenario. The import function in the console would not be able to properly manage the diverse file types and perform efficient ETL transformations, as its primary purpose is to handle structured data.

Option D: Cloud Datastore is another NoSQL database, similar to Cloud Firestore but primarily focused on high scalability. While it is part of the Google Cloud Platform, it is not suitable for handling large amounts of unstructured data that needs to be processed with ETL transformations. The gcloud command line tool is geared towards managing the Google Cloud Platform resources and not an appropriate choice for this scenario.

Option C is the right choice because Google Cloud Storage is designed for storing large amounts of unstructured data and supports various file formats, making it a suitable storage solution for ETL purposes. The gsutil command line tool is specifically created for uploading, downloading, and managing Cloud Storage data, which would be convenient and effective for a data engineer working with vast amounts of unstructured data from various sources. Uploading the data to Cloud Storage allows the Dataflow job to process it efficiently, as it has built-in support for reading data from Cloud Storage and performing ETL transformations.

Solution to Question 11: B

The correct answer is B, which involves viewing Data Access audit logs in Cloud Logging and searching for the user's email as the principal.

Option B is the most appropriate method because Data Access audit logs specifically store information about Google Cloud resources being read, updated, or deleted. By searching for the user's email as the principal, you can determine if the former employee accessed any sensitive customer data during the two-week period.

Option A is not ideal because Admin Activity logs primarily deal with administrative actions, such as user modifications and permissions changes. While these logs also contain information about accessed resources, they do not provide the granular detail found in Data Access audit logs.

Option C is incorrect because System Event Logs mainly record changes to system configurations or operation status. These logs are not concerned with data access and wouldn't help in identifying if the user accessed sensitive customer data.

Option D is also incorrect because it suggests searching for the service account associated with the user, rather than the user's email. Service accounts are used for access control for applications and services, not individuals. By searching for the service account instead of the former employee's email, you would not get accurate and relevant data access information.

In summary, to determine whether the former employee accessed sensitive customer data, you should proceed with Option B, viewing Data Access audit logs in Cloud Logging, and searching for the user's email as the principal.

Solution to Question 12: C

The best approach to take in this scenario is option C, and here's why:

Option C:

1. In the Cloud Console, go to the Compute Engine Disks page and select your instance's disk. 2. In the Snapshot Schedule section, select Create Schedule and configure the following parameters: - Schedule frequency: Daily - Start time: 1:00 AM - 2:00 AM - Autodelete snapshots after: 30 days

This is the recommended solution because it uses the functionality provided by Google Cloud Platform (Compute Engine) directly, with the least number of services involved. Moreover, it doesn't require any management overhead and is the most straightforward solution.

Using snapshot scheduling, you can create daily snapshots of the instance disk and set the retention period (autodelete) to exactly 30 days. This ensures that backups are taken daily and retained only for the required period.

Now, let's look at the other options and why they are not suitable:

Option A: 1. Create a Dataflow job that backs up the instance's disk to BigQuery daily. 2. Configure the Dataflow job to delete the backups older than 30 days.

This is not the recommended solution, as it adds unnecessary complexity by involving additional services such as Dataflow and BigQuery. The process will require extra data processing and management overhead, making it less efficient compared to option C.

Option B: 5. Update your instances' metadata to add the following value: backup-frequency: daily backup-retention: 30

This option is invalid because updating the instance metadata with these values does not affect any backup processes. The provided metadata values are not recognized by the Compute Engine service.

Option D: 1. Update your instances' metadata to add the following value: snapshot-schedule: 0 1 * * * 2. Update your instances' metadata to add the following value: snapshot-retention: 30

Similar to option B, this option is also not recommended because the values provided in the instance metadata are not recognized by the Compute Engine service and will not affect any backup processes.

In conclusion, option C is the most suitable approach as it uses the built-in snapshot scheduling feature within Compute Engine, minimizing the management overhead, and requiring the least number of services involved.

Solution to Question 13: A

The answer should be A. When creating the VM, use machine type n1-standard-96, and here's why:

A. Using an n1-standard-96 machine type ensures that the virtual machine will have 96 vCPUs available, which is the exact requirement of the on-premises application. This allows for a seamless and efficient migration to Google Cloud Platform, ensuring that the application operates smoothly in a similar environment.

B. Opting for a machine type with 48 vCPUs and then increasing the number of VM instances to 2 does not guarantee the same efficient functionality as with a single 96 vCPU machine. This is due to potential communication, data sharing, and consistency issues that could arise between the instances, which were not present in the on-premises environment.

C. Creating the VM with default settings and attempting to modify the running instance to have 96 vCPUs using gcloud is not an efficient approach. This method requires extra work, and VMs can't be modified on-the-fly to increase vCPU count. You would need to either create a new VM with the necessary resources or stop and resize the existing VM, leading to downtime and unnecessary complexity.

D. Using Cloud Functions to split the workload into smaller tasks and deploying to a serverless environment might not be a suitable option due to the crucial nature of the application. Rewriting the application to fit into a serverless model may require significant development effort and could introduce additional latency and architectural complexities. Furthermore, not all applications can be easily modified to utilize serverless architectures, which might be the case for this on-premises application.

In conclusion, choosing Option A, creating a VM with an n1-standard-96 machine type, ensures that the application has the required 96 vCPUs to run efficiently and provides a similar environment to its on-premises counterpart, making it the best option.

Solution to Question 14: B

The correct answer is B: Using the GCP Console, filter the Activity log to view the information.

Explanation: As an IT specialist, your task is to audit a specific employee's

activities while taking the fewest steps. Google Cloud Platform (GCP) Console enables you to filter and view the Activity log, allowing you to monitor the actions taken by the employee regarding the addition of metadata labels and viewing files in the Cloud Storage buckets. Filtering the Activity log will directly provide the needed information, ensuring data security while minimizing time and effort.

Reasons why other options will not work:

A. Use Cloud Pub/Sub to access the logs and filter the activity you need to verify: While Cloud Pub/Sub facilitates real-time messaging and can be used for accessing logs, it is not the most efficient solution for this specific scenario. Filtering the Activity log directly through GCP Console is quicker and more straightforward, requiring fewer steps.

C. Create a trace in Cloud Monitoring to view the information: Cloud Monitoring is designed to monitor and manage the performance, availability, and health of the applications and services, not necessarily to audit user activities. Creating a trace in Cloud Monitoring would not directly address the audit requirement for the specific employee's actions in Cloud Storage buckets.

D. Create a trace in Stackdriver to view the information: Stackdriver, now known as Operations suite, is primarily for infrastructure and application monitoring. It is not the most suitable solution for this scenario, where you need to check user activities on Cloud Storage. Filtering the Activity log in GCP Console provides a more direct option to audit the required employee actions.

Solution to Question 15: B

The correct answer is B, "Install and configure the Cloud Logging Agent and view the logs from Cloud Logging," and here's why the other options will not work:

A. Configure Cloud Pub/Sub to receive logs and analyze them externally. Cloud Pub/Sub is a messaging service which can send and receive messages between independent applications, but it won't automatically collect logs from the Compute Engine instance. It requires manual configuration to send logs to Pub/Sub and another external service to analyze them, which is more complex than option B.

B. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging. This is the recommended approach because, by installing the Cloud Logging Agent, it will automatically collect logs from the Compute Engine instance. You can then easily view and analyze them through Google Cloud's Cloud Logging platform, which provides various tools to diagnose the issue.

C. Create a Google Cloud Function to process and analyze the application logs. Cloud Functions are designed for event-driven scenarios. In this case, you would need extra effort to create a trigger and manually collect logs for the Cloud

Function to process them. This solution, although possible, is more complex and over-engineered compared to simply using Cloud Logging.

D. Use the command `gcloud beta logging read` to connect to the instance and read the application logs. This command is deprecated, and gcloud no longer supports it. Moreover, this would only provide one-time access to the logs, and would not allow for easy ongoing log monitoring and management.

In summary, the best option to diagnose the issue is to install and configure the Cloud Logging Agent (option B) to view logs in real-time and access advanced analysis tools provided by the Cloud Logging platform.

Solution to Question 16: B

The correct approach to take in this situation is B. Invite the user to transfer their existing account.

Option B is the best solution because it aligns with Google's best practices for managing multiple Google accounts. Inviting users to transfer their existing accounts allows them to merge their personal and work-related Google services, thereby minimizing potential conflicts. It streamlines the account management process and ensures that all users have access to work-related resources under a single account.

Option A, inviting the user to use an email alias, is not ideal because it does not resolve account conflicts. Email aliases can create confusion for users and make account management more complex. Additionally, an email alias does not grant the user access to Cloud Identity or any other Google Workspace services that they may require for their job.

Option C, creating a new Google account for each user, is not appropriate as it does not adhere to Google's best practices for managing multiple accounts. Creating separate accounts for work and personal use can contribute to inefficiencies when switching between accounts and cause potential conflicts between the two.

Option D, asking users to create a separate Google Workspace account and migrate their data, tends to be a time-consuming process and does not comply with Google's best practices for managing multiple accounts. This process would require users to manually migrate their data, which can lead to mistakes and incomplete transfers.

In conclusion, option B is the most effective and practical solution that aligns with Google's best practices, reduces conflicts between accounts, and maintains a smooth account management experience for users.

Solution to Question 17: C

The correct answer is C - Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

Here's why the other options will not work:

Option A: Open the BigQuery console, and check audit logs for Cloud Spanner IAM roles. BigQuery is a separate Google Cloud Platform service primarily used for analyzing large datasets using SQL-like queries. It is not the appropriate place to review audit logs for Cloud Spanner IAM roles since it focuses on data analytics rather than logging and monitoring.

Option B: Open the Cloud Spanner console to review configurations. The Cloud Spanner console can be used for managing and configuring Cloud Spanner instances, databases, and tables. It does not provide detailed information about when users were added to IAM roles; this information is tracked in the admin activity logs, which are accessible through Stackdriver Logging.

Option D: Go to the Stackdriver Monitoring console and review information for Cloud Spanner. Stackdriver Monitoring provides real-time performance monitoring and alerting for Google Cloud Platform services, such as Cloud Spanner. While it gives insights on performance and resource utilization, it does not store admin activity logs needed for determining when users were added to IAM roles.

In conclusion, the best approach for determining when users were added to Cloud Spanner IAM roles is by going to the Stackdriver Logging console, reviewing admin activity logs, and filtering them for Cloud Spanner IAM roles.

Solution to Question 18: B

The correct answer is B: Use gcloud to create a key file for the service account with appropriate permissions.

Explanation: To enable authentication to the Google Cloud Platform APIs from your on-premises environment, you should use a key file for the service account that has appropriate permissions. A key file contains the credentials necessary to authenticate API calls made by your application. By creating a key file for the service account which already has access to AutoML, you can ensure secure connections between your on-premises application and the Google Cloud Platform.

Why other options will not work:

A. Configure a Compute Engine instance with appropriate permissions and connect your on-premises application to it - This option is not effective since it doesn't address the authentication part between your on-premises application and GCP services. You would need a key file with the appropriate permissions for successful authentication.

C. Create a user-managed service account with no permissions and use it for on-premises authentication - This option won't work because it suggests using a service account with no permissions. To allow your on-premises application to access GCP services like AutoML, you need a service account with the appropriate permissions.

D. Use service account credentials in your on-premises application - This option is incomplete because it doesn't mention how to obtain and utilize the service

account credentials. The key file for the service account can provide the necessary credentials. Therefore, you need to create a key file for the service account first (option B).

Solution to Question 19: B

The correct answer is B. Configure an External Network load balancer in front of the application servers.

Explanation: An external load balancer is designed to distribute incoming traffic from the internet across multiple VMs in a scalable way. Since the multiplayer game is hosted on Google Cloud and gamers will be connecting to the services over the internet through their phones, an external network load balancer is required. Moreover, the game sends UDP packets to update the servers about the players' actions, and the external network load balancer can handle such UDP traffic effectively.

A. Utilize Cloud Armor with the application servers to distribute traffic. - Cloud Armor is not the right option as it primarily provides security features such as DDoS protection and application defense. Although Cloud Armor works with HTTP(S) Load Balancing, it's not explicitly designed for distributing traffic across VMs in a gaming scenario that uses UDP packets.

C. Configure an Internal TCP/UDP load balancer in front of the application servers. - Internal TCP/UDP load balancers are designed for load balancing internal traffic within a Google Cloud Virtual Private Cloud (VPC), not for publicly accessible services like a multiplayer game over the internet. Since gamers connect to the game using their phones over the internet, an internal load balancer is not suitable for this use case.

D. Configure an Internal UDP load balancer in front of the application servers. - Similar to option C, this option focuses on internal load balancing for UDP traffic within a VPC. It's not designed for handling external traffic from the internet such as gamers connecting via their phones.

In conclusion, the appropriate solution to expose multiple VMs through a single IP address for the mobile multiplayer game is to configure an External Network load balancer in front of the application servers, which is option B.

Solution to Question 20: A

The correct answer is A, as it allows us to manage multiple GCP accounts efficiently and in an organized manner, unlike the other options. Here's a breakdown of why A is the best choice and the other options are not suitable:

A. Create two configurations using `gcloud config configurations create [NAME]`. Run `gcloud config configurations activate [NAME]` to switch between accounts when running the commands to start the Compute Engine instances. This is the correct choice since creating two different configurations, one for each account, helps separately manage each account. Activating the

required configurations as needed ensures that the correct account and corresponding settings are in use while deploying new Compute Engine instances.

B. Create one configuration using `gcloud config configurations create [NAME]`. Run `gcloud config configurations activate [NAME]` to switch between accounts when running the commands to start the Compute Engine instances. This option is not suitable because creating only one configuration for managing both accounts will overcomplicate things. It would require constant editing and updating of project, region, and zone settings when switching between accounts, which is not efficient.

C. Create a configuration file for each account and use the –configuration flag when running gcloud command to start Compute Engine instances. This option is not ideal because while it might seem feasible to use separate configuration files, using the –configuration flag every time increases complexity in running commands. Moreover, it can lead to errors if the flag is forgotten or misused. It is better to activate a configuration before running any Compute Engine-related commands like in option A.

D. Activate two configurations using `gcloud configurations activate [NAME]`. Run `gcloud configurations list` to start the Compute Engine instances. This option is incorrect because it has two flaws. First, there is no command called `gcloud configurations activate [NAME]`. The correct command is `gcloud config configurations activate [NAME]`. Secondly, running `gcloud configurations list` will not start any Compute Engine instances. It just lists the existing configurations. For starting Compute Engine instances, specific gcloud commands need to be executed after activating the appropriate configurations.

Solution to Question 21: A

The correct answer is A, and here's why:

A: "Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods." This is the most appropriate course of action because creating a new node pool in the existing GKE cluster allows you to have a mixed cluster with different machine types. In this case, you'll be able to use both n1-standard-2 and n2-highmem-16 nodes. This way, your additional pods can run on the n2-highmem-16 nodes while the existing application continues to operate on the n1-standard-2 nodes, ensuring no downtime during the deployment process.

B: "Create a new cluster with n2-highmem-16 nodes. Redeploy the pods and delete the old cluster." This is not the most appropriate course of action since it will create downtime while your application is moved from one cluster to another. Also, it's neither efficient nor cost-effective as you'll need to manage and maintain separate clusters, despite both running the same application.

C: "Create a new cluster with both n1-standard-2 and n2-highmem-16 nodes. Redeploy the pods and delete the old cluster." This option can also lead to downtime when redeploying the pods and deleting the old cluster. You don't

need to create a new cluster as you can achieve the same by creating a new node pool in the existing cluster which can handle mixed machine types.

D: "Use Deployment Manager to change the node type to n2-highmem-16 and redeploy the services." This alternative isn't appropriate because it doesn't account for the need to maintain existing application functionality on n1-standard-2 nodes and will also likely cause downtime during the switch to n2-highmem-16 nodes due to service redeployment.

Given all these reasons, the most appropriate course of action is option A.

Solution to Question 22: A

The correct answer is A. Use Cloud Spanner for data storage.

Explanation:

Cloud Spanner is a horizontally-scalable, globally-distributed database service built on Google Cloud Platform. It offers strong consistency and high availability, making it an ideal choice for mission-critical applications requiring low-latency, like a financial trading platform.

Here's why the other options will not work:

B. Use Firestore for data storage.

Firestore is a NoSQL document-based database, making it suitable for applications that require semi-structured data storage. However, the question states that the data must be stored and queried using a relational structure, which Firestore does not support.

C. Use Cloud Filestore for data storage.

Cloud Filestore is a managed file storage service designed for applications that require a shared file system to store and access data. However, Filestore doesn't provide the relational querying and global consistency features required for a financial trading platform.

D. Use Cloud Storage for data storage.

Cloud Storage is an object storage service ideal for storing and serving unstructured data, such as images, videos, or documents. It is not designed for use with relational data or for ensuring the exact identical state of data worldwide.

In conclusion, using Cloud Spanner for data storage will provide the necessary relational data structure and global consistency required for a financial trading platform, while minimizing latency for end users.

Solution to Question 23: C

The correct answer is C. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

Explanation:

Option A: This command adds an IAM policy binding on the entire project instead of the specific Cloud Spanner instance. Furthermore, this command would work if you wanted to add all members of a group to the role, but in this case, the manager has asked to grant permissions to only three team members, not an entire group.

Option B: This command also adds an IAM policy binding on the entire project and not the specific Cloud Spanner instance. Additionally, it only adds one user to the role, which is not practical when you need to add multiple users. Managing individual users for each policy binding can become difficult as the number of users grows.

Option C: This is the correct approach because it ensures that you are granting permissions on the required Cloud Spanner instance. By creating a new group and adding the three team members to the group, you can manage their access collectively. Then, by adding the group to the role, you grant the necessary permissions of editing and viewing for the specified Cloud Spanner instance.

Option D: This command adds an IAM policy binding on the entire project instead of the specific Cloud Spanner instance. Furthermore, it uses the roles/spanner.databaseAdmin role, which grants database administration permissions rather than the required editing and viewing permissions. Using this role for the given scenario would provide more permissions than necessary.

Solution to Question 24: D

The correct answer is D, which involves creating a configuration for each project you need to manage and activating the appropriate configuration when you work with each of your assigned Google Cloud projects. This approach allows for efficient management of multiple projects using the Google Cloud SDK CLI without the need to repeatedly update environment variables or switch between different terminal sessions. It also keeps the settings for each project separate and organized.

Option A is not ideal because creating separate terminal sessions for each project can quickly become disorganized and confusing, especially when dealing with a large number of projects. Moreover, updating the environment variable for the project ID in each terminal session can be time-consuming and prone to errors.

Option B is also not efficient because it requires you to constantly update the configuration values when working with non-default projects. This can lead to confusion and errors, especially if you need to switch between multiple projects frequently.

Option C is not a suitable solution because creating an App Engine application for every project is unnecessary and inefficient. App Engine applications do not directly provide the desired functionality of managing multiple projects at once. Moreover, the gcloud app commands are intended for managing App Engine resources rather than handling multiple Google Cloud projects simultaneously.

In conclusion, Option D is the best approach for managing multiple Google Cloud projects efficiently using the Google Cloud SDK CLI. By creating a separate configuration for each project and activating the appropriate one when needed, you can easily switch between different projects and keep your environment organized and error-free.

Solution to Question 25: D

The correct answer should be D, SSL Proxy Load Balancer.

Explanation: D. SSL Proxy Load Balancer is designed specifically for efficiently distributing incoming SSL-encrypted TCP traffic on port 443, making it the best option for the given scenario. It minimizes latency by providing regional load balancing and managing SSL connections to the backend instances, allowing the clients to connect faster. It also supports HTTP/2 and QUIC protocols, ensuring optimal performance for end users.

Reasons why other options will not work: A. NAT Gateway Load Balancer is designed for translating internal IP addresses to external ones, typically for outbound internet access. It is not an ideal solution for minimizing latency for incoming SSL-encrypted TCP traffic from clients worldwide.

B. Cloud VPN Load Balancer is a solution for securely connecting multiple networks over the public internet. This option is not focused on minimizing latency for SSL-encrypted TCP traffic or distributing application loads globally.

C. Internal HTTP(S) Load Balancer is designed for distributing traffic among instances within a single VPC (virtual private cloud) network. This solution would not work well for receiving traffic from clients worldwide efficiently, as it doesn't provide regional or global load distribution functionality and is meant for internal use within a VPC network.

Solution to Question 26: C

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

Here is the explanation for why the answer should be C, and why other options will not work:

A. Create a service account and add it to the IAM role 'storage.buckets.get' for that bucket. This option will not work because the 'storage.buckets.get' role only allows for reading the metadata from the bucket, not writing any data into it. The task explicitly requires the ability to write data to the bucket, so this role is not sufficient.

B. Create a user account and add it to the IAM role 'storage.objectCreator' for that bucket. This option will not work because, in a professional environment, it is not recommended to use individual user accounts for managing permissions on cloud resources. Instead, Google recommends using service accounts, which provide better access control and security.

C. Create a service account and add it to the IAM role 'storage.objectCreator' for that bucket. (Correct answer) This option follows Google-recommended practices for setting up permissions in a tech environment: using a service account instead of a user account. The 'storage.objectCreator' role allows the Compute Engine instances to write data to the specified Cloud Storage bucket, which is the required task.

D. Create a user account and add it to the IAM role 'storage.objectAdmin' for that bucket. This option is not recommended because it involves using a user account to manage permissions, which does not follow best practices. Furthermore, the 'storage.objectAdmin' role grants more access than what is necessary for the task, as it provides full control over the objects in the bucket. The 'storage.objectCreator' role should be used instead to only grant writing permissions, as required by the task.

Solution to Question 27: A

The correct answer is A. Use gcloud iam roles copy and specify the production project as the destination project. This is because it allows you to copy the same IAM roles from the development project to the new production project in the fewest possible steps, using a single command, ensuring that the roles are identical. This streamlines the process.

Option B is incorrect because it suggests copying the IAM roles to the development project itself, rather than the new production project. This would not result in having the necessary IAM roles in the production project.

Option C is incorrect because manually creating a role and selecting all applicable permissions would take longer and may result in errors. The process would not be as efficient as using gcloud iam roles copy, which ensures identical roles between projects.

Option D is incorrect because gsutil iam setaclexamples is not a real command in Google Cloud Platform, and it doesn't specifically address copying IAM roles between projects.

Solution to Question 28: A

The correct answer is A: "1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work." This course of action enables a swift migration to Google Cloud, minimizes support efforts, and provides the required isolated development environments for the development teams. The Cloud Marketplace offers preconfigured Cassandra images that can be quickly launched, saving time and reducing setup complexity.

Option B is incorrect because setting up managed instance groups and configuring VPC Network Peering for each team would require significant efforts and increased maintenance. Additionally, it would increase complexity and would not achieve the goal of a swift migration.

Option C is also incorrect because deploying multiple Cassandra instances on Cloud Run using Docker containers would add unnecessary overhead and additional work in managing and configuring the containers. Moreover, Cloud Run is designed for stateless applications, while Cassandra is a stateful application, making this option unsuitable for the requirement.

Option D is inappropriate because replacing Cassandra with Cloud Datastore would introduce potential inconsistencies and further migrations down the line. Using a different database system would require developers to adjust their applications to work with the new system, which is neither swift nor minimizes support efforts. The goal is to maintain the use of Cassandra while moving to Google Cloud, so this option does not fulfill the requirement.

Solution to Question 29: A

The correct answer is A: Use Cloud Spanner to store user data mapped to the game statistics.

Here's why option A is the best choice:

Cloud Spanner is a globally distributed, scalable, and fully managed relational database service provided by Google Cloud Platform, built for strong consistency and high availability. It allows you to deploy a global database that is automatically replicated across multiple regions, ensuring optimal gaming performance for users all over the world without increasing management complexity.

Option B is not ideal because Cloud Redis (in-memory key-value store) is primarily designed for caching and is not intended to be a primary data store for performance-critical applications. Additionally, regional replication is not the same as global replication, which means that you might still experience latency across regions.

Option C is not suitable because Bigtable (a wide-column store) does not provide the strong consistency guarantees needed for a multi-player gaming application. Additionally, partitioning the database by username does not ensure optimal performance for users located around the world.

Option D is not the optimal solution because BigQuery is an analytical data warehouse designed for running complex queries and not suitable for real-time game statistics storage. Additionally, using Redis on Memorystore as a front-end cache does not provide global consistency, as the cache needs to be maintained and can become a bottleneck for the application.

Solution to Question 30: D

The correct answer is D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

Here's why the other options will not work:

Option A: Create a new GCP project and add a Compute Engine instance in the asia-northeast1 region, then migrate the App Engine application to it. This option is incorrect because Compute Engine and App Engine are different services within GCP. While Compute Engine provides infrastructure as a service (IaaS) with virtual machines running your code, App Engine is a platform as a service (PaaS) that manages the infrastructure for you, allowing you to focus on the application code. Migrating an App Engine application to a Compute Engine instance would require significant changes in the architecture. Moreover, the question explicitly states that the application is deployed on an App Engine application.

Option B: Use a custom domain and map it to the asia-northeast1 region for the existing App Engine application. This option does not effectively change the region where the application is served. Mapping a custom domain will change the URL of your application, but it will still be hosted in the us-central region.

Option C: Change the region property setting in the existing App. Changing the region property setting in the existing App Engine application from us-central to asia-northeast1 might seem like a valid option, but in reality, the region assigned to an App Engine application cannot be changed after the project is created.

Hence, option D is the best way to serve the App Engine application from the asia-northeast1 region. Creating a new GCP project allows you to specify the desired region when deploying a new App Engine application within this project.

Solution to Question 31: B

The correct answer is B. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

The reason for choosing option B is that Google App Engine is a fully managed platform specifically designed for deploying, managing, and scaling web applications. The application updates can be deployed as separate versions of the same service. Google App Engine's traffic splitting feature allows diverting a small percentage of real user traffic to the new version while the majority of users access the stable version.

Option A is not suitable because it suggests creating a new service for each update. This approach would complicate application management and is unnecessary when using App Engine's versioning feature, which allows running multiple versions of the same service.

Option C is not the best choice because it involves deploying the application on Compute Engine using custom images and managed instance groups. While this approach can work for scaling applications, it doesn't offer the same level of simplicity and ease of management as App Engine, which provides built-in traffic splitting features for versioning.

Option D is not appropriate because it uses Kubernetes Engine and State-

fulSets for updates. Although Kubernetes is a powerful container orchestration platform, this approach is more complex and requires managing Kubernetes resources, such as Ingress and StatefulSets, instead of leveraging App Engine's straightforward built-in traffic splitting and versioning features. Moreover, StatefulSets are intended to run stateful applications, like databases, rather than a standard web application.

Solution to Question 32: B

The correct answer is B. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

Explanation: By reserving the IP address 10.0.3.21 and assigning it as a static internal IP address to the licensing server, the application will be able to access the server with the desired IP address without requiring any configuration changes. This allows the application to perform its functions without any interruptions or additional adjustments.

Reasons why other options will not work:

Option A: Configuring the licensing server to listen on all IP addresses in the 10.0.3.0/24 subnet and assigning a different static internal IP address to the server does not fulfill the requirement of the application to access the licensing server using the IP 10.0.3.21 specifically. This option might lead to issues such as IP conflicts and potentially affect the software's functionality.

Option C: Configuring the application to use a different IP address requires configuration changes, which is contrary to the problem statement. Although reserving a static internal IP address using gcloud and assigning it to the licensing server is a good practice, changing the application's configuration would create unnecessary work and complications.

Option D: Creating a custom routing rule to route traffic destined for 10.0.3.21 to the licensing server's actual IP address is an unnecessarily complex solution for this problem, as it involves creating routing tables and updating them whenever there are network changes. This could make the system more challenging to manage and less efficient compared to directly assigning the desired IP address (10.0.3.21) to the licensing server as a static internal IP, as described in option B.

Solution to Question 33: D

The correct answer is D. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

Explanation:

Option D is the most appropriate approach for consolidating and visualizing cost data from multiple Google Cloud projects with separate billing accounts. By exporting the billing data to BigQuery, it allows you to organize, analyze, and combine data from different billing accounts effectively. With the integration

of Data Studio, you will be able to create custom visualizations and reports to efficiently forecast expenses across your projects. Moreover, this method ensures that new cost data is promptly included, providing an effective way to monitor your costs in real-time.

Option A is not suitable because the Reports view in the Cloud Billing Console only allows you to view cost information for a single billing account at a time, making it difficult to consolidate data across multiple accounts or projects efficiently.

Option B would not be practical since creating individual billing report alerts in each project using Cloud Monitoring would lead to numerous alerts that would need to be managed separately. This approach would not consolidate cost data for better visibility and efficient forecasting.

Option C is not the right choice because Stackdriver Monitoring (now called Google Cloud Monitoring) does not natively display cost data for all projects on a single dashboard. While Cloud Monitoring can help you monitor the performance of various Google Cloud services, it does not focus on consolidating billing data from multiple projects and accounts.

Therefore, the best approach is to configure Billing Data Export to BigQuery and visualize the data in Data Studio (Option D), as it provides a consolidated view of all cost data, making it easier for you to monitor and forecast expenses.

Solution to Question 34: D

The correct answer is D. 10.0.0.0/8. Here's why:

The company requires the subnet's range to be as large as possible. Therefore, you should select the IP address range which contains the maximum potential addresses.

Looking at the options provided:

A. 203.0.113.0/24: This IP address range belongs to the class C network. The /24 subnet mask provides 256 unique IP addresses (8 bits for host addresses).

B. 192.168.0.0/16: This IP address range belongs to the class B private network. The /16 subnet mask provides 65,536 unique IP addresses (16 bits for host addresses).

C. 169.254.0.0/16: This IP address range is reserved for Automatic Private IP Addressing (APIPA) space. It is not valid for the custom VPC as it is meant for local link communication in cases of DHCP configuration issues.

D. 10.0.0.0/8: This IP address range is a class A private network. The /8 subnet mask provides 16,777,216 unique IP addresses (24 bits for host addresses), which is the largest range among the provided options.

Comparing these options, it is clear that option D (10.0.0.0/8) offers the largest IP address range, making it the most suitable choice for the company's require-

ments. The other options don't provide as many unique IP addresses and are not suitable for a rapidly growing tech company that needs a large subnet range.

Solution to Question 35: B

The correct answer is B: Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

Explanation for B: Adding a new GPU-enabled node pool to the GKE cluster is the most efficient and cost-effective solution. This action allows the ML team to get their required resources without impacting the rest of the teams working on the same GKE cluster. The cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector ensures that the ML team's workload is scheduled only on nodes with the necessary GPU resources. This minimizes both effort and cost as only specific nodes in the pool will have GPUs, and other teams can continue using non-GPU nodes.

Explanation for why A will not work: TPUs (Tensor Processing Units) are different from GPUs (Graphics Processing Units). While TPUs can deliver similar or sometimes better performance than GPUs, they are optimized for different workloads, specifically TensorFlow-based machine learning. Forcing the ML team to shift to TPUs might require significant changes to their ML workflows. Additionally, TPUs are not directly available as a GKE node pool option.

Explanation for why C will not work: Creating a separate Kubernetes cluster on top of Compute Engine will require additional management effort compared to adding a new node pool to the existing GKE cluster. This approach also makes it more difficult to manage resources between different teams within the company, and it may lead to overprovisioning and increased costs. Using GKE instead provides managed Kubernetes, reducing maintenance workload and offering better integration with other Google Cloud services.

Explanation for why D will not work: Recreating all the nodes of the GKE cluster to enable GPUs on all of them is neither efficient nor cost-effective. It will ensure that all teams use GPU-enabled nodes, regardless of whether they need those resources. As a result, this leads to significant increases in the cost of running the GKE cluster. In addition, updating all nodes in the cluster can cause disruptions to other teams' workloads. This option is the least effective approach for providing the ML team with the needed GPU resources.

Solution to Question 36: D

The correct answer should be D because it covers all the necessary steps to properly create and bill the Marketing department for their Google Cloud services used in the new initiative within their team. Here's an explanation of why each option may or may not work:

Option A: Creating separate Google Cloud projects without linking a billing

account would only cause confusion and not properly account for the services provided by the Marketing department. Furthermore, without linking a billing account, these projects will not have any way to pay for the resources used.

Option B: While having the Billing Administrator IAM role is essential, creating a budget for the Marketing department without creating a separate project or billing account would not sufficiently track the use of Google Cloud services specific to the Marketing team's new initiative. This lack of proper tracking could lead to inaccurate budget allocations.

Option C: The Project Creator IAM role would allow you to create a new Google Cloud project but would not grant you the necessary permissions to manage billing for that project. Additionally, sharing the billing account with other projects could lead to difficulty in accurately attributing costs to the Marketing department's initiative.

Option D: Verifying that you are assigned the Billing Administrator IAM role for the Marketing department's Google Cloud project ensures you have the necessary permissions to manage billing for that project. By linking the new project specifically to a Marketing Billing Account, you can accurately track and attribute costs to the Marketing department for their Google Cloud services usage in the new initiative. This approach allows for proper budget allocation and transparency in the organization.

Solution to Question 37: B

The correct answer is B, and here's why:

Option A: Enabling Cloud Spanner to store medical images is not an ideal solution, as Cloud Spanner is a relational database management service meant for storing structured data, while the company aims to use Cloud Storage for archival purpose. Moreover, it doesn't provide a synchronization mechanism with on-premises storage.

Option B: Creating a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage is the best solution. This way, you can set up a cron job to automate the process, ensuring timely syncing of any new research documents added to the on-premises storage. Cloud Storage will serve the purpose of archival storage efficiently.

Option C: Cloud Storage Transfer Service is not the answer because it cannot be used for transferring data from on-premises storage to Cloud Storage. It is mainly designed for transferring data among cloud storage services like from Amazon S3 to Google Cloud Storage.

Option D: Cloud SQL is not suitable for this use case since it is a relational database service that's not optimized for storing and serving research documents. Moreover, it doesn't provide an automated process for synchronization with on-premises storage, which the company needs.

In conclusion, option B is the best solution as it effectively addresses the company's requirements to utilize Cloud Storage for archival storage and automates the synchronization process between the on-premises storage and Cloud Storage.

Solution to Question 38: A

The correct answer is A: Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

Explanation for the selection of answer A: Google Cloud Platform (GCP) allows you to deploy multiple versions of your App Engine application in a single project. By choosing this option, you can use App Engine's built-in traffic splitting feature to divert a predefined percentage (1% in this case) of your user traffic from the current version to the new version. Traffic splitting can be done based on either IP address or cookie. This allows for an efficient and controlled transition to your new version while maintaining performance, monitoring, and scaling capabilities.

Explanation for why other options will not work:

B: Deploying the new version of your application in a separate project within App Engine doesn't allow for traffic splitting between different projects. All versions should be within the same project to enable traffic splitting.

C: Cloud Pub/Sub is a messaging service used for asynchronous event-driven systems and is not designed to handle traffic splitting for application versions. Traffic splitting needs to be done within App Engine's configuration.

D: Deploying a new version of your application in a Compute Engine instance instead of App Engine not only adds additional workload but is also unnecessary. App Engine already supports traffic splitting and version management, whereas Compute Engine is designed to be a more generic infrastructure service without those specific features. Transitioning to a Compute Engine instance for this purpose is inefficient and not recommended.

Solution to Question 39: B

The correct answer is B. Create a custom role that combines the required permissions. Grant the DevOps team the custom role on the production project.

Here's why:

B is correct because creating a custom role allows you to grant the DevOps team the exact permissions they need to work on the production project while adhering to the principle of least privilege. This ensures their access rights will remain consistent and prevent unintended access to Google Cloud resources that may be introduced with future updates.

A is incorrect because, although creating a custom role helps define the required permissions, granting only the Project Viewer role on the production project

would not allow the DevOps team to perform any modifications, which is not suitable for managing production services.

C is incorrect because granting the Project Editor role on the organization level would provide too much access to the DevOps team members, violating the principle of least privilege. Also, it could potentially impact other projects in the organization that the DevOps team should not access.

D is incorrect because granting only the Project Viewer role to the DevOps team limits them to "read-only" access. Giving them viewer access on the production project would not allow them to manage production services effectively, as they would need permission to modify and configure resources, which the Project Viewer role does not provide.

Solution to Question 40: B

The correct answer is B: Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles.

Explanation: As a DevOps engineer, when you are asked to check and verify the IAM users and roles assigned within a GCP project, it is important to go directly to the source of information - the IAM section in the GCP Console. In this case, navigating to my-project and accessing the IAM section in the GCP Console, you can easily review the members and roles. This will provide you with a clear and organized view of the IAM users and their assigned roles.

Why other options will not work:

A. Use Stackdriver Logging to review IAM logs for my-project: Stackdriver Logging is now called Cloud Logging. While it is used to store, search, analyze, monitor, and set alerts on log data and events from GCP and other sources, it does not provide a clear view of IAM users and roles assigned within a GCP project. It is more focused on logs and events rather than IAM management.

C. Run the command: gcloud projects get-iam-policy my-project. Review the output section: This command will return the IAM policy for the specified project, which includes information about bindings of members to roles. However, this output can be less user-friendly to review and analyze, compared to the organized view available in the GCP Console's IAM section.

D. Use Cloud Audit Logs to review IAM activity for my-project: Cloud Audit Logs are used to record administrative activities and data access events in the GCP environment, which can help in monitoring and investigating security incidents. However, this is not a convenient method to simply review IAM users and roles assigned within a GCP project, as the audit logs can contain unrelated data and events.

As a result, B is the best option to review and verify IAM users and roles directly in the GCP Console's IAM section for the project my-project.

Solution to Question 41: D

The correct answer is D. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

Explanation: Data Access Logs are specifically designed to track access to data in Cloud Storage buckets, which is exactly what the auditor wants to review. By enabling Data Access Logs for the buckets of interest, and building a query in the log viewer, it will assist the auditor in obtaining relevant information about who accessed the data. This provides a focused and suitable solution to the auditor's request.

Reasons why other options will not work:

A. Tthe Cloud Asset Inventory is designed to provide an organization with a snapshot of their Google Cloud assets, rather than tracking specific data access in Cloud Storage buckets. While it does track asset metadata, it does not provide the detailed level of access information needed for the auditor's purposes.

B. Stackdriver Error Reporting is a tool for monitoring and resolving runtime errors in applications and services running on Google Cloud. While this tool might help to identify errors and issues with data access, it is not specifically designed for auditing data access in Cloud Storage buckets, and therefore will not provide the required information for the auditor.

C. Configuring a Cloud Pub/Sub topic to stream logs related to Cloud Storage access might provide a real-time stream of log events, but it is not specifically designed for auditing purposes. Additionally, setting up a pub/sub topic requires more setup and maintenance work than simply turning on Data Access Logs. It makes more sense to use a dedicated tool for auditing, which is Data Access Logs in this case.

Solution to Question 42: D

The correct answer is D. Deploy a private autopilot cluster.

Here's why the other options will not work and why the correct answer is the most appropriate choice:

A. Deploy a public autopilot cluster: While autopilot mode is an excellent way of minimizing management overhead and following Google-recommended best practices, deploying a public cluster does not fulfill the requirement of ensuring that nodes cannot be accessed from the internet. Public clusters expose nodes to potential external threats, so this option is not suitable for meeting the necessary security requirements.

B. Deploy a public regional cluster and enable shielded nodes: Though enabling shielded nodes will provide verifiable node identity and integrity, deploying a public regional cluster will not satisfy the security requirement to prevent node access from the internet. Additionally, using a regional cluster does not minimize the operational cost of managing the cluster in comparison to an autopilot cluster.

C. Deploy a private zonal cluster and enable shielded nodes: This option, while providing the necessary security by creating a private zonal cluster and enabling shielded nodes, does not minimize operational cost because it relies on manual cluster management. An autopilot cluster would be more suitable for minimizing the operational cost.

D. Deploy a private autopilot cluster (Correct Answer): This approach meets all requirements. A private cluster ensures that nodes cannot be accessed from the internet, and using autopilot mode provides minimal operational management cost by automating many tasks. Additionally, autopilot clusters come with shielded nodes by default, ensuring verifiable node identity and integrity. Therefore, deploying a private autopilot cluster is the best approach to fulfill the security requirements, minimize operational cost, and follow Google-recommended best practices.

Solution to Question 43: C

The correct answer is C. The reason being is that the Google Cloud Pricing Calculator takes into account all the required resources and their corresponding costs to provide a fairly accurate estimate of the expenses you would incur after migration. By using instances similar to your current on-premises machines and comparing them with Cloud SQL, you would get a precise idea of your costing needs. This method provides a transparent method of understanding the actual costs that will be involved once you switch the infrastructure for your web application.

Option A is not the most effective method because implementing a similar architecture in Google Cloud and running load tests on a smaller scale might not always accurately represent the real load your system would handle. Thus, it might lead to incorrect cost estimations.

Option B is not suitable because Google BigQuery is designed for analyzing large datasets and running analytics. It is not primarily a tool for cost prediction. While you might gain some insights, it is not the most efficient or effective method to estimate the costs associated with infrastructure migration.

Lastly, option D is not the best choice because using the GCP Marketplace to estimate the cost of deploying a pre-built web application might not account for the unique architecture and requirements of your existing application. Thus, it would not give an accurate estimate.

Therefore, using the Google Cloud Pricing Calculator (Option C) is the most effective method to estimate the total cost of transitioning your three-tier web application from virtual machines that use a MySQL database to Google Cloud instances and Cloud SQL.

Solution to Question 44: C

The correct answer is C. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

Explanation:

When deploying container images in a GKE cluster, it's essential that the cluster's nodes can access and download the images from the Container Registry. In this scenario, since the Container Registry and the GKE cluster are in separate projects, you need to grant appropriate access for the nodes to pull images from the Container Registry.

C: Granting the Storage Object Viewer IAM role allows the Kubernetes nodes to read and access the images stored in the Container Registry across projects. This role grants the required permission to download the images and ensures proper communication between the GKE cluster and the Container Registry.

Why other options will not work:

A: Enabling the Kubernetes Engine API in the project where the GKE cluster is being created is a necessary step when creating the cluster itself; however, this is not enough to provide access to the images stored in the Container Registry in a different project.

B: The option "Allow full access to all Cloud APIs" under 'Access scopes' is too broad and potentially insecure. It would grant excessive permissions to the GKE cluster, which may not be required for this specific task. It is always better to grant the least possible privileges needed for the task, and in this case, granting the Storage Object Viewer IAM role is more appropriate.

D: Workload Identity Federation is a method for providing access and identity to your workloads running on Google Cloud. While it can be used to manage access to resources, it is not the most straightforward and relevant solution to ensure that Kubernetes can access and download images from the Container Registry in the context of this question.

Solution to Question 45: D

The correct answer is D: Install the cloud-datastore-emulator component using the gcloud components install command.

Explanation: As a software engineer testing a Google Cloud application locally on an Ubuntu developer laptop, you need the cloud-datastore-emulator for emulating the required Google Cloud services, like Cloud Datastore, locally on your machine.

Option D is the correct choice because installing the cloud-datastore-emulator component using the gcloud components install command will provide you with the necessary tools you need to run and test the Cloud Datastore service on your local machine.

Option A is incorrect because it suggests launching the emulator without installing it. However, in order to use the emulator, you first need to have the cloud-datastore-emulator component installed using the gcloud components install command.

Option B is incorrect because Firebase Realtime Database is a separate service and not an emulator for Cloud Datastore. Although it can be useful for real-time updates in mobile and web applications, it won't help with testing your existing Cloud Datastore-dependent application locally.

Option C is incorrect because it suggests creating a Cloud Datastore index. While creating an index is essential for querying your data in Cloud Datastore, it does not help with testing the application locally. You need the cloud-datastore-emulator to run the Cloud Datastore locally for testing purposes.

Solution to Question 46: C

The correct answer is C because setting the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool ensures that the proxy credentials are not recorded in the gcloud CLI logs. This method offers a secure way to use the credentials without exposing them in the logs.

Option A is not appropriate because encrypting your proxy credentials using asymmetric encryption and setting them in the gcloud CLI still stores the credentials in the CLI, and it might not prevent them from being logged.

Option B would not work because storing your proxy credentials in a JSON file and using the gcloud auth activate-service-account command is intended for service account credentials and not proxy credentials. So, this method will not ensure the security of your proxy credentials while using the CLI.

Option D is not a feasible choice because disabling logging for the entire gcloud CLI by issuing the command gcloud config set logging/verbosity none could hinder troubleshooting and monitoring of the CLI operations, which is, in fact, vital in identifying and mitigating issues.

Solution to Question 47: B

The correct approach to adopt in this scenario would be option B. This is because asking each team member to generate a new SSH key pair and adding the public key to their Google account helps maintain individual accountability. By granting the 'compute.osAdminLogin' role to the Google group corresponding to the team, you ensure that only team members with appropriate permissions can access the servers. This approach allows for efficient deployment of credentials and easy tracking of who accessed each instance.

Option A is not a suitable choice because distributing the same private key to all team members would eliminate individual accountability, making it difficult to track server access. Additionally, this approach increases the risk of compromised security if the private key is ever leaked or mishandled.

Option C has some significant drawbacks as well. While it suggests generating a new SSH key pair and restricting access using firewall rules, it still recommends giving the private key to each team member, which is not a secure practice. Granting the 'compute.osAdminLogin' role to the Google group does not provide

an efficient deployment of credentials since every team member shares the same key.

Option D is not the best option because while Cloud Identity-Aware Proxy can authenticate users and provide access to resources, it does not rely on SSH keys for authentication and connection tracking. Granting the 'compute.osAdminLogin' role to the Google group allows for some access control, but it lacks the ability to enforce or track the use of individual SSH keys for team members in the context of accessing Compute Engine instances.

In conclusion, option B is the most secure and efficient way to manage credentials and monitor access to the instances, while also maintaining individual accountability for team members within the growing software development company.

Solution to Question 48: C

The best approach for the given requirements is option C: Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

Explanation:

Option C effectively addresses the outlined requirements and adheres to Google-recommended practices:

1. Enabling object versioning allows storing up to five revisions of the same invoice document, which satisfies the requirement for allowing corrections.
2. Lifecycle conditions can be used to change the storage class of the objects as they age, moving documents older than 365 days to lower cost storage tiers.
3. Setting the number of versions ensures that only the required number of revisions are stored, minimizing storage costs.
4. Deleting old files automatically after five years is achieved with the lifecycle conditions, fulfilling the five-year retention policy.

Why other options won't work:

Option A: While enabling retention policies on the bucket is useful, using Firestore for handling document revisions is not recommended as it increases complexity and operational costs. Cloud Functions are not necessary for managing storage classes of objects, as lifecycle conditions can do this more efficiently.

Option B: While this option correctly enables retention policies on the bucket, it introduces unnecessary complexity by using Cloud Scheduler and Cloud Functions to move or delete documents based on metadata. Moreover, it does not address the requirement of storing up to five revisions of the same invoice document.

Option D: Although this option enables lifecycle rules on the bucket, the Cloud Data Transfer Service is better suited for transferring data between cloud storage

locations, not for managing the storage class and document lifecycle based on requirements. Additionally, it does not provide a solution for storing multiple revisions of the same invoice document.

Solution to Question 49: A

The correct answer is A. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

Explanation for answer A: By setting up a low-priority rule that blocks all egress traffic and a high-priority rule that allows only the appropriate ports, you effectively minimize open egress ports. The client's concern for data egress control will be addressed by these firewall rules, which ensure that only the necessary ports are permitted, reducing the risk of unwanted traffic and potential security breaches.

Why other options will not work:

B. Configure a NetworkPeering policy to limit egress traffic to specific subnets. This option doesn't address the requirement of minimizing open egress ports. Network Peering allows separate VPCs to share routes but does not directly control the egress traffic through specific ports.

C. Configure custom routes to block egress traffic on undesired ports. Using custom routes in this situation is not efficient because they operate on the IP address level rather than the port level. Egress traffic control through custom routes is not as precise as it should be for fine-grained control over allowed egress ports.

D. Use a shared VPC to limit egress ports without configuring firewall rules. A shared VPC provides shared access to resources within different VPCs, making it easier to manage network resources but does not directly address the concern of minimizing open egress ports. Relying on a shared VPC without configuring firewall rules may lead to inadequate control over egress traffic and potential security threats.

Solution to Question 50: B

The correct answer is B, and here is the explanation for why it is the right choice and why the other options don't work:

Option B: This option suggests creating service accounts sa-app and sa-db. Associating the service account sa-app with the application servers and the service account sa-db with the database servers ensures that the correct permissions and roles are assigned to the respective servers. By creating an ingress firewall rule to allow network traffic from the source service account sa-app to the target service account sa-db, you are allowing only database traffic from the application servers to the database servers, thus securing the network connections.

Option A: This option proposes creating a service account and a network tag, which is not the appropriate way to differentiate between the application and

database servers. Furthermore, creating an ingress firewall rule targeting subnet-b instead of subnet-a mistakenly focuses on the web servers instead of the database servers. This configuration will not limit traffic to only database interactions from application servers.

Option C: Similar to option A, this option suggests using a network tag instead of a service account to identify the database servers. Also, creating an ingress firewall rule to allow network traffic from source VPC IP addresses doesn't provide the granularity required to limit access to only application servers. Besides, targeting the subnet-a IP addresses does not properly secure the actual database traffic from the application servers.

Option D: This option proposes reversing the service accounts' assignment, associating the sa-db service account with the application servers and the sa-app service account with the database servers. This incorrect association goes against the initial requirement of identifying the two types of servers correctly. Additionally, creating an egress firewall rule instead of an ingress rule misses the focus on securing incoming traffic between the two subnets.

In conclusion, the best option to secure the firewall and allow only database traffic between the application servers and database servers is option B. Using distinct service accounts for both application and database servers and creating an ingress firewall rule to control the incoming traffic provides the required security and traffic limitation needed.

Practice Exam 16

Question 1: As a network administrator at a software development company, you are tasked with transitioning the company's entire workload to Google Cloud Compute Engine. The infrastructure should allow some servers to be accessible through the Internet, while others should only be accessible via the internal network. All servers must be able to communicate using specific ports and protocols. The current on-premises network has a demilitarized zone (DMZ) for public servers and a Local Area Network (LAN) for private servers. How should you design the networking infrastructure on Google Cloud to meet these requirements?

A. 7. Create a single VPC with several subnets for the DMZ and the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

B. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public egress traffic for the DMZ.

C. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

D. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to block all traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Question 2: As a software engineer working for a tech company, you have been utilizing Google Cloud to run various projects using your personal credit card, and your company has been reimbursing you for the expenses. Now, your company wants to simplify the billing procedure and transfer the costs of your projects directly to their corporate invoice. What action should you take?

A. Create a separate Google Cloud account for your company and manually transfer your projects.

B. Generate a billing report from the Google Cloud Console and email it to your finance department monthly.

C. Create a shared Google Workspace account to manage project billing.

D. Change the billing account of your projects to the billing account of your company.

Question 3: You are working as a DevOps engineer in a media-based company and managing several microservices on a Kubernetes Engine cluster. One critical microservice is involved in rendering high-quality images, requiring significantly

more CPU usage than memory. The remaining microservices are workload-based, optimized for n2-standard machine types. To ensure that all workloads within the cluster operate as efficiently as possible, what configuration should you implement?

A. Create a node pool with memory-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

B. Use the node pool with general-purpose machine type nodes for the image rendering microservice. Create a node pool with compute-optimized machine type nodes for the other microservices.

C. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

D. Configure the required amount of CPU and memory in the resource limits specification of the image rendering microservice deployment. Keep the resource requests for the other microservices at the default.

Question 4: While working as a lead developer in a company, you find out that your fellow developers are frequently using multiple service account keys during their development process. To enforce short-lived service account credentials across the company and work towards a more secure solution, you decide to implement a new policy with the following requirements:

- All service accounts needing a key must be created in a centralized project called pj-sa.
- Service account keys should only be valid for one day.

Considering these requirements, what Google-recommended solution can you use that will also minimize cost?

A. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

B. Use a custom App Engine task runner to rotate service account keys every day. Enforce an org policy to allow service account key creation with no exceptions across all projects.

C. Implement a Cloud Run job to purge all service account keys periodically. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours with an exception on pj-sa.

D. Implement a Pub/Sub job to rotate all service account keys daily in pj-sa. Enforce an org policy constraint denying service account key creation in all other projects.

Question 5: Working at a leading innovative tech company, you are tasked with developing a backend service for an ecommerce platform that will handle

transaction data from various global mobile and web clients. Upon launch, immense levels of worldwide transactions are expected. The business team intends to perform SQL queries for data analysis purposes. Your responsibility is to create a highly available and scalable data storage solution for this platform. What action should you take?

A. Create a multi-region Firestore database with aggregation query enabled.

B. Create a multi-region Memorystore for Redis instance to store transaction data.

C. Create a multi-region Cloud Spanner instance with an optimized schema.

D. Create a multi-region Cloud Storage bucket and save transaction data as CSV files.

Question 6: As an IT administrator in a tech company, you manage several VMs running in a subnet with a subnet mask of 255.255.255.240. The current subnet has no more free IP addresses, and you need an additional 10 IP addresses for new VMs to be deployed. It is essential that the existing and new VMs can reach each other without additional routes. What should you do to achieve this?

A. Use gcloud to expand the IP range of the current subnet.

B. Resize the current subnet using Cloud Console.

C. Delete the subnet, and recreate it using a wider range of IP addresses.

D. Upgrade the VMs to larger machine types to increase the number of available IP addresses.

Question 7: You work in a mobile app development company where you manage an App Engine Service that aggregates and visualizes data from BigQuery for one of your company's applications. The application is deployed with the default App Engine Service account. The data that needs to be visualized is stored in a separate project managed by another team within your company. You currently do not have access to this project, but you want your application to read data from the BigQuery dataset. What action should you take?

A. Create your own BigQuery dataset in your project and ask the other team to sync their data with your dataset.

B. In Cloud IAM of your project, grant a newly created service account from the other team the role of BigQuery Job User in your project.

C. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

D. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.

Question 8: As a network engineer at a tech company, you are tasked with enabling traffic between multiple groups of Compute Engine instances within

two different GCP projects your company is working on. Each group of these instances operates in its own VPC. How can you achieve this?

A. Verify that both projects are in a GCP Organization. Share the VPC from one project and request that the Compute Engine instances in the other project use this shared VPC.

B. Use a Google Cloud Function to forward traffic between Compute Engine instances running in different GCP projects and VPCs.

C. Create a VPN tunnel between the two existing VPCs to allow traffic between Compute Engine instances from both projects.

D. Configure two Cloud NAT gateways for each group of instances and set up a VPC peering between the two new gateways.

Question 9: You are working as a system administrator in a software development company and are responsible for managing your company's virtual machines. One of the virtual machines, which is currently configured with 2 vCPUs and 4 GB of memory, is frequently running out of memory. In order to address this issue and upgrade the virtual machine to have 8 GB of memory, what should you do?

A. Upgrade the Cloud SDK to allow for increased memory usage.

B. Attach another boot disk with 4 GB of memory and restart the VM.

C. Stop the VM, increase the memory to 8 GB, and start the VM.

D. Stop the VM, change the machine type to n1-standard-8, and start the VM.

Question 10: You work for a software development company that has recently deployed an application on a Compute Engine instance. A remote contractor has been hired to perform additional tasks on the Linux-based instance. The contractor is connected to your company's network via a VPN connection but does not have a Google account. How can you provide access to the instance for the contractor?

A. Use Google Cloud IAM to create a temporary service account and provide the consultant with the JSON key file to access the instance.

B. Instruct the external consultant to generate an SSH key pair, and request the public key from the consultant. Add the public key to the instance yourself, and have the consultant access the instance through SSH with their private key.

C. Enable Cloud Identity-Aware Proxy for Compute Engine instances and provide the consultant with a client certificate.

D. Instruct the external consultant to use the gcloud compute ssh command line tool by using the public IP address of the instance to access it.

Question 11: You are working as a cloud engineer in a tech company, and you have successfully downloaded and installed the gcloud command line interface

(CLI) and authenticated it with your Google Account. Most of the company's Compute Engine instances in the project run in the europe-west1-d zone. In order to streamline your workflow and save time, you'd like to prevent the need to specify this zone with each CLI command when managing these instances. What is the most appropriate action to take?

A. Create a text file named default_zone.txt containing europe-west1-d and place it in the .config folder of your user directory.

B. Create a bash script that automatically adds –zone=europe-west1-d to all gcloud CLI commands.

C. Modify the gcloud CLI source code to include europe-west1-d as the default zone.

D. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

Question 12: As a software development company working on multiple Google Cloud projects, you need to ensure that all developers have the same permissions across all projects, limited to Compute Engine, Cloud Functions, and Cloud SQL, according to the company's security policy. How can you implement this policy with minimal effort?

A. • Assign the default role of Viewer to the Google group for each project in the Google Cloud organization, instead of creating a custom role with specific permissions.

B. • Add all developers to a Google group in Cloud Identity. • Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level. • Assign the custom role to the Google group.

C. • Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions in one project within the Google Cloud organization. • Copy the role across all projects created within the organization with the gcloud iam roles copy command. • Assign the role to developers in those projects.

D. • Assign the default role of Editor to the Google group for each project in the Google Cloud organization.

Question 13: As a financial analyst in a tech company, you are tasked with estimating the total cost of migrating their three-tier web application, currently running on virtual machines with MySQL database, to Google Cloud infrastructure. How should you approach calculating the cost of running this application on Google Cloud instances and Cloud SQL?

A. Calculate the costs manually based on the Google Cloud product pricing listed in their documentation, without considering the specific resource usage of your web application.

B. Use the Google Cloud Pricing Calculator to determine the cost of every Google Cloud resource you expect to use. Use similar size instances for the web

server, and use your current on-premises machines as a comparison for Cloud SQL.

C. Look for a pre-existing pricing structure of a similar 3-tier web application on Google Cloud Platform Forums, and adapt this structure to your own use case.

D. Use the GCP Marketplace to estimate the cost of deploying a pre-built web application similar to your existing application.

Question 14: As an IT manager at a fast-growing media company, you need to ensure that the video encoding software running on Google Compute Engine can handle the rapidly increasing user base. Users must be able to encode their videos without interruption or CPU limitations, and it's crucial to maintain high availability while adhering to Google-recommended practices for automating operations. How should you deploy the encoding solution?

A. Deploy your solution on multiple standalone Compute Engine instances, and replace existing instances with high-CPU instances when CPU utilization on Cloud Monitoring reaches a certain threshold.

B. Deploy your solution on multiple Compute Engine instances within a single zone, and set up autohealing with Cloud Monitoring alerts.

C. Deploy your solution using Cloud Run services without autoscaling, and monitor CPU utilization using Cloud Monitoring.

D. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

Question 15: You are working as an IT administrator in a fintech company that utilizes a single sign-on (SSO) identity provider supporting Security Assertion Markup Language (SAML) integration with service providers. The company maintains user accounts in Cloud Identity. In order to enable users to authenticate through the company's SSO provider, which step should you take?

A. In Cloud Identity, set up SSO with Google as an identity provider to access GCP Native services.

B. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

C. Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps.

D. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service consumer.

Question 16: As a project manager at a cybersecurity company, you are tasked with storing sensitive client information in a Cloud Storage bucket. To comply with legal requirements, it is crucial to record all requests that access any of the stored data. What action should you take to ensure compliance?

A. Encrypt the bucket data with Cloud KMS.

B. Enable the Identity Aware Proxy API on the project.

C. Enable the Security Command Center service.

D. Enable Data Access audit logs for the Cloud Storage API.

Question 17: As a leading technology company in the industry, your organization places great importance on maintaining strict access control over its Google Cloud projects. To ensure adherence to Google-recommended best practices, you need to provide your Site Reliability Engineers (SREs) the authority to approve requests from Google Cloud support team whenever they open a support case. What steps should you take to achieve this?

A. Add your SREs to a group and then add this group to roles/cloudsql.admin role.

B. Add your SREs to a group and then add this group to roles/accessapproval.approver role.

C. Add your SREs to a group and then add this group to roles/cloudfunctions.admin role.

D. Add your SREs to roles/cloudscheduler.admin role.

Question 18: You are a network architect at a growing technology company and have been tasked with migrating the entire IT infrastructure to Google Cloud Compute Engine. The company requires certain servers to be accessible via the internet while others should remain limited to internal network access. Inter-server communication should occur on specific ports and protocols. The existing on-premises network utilizes a demilitarized zone (DMZ) for public servers and a Local Area Network (LAN) for private servers. How should you design the networking infrastructure on Google Cloud to meet these requirements?

A. 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

B. 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

C. 8. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up only specific traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for both the DMZ and the LAN.

D. 5. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up all traffic between the DMZ

and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Question 19: As an IT specialist working for a company in the e-learning industry, you are responsible for managing a static website on Cloud Storage which features various educational resources, including PDF files. The current setup prompts users to save the PDF files locally when they click on the links. However, your company prefers if users could view the PDF files directly within the browser window without having to save them. What action should be taken to achieve this desired outcome?

A. Enable Cloud CDN on the website frontend.

B. Enable object versioning for the bucket containing PDF files.

C. Configure the bucket IAM policy to allow allUsers to view the PDF files.

D. Set Content-Type metadata to application/pdf on the PDF file objects.

Question 20: As a Cloud Engineer at a tech company, you have multiple Google Cloud Platform projects that you need to oversee. The company requires you to consolidate the monitoring of all project resources under the same Stackdriver Monitoring dashboard for a streamlined reporting process. How should you proceed?

A. Create a single Google Cloud project with separate folders for each monitored project and link Stackdriver to the project.

B. Create a custom Google API to fetch monitoring data from multiple projects and configure Stackdriver to use this API.

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

D. Enable Stackdriver Monitoring on each project and use cross-project querying to consolidate data.

Question 21: As a financial analyst in a large tech company, you are responsible for monitoring multiple projects linked to a single billing account in Google Cloud. Your company requires you to regularly present the costs with specific metrics that are dynamically calculated based on company-specific criteria. To streamline this process and minimize manual effort, how can you automate the visualization of cost metrics?

A. Set up Cloud Pub/Sub to receive billing notification events and build a custom dashboard for visualization.

B. Configure Cloud Billing data export to BigQuery for the billing account. Create a Looker Studio dashboard on top of the BigQuery export.

C. Configure Cloud Billing export to Firestore, and use Google Charts to create custom visualizations based on the exported data.

D. Use Stackdriver Monitoring to create custom cost metrics for the projects and visualize them in the Google Cloud console.

Question 22: In your company, you manage a team working on various projects that require accessing Linux instances hosted on Google Cloud. To ensure the most secure and cost-efficient method for your team to log in to these instances, what approach should you take?

A. Use a proxy server with public internet access and allow traffic on port 22 for SSH. Allow ingress traffic from the proxy server's IP range.

B. Grant all users Compute Engine Instance Admin role to manage instances and access them through Google Cloud Console SSH.

C. Use Cloud Storage as an intermediary for file transfer instead of directly connecting to instances through SSH.

D. Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port 22.

Question 23: As a data analyst in a leading tech company, your team requires access to query datasets in BigQuery without the risk of accidentally deleting the datasets. You must ensure the solution aligns with Google-recommended practices. How should you proceed?

A. Add users to roles/bigquery.jobUser role, instead of roles/bigquery dataOwner.

B. Create a custom role by removing delete permissions. Add users to the group, and then.add the group to the custom role.

C. Create a custom role by adding only read permissions, and add users to that role only.

D. Set up Cloud Identity Platform to manage user access, instead of assigning roles in GCP directly.

Question 24: As a data analyst at a tech company, you are responsible for managing an App Engine Service that aggregates and visualizes data from BigQuery. Your application is deployed with the default App Engine Service account, and the data that needs to be visualized is stored in a separate project managed by another team within your company. Without access to their project, how can you enable your application to read data from the BigQuery dataset in the other team's project?

A. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Job User.

B. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

C. In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer.

D. Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer.

Question 25: As an IT professional working in a company that specializes in disaster recovery solutions, you are tasked with implementing Google Cloud Storage for storing application backup files. Which storage option aligns with Google's recommended best practices?

A. Multi-Regional Storage

B. Coldline Storage

C. Archive Storage

D. Filestore

Question 26: You're working as a security analyst for a company that relies on Google Cloud services. Recently, an employee was terminated, but their access was not revoked until two weeks later. You need to determine whether this employee accessed any confidential client data during this period. How should you proceed?

A. View System Event Logs in Cloud Logging. Search for the service account associated with the user.

B. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

C. View VPC Flow Logs in Cloud Logging. Search for the IP address associated with the user.

D. View the Admin Activity log in Cloud Logging. Search for the service account associated with the user.

Question 27: While working at a tech-based company, your team leader assigns you the task of deploying a workload to a Kubernetes cluster within the organization's infrastructure. As you're uncertain about the precise resource requirements and their potential fluctuations due to factors like usage patterns or external dependencies, you need to determine a cost-effective solution that will cater to CPU and memory demands. Your goal is to ensure the workload functions consistently in any situation while adhering to Google's recommended practices. What course of action should you take?

A. Configure the Vertical Pod Autoscaler recommendations for availability, and configure the Cluster autoscaler for suggestions.

B. Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

C. Configure the Node Auto Provisioning for latency optimization, and configure the Horizontal Pod Autoscaler for cost optimization.

D. Configure the Vertical Pod Autoscaler recommendations for availability, and configure the Horizontal Pod Autoscaler for suggestions.

Question 28: As a software engineer at a tech company, you need to use Container Registry to manage your organization's container images in an isolated project. You plan to establish a Google Kubernetes Engine (GKE) cluster in another project and want to guarantee that Kubernetes can access images from Container Registry. What action should you take?

A. Enable the Cloud Storage API in the project where the GKE cluster is being created.

B. Enable the Kubernetes Engine API in the project where the GKE cluster is being created.

C. Grant the Storage Object Viewer IAM role to the default service account of the project where the GKE cluster is being created.

D. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

Question 29: As a software engineer working for a tech company, you are required to deploy a Dockerfile on Kubernetes Engine in your company's infrastructure. How should you proceed with this task?

A. Create a docker image from the Dockerfile and upload it to Container Registry. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

B. Use gcloud app deploy .

C. Use kubectl app deploy .

D. Create a docker image from the Dockerfile and upload it to Cloud SQL. Create a Deployment YAML file to point to that image. Use kubectl to create the deployment with that file.

Question 30: As a developer at a tech company, you are tasked with updating the company's website hosted on App Engine standard environment. You need to implement a solution that allows only 1% of users to access a test version of the site while minimizing complexity. What should you do?

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

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

C. Deploy the new version using Firebase Hosting and use Cloud Functions to redirect 1% of the traffic to the new version.

D. Deploy the new version using the same application and enable traffic splitting in App Engine by assigning 1% traffic to the new version using the Console.

Question 31: You are a data storage administrator working for a medical imaging company. The company currently stores its medical images in an on-premises data room and would like to utilize Cloud Storage for archival purposes, while also automating the process of uploading new medical images to Cloud Storage. How should you design and implement this solution?

A. Configure a Cloud Storage Transfer Service to sync the on-premises storage with Cloud Storage daily, without using a cron job or script.

B. Use Datastore to store the medical images and create a script that transfers the images from on-premises storage to Datastore. Schedule the script as a cron job.

C. Enable Cloud Spanner to store the medical images and create a script that transfers the images from on-premises storage to Cloud Spanner. Schedule the script as a cron job.

D. Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

Question 32: You have recently joined a software company that is transitioning their continuous integration and delivery (CI/CD) pipeline to Compute Engine instances within the cloud. This pipeline will be responsible for managing the entire cloud infrastructure using code. As a team member, how do you ensure that the pipeline has the necessary permissions while adhering to the organization's security best practices?

A. • Attach a single service account to the compute instances. • Add minimal rights to the service account. • Allow the service account to impersonate a Cloud Identity user with elevated permissions to create, update, or delete resources.

B. • Create multiple service accounts, one for each pipeline with the appropriate minimal Identity and Access Management (IAM) permissions. • Use a secret manager service to store the key files of the service accounts. • Allow the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline.

C. Use API keys for authentication on compute instances.

D. Use Compute Engine default service account for provisioning resources.

Question 33: As an engineer at a software development company, you recently deployed a new application to your team's Google Kubernetes Engine cluster using the YAML file provided. After checking the status of the deployed pods, you discover that one is still in PENDING status. To identify the issue causing the pod to remain in pending status, what should you do?

A. Review details of the myapp-service Service object and check for error messages.

B. View logs of the container in myapp-deployment-58ddbbb995-lp86m pod and check for error messages.

C. Review details of the myapp-service Service object and check for warning messages.

D. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

Question 34: As a software engineer in a tech company, you are tasked with deploying an application on Google Cloud using serverless technology. You need to test a new version of the application by exposing it to a small portion of the production traffic. What procedure should you follow?

A. Deploy the application to Datastore. Use indexes for traffic splitting.

B. Deploy the application to Cloud Run. Use gradual rollouts for traffic splitting.

C. Deploy the application to Google Kubernetes Engine. Use Anthos Service Mesh for traffic splitting.

D. Deploy the application to Cloud Storage. Use object ACLs for traffic splitting.

Question 35: As a software developer at a multinational trading company, you are tasked with designing a financial trading application with a global user base. The data storage should have a relational structure, ensuring that clients worldwide access the same data, and the application should have minimal latency when deployed across multiple regions. Which storage option would best suit these requirements?

A. Use Firestore for data storage.

B. Use Cloud Memorystore for data storage.

C. Use Cloud Spanner for data storage.

D. Use Cloud Pub/Sub for data storage.

Question 36: As a data analyst at a tech company, you need to quickly transfer a 32 GB file to a Nearline Storage bucket for an urgent project. Your dedicated 1 Gbps WAN connection is available, and you're the sole user of the connection. To ensure the fastest possible transfer, how should you upload the file?

A. Enable parallel composite uploads using gsutil on the file transfer.

B. Increase the latency on the machine initiating the transfer.

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

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

Question 37: As a software engineer at a tech company, you've developed a containerized web application to be used internally by your colleagues during business hours. To avoid any unnecessary costs outside of the application's active hours, you've created a new Google Cloud project for deployment. What would be the most appropriate method to deploy the application?

A. Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

B. Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero.

C. Deploy the container on Google Compute Engine (GCE) with VM instance scheduling to automatically shut down during non-business hours.

D. Deploy the container on Cloud Functions, configuring the function to trigger during business hours only.

Question 38: You are working as a data analyst in a large tech company and need to share a crucial file containing sensitive information with a third-party organization for collaboration purposes. The third-party does not have a Google account, and you want to ensure that they only have access to the file for four hours using the most secure and efficient method possible. What approach should you follow?

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

B. Create an API key with access to Cloud Storage and share this key with the external company to access the object. Delete the API key after four hours.

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

D. Use Cloud Functions to create an endpoint that provides temporary read access to the object. The external company will be allowed access for only four hours before the endpoint stops working.

Question 39: As an IT administrator for a leading tech company, you oversee a business-critical workload running on Google Compute Engine. To ensure the data on the boot disk is regularly backed up and can be quickly restored in case of disaster, you also want older backups to be cleaned automatically to save costs while following Google-recommended practices. What should you do?

A. Create a snapshot schedule for the disk using the desired interval.

B. Use Cloud Memorystore for Redis to keep regular copies of the boot disk data.

C. Create a Managed Instance Group using the existing instance as a template.

D. Create a Cloud Scheduler job to clone the VM instance at the desired interval.

Question 40: You are working as a software engineer at a rapidly growing startup company, developing an application that stores relational data from users across various industries globally. Given the uncertainty of the potential user base size, your CTO is worried about the scalability of the application with minimal configuration changes. Which storage solution would be the best choice to address this concern?

A. Cloud Spanner

B. Compute Engine

C. Datastore

D. Cloud SQL

Question 41: As a software developer at a fast-growing tech company, you've noticed that your projects encountered higher expenses than anticipated last month. Upon investigation, you discovered that a development GKE container produced a significant amount of logs, resulting in increased costs. You need to disable the logs as quickly as possible with the least number of steps. What should you do?

A. 1. Go to the Logs ingestion window in Stackdriver Logging, and disable the log source for the GKE container resource.

B. 1. Go to the GKE console, and delete existing clusters. 2. Recreate a new cluster. 3. Clear the option to enable legacy Stackdriver Monitoring.

C. 1. Go to the IAM console, and remove permissions for the GKE container to write logs to Stackdriver Logging.

D. 2. Go to the Log Router in Stackdriver Logging, and create a sink with a no-op destination for the GKE container resource.

Question 42: In your IT company, you are managing several applications that will run on different Compute Engine instances within the same project for various clients. To ensure proper control over access to Google Cloud APIs, you need to assign service accounts to each instance with a finer level of granularity. What should be your course of action?

A. When creating the instances, specify a Service Account for each instance.

B. Use gcloud beta compute instances update to specify a Service Account for each instance.

C. Assign the IAM role for each Service Account to their respective instance's metadata.

D. Assign a single project-wide service account for all Compute Engine instances.

Question 43: As a software engineer working for a tech company, you find that your application running on a general-purpose Compute Engine instance is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk.

The application primarily deals with reading large files from disk and the disk size is currently 350 GB. Your goal is to ensure the maximum throughput while keeping costs low. What should you do?

A. Use a Standard Persistent Disk instead of Zonal SSD Persistent Disk.

B. Migrate to use a Local SSD on the instance.

C. Increase the size of the disk to 2 TB.

D. Configure the instance with more RAM.

Question 44: An external collaborator is working with your software development company on a project that requires them to have access to compute images and disks within the project. You want to ensure that you are adhering to Google-recommended practices when granting the necessary permissions to this user. What is the appropriate course of action?

A. Create a custom role, and add all the required compute.disks.list and compute.images.list permissions as includedPermissions. Grant the custom role to the user at the project level.

B. Create a custom role based on the Compute Storage Admin role. Exclude unnecessary permissions from the custom role. Grant the custom role to the user at the project level.

C. Grant the Compute Storage Admin role at the project level.

D. Grant the Compute Storage Admin role and the Compute Image Admin role at the organization level.

Question 45: As an IT administrator for a large company, you recently conducted an audit of your organization's Google Cloud resources and found multiple users with email addresses that don't belong to your company's Google Workspace domain. To ensure that your resources are only shared with users within your domain, you need to eliminate these mismatched users and prevent similar issues from occurring in the future without having to continuously audit your resources. What action should you take?

A. Set an organizational policy constraint to limit identities by domain, and then retroactively remove the existing mismatched users.

B. Create a custom IAM role to restrict access to users within your domain.

C. Configure a Pub/Sub topic to monitor resource sharing and notify you if a mismatched user is detected.

D. Set an organizational policy constraint to limit identities by domain to automatically remove mismatched users.

Question 46: You are working as a developer in a marketing company that uses Google Cloud to host its infrastructure. Your team has decided to implement a specific content management system (CMS) solution to improve web content

collaboration company-wide. You've been assigned to find the most efficient method to deploy and install the CMS solution on Google Cloud. What should you do?

A. Use the installation guide of the CMS provider. Perform the installation through your configuration management system.

B. Create a custom VM image with the CMS pre-installed, then deploy the image to a new Compute Engine instance.

C. Manually install the CMS on a new App Engine standard environment instance.

D. Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

Question 47: As a project manager at a software development company, what should you do to allow an external auditor to only view but not modify resources in a project where Domain Restricted Sharing is enabled?

A. Create a temporary account for the auditor in Cloud Identity and give that account the Organization Viewer role on the project.

B. Give the auditor App Engine Viewer role on the project.

C. Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project.

D. Create a temporary account for the auditor in Cloud Identity, and give that account the Editor role on the project.

Question 48: As a software development company operating primarily in the United States, your company has multiple development teams each with their own Google Cloud project. To ensure compliance and maintain localization, you need to restrict each team's access so that they can only create cloud resources within the US. How should this be accomplished?

A. Create a label for all dev projects with a "US-only" value. Implement a custom IAM policy based on this label to restrict resources to US locations.

B. Manually review and approve all new dev project resources to ensure they are in the US regions.

C. Configure Cloud Monitoring to alert the organization if resources are created outside of the US. Set up manual deletion for those resources.

D. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations. Most Voted

Question 49: As a data analyst at a fast-growing tech company, you have been tasked with managing BigQuery for the organization's vast data warehousing needs. The company has over 1000 datasets across several projects, contributed by various business units. Your CIO has asked you to identify any tables that

have an employee_ssn column. What approach would be the most efficient to complete this task while minimizing effort?

A. Write a script using the Google Cloud SDK to scan through every table in all the projects looking for the employee_ssn column.

B. Write a Cloud Dataflow job that loops through all the projects in your organization and runs a query on INFORMATION_SCHEMA.COLUMNS view to find employee_ssn column.

C. Use Stackdriver Logging to search for logs containing the term "employee_ssn" and manually examine the related datasets.

D. Go to Data Catalog and search for employee_ssn in the search box.

Question 50: You are working as a cloud engineer at a technology company, and you've installed the gcloud command line interface (CLI) to manage Google Compute Engine instances for your projects. Most instances run in the europe-west1-d zone. To save time and increase efficiency, you want to set this zone as the default when using the CLI to manage your instances. What should you do?

A. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

B. Create a bash script that automatically adds –zone=europe-west1-d to all gcloud CLI commands.

C. In the Settings page for Compute Engine under Default location, set the zone to europe-west1-d.

D. Create an environment variable named DEFAULT_ZONE with the value europe-west1-d.

Practice Exam 16 Solutions

Solution to Question 1: C

The correct answer is C because it meets all the requirements mentioned in the question.

1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN: This setup allows you to create a demilitarized zone (DMZ) to host the public servers and a local area network (LAN) for the private servers, replicating the current on-premises network configuration.
2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets: This setup enables specific communication between the public-facing DMZ servers and the internal LAN servers using the required ports and protocols.
3. Set up another firewall rule to allow public ingress traffic for the DMZ: This rule ensures that the public servers in the DMZ are accessible through the internet, which is one of the requirements.

Options A, B, and D are incorrect for the following reasons:

A: It is wrong because it suggests creating several subnets for both DMZ and LAN, which is unnecessary and can lead to network complexity. It is best to have separate subnets for DMZ and LAN to manage traffic between public-facing and private servers.

B: It is incorrect because it suggests allowing public egress traffic for the DMZ. However, the requirement is to allow public ingress traffic to the DMZ, enabling internet users to access the public servers.

D: This option is wrong because it suggests setting up firewall rules to block all traffic between the DMZ and LAN subnets. The requirement is to allow specific communication between the public servers in the DMZ and the private servers in the LAN using designated ports and protocols. Blocking all traffic would make communication between the servers impossible.

Solution to Question 2: D

The correct answer is D. Change the billing account of your projects to the billing account of your company.

Explanation:

Option A: Creating a separate Google Cloud account for your company and manually transferring your projects may seem like a solution, but it would involve a time-consuming and potentially error-prone process, especially for complex projects with multiple resources and dependencies. Additionally, project transfers can lead to service downtime which is not ideal.

Option B: Generating a billing report from the Google Cloud Console and emailing it to your finance department monthly could result in a delay in processing and payment, as well as potential confidentiality concerns, especially if sensitive project data is included in the billing reports. This approach also requires continuous manual work and communication, therefore is not the most efficient choice.

Option C: Creating a shared Google Workspace account to manage project billing is not directly related to the billing account feature built-in Google Cloud. Instead, Google Workspace focuses on providing collaboration, productivity, and communication tools. It is not related to billing management for your company's Google Cloud usage.

Option D: Changing the billing account of your projects to the billing account of your company is the best approach because it allows the company to directly pay for the costs related to your projects without involving your personal credit card or requiring manual transfers. This simplifies the billing process and ensures that your project-related expenses are directly handled by your company's billing account, eliminating the need for reimbursements. This is the most suitable and seamless way to transition billing responsibility to the company's account.

Solution to Question 3: C

The correct answer is C. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Here's why the other options won't work:

Option A: Creating a node pool with memory-optimized machine type nodes for the image rendering microservice does not address the actual needs of the microservice, which requires more CPU usage than memory. Using a memory-optimized machine type would only allocate more memory to the microservice, not providing it the additional CPU power it requires, resulting in inefficient usage of resources.

Option B: Using the node pool with general-purpose machine type nodes for the image rendering microservice would not allow it to perform optimally, since it requires more CPU resources than the general-purpose machines provide. Creating a node pool with compute-optimized machine type nodes for the remaining microservices is unnecessary because they are already workload-based and optimized for n2-standard (general-purpose) machine types.

Option D: Configuring the required amount of CPU and memory in the resource limits specification could lead to inefficient resource allocation. By only setting the limits and not specifying the best machine type to cater to the high CPU requirement of the image rendering microservice, it may still struggle with performance. This approach also does not account for the specific requirements of

the remaining microservices, as they have optimized workloads for n2-standard machine types.

Thus, Option C is the best choice as it caters to the specific CPU requirements of the image rendering microservice by providing compute-optimized nodes, while also addressing the needs of the workload-based microservices by continuing to utilize general-purpose machine type nodes. This configuration ensures efficient operation of the entire cluster.

Solution to Question 4: A

Answer: A. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

Explanation:

Option A is the most suitable solution because it meets all requirements and follows the Google-recommended guidelines while minimizing cost. By enforcing an org policy constraint to allow service account keys to have a lifetime of 24 hours, it ensures short-lived credentials across the company. Additionally, having a constraint that denies service account key creation for projects, except for pj-sa, centralizes service account creation in one project, making it a more secure and manageable solution.

Option B is not ideal because using a custom App Engine task runner to rotate service account keys every day may result in higher operational costs and administrative overhead. Furthermore, it does not restrict service account key creation to a central project, going against the given requirements.

Option C is not a suitable solution because implementing a Cloud Run job to purge all service account keys periodically may lead to a less reliable and costlier approach than using org policy constraints. Also, it doesn't correctly implement the exception on pj-sa, making it a less aligned solution with the requirements.

Option D is not the best choice because using a Pub/Sub job to rotate all service account keys daily in pj-sa may incur additional costs and complexity compared to implementing org policy constraints. It also doesn't enforce the 24-hour expiration requirement for service account keys, making it less secure compared to option A.

Solution to Question 5: C

The correct answer is C. Create a multi-region Cloud Spanner instance with an optimized schema. Here's why this is the best choice and why the other options are not ideal:

A. Create a multi-region Firestore database with aggregation query enabled: Creating a Firestore database with aggregation query enabled is not suitable for this specific requirement. Firestore is great for real-time data updates, but

it's not built for global transaction-intensive applications or performing complex SQL-based data analysis, which is a requirement in this scenario.

B. Create a multi-region Memorystore for Redis instance to store transaction data: Memorystore for Redis is designed for caching and can also handle real-time data, but it is not designed for long-term, high-volume transaction data storage and complex SQL-based data analysis. Memorystore is an in-memory database, which is not ideal for this use case.

C. Create a multi-region Cloud Spanner instance with an optimized schema: Cloud Spanner is a globally distributed, highly scalable, and strongly consistent relational database designed for handling transactional workloads. It can easily handle the requirements of global transactions and enables businesses to perform complex SQL queries for data analysis. Creating a multi-region Spanner instance with an optimized schema will ensure high availability, scalability, and the ability to process various SQL query-based data analyses.

D. Create a multi-region Cloud Storage bucket and save transaction data as CSV files: Cloud Storage is an object storage service designed for storing and serving unstructured data, such as images and videos. While it can store CSV files, it's not built for real-time or transactional data storage, and it doesn't support SQL queries natively. This approach would also require significant post-storage ETL (Extract, Transform, Load) and data processing which is inefficient and doesn't meet the specified requirements.

In conclusion, the best action to take is to create a multi-region Cloud Spanner instance with an optimized schema (option C), which provides a highly available, scalable data storage solution for transaction data and supports complex SQL-based data analysis.

Solution to Question 6: A

The correct answer is A: Use gcloud to expand the IP range of the current subnet.

Explanation: As an IT administrator working with VMs in a subnet with no more free IP addresses, you need to ensure that the existing and new VMs are able to communicate with each other without additional routes. To achieve this, you should opt for expanding the IP range of the current subnet.

Option A is the best choice because by using the gcloud command-line tool, you can easily expand the IP range of the existing subnet. This will ensure that the new VMs can obtain IP addresses from the same subnet, providing seamless communication between all the VMs without the need for any additional routes.

Option B, resizing the current subnet using Cloud Console, is not possible because you cannot resize a subnet directly in Cloud Console. The only way to achieve this is through gcloud or API.

Option C, deleting the subnet and recreating it with a wider range of IP addresses, is not advised because it would cause a significant amount of downtime

and could potentially disrupt the connectivity and functionality of existing VMs in the subnet.

Option D, upgrading the VMs to larger machine types to increase the number of available IP addresses, is not a valid solution. Upgrading the machine types will not increase the number of IP addresses on the subnet, as they are determined by the subnet mask and not the VM size.

In conclusion, the best way to achieve the desired outcome of adding 10 more IP addresses for new VMs to the subnet and ensuring that existing and new VMs can communicate without additional routes is by using gcloud to expand the IP range of the current subnet (Option A).

Solution to Question 7: C

The correct answer is C: Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

Explanation: The BigQuery Job User role allows your App Engine Service account to run queries to access the data stored in the other team's BigQuery dataset. This approach maintains project separation, allows your application access to the data without duplicating it, and minimizes setup complexity.

Reasons why other options will not work:

A. Creating your own BigQuery dataset in your project and asking the other team to sync their data with your dataset would add extra complexity and maintenance overhead for both parties. It would require additional steps, such as syncing the data on a regular basis and keeping track of changes. This option is also less efficient by duplicating the data, increasing overall storage costs.

B. Granting a newly created service account from the other team the role of BigQuery Job User in your project is not a viable solution because the service account from the other team would have no knowledge of the App Engine Service that needs to access the data. The objective is to allow the application to read data from the other project's BigQuery dataset, not to provide the other team access to your project.

D. Granting your default App Engine Service account the role of BigQuery Data Viewer would only provide read access to the dataset but would not allow your application to run queries, which is needed for data aggregation and visualization. The BigQuery Job User role, on the other hand, can also read data and perform query operations required by the application.

Solution to Question 8: A

The correct answer is A, and here's why:

A. Verifying that both projects are in a GCP Organization and sharing the VPC from one project with the other allows the Compute Engine instances to operate in the same shared VPC. This method provides an efficient and secure way of

enabling the traffic between multiple groups of instances within different GCP projects. It is the most practical solution in contrast to the other options.

B. Using a Google Cloud Function to forward traffic between Compute Engine instances is not a suitable solution for this issue. Cloud Functions are designed to execute serverless functions in response to specific events, not to handle network traffic between Compute Engine instances in different GCP projects and VPCs.

C. Creating a VPN tunnel between the two existing VPCs can allow traffic to flow between the Compute Engine instances. However, this option may be overly complicated and introduce additional latency, while the shared VPC approach offers a more efficient and streamlined solution without the need for additional network configurations.

D. Configuring two Cloud NAT gateways for each group of instances and setting up a VPC peering between them is an unnecessary and over-complicated solution. Cloud NAT is designed for allowing private VM instances to access the internet, not for interconnecting VM instances between different VPCs. VPC peering provides direct network connectivity between two VPCs but without the added benefits of a shared VPC present in option A.

Therefore, the best approach to enable traffic between multiple groups of Compute Engine instances within two different GCP projects is option A. Sharing the VPC from one project and having the other project use the shared VPC ensures a seamless and efficient connection between the instances while adhering to Google Cloud's best practices.

Solution to Question 9: C

The correct answer is C. Stop the VM, increase the memory to 8 GB, and start the VM.

Explanation:

Option A is incorrect because upgrading the Cloud SDK has nothing to do with increasing the memory of a virtual machine. The Cloud SDK is a set of tools used to interact with cloud services, not to provision resources for a virtual machine.

Option B is incorrect because attaching another boot disk with 4 GB of memory does not actually increase the memory of the virtual machine. Adding a boot disk would expand storage space, not memory.

Option C is the correct answer. Stopping the virtual machine allows you to modify its hardware configurations, such as increasing memory allocated to it. Once you increase the memory to 8 GB and start the VM again, it will have the desired memory size to avoid running out of memory.

Option D is incorrect because changing the machine type to n1-standard-8 is unnecessary and unrelated to the issue. N1-standard-8 is a specific predefined machine type that comes with 8 vCPUs and 30 GB of memory, which might be

more resources than needed, leading to waste and increased costs. Therefore, simply increasing the memory to 8 GB is the best solution in this case.

Solution to Question 10: B

The correct answer is B because it enables the contractor to access the Compute Engine instance without having a Google account. By having the contractor generate an SSH key pair and providing you with the public key, you can add that public key to the instance. Then, the contractor can access the instance securely using their private key through SSH. This method is secure, preserves the contractor's privacy, and does not require the contractor to have a Google account.

Option A is not appropriate because it requires creating a temporary service account, which involves granting additional permissions and requires the contractor to have a Google account to access the instance.

Option C is not suitable because Cloud Identity-Aware Proxy requires a Google account, and the contractor does not have one.

Option D does not work either, as using the gcloud compute ssh command line tool would also require the contractor to have a Google account to authenticate and access the Compute Engine instance.

Solution to Question 11: D

The correct answer is D. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

The reason option D is the most appropriate action to take is because the gcloud config subcommand allows you to update and view the configuration, which includes properties such as the active account, project, and the default region and zone. By setting the default zone using this subcommand, you can streamline your workflow and avoid having to specify the europe-west1-d zone every time you use the gcloud CLI to manage instances in this zone.

To set the default zone, use the following command:

```
gcloud config set compute/zone europe-west1-d
```

Options A, B, and C are not appropriate for the given scenario, and here's why:

A. Creating a text file named default_zone.txt containing europe-west1-d and placing it in the .config folder of your user directory does not affect the behavior of the gcloud CLI. The CLI does not recognize this file when determining the default zone.

B. Creating a bash script that automatically adds –zone=europe-west1-d to all gcloud CLI commands would require manually wrapping every gcloud command within this script, which is less efficient and would not provide a straightforward solution for configuring the CLI tool.

C. Modifying the gcloud CLI source code to include europe-west1-d as the default zone is not recommended, as this interferes with the integrity of the tool and would make it difficult to update and manage the CLI. Additionally, this approach might introduce errors or inconsistencies when working with other team members who use the standard gcloud CLI version.

Solution to Question 12: B

The correct answer is B because it provides the simplest and most efficient method to achieve the requirement without violating the company's security policy.

1. B: • Adding all developers to a Google group in Cloud Identity streamlines operations by allowing you to manage users and permissions within a single group, while minimizing the effort on individual user management. • Creating a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level ensures that the necessary permissions are granted across all projects, which adheres to the security policy. • Assigning the custom role to the Google group makes it easy to maintain and update permissions for all developers in the organization.

Reasons why other options are not the correct choice:

2. A: • Assigning the default role of Viewer would not be sufficient because it only allows for read access across Google Cloud resources, which does not include Compute Engine, Cloud Functions, and Cloud SQL permissions as required by the security policy.
3. C: • Creating and copying custom roles within individual projects requires more effort on every new project creation and turns into a complex operation when dealing with multiple projects. • It does not mention assigning the role to Google group, which might require additional steps such as assigning the role to developers individually, increasing management complexity.
4. D: • Assigning the default role of Editor to the Google group for each project will not work because it gives developers broader permissions than needed according to the company's security policy. The requirement is to only allow access to Compute Engine, Cloud Functions, and Cloud SQL.

Solution to Question 13: B

The best approach to calculating the cost of running the three-tier web application on Google Cloud instances and Cloud SQL would be option B. This is because the Google Cloud Pricing Calculator allows you to provide detailed information about your specific resource usage and application needs, which is key to producing accurate cost estimates. Additionally, comparing the instances you'll use for your web server and Cloud SQL to your current on-premises instances will help ensure that you're making a fair and genuine comparison.

Option A is not ideal, as it would only calculate the costs based on the product pricing, without considering the particular resource usage of your web application. This may result in less accurate estimates that don't account for the actual requirements of your application, leading to potential budget overruns or inefficient resource allocation.

Option C is also not a good choice, as using a pre-existing pricing structure from a forum might not suit your specific use case. Such structures may be outdated, missing certain critical components, or based on different application architectures that do not exactly match your web application. Relying on someone else's cost estimates could lead to inaccurate predictions for your project.

Option D, using the GCP Marketplace to estimate the cost of deploying a pre-built web application, is not recommended either. Pre-built applications are likely to have different requirements and resource usage patterns compared to your existing application, which means that the cost estimates produced may not be suitable or applicable to your specific situation. Moreover, pre-built applications may include additional features that don't align with your business goals, further skewing cost estimates.

In summary, option B provides the most accurate and tailored cost estimation for migrating your three-tier web application to Google Cloud infrastructure, ensuring that you account for the specific resource usage and requirements of your application.

Solution to Question 14: D

The correct answer is D. Deploy your solution to an instance group, and set the autoscaling based on CPU utilization.

Option D should be chosen because it provides an efficient, highly available, and automated solution to handle the rapidly increasing user base. Deploying the encoding software to an instance group, which contains multiple identical instances, will allow it to scale horizontally based on CPU utilization. This load balancing ensures users can encode their videos without interruption or CPU limitations and maintains high availability. By using Google-recommended practices, such as autoscaling based on CPU utilization, you can achieve rapid response to changing demand without manual intervention.

Option A is not the best choice because it only replaces existing instances with high-CPU instances when CPU utilization reaches a specific threshold. This solution is not fully automated, and may cause latency or disruption when instances are replaced, which can harm the user experience and system availability.

Option B is also not suitable as it deploys the solution in a single zone, making it less resilient to outages and less scalable than option D. Although it involves autohealing with Cloud Monitoring alerts, it does not address the crucial requirement of automating operations and scaling based on CPU utilization to handle the rapidly increasing user base without interruption.

Option C is not appropriate as it uses Cloud Run services without autoscaling. This approach does not satisfy the requirement of handling the growing user base with uninterrupted encoding capabilities and maintaining high availability. Cloud Run without autoscaling lacks the necessary resource adjustments to automatically adapt to the increasing demand on the system. Monitoring CPU utilization with Cloud Monitoring alone will not automatically manage the operational scaling needed to support the user base.

Solution to Question 15: B

The correct answer is B. In Cloud Identity, set up SSO with a third-party identity provider with Google as a service provider.

Explanation: The company is using a single sign-on (SSO) identity provider that supports SAML integration. To enable users to authenticate through the company's SSO provider, the logical next step is to set up SSO in Cloud Identity with a third-party identity provider (IdP), designating Google as the service provider. This way, the company's users will be able to authenticate using their SSO credentials, and the company can leverage the advantages of SSO and centralized user management.

Reasons why other options will not work:

Option A: In Cloud Identity, set up SSO with Google as an identity provider to access GCP Native services. - This option would not work because the company is using a third-party SSO identity provider that supports SAML integration. Choosing Google as the identity provider would disregard the company's existing SSO infrastructure.

Option C: Obtain OAuth 2.0 credentials, configure the user consent screen, and set up OAuth 2.0 for Mobile & Desktop Apps. - This option is not relevant to the company's requirements because OAuth 2.0 is an authorization protocol rather than an authentication protocol like SAML. It is primarily used for delegating access to protected resources, not for managing SSO access and user authentication.

Option D: In Cloud Identity, set up SSO with a third-party identity provider with Google as a service consumer. - This choice is incorrect because, in SSO terminology, service consumers represent client-side applications that consume the services or APIs provided by service providers. In this context, Google should be a service provider rather than a service consumer to meet the company's need to authenticate users through their existing SSO provider.

Solution to Question 16: D

The correct answer is D. Enable Data Access audit logs for the Cloud Storage API.

Here's why other options will not work and why the answer should be option D:

Option A: Encrypt the bucket data with Cloud KMS. Cloud KMS (Key Management Service) provides a way to manage cryptographic keys and perform cryptographic operations in a cloud environment. However, it does not provide the necessary audit logging for requests accessing bucket data as required for compliance. It only takes care of the encryption aspect, not the logging.

Option B: Enable the Identity Aware Proxy API on the project. Identity Aware Proxy (IAP) allows you to control access to your cloud applications by deploying an authentication and authorization layer. It does not offer features for recording requests or tracking access to stored data in a Cloud Storage bucket. While it could be useful for controlling access, it doesn't satisfy the specific logging requirement.

Option C: Enable the Security Command Center service. Security Command Center is a security management service that provides insights, monitoring, and compliance reporting for your Google Cloud resources. While it offers information on potential security risks and vulnerabilities, it doesn't specifically address the requirement to record all requests for accessing stored data.

Option D: Enable Data Access audit logs for the Cloud Storage API. (Correct Answer) Enabling Data Access audit logs for the Cloud Storage API will allow you to record all requests that access any of the stored data in the Cloud Storage bucket. This option directly addresses the legal requirement to maintain a record of all requests accessing the sensitive client data, thus ensuring compliance.

In conclusion, to comply with legal requirements and record all requests that access the sensitive client information stored in a Cloud Storage bucket, you should enable Data Access audit logs for the Cloud Storage API (Option D). The other options might be useful in different contexts but do not fulfill the specific requirement mentioned in the question.

Solution to Question 17: B

The correct answer is B: Add your SREs to a group and then add this group to roles/accessapproval.approver role.

Explanation:

Option B is the correct choice because the access approval process requires the 'roles/accessapproval.approver' role to grant the necessary permissions for approving requests from the Google Cloud support team. By adding SREs to a group and assigning this role, you're giving them the authority to approve support case requests as per the organization's requirements.

Why other options will not work:

A. The 'roles/cloudsql.admin' role focuses on managing Cloud SQL instances and has nothing to do with approving requests from Google Cloud support. Therefore, this option doesn't satisfy the requirement.

C. The 'roles/cloudfunctions.admin' role is related to managing Cloud Functions,

which is a Google Cloud service for creating and running serverless applications. It is not relevant to the access approval process for support cases.

D. By directly adding SREs to the 'roles/cloudscheduler.admin' role, you're giving them permissions related to Cloud Scheduler, which is used to schedule and run jobs. This role doesn't have the necessary permissions to approve requests from the Google Cloud support team. Moreover, adding individual users instead of using a group is not an efficient way to manage permissions and roles.

Solution to Question 18: A

The correct answer is Option A and here's the explanation for why the answer should be A and why other options will not work:

Option A: 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Explanation: Creating a single VPC with separate subnets for DMZ and LAN allows you to efficiently mimic the existing on-premises architecture on Google Cloud. By setting up firewall rules that open up only relevant traffic between DMZ and LAN, you ensure inter-server communication on specific ports and protocols as per the company's requirements. Additionally, creating a separate firewall rule to allow public ingress traffic only for the DMZ subnet will restrict public access to only the required servers in the DMZ. This setup meets all the requirements, making Option A the best choice.

Option B: 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up relevant traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Explanation: While this option may seem viable, using separate VPCs for DMZ and LAN is unnecessary and can lead to increased complexity in managing network configurations. A single VPC with separate subnets, as described in Option A, is a simpler and more effective solution.

Option C: 1. Create a single VPC with a subnet for the DMZ and a subnet for the LAN. 2. Set up firewall rules to open up only specific traffic between the DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for both the DMZ and the LAN.

Explanation: This option fails to meet the requirement of limiting public access to only the DMZ servers. Allowing public ingress traffic for both the DMZ and LAN subnets will expose the private servers on the LAN, which is against the company's requirements.

Option D: 1. Create a VPC with a subnet for the DMZ and another VPC with a subnet for the LAN. 2. Set up firewall rules to open up all traffic between the

DMZ and the LAN subnets, and another firewall rule to allow public ingress traffic for the DMZ.

Explanation: This option contains two flaws. Firstly, using separate VPCs for DMZ and LAN is unnecessary and complicates network management. Secondly, opening up all traffic between the DMZ and LAN subnets contradicts the requirement to limit inter-server communication to specific ports and protocols.

In conclusion, Option A is the most suitable choice, as it meets all the stated requirements. The other options either violate one or more requirements or introduce unnecessary complexity.

Solution to Question 19: D

Option D is the correct answer because when the `Content-Type` metadata is set to `application/pdf` for the objects (PDF files) in Cloud Storage, it instructs the browser to interpret and display the content as a PDF within the browser window, rather than prompting the user to download the file.

Option A, enabling Cloud CDN on the website frontend, won't solve the problem since Cloud CDN is used for caching and delivering content closer to the users, improving load times. It doesn't change the way PDF files are being handled in the browser.

Option B, enabling object versioning for the bucket containing PDF files, also won't help in this case. Object versioning enables you to preserve and restore previous versions of objects in Cloud Storage, but it doesn't control how PDFs are displayed in the browser.

Option C, configuring the bucket IAM policy to allow allUsers to view the PDF files, concerns access control rather than PDF viewing preferences. While this action controls user permissions to access the objects, it doesn't specifically address the requirement of displaying PDF files in the browser.

Solution to Question 20: C

The correct answer is C: Configure a single Stackdriver account, and link all projects to the same account.

Explanation:

Option C is the most appropriate way to consolidate monitoring from multiple Google Cloud Platform (GCP) projects into a single Stackdriver dashboard. By linking all projects to the same Stackdriver account, you can effectively manage and monitor resources from various projects under one dashboard.

Option A suggests creating a separate Google Cloud project with separate folders for each monitored project, but this would complicate the infrastructure without achieving the goal of monitoring the resources in a consolidated dashboard. Stackdriver Monitoring does not recognize folder-level separation, so it will not suffice.

Option B proposes creating a custom Google API to fetch monitoring data from multiple projects and configuring Stackdriver to use this API. While this seems like a viable choice, it requires additional development work and maintenance. The recommended approach is to utilize built-in Stackdriver functionality by linking projects to a single account.

Option D suggests enabling Stackdriver Monitoring on each project and using cross-project querying to consolidate data. Although cross-project querying can display information from multiple projects, it does not create a single, unified dashboard to oversee all resources. Additionally, this option lacks the convenience and simplicity offered by option C.

Therefore, the best approach to consolidate monitoring from multiple GCP projects under the same Stackdriver dashboard is by configuring a single Stackdriver account and linking all projects to the same account (Option C).

Solution to Question 21: B

The correct answer is B because it leverages the powerful combination of Cloud Billing data export to BigQuery for the billing account and then builds a Looker Studio dashboard on top of the BigQuery export. This approach ensures that you can automate the visualization of cost metrics in real-time, adhering to the company-specific calculation requirements. It minimizes manual effort, streamlines the process, and uses native integrations within the Google Cloud ecosystem.

Option A is not ideal because Cloud Pub/Sub is more focused on handling real-time messaging or event-driven systems. Though it can receive billing notification events, you would still need to build a custom dashboard for visualization manually, which might require additional resource allocation to manage and scale the system.

Option C does not work because, as of now, there is no direct Cloud Billing export to Firestore. Even if you manually export the data to Firestore, it would involve extra work and complexity to use Google Charts to create custom visualizations based on the exported data. This option may not scale well with the growing requirements of your company.

Option D is not suitable because Stackdriver Monitoring focuses on monitoring infrastructure, application, and services in Google Cloud. Although you can create custom metrics, it is not specifically designed for cost metrics of billing accounts. Visualizing costs in Google Cloud Console may not always reflect the complex, company-specific metrics needed for the financial analyst role.

Overall, option B is the best choice for automating the visualization of cost metrics with minimal manual effort and meeting company-specific criteria.

Solution to Question 22: D

The correct answer is D. Use the gcloud compute ssh command with the –tunnel-through-iap flag. Allow ingress traffic from the IP range 35.235.240.0/20 on port

22.

Explanation:

D is the most secure and cost-efficient method because it combines the gcloud command and Identity-Aware Proxy (IAP). IAP allows you to establish a central access point to your Google Cloud instances and verify users' identities while controlling access to resources. This method allows you to restrict access to authorized users only and logs their activities for audit purposes.

Option A is not secure because using a proxy server with public internet access and allowing traffic on port 22 (SSH) exposes your instances to potential attacks. This method could lead to unauthorized access to your Linux instances, compromising the security of your infrastructure.

Option B is neither secure nor efficient because granting all users the Compute Engine Instance Admin role would give them excessive permissions, which may not be necessary for their tasks. This approach might allow them to manage instances beyond their required responsibilities, introducing potential security risks and human errors.

Option C is not appropriate because this method only provides indirect access to the instances through file transfers, rather than allowing users to log in and perform tasks directly on the instances. This approach does not address the central question of secure and efficient login management and may further complicate the workflow of your team.

Solution to Question 23: B

The correct answer is B.

An ideal solution to ensure that your team has access to query datasets in BigQuery without the risk of accidentally deleting them is to create a custom role with the appropriate permissions. By doing this, you can still provide your team members the necessary access to read and manipulate the data without having the ability to delete datasets.

Option B reflects this recommended practice, as it proposes creating a custom role that has delete permissions removed. By adding users to a group and then adding the group to the custom role, you can confidently grant your team the access they need without the risk of unintended data loss.

Here's why the other options are not ideal:

Option A: Adding users to roles/bigquery.jobUser role instead of roles/bigquery.dataOwner is not suitable because the jobUser role simply allows users to run jobs, like queries and load data, but it does not grant them permissions to read the data, which is necessary for a data analyst.

Option C: Creating a custom role with only read permissions is insufficient because data analysts might need additional permissions, like the ability to update or create new tables with query results, for their work. By only having

read permissions, the role would be too restrictive to meet their requirements effectively.

Option D: Setting up Cloud Identity Platform to manage user access is not the right approach for this scenario because it does not specifically address the need to limit user access in BigQuery. The Cloud Identity Platform oversees identity and authentication management across various GCP services but does not directly control role assignment and permission management in BigQuery.

Solution to Question 24: B

The correct answer is B. Ask the other team to grant your default App Engine Service account the role of BigQuery Job User.

Here's why option B is the right answer and why the other options will not work:

Option A: In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Job User. This option is incorrect because it only grants the App Engine Service account access to the BigQuery resources in your own project. Since the data is stored in the other team's project, you need to have the other team grant the appropriate permissions to your service account.

Option B: Ask the other team to grant your default App Engine Service account the role of BigQuery Job User. This is the correct answer. By having the other team grant your default App Engine Service account the role of BigQuery Job User in their project, your application will be able to execute queries and read data from the BigQuery dataset in the other team's project.

Option C: In Cloud IAM of your project, ensure that the default App Engine service account has the role of BigQuery Data Viewer. This option is incorrect because the BigQuery Data Viewer role only allows you to view the data and metadata of BigQuery tables within your own project. It does not grant the necessary permissions to access BigQuery resources in the other team's project.

Option D: Ask the other team to grant your default App Engine Service account the role of BigQuery Data Viewer. This option is incorrect because the BigQuery Data Viewer role only allows viewing data and metadata of BigQuery tables. However, it doesn't allow executing the necessary queries required for the App Engine service to visualize the data. To achieve this, the App Engine Service account needs to have the role of BigQuery Job User, which allows running query jobs and fetching the results.

Solution to Question 25: B

The answer is B. Coldline Storage.

Explanation:

As an IT professional working in a company that specializes in disaster recovery solutions, the main priority should be to store application backup files securely

in a cost-effective way while ensuring data durability and availability in the event of a disaster. Google Cloud Storage offers a variety of storage options that cater to different use cases, and it's essential to select the storage class that best meets the needs of disaster recovery scenarios.

B. Coldline Storage: Google's Coldline Storage is designed for long-term storage of infrequently-accessed data, making it a perfect fit for storing application backup files. It offers low storage costs, high durability and availability, and swift access to the data when needed for disaster recovery. Its ability to balance cost savings with reliable access makes it the recommended best practice storage option for backup files in comparison to the other storage classes.

Here are the reasons why other options are not recommended in this scenario:

A. Multi-Regional Storage: While Multi-Regional Storage provides high availability and durability, it's designed for frequently-accessed data, making it more expensive than Coldline Storage. For application backup files, which are typically infrequently accessed, Multi-Regional Storage can lead to unnecessary costs without significantly improving disaster recovery capabilities.

C. Archive Storage: Archive Storage is designed for long-term storage of data that is accessed extremely infrequently. Although it offers even lower storage costs than Coldline Storage, its data retrieval time is slower, which could impact disaster recovery time objectives. In a disaster recovery scenario, the balance between cost savings and quick data access is crucial, making Coldline Storage more suitable than Archive Storage.

D. Filestore: Filestore is a managed file storage service primarily used for shared file storage needs. It is not designed for storing application backup files, as it does not provide the same durability, availability, and cost-effectiveness as object storage options like Coldline Storage.

In conclusion, Coldline Storage is the best option for implementing Google Cloud Storage for storing application backup files in a company that specializes in disaster recovery solutions. It provides a balance between cost savings, data durability, and swift access for data retrieval, aligning with Google's recommended best practices.

Solution to Question 26: B

The correct answer is B. View Data Access audit logs in Cloud Logging. Search for the user's email as the principal.

Explanation: Data Access audit logs in Google Cloud record all API calls that create, modify or read user-provided data. These logs are the most suitable source to track any unauthorized access to confidential client information by the terminated employee. By filtering the logs using the user's email as the principal, the search results will spotlight the actions taken by the specific employee, allowing you to identify potential security breaches.

Why other options will not work:

A. System Event Logs are used to monitor Google Cloud infrastructure and services and do not provide insights into user activities or unauthorized data access attempts. Additionally, searching for a service account instead of the user's email would not give relevant results about the employee's activity.

C. VPC Flow Logs in Cloud Logging provide information on network flows within Virtual Private Cloud networks. This data is not directly related to the access of confidential client data, and searching for an IP address would not show essential insights into the employee's actions.

D. Admin Activity logs in Cloud Logging record events related to administrative actions such as service and resource management and configuration changes. These logs are not focused on data access, so they would not be useful in this scenario. Moreover, searching for a service account instead of the user's email would not highlight the specific employee's activities.

Solution to Question 27: B

The correct answer is B: Configure the Horizontal Pod Autoscaler for availability, and configure the Vertical Pod Autoscaler recommendations for suggestions.

Explanation:

In order to deploy a workload to a Kubernetes cluster with fluctuating resource requirements, you need to ensure that the workload has both sufficient availability and scalability according to its CPU and memory demands. Google's recommended practice involves utilizing both the Horizontal Pod Autoscaler (HPA) and the Vertical Pod Autoscaler (VPA).

The Horizontal Pod Autoscaler (HPA) ensures that there are enough pods to cater to the workload's demands by increasing or decreasing the number of running pods based on the observed CPU and memory usage. The HPA is a perfect solution for handling dynamic traffic patterns and guaranteeing the workload's availability in any situation. Therefore, it should be configured for availability.

The Vertical Pod Autoscaler (VPA) adjusts the CPU and memory limits of each pod by making recommendations based on historical usage data. These suggestions assist you in determining the appropriate resource requirements so that your workload runs efficiently without wasting resources or getting throttled due to reaching resource limits. Hence, it should be configured for recommendations.

The other options are not appropriate for the following reasons:

A. Configuring the Vertical Pod Autoscaler (VPA) for availability is incorrect because it doesn't manage the number of pods, it only adjusts each pod's CPU and memory limits. Also, the Cluster Autoscaler adjusts the size of the cluster, not individual pod recommendations.

C. Configuring the Node Auto Provisioning for latency optimization doesn't address the fluctuating requirements of your workload. Moreover, using the

Horizontal Pod Autoscaler for cost optimization does not provide the necessary availability and resource demands.

D. Configuring the Vertical Pod Autoscaler (VPA) for availability would not handle the desired pod count. Similarly, using the Horizontal Pod Autoscaler for suggestions doesn't provide the required CPU and memory scaling.

In conclusion, the best solution is to configure the Horizontal Pod Autoscaler for availability and configure the Vertical Pod Autoscaler recommendations for suggestions (Option B) to ensure the workload functions consistently and cost-effectively in any situation.

Solution to Question 28: D

The correct answer is D. Grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

To explain why the other options will not work, let's review each of them:

A. Enabling the Cloud Storage API in the project where the GKE cluster is being created is not sufficient because it merely allows the project to use the Cloud Storage API. It doesn't provide the necessary permissions to access images stored in Container Registry.

B. Enabling the Kubernetes Engine API in the project where the GKE cluster is being created is necessary to use GKE itself, but it doesn't grant the permissions to access the container images stored in the Container Registry in another project.

C. Granting the Storage Object Viewer IAM role to the default service account of the project where the GKE cluster is being created wouldn't address the specific access requirements for the Kubernetes nodes. Default service accounts are generally discouraged and may have a wider scope of permissions than necessary, whereas the desired scope should be focused on the Kubernetes nodes themselves.

D. Granting the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes is the correct choice. This allows the Kubernetes nodes running in the GKE cluster to access and pull container images stored in the Container Registry in the isolated project. By binding the IAM role to the service account associated with the Kubernetes nodes, you are granting the appropriate permissions for the nodes to access Container Registry while maintaining proper access control and security.

Solution to Question 29: A

Option A is the correct answer because it follows the recommended steps for deploying a Dockerfile on Kubernetes Engine:

1. First, create a Docker image from the provided Dockerfile. A Docker image is a lightweight, stand-alone, executable package that includes everything needed to run an application.

2. Upload the created image to Container Registry. Google Cloud's Container Registry is a private registry that securely stores your Docker images. This enables you to easily manage and deploy those images using Kubernetes Engine.
3. Create a Deployment YAML file that points to the uploaded image. This file will instruct Kubernetes Engine on how to manage the deployment and scale your application.
4. Use "kubectl" command-line tool to create and manage the deployment on Kubernetes Engine by applying the Deployment YAML file.

Options B and C are incorrect because neither "gcloud app deploy" nor "kubectl app deploy" commands are valid ways of deploying a Dockerfile in Kubernetes Engine. These commands don't follow the required steps to deploy a Dockerfile in Kubernetes Engine and are not used for deploying Docker containers into Kubernetes Engine.

Option D is incorrect because it suggests uploading the Docker image to Cloud SQL, which is a fully managed database service. Cloud SQL is not the right place to store Docker images, as it is designed for storing and managing relational databases. Instead, Store the Docker image in Container Registry as described in Option A.

Solution to Question 30: B

The correct answer should be B, and here's why:

Option A is not an ideal solution because creating a new App Engine application would increase the complexity of the project, which is something we want to minimize. Also, configuring a network load balancer for this case would make the solution more complicated than necessary.

Option B is the best solution because it specifically addresses the requirement of allowing only 1% of users to access the test version while minimizing complexity. By deploying the new version in the same application and using the –splits option with a weight of 99 (current version) and 1 (new version), you are effectively restricting access to the new version of the website to only a small fraction (1%) of users, and with less complexity than option A.

Option C is not a good solution for this scenario because using Firebase Hosting and Cloud Functions introduces additional complexity and services which may not be inline with the tech stack and App Engine requirements. Also, this approach might require a considerable amount of development effort to manage the redirection of users.

Option D seems plausible at first glance but enabling traffic splitting in App Engine only supports splitting traffic across multiple services, not versions within the same service. Therefore, it does not fulfill the specific requirement of updating the company's website hosted in App Engine standard environment and allowing only 1% of users to access the test version of the site.

In conclusion, Option B best meets the requirements stated in the question by allowing only 1% of users to access a test version of the site while minimizing complexity. Other options would either introduce unnecessary complexity or not fulfill the specific requirement.

Solution to Question 31: D

The correct answer is D: Create a script that uses the gcloud storage command to synchronize the on-premises storage with Cloud Storage, Schedule the script as a cron job.

Let's break down why this is the best option:

1. This approach allows the use of Cloud Storage, which is a more appropriate service for storing large amounts of unstructured medical images data compared to other options. Cloud Storage is specifically designed for large-scale object storage, providing low latency and high availability, which is crucial in the medical industry.
2. The gcloud storage command makes it possible to directly transfer the medical images from the on-premises storage to Cloud Storage, avoiding unnecessary complexity.
3. The use of a cron job ensures the automation of image transfers at a scheduled interval, making it easier to maintain and update the process.

Now, let's discuss why the other options are not suitable:

Option A: Though this option uses Cloud Storage for storing the medical images, it does not automate the process since it does not use a cron job or script.

Option B: The use of Datastore is inappropriate for storing medical images. Datastore is a NoSQL database designed for structured data, not for large unstructured files like medical images. Moreover, in this option, the script is transferring images to Datastore, which is less efficient than directly syncing images to Cloud Storage.

Option C: The use of Cloud Spanner is inappropriate for the same reasons as Datastore. Cloud Spanner is a global, highly scalable relational database, but it's not suitable for storing large unstructured files like medical images. Additionally, the script transferring the images to Cloud Spanner would be less efficient than directly synching images to Cloud Storage.

In conclusion, option D is the most suitable choice to design and implement the solution, as it utilizes Cloud Storage and automates the process with a cron job. This ensures seamless backup of the medical images while providing the required availability and durability.

Solution to Question 32: B

The correct answer is option B, and here's why:

Option B is the best practice in this scenario because it adheres to the principle of least privilege, which is a core aspect of any organization's security best

practices. By creating separate service accounts for each pipeline, you ensure that each CI/CD pipeline has the necessary permissions without providing excessive access. Minimal IAM permissions limit the risk of unauthorized actions or resource manipulation.

Using a secret manager service is also a recommended approach to store and manage key files securely. The CI/CD pipeline requests the appropriate secrets during execution, which helps to automate the process, reduce human errors, and improve overall security.

Option A is not the best solution because allowing a service account to impersonate a Cloud Identity user with elevated permissions can lead to potential security risks and misconfiguration. It violates the principle of least privilege by providing more access than required for the specific task, potentially opening up the system to vulnerabilities.

Option C is not advisable as using API keys for authentication on compute instances is not a secure way of handling permissions. API keys can be easily leaked, and they don't provide the granular permission control and auditing features that service accounts offer with IAM permissions.

Option D is not a good choice because using the Compute Engine default service account for provisioning resources usually means broad access to many or all services. This setup violates the principle of least privilege and is not optimal for security best practices.

Solution to Question 33: D

The correct answer is D. Review details of myapp-deployment-58ddbbb995-lp86m Pod and check for warning messages.

Explanation: When a pod is in PENDING status, it indicates that there might be an issue at the pod level or related to Kubernetes cluster resources. In this case, examining the details and warning messages of the pending pod can help to identify any potential issues.

Option A, reviewing details of the myapp-service Service object and checking for error messages, is not the right choice because Service objects are responsible for exposing the application to the network or other services. If there were an issue with the Service object, the application might not be reachable, but it would not cause a pod to remain in PENDING status.

Option B, viewing logs of the container in myapp-deployment-58ddbbb995-lp86m pod and checking for error messages, is not suitable as the logs are only accessible when a container is running. Since the pod is still in PENDING status, we cannot access the container logs yet.

Option C, reviewing details of the myapp-service Service object and checking for warning messages, is also incorrect for the same reason as option A. Issues with the Service object would not cause the pod to remain in PENDING status.

Hence, option D is the most appropriate choice to address the issue at hand. Reviewing the details of the pending pod (myapp-deployment-58ddbbb995-lp86m) and looking for warning messages will help in identifying the problem causing the pod to remain in PENDING status.

Solution to Question 34: B

The correct answer is B. Deploy the application to Cloud Run and use gradual rollouts for traffic splitting. This is the best approach for a serverless deployment in Google Cloud because Cloud Run is specifically designed for serverless applications. Gradual rollouts enable you to control the traffic distribution between two revisions of a service, which is perfect for testing a new version of the application by exposing it to a small portion of the production traffic.

Option A is incorrect because Datastore, now Cloud Firestore, is a NoSQL database service designed for storing, retrieving, and managing semi-structured data. It does not cater to serverless application deployment and traffic splitting.

Option C is not the best choice because Google Kubernetes Engine (GKE) is an orchestration service for managing Docker containers, not primarily designed for serverless deployments. Although GKE can deploy serverless applications using Cloud Run for Anthos, using Anthos Service Mesh for traffic splitting adds complexity and is not a serverless-native solution like Cloud Run. Gradual rollouts in Cloud Run provide a simpler and more suitable solution.

Option D is also incorrect because Cloud Storage is an object storage service that is used for storing and serving unstructured data like images, audio, video, or other large objects. It is not a platform for deploying serverless applications, and object ACLs are used for controlling access to those objects, not for traffic splitting.

Solution to Question 35: C

The correct answer is C. Use Cloud Spanner for data storage.

Here's why the other options do not work:

A. Use Firestore for data storage: Although Firestore is a flexible, scalable NoSQL cloud database, it does not provide the relational structure required for a financial trading application. Firestore is better suited for mobile and web applications demanding flexible data structures, real-time updates, and offline support.

B. Use Cloud Memorystore for data storage: Cloud Memorystore is a managed in-memory cache service that works with Redis and Memcached. While it's useful for enhancing the performance of applications by caching frequently-used data, Memorystore is not designed for storing relational data or serving as the primary data storage for an application.

D. Use Cloud Pub/Sub for data storage: Cloud Pub/Sub is a messaging service that allows applications to communicate through messages. It is not a storage

system, and therefore, inappropriate for storing relational data required for a financial trading application.

Now, let's focus on why the Cloud Spanner (option C) is the best choice for these requirements:

C. Use Cloud Spanner for data storage: Cloud Spanner is a fully managed, horizontally scalable, strongly consistent relational database service designed for mission-critical applications. It provides low-latency global data access and ensures that clients worldwide access the same data.

1. Relational structure: Cloud Spanner supports relational data modeling, which is crucial for financial applications. It combines the benefits of traditional relational databases with the scalability and performance of modern cloud-based databases.
2. Global user base: Cloud Spanner is designed for worldwide deployment, providing high availability and strong consistency across regions. This capability ensures that all clients, regardless of location, access up-to-date and accurate data.
3. Minimal latency: Cloud Spanner can span multiple regions, providing low-latency data access for users in different geographical locations. This feature is essential for a financial trading application, as it supports fast data retrieval and update processes, ultimately leading to better user experiences.

In summary, Cloud Spanner best suits the requirements of designing a financial trading application with a global user base, relational data structure, and minimal latency for clients worldwide.

Solution to Question 36: A

The correct answer is A: Enable parallel composite uploads using gsutil on the file transfer.

Explanation for why the answer should be A: Enabling parallel composite uploads using gsutil on the file transfer is the right choice because it will significantly increase the transfer speed. Parallel composite uploads divide the file into multiple parts and upload them simultaneously, making the most of the available 1 Gbps WAN connection. This method also ensures a faster and more efficient transfer of the large 32 GB file from your machine to the Nearline Storage bucket.

Why other options will not work:

B. Increase the latency on the machine initiating the transfer: Increasing the latency on the machine initiating the transfer is counterproductive to our goal of ensuring the fastest possible transfer. High latency typically results in slowed data transfer rates, as it causes more waiting time and slows down communication between the server and client.

C. Change the storage class of the bucket from Nearline to Multi-Regional: Changing the storage class of the bucket from Nearline to Multi-Regional is not helpful in speeding up the file transfer process. The storage class relates to the redundancy and pricing model of the data storage rather than its data transmission rate. While Multi-Regional may be useful for frequently accessed data, it doesn't inherently improve the data transfer speed.

D. Use the GCP Console to transfer the file instead of gsutil: Using the GCP Console instead of gsutil might not offer the same level of upload optimization. gsutil, when configured correctly (such as enabling parallel composite uploads), is built specifically with the flexibility to optimize and manage file transfers to Google Cloud Storage, whereas the GCP Console is meant for more general interactions with the platform. It may not have the ability to fully utilize the available bandwidth or perform parallel composite uploads for faster transfers.

Solution to Question 37: A

The correct answer should be A: Deploy the container on Cloud Run (fully managed), and set the minimum number of instances to zero.

Reasoning for A being the correct answer: Google Cloud Run (fully managed) is designed specifically for deploying containerized applications in a serverless environment. Setting the minimum number of instances to zero allows the application to automatically scale down to zero instances outside of business hours, thus avoiding any unnecessary costs during non-business hours. Cloud Run also automatically scales based on demand during business hours, making it well-suited for internal use during the specified time.

Reasoning for why other options are incorrect:

B. Deploy the container on Cloud Run for Anthos, and set the minimum number of instances to zero. Cloud Run for Anthos is more suitable for organizations that rely on Kubernetes for their infrastructure. It requires a GKE (Google Kubernetes Engine) cluster, which incurs additional costs and management overhead. Given that the application is meant for internal use and cost optimization, Cloud Run for Anthos is not the most appropriate method compared to fully managed Cloud Run.

C. Deploy the container on Google Compute Engine (GCE) with VM instance scheduling to automatically shut down during non-business hours. While deploying on Google Compute Engine (GCE) with VM instance scheduling can save costs during non-business hours, it does not offer the same ease of deployment, management, and flexibility as Cloud Run. Handling the container scaling and resource allocation on GCE requires more manual work compared to Cloud Run, which automatically scales based on demand.

D. Deploy the container on Cloud Functions, configuring the function to trigger during business hours only. Cloud Functions are designed for event-driven, single-purpose applications, rather than containerized web applications. Deploying the container on Cloud Functions would require re-writing or re-packaging

the application as individual functions. Configuring the function to trigger only during business hours may not be possible, as they are typically triggered by user-defined events or HTTP requests. Therefore, this method would neither be cost-efficient nor suitable for deploying a containerized web application.

Solution to Question 38: A

The correct answer is A. Create a signed URL with a four-hour expiration and share the URL with the company. This method is the most secure and efficient way to share sensitive information with a third-party organization that does not have a Google account. A signed URL allows you to grant temporary access to a specific file for a limited period, in this case, four hours.

Option B, creating an API key and sharing it with the third-party organization, is not the best approach because API keys are a means of authentication, and sharing them poses considerable security risks. Moreover, deleting the API key after four hours does not guarantee that access to the resources will be revoked in a seamless manner.

Option C, creating a new Cloud Storage bucket and deleting it after four hours, is inefficient as it involves unnecessary overhead for managing and securing a temporary bucket. This might lead to faulty configurations that could leave sensitive data exposed.

Option D, using Cloud Functions to create a temporary endpoint, is not as efficient as using a signed URL. This method involves an additional layer of complexity by introducing a serverless function to manage access when a simpler solution, such as the signed URL, exists. Furthermore, depending on how the endpoint is configured, there could be potential security risks or access limitations.

In conclusion, the best approach to sharing a sensitive file with a third-party organization for a limited time is to create a signed URL with a four-hour expiration (Option A) because it provides a secure, efficient, and straightforward solution.

Solution to Question 39: A

The correct answer is A: creating a snapshot schedule for the disk using the desired interval. This is because snapshot schedules in Google Compute Engine provide an automated, cost-effective, and Google-recommended solution for creating, storing, and managing boot disk backups. These snapshots can be used to quickly restore the data in case of disaster, and older backups are automatically cleaned according to the specified retention policy, which helps save costs.

Option B is not suitable because Cloud Memorystore for Redis is specifically designed for managing in-memory data structures, such as caches, and not for storing boot disk backups. Furthermore, it would not provide a way to clean older backups automatically.

Option C is not appropriate because Managed Instance Groups are designed to scale and manage groups of similar instances, not to create periodic backups of a single instance's boot disk. The focus of this feature is on scaling and high availability, not on disaster recovery.

Option D is not the best choice because although you could use Cloud Scheduler to clone the VM instance at the desired interval, it would create a new instance every time instead of creating a backup of the boot disk. This approach would lead to unnecessary complexity, higher costs, and a lack of automatic cleanup for older backups. Therefore, option A, creating a snapshot schedule for the disk, is the most appropriate solution.

Solution to Question 40: A

The answer should be A: Cloud Spanner, because it provides a highly scalable, globally distributed, strongly consistent database service that can handle massive amounts of relational data with minimal configuration changes.

Reasons why other options do not work:

B. Compute Engine is not a storage solution. It is an Infrastructure-as-a-Service (IaaS) platform that provides customizable virtual machines, but does not inherently address the issue of scalable storage for relational data that may grow rapidly.

C. Datastore is a NoSQL database service primarily designed for unstructured, schema-less data, optimized for horizontal scaling with high availability. As your main concern is handling relational data and providing strong consistency, this is not the best fit for your scenario.

D. Cloud SQL provides a managed relational database service, but its scalability is limited compared to Cloud Spanner. Cloud SQL is a regional service rather than a global one, and while it offers limited horizontal scaling, it is not designed for the uncertain, potentially massive user base size your CTO is concerned about.

In conclusion, Cloud Spanner addresses the concerns of a rapidly growing user base and storing relational data with minimal configuration changes, making it the best storage solution in this case.

Solution to Question 41: A

The correct answer is A, and here's why:

A. Going to the Logs ingestion window in Stackdriver Logging and disabling the log source for the GKE container resource is the fastest and most efficient way to disable logs for that container. This method will stop logs from being ingested for that specific container, effectively reducing the costs.

B. Deleting and recreating clusters in the GKE console is not an efficient or quick solution. This approach would involve much more work, cause unnecessary downtime for your applications, and could potentially lead to data loss.

Moreover, disabling legacy Stackdriver Monitoring is not related to the logs ingestion issue.

C. Removing permissions for the GKE container in the IAM console will not necessarily stop the logs from being produced. Instead, it may cause unintended side effects and disrupt the functionality of the container. This could, in turn, lead to other issues within your application.

D. Creating a "no-op" sink for the GKE container resource in the Log Router would, in theory, prevent the logs from being sent to their destination. However, this method is more complex and less efficient compared to disabling logs directly at the log source (Option A). Additionally, the option is labelled incorrectly as it should be option 1 instead of 2.

Thus, Option A is the correct choice as it offers a quick, efficient and targeted solution to disable logs for the GKE container resource. The other options either require more work, lead to potential issues, or are not directly related to the problem at hand.

Solution to Question 42: A

The correct answer is A. When creating the instances, specify a Service Account for each instance.

Option A is the best choice because specifying distinct service accounts during the creation of each instance will allow you to control access to Google Cloud APIs with greater granularity. This will provide appropriate access control on a per-instance and per-client basis, ensuring that only necessary APIs are accessible and reducing the potential for unauthorized access or API abuse.

Option B is not a valid choice because using "gcloud beta compute instances update" cannot be used to change the service account associated with an instance after it has been created. The only way to change the service account would be to recreate the instance.

Option C is incorrect as assigning the IAM role for each service account to their respective instance's metadata does not actually associate the service account with the instances. Metadata can store configuration information about an instance, but it does not grant access privileges like a service account.

Option D is not optimal since assigning a single project-wide service account for all Compute Engine instances will not provide a finer level of granularity. Combining all instances under a single service account would make it more difficult to manage granular access control and may expose unnecessary access to APIs to some instances that shouldn't have them.

In conclusion, the best option in this scenario is A, as specifying a distinct service account for each instance upon creation ensures proper control over access to Google Cloud APIs with the necessary granularity.

Solution to Question 43: B

The correct answer is B: Migrate to use a Local SSD on the instance.

Explanation: The application is primarily dealing with reading large files from disk, and is experiencing excessive disk read throttling on its Zonal SSD Persistent Disk. To ensure maximum throughput while keeping costs low, migrating to use a Local SSD is the most appropriate solution.

Local SSDs provide high-performance block storage, with lower latency and higher IOPS than Zonal SSD Persistent Disks. This can help alleviate the disk read throttling issue by providing better read performance for large files. Additionally, since Local SSDs are physically attached to the instance, they can offer more predictable performance compared to network-attached storage like Zonal SSDs.

Now let's look at why the other options are not suitable:

A. Use a Standard Persistent Disk instead of Zonal SSD Persistent Disk: Standard Persistent Disks have lower performance than Zonal SSD Persistent Disks, and they generally provide lower throughput and IOPS. Switching to Standard Persistent Disk would most likely exacerbate the disk read throttling issue, rather than resolve it.

C. Increase the size of the disk to 2 TB: Although increasing the disk size can improve IOPS (Input/output operations per second), it's not guaranteed to solve the excessive disk read throttling issue completely. Zonal SSD Persistent Disks are still subject to network constraints, which may still cause performance issues while dealing with large files. Additionally, increasing the storage size may incur unnecessary costs without truly solving the problem.

D. Configure the instance with more RAM: While adding more RAM could potentially improve the instance's performance in general, it won't directly address the issue of excessive disk read throttling. The application is primarily dealing with disk reads, so improving disk performance will have a more significant impact on the overall performance.

Solution to Question 44: A

The correct answer is A because creating a custom role that includes only the necessary permissions, such as compute.disks.list and compute.images.list, follows the Google-recommended practice of the Principle of Least Privilege (PoLP). This principle states that a user should only have the minimum permissions required to perform their tasks. By granting the custom role to the user at the project level, you can ensure that the external collaborator has access only to the specific project resources they need without giving them broader access to other areas.

Option B is incorrect because, although it involves creating a custom role, it is based on the Compute Storage Admin role, which includes many other permissions that may not be necessary for the collaborator's tasks. By excluding unnecessary permissions, you can still achieve the principle of least privilege;

however, it would be more efficient and secure to create a custom role from scratch with only the needed permissions.

Option C is incorrect because granting the Compute Storage Admin role at the project level will provide the collaborator with a wide range of permissions that may not be necessary for their work. This violates the Principle of Least Privilege and could lead to potential security risks by giving the collaborator more access than they need.

Option D is incorrect because granting the Compute Storage Admin role and the Compute Image Admin role at the organization level would give the collaborator access to resources across the entire organization, not just the specific project they are working on. This can lead to unnecessary exposure of sensitive data and resources, as well as violations of the Principle of Least Privilege.

Solution to Question 45: A

Option A is the correct answer because setting an organizational policy constraint on your Google Cloud resources will help ensure that only users within the specified domain have access to your company's resources. By limiting identities by domain, you can prevent the addition of mismatched users in the future. After setting this constraint, you can then go back and remove any current mismatched users to ensure your resources are only shared with users within your domain.

Option B is incorrect because creating a custom IAM role alone will not prevent mismatched users from being granted access to your resources. You would still need to manually manage and audit permissions for each user.

Option C is incorrect because configuring a Pub/Sub topic simply acts as a monitoring tool to notify you of mismatched users but doesn't proactively prevent their access. You would still need to manually remove these users and this wouldn't prevent new mismatched users being added.

Option D is incorrect because setting an organizational policy constraint to limit identities by domain is an essential step, but it won't automatically remove existing mismatched users. You must take the additional step of retroactively removing these users to ensure full compliance with the organizational policy constraint.

Solution to Question 46: D

The correct answer is D: Search for the CMS solution in Google Cloud Marketplace. Deploy the solution directly from Cloud Marketplace.

Explanation:

Option D is the most efficient method because Google Cloud Marketplace is a centralized platform where developers can easily find, research, and deploy preconfigured and pre-tested applications and solutions. Since the CMS solution you're implementing is specific and popular, it's likely to be available on Google

Cloud Marketplace. This method will save you time and effort compared to setting up and configuring the solution manually.

Reasons why other options will not work:

A. Use the installation guide of the CMS provider. Perform the installation through your configuration management system.

This option will not be the most efficient method because it requires manual configuration and manual installments that can take more time compared to deploying directly from the Cloud Marketplace. It might also increase the chances of installation errors or misconfigurations.

B. Create a custom VM image with the CMS pre-installed, then deploy the image to a new Compute Engine instance.

While this option is possible, creating a custom VM image with the CMS pre-installed can be time-consuming and may require significant effort to ensure proper configuration. Additionally, this method does not take advantage of the convenience and efficiency provided by Google Cloud Marketplace.

C. Manually install the CMS on a new App Engine standard environment instance.

This option is not suitable as the App Engine standard environment is designed to automatically scale applications and may impose certain restrictions (e.g., specific runtime environments, limitations on certain APIs) that could cause compatibility issues with the CMS. Moreover, manually installing the CMS could also be more time-consuming and error-prone compared to deploying it through the Cloud Marketplace.

Solution to Question 47: C

The correct answer is C - Create a temporary account for the auditor in Cloud Identity, and give that account the Viewer role on the project. This is the most suitable option for the following reasons:

1. Option C ensures that the external auditor has only view access and cannot modify project resources. The Viewer role has "read-only" permissions, which means the auditor can view the project's resources and configurations but cannot make changes.
2. It addresses the "Domain Restricted Sharing" requirement by creating a temporary account for the auditor within Cloud Identity. This guarantees that the access is limited to the specific auditor, and the company maintains control over the level of access the auditor has within the project.

Options A, B, and D are not correct due to the following reasons:

A - Giving the Organization Viewer role on the project still allows the auditor access to other projects within the organization, not just the specific project

required for the audit. It also does not address the Domain Restricted Sharing requirement.

B - The App Engine Viewer role provides access to only App Engine resources, and not to all the resources and services within the project. An auditor would require broader access for a complete and comprehensive audit.

D - Giving the auditor the Editor role is a potential security risk, as it allows the external auditor to modify resources, which is contrary to the objective of providing only view access.

Solution to Question 48: D

The correct answer is D. Create a folder to contain all the dev projects. Create an organization policy to limit resources in US locations.

Here is why the other options do not work:

Option A: Creating a label with a "US-only" value and implementing a custom IAM policy based on this label is not the most effective way to restrict resources to US locations. The IAM policy will need constant updates as new resources are added and there is a higher margin for error. Additionally, IAM policies should typically be used for access control, rather than resource location restrictions.

Option B: Manually reviewing and approving all new dev project resources is labor-intensive and inefficient. This approach relies on human effort and increases the likelihood of overlooking resource placements outside the US, leading to potential non-compliance issues.

Option C: Configuring Cloud Monitoring to alert the organization when resources are created outside the US may provide visibility into non-compliant resource creation, but it does not prevent the deployment of such resources in the first place. Moreover, manual deletion of non-US resources is not ideal, as it is an inefficient and reactive approach to ensuring compliance. Relying on manual intervention also introduces the risk of human error.

Option D: Creating a folder to contain all the dev projects and setting up an organization policy to limit resources to US locations is the most effective and efficient solution. This approach enforces compliance by preventing the creation of resources outside the US in the first place, thus minimizing manual intervention and the margin for error. It ensures consistency and simplifies management of resources across all dev projects. For these reasons, Option D should be chosen.

Solution to Question 49: D

The most efficient approach to complete this task while minimizing effort is option D: Go to Data Catalog and search for employee_ssn in the search box.

Explanation:

Option D takes advantage of Google Cloud's Data Catalog, a fully-managed data discovery and metadata management service. By using Data Catalog, you can easily search and discover the needed datasets containing the employee_ssn column with a simple search query. This approach requires minimal effort and is highly efficient.

Option A, writing a script using the Google Cloud SDK, is not the most efficient approach because scanning through every table in all the projects manually would take a significant amount of time and effort. Additionally, writing a script might introduce bugs and require extensive testing to ensure accurate results.

Option B, writing a Cloud Dataflow job, would be more efficient than Option A, but it is still more complex and time-consuming than simply using Data Catalog. Writing a Cloud Dataflow job requires development, testing, and execution efforts – which are more resource-intensive than option D.

Option C, using Stackdriver Logging, would be a highly inefficient solution since it relies on searching logs, which might not even contain the term "employee_ssn" if it's not explicitly logged. Moreover, manually examining the related datasets is a time-consuming process and not a practical approach for managing over 1000 datasets.

In conclusion, option D is the most efficient and optimal approach for this task as it directly addresses the requirement with minimal effort and high accuracy by leveraging the capabilities of Google Cloud's Data Catalog.

Solution to Question 50: A

The correct answer is A. Set the europe-west1-d zone as the default zone using the gcloud config subcommand.

Explanation: Using the gcloud config subcommand allows you to configure various settings under your gcloud CLI environment, including setting a default zone. By executing a command like "gcloud config set compute/zone europe-west1-d", you can set the default zone to europe-west1-d, which will increase efficiency by automatically applying this zone to any commands that require a zone specification.

Reasons why the other options will not work:

B. Creating a bash script that automatically adds –zone=europe-west1-d to all gcloud CLI commands might seem like a viable solution, but it provides a one-off workaround rather than a permanent solution and introduces additional complexity. Furthermore, it cannot handle situations where you might want to use a different zone temporarily or permanently.

C. The Settings page for Compute Engine under the Default location in the Google Cloud Console allows you to set default settings for the Cloud Console, not for the gcloud CLI. The gcloud CLI and Cloud Console are separate environments, each with their own configuration settings.

D. Creating an environment variable named DEFAULT_ZONE with the value europe-west1-d is insufficient, as the gcloud CLI does not recognize this environment variable for setting the default zone. This option may also cause confusion with other applications that might rely on environment variables, making it a less clear and less efficient solution.

Practice Exam 17

Question 1: As a software engineer in a fast-paced tech company, you are tasked with updating a deployment in Deployment Manager while ensuring no resource downtime occurs. Which command should you execute?

A. gcloud deployment-manager resources delete –config

B. gcloud deployment-manager resources list –config

C. gcloud deployment-manager resources update –config

D. gcloud deployment-manager deployments update –config

Question 2: As a software engineer working in a newly established tech company, you are tasked with deploying a containerized application for a new project. The application features an HTTP endpoint with very low daily request volume. To keep costs at a minimum, what is the most appropriate deployment method?

A. Deploy the container on GKE with cluster autoscaling and horizontal pod autoscaling enabled.

B. Deploy the container on Dataflow.

C. Deploy the container on Cloud Run.

D. Deploy the container on Dataproc with auto scaling enabled.

Question 3: As a software engineer working at a cloud-based startup, you create a new Google Kubernetes Engine (GKE) cluster for your company. How can you ensure the cluster consistently runs a supported and stable version of Kubernetes?

A. Create a custom node pool for your GKE cluster.

B. Enable the "Ingress" feature for your GKE cluster.

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

D. Select the "Autoscaling" option for your GKE cluster.

Question 4: You are a software engineer at a company, and your team is tasked with implementing a message processor using Google Cloud services. You need to deploy an application on Cloud Run that will process messages from a Cloud Pub/Sub topic while following Google-recommended practices. What steps should you take to ensure that your setup is compliant with these recommendations?

A. 3. Create an App Engine service that subscribes to the Cloud Pub/Sub topic and then HTTP requests to your Cloud Run application for each message.

B. 7. Use Cloud IoT Core to subscribe to the Cloud Pub/Sub topic and then configure it to push messages to your Cloud Run application using the REST

API.

C. 1. Deploy your application on Cloud Run on GKE with the connectivity set to Internal. 2. Create a Cloud Pub/Sub subscription for that topic. 3. In the same Google Kubernetes Engine cluster as your application, deploy a container that takes the messages and sends them to your application.

D. 1. Create a service account. 2. Give the Cloud Run Invoker role to that service account for your Cloud Run application. 3. Create a Cloud Pub/Sub subscription that uses that service account and uses your Cloud Run application as the push endpoint.

Question 5: You are working as a Cloud Engineer at a software company and have recently made significant changes to a complex Deployment Manager template. To ensure that the dependencies of all defined resources are properly met before committing it to the project, you want to receive the fastest possible feedback on your updates. What step should you take?

A. Execute the Deployment Manager template using the "-preview" option in the same project, and observe the state of interdependent resources.

B. Modify the Deployment Manager template to include real-time monitoring using Firebase and identify any discrepancies in the resources.

C. Copy the Deployment Manager template to a separate storage bucket and set up object versioning to track changes over time.

D. Leverage a custom Cloud Function to validate the Deployment Manager template's resource dependencies before executing it.

Question 6: As a software engineer at a tech company, you have successfully established a development environment for an application utilizing Compute Engine and Cloud SQL. Now, you need to create a production environment for the same application. The security department has strictly prohibited any network routes between the two environments and has requested that you adhere to Google's best practices. What course of action should you take?

A. Create a new project, modify your existing VPC to be a Shared VPC, share that VPC with your new project, and replicate the setup you have in the development environment in that new project in the Shared VPC.

B. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

C. Create two new Cloud SQL instances in the existing project, one for the development environment and one for the production environment, and restrict traffic between them using firewall rules.

D. Create a new separate VPC for the production environment within the existing project and connect the two environments using VPC peering.

Question 7: As a data analyst at a tech company, you need to run an important query in BigQuery to analyze user behavior data. You expect the query to return a large number of records and want to determine the cost of running it while using the on-demand pricing model. What should you do to estimate the cost?

A. Run the query in multiple parts and pay for each part separately.

B. Run the query using the Cloud Dataflow to manage costs for BigQuery.

C. Use the BigQuery UI to estimate the cost without actually running the query.

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

Question 8: As a security engineer at a financial services company, you are tasked with setting up IAM access audit logging in BigQuery for a team of external auditors, following Google's best practices. How should you proceed?

A. Add the auditor user accounts to the 'bigQuery.projectViewer' and 'logging.writer' predefined IAM roles.

B. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

C. Add the auditor user accounts to the 'bigQuery.jobUser' and 'bigQuery.dataOwner' predefined IAM roles.

D. Add the auditors group to the 'bigQuery.viewer' and 'logging.writer' predefined IAM roles.

Question 9: As a cybersecurity professional in a large organization, your company relies heavily on Google Suite and its Google accounts for communication and collaboration. The organization has an operational team responsible for managing a significant number of instances on Compute Engine, and they require only administrative access to these servers. Your company's security team emphasizes the importance of operationally efficient credential deployment, as well as the ability to track individual access to instances. What is the most efficient and secure way to grant the required access to the operational team?

A. Use Cloud Identity-Aware Proxy to authenticate and provide administrative access to the servers. Grant the 'compute.osAdminLogin' role to the Google group corresponding to this team.

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

C. Generate a new SSH key pair. Give the private key to each member of your team. Restrict the access using firewall rules and grant 'compute.osAdminLogin' role to the Google group corresponding to this team.

D. Generate a new SSH key pair. Give the private key to each member of your team. Configure the public key as a project-wide public SSH key in your Cloud

Platform project and allow project-wide public SSH keys on each instance.

Question 10: As a network administrator at a software development company, you currently have a subnet with a mask of 255.255.255.240 that hosts VMs for your development team. The current subnet has no more free IP addresses, and you need to accommodate an additional 10 IP addresses for new VMs without disrupting the existing setup. All VMs, both existing and new, should be able to reach each other without additional routes. What action should you take?

A. Use gcloud to expand the IP range of the current subnet.

B. Create a new project. Use Shared VPC to share the current network with the new project.

C. Upgrade the VMs to larger machine types to increase the number of available IP addresses.

D. Change the subnet mask of the existing subnet to 255.255.255.224.

Question 11: You are an IT specialist at a software company, responsible for managing production and testing workloads of multiple projects. Your company decides to deploy these workloads on Google Compute Engine. The production VMs and test VMs must be hosted in separate subnets but should be able to communicate with each other using Internal IPs without any additional routing configuration. What is the appropriate setup for the VPC and its two subnets to achieve these requirements?

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

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

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

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

Question 12: As a software engineer in a tech company, you've developed an application and packaged it into a Docker image. Your next task is to deploy this Docker image as a workload on Google Kubernetes Engine. What steps should be taken to achieve this?

A. Upload the image to Firestore and create a Kubernetes Service referencing the image.

B. Upload the image to Compute Engine and create a Kubernetes Deployment referencing the image.

C. Upload the image to Container Registry and create a Kubernetes Service referencing the image.

D. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Question 13: As a software engineer at a tech company, you are tasked with deploying a licensing server on Compute Engine for an application that looks for its licensing server on IP 10.0.3.21. The company does not want to change the application configuration, and the application must be able to reach the licensing server. What is the best course of action?

A. Create a custom routing rule to route traffic destined for 10.0.3.21 to the licensing server's actual IP address.

B. Configure the licensing server to listen on all IP addresses in the 10.0.3.0/24 subnet and assign a different static internal IP address to the server.

C. Use the IP 10.0.3.21 as a secondary IP address for the licensing server, and assign it a primary IP address from the same subnet.

D. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

Question 14: As a data analyst working for a logistics company, you are tasked with setting up an archiving process for data stored in a Cloud Storage bucket. The solution must be cost-effective while allowing for occasional access to previous versions of the data for monthly reporting and updates at the end of each month. How should you configure the archiving process?

A. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

B. Add a bucket lifecycle rule that archives data from multi-regional storage after 30 days to Nearline Storage.

C. Add a bucket lifecycle rule that archives data from regional storage after 30 days to Nearline Storage.

D. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Coldline Storage.

Question 15: You are an IT manager at a leading financial services company that extensively uses a Cloud SQL MySQL database for its operations. To comply with regulatory policies, it is necessary to retain a month-end copy of the database for three years for auditing purposes. What should you do?

A. Set up an on-demand backup for the first of the month. Write the backup to an Archive class Cloud Storage bucket.

B. Save the automatic first-of-the-month backup for three years. Store the backup file in an Archive class Cloud Storage bucket.

C. Configure an on-demand backup for the first of the month. Store the backup file directly within the Cloud SQL MySQL database. Create a snapshot of the first-of-the-month database, and store it in an Archive class Cloud Storage

bucket. Set up a scheduled Cloud Scheduler job that will trigger a Cloud Function to extract the month-end database data and store it in a Firestore. Set up a Data Transfer Service to copy the database to Bigtable and retain the month-end copy in an Archive class Cloud Storage bucket. Create a BigQuery scheduled query to transfer a copy of the database into a new dataset on the first of the month and store it in an Archive class Cloud Storage bucket. Configure a serverless export solution using Cloud Run to export the database first-of-the-month to Cloud Spanner, and store in an Archive class Cloud Storage bucket. Configure automated daily export of the entire database, and only store the first of the month copies in a Coldline class Cloud Storage bucket. Create a continuous Dataflow synchronization for the month-end database copy, and store the replicated data into an Archive class Cloud Storage bucket.

D. Set up an export job for the first of the month. Write the export file to an Archive class Cloud Storage bucket.

Question 16: As a developer in a leading software company, you received a notification that your managed instance group raised an alert stating that new instance creation has failed to create new instances. To efficiently handle the expected application traffic, it's crucial to maintain the number of running instances specified by the template. What should be your course of action to resolve this issue?

A. Enable Shielded VMs on the instances and create an instance template that contains valid syntax which will be used by the instance group.

B. Create an instance template with valid syntax, but set the minimum number of instances lower than the expected application traffic in the instance group.

C. Modify the network settings to allow instance creation traffic and delete any persistent disks with the same name as instance names.

D. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

Question 17: As a leading tech company in the software development industry, your organization relies on Google Workspace to manage employee accounts. Your company plans to expand and anticipates an increase in personnel from 100 to 1,000 employees within the next 2 years. The majority of your employees will require access to the company's Google Cloud account. To ensure that your systems and processes can handle this 10x growth without any performance decline, added complexity, or security breaches, what course of action should you take?

A. Turn on Google Cloud Directory Sync (GCDS) for Cloud Identity and skip Multi-Factor Authentication.

B. Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

C. Connect Google Workspace directly to an on-prem LDAP server for authentication and user management.

D. Deploy a custom SSO service using Cloud Functions and connect it to Google Workspace.

Question 18: As a software developer in a tech company, you are managing multiple microservices in a Kubernetes Engine cluster for your organization's applications. One of these microservices is dedicated to rendering images and demands significantly more CPU time compared to the memory it requires. Meanwhile, the other microservices are workloads optimized for n2-standard machine types. To ensure that all workloads utilize resources as efficiently as possible, what should be your approach?

A. Use the node pool with general-purpose machine type nodes for the image rendering microservice. Create a separate node pool with preemptible machine type nodes for the other microservices.

B. Assign the pods of the image rendering microservice a higher pod priority than the other microservices but use the same general-purpose machine type nodes for all microservices.

C. Use the node pool with general-purpose machine type nodes for the image rendering microservice. Create a node pool with compute-optimized machine type nodes for the other microservices.

D. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Question 19: As an IT manager in a growing technology company, you have been tasked with verifying the IAM users and roles assigned within a GCP project named my-project. What is the best course of action to accomplish this task?

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

B. Navigate to the project and then to the APIs & Services section in the GCP Console. Review the roles and project settings.

C. Run gcloud projects describe my-project. Review the output section.

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

Question 20: As a software engineer in a tech company, you are tasked with refactoring the configuration in your company's Kubernetes cluster to prevent the database password from being stored in plain text. In order to adhere to Google-recommended practices, which solution should you implement?

A. Store the database password inside a Cloud Storage bucket and use a Cloud Function to retrieve it during runtime.

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

C. Store the database password in the Compute Engine instance metadata and use a startup script to extract it.

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

Question 21: As a team lead at a software development company, you need to ensure that all developers have the same permissions for Compute Engine, Cloud Functions, and Cloud SQL across various Google Cloud projects while adhering to the company's security policy. Your goal is to enforce this policy with minimal effort. How should you proceed?

A. • Create individual custom roles for Compute Engine, Cloud Functions, and Cloud SQL permissions in each project and assign them to developers.

B. • Assign the default role of Editor to the Google group for each project in the Google Cloud organization.

C. • Enable API access to Compute Engine, Cloud Functions, and Cloud SQL for all developers, without creating custom roles or assigning Google group permissions.

D. • Add all developers to a Google group in Cloud Identity. • Create a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level. • Assign the custom role to the Google group.

Question 22: As a developer at a software company, you are setting up service accounts for an application that spans across multiple projects. Your virtual machines (VMs) operating in the web-applications project require access to BigQuery datasets in the crm-databases-proj. To follow Google's recommended best practices for granting access to the service account in the web-applications project, what action should you take?

A. Create a new project and link crm-databases-proj and web-applications, then give bigquery.dataViewer role to the linked project.

B. Disable BigQuery API in web-applications project and enable it in crm-databases-proj with bigquery.dataViewer role.

C. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

D. Give project owner for web-applications appropriate roles to crm-databases-proj.

Question 23: You are an IT manager at a rapidly growing e-commerce company that was established six months ago. As more clients use your platform, the demand for Google Cloud services continues to rise. To streamline the process for your engineering team, you want them to be able to create new projects

without needing their credit card details. What is the most suitable course of action to achieve this?

A. Grant all engineers permission to create their own billing accounts for each new project.

B. Request Google Cloud to provide a corporate credit card for the entire engineering team.

C. Create a billing account, associate it with a monthly purchase order (PO), and send the PO to Google Cloud.

D. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

Question 24: As an employee of a software development company, you realize that several team members have been launching cloud-based projects and paying for them using their personal credit cards, which are later reimbursed by the company. To streamline and centralize this process, the organization wants to bring all these projects under one billing account. What should be done to accomplish this?

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

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

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

D. Create a billing account in the Google Cloud Console with the company's GCP-related expenses only.

Question 25: As a DevOps engineer in a start-up tech company, you are responsible for deploying a new application using Google Kubernetes Engine with autoscaling enabled. Your task is to ensure that this application is accessible to the public via HTTPS on a public IP address. What should be your approach to accomplish this?

A. Use Google Cloud Endpoints to create a public API for your application, then deploy your application in a GCE instance and configure the public DNS to point to the Endpoints IP.

B. Create a Kubernetes Service of type LoadBalancer for your application, and configure the public DNS to point to the external IP of the LoadBalancer without enabling HTTPS.

C. Create a Google Cloud Storage bucket and upload your application, then use Cloud CDN to expose the public HTTPS endpoint.

D. Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

Question 26: As a network administrator for a growing tech company, you are facing a shortage of primary internal IP addresses in a subnet for your custom mode VPC. The current subnet, with an IP range of 10.0.0.0/20, is primarily used by virtual machines in your department. To accommodate the increasing demands, you need to expand the number of IP addresses available for the virtual machines. What should be your best course of action?

A. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18.

B. Implement Cloud VPN for additional address space.

C. Change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/22.

D. Configure a NAT gateway for the virtual machines.

Question 27: As an IT manager at a corporation, you have been asked to grant an external auditor access to your company's Google Cloud Platform (GCP) Audit Logs and Data Access logs for a security review. Which action should you take to assign the appropriate Cloud Identity and Access Management (Cloud IAM) role to the auditor?

A. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

C. Assign the auditor's IAM user to a custom role that has logging.logEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

D. Assign the auditor's IAM user to a custom role with the permission monitoring.logsWriter. Perform the export of logs to Cloud Storage.

Question 28: As a DevOps engineer at a tech company, you're managing a Google Kubernetes Engine (GKE) cluster that hosts non-production workloads for various teams. Your Machine Learning (ML) team requires access to Nvidia Tesla P100 GPUs for model training, and you need to minimize effort and cost. What action should you take?

A. Configure your cluster to use only GPUs by default for all nodes.

B. Manually install Nvidia Tesla P100 GPUs on the cluster's nodes for your ML team.

C. Ask your ML team to use TPUs instead of GPUs for their training.

D. Add a new, GPU-enabled, node pool to the GKE cluster. Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to

their pod specification.

Question 29: As a software engineer at a tech company, you are responsible for deploying an application on Compute Engine virtual machines (VMs) in us-central1-a. Your goal is to modify the infrastructure to handle the failure of a single Compute Engine zone, avoiding downtime and keeping costs low. What is the most suitable course of action?

A. Use Cloud Pub/Sub with a regional endpoint to balance the load between VMs in us-central1-a and us-central1-b.

B. Create a global Cloud Spanner instance and configure the VMs in us-central1-a and us-central1-b to share the same Spanner database.

C. Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

D. Perform regular backups of your application. Create a Cloud Monitoring Alert and be notified if your application becomes unavailable. Restore from backups when notified.

Question 30: You are working as a system administrator for a software company, and you have been tasked with managing the company's Linux workloads on Compute Engine instances. The company is about to collaborate with a new operations partner who doesn't use Google Accounts. Your responsibility is to provide the operations partner with access to the instances to handle the maintenance of the installed tools. What should be your course of action?

A. Configure a Google Cloud Pub/Sub topic that allows the operations partner to send and receive messages related to instance maintenance.

B. Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User.

C. Enable Cloud NAT and grant the operations partner access to the Cloud NAT gateway to allow traffic redirection.

D. Use Cloud Identity Groups to create a group for the operations partner and add their non-Google account emails to the group.

Question 31: As an IT specialist in a fast-growing tech company, you have been tasked with creating a Compute Engine instance in a new project that has not been created yet. What should you do to accomplish this task?

A. Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

B. Enable Kubernetes Engine API in the Cloud Console, and then use the Cloud SDK to create a Compute Engine instance specifying the new project.

C. Using the Cloud SDK, create the new instance, and use the –project flag to specify the new project. Answer yes when prompted by Cloud SDK to enable the Compute Engine API.

D. Enable the Compute Engine API in the Cloud Console, use the Cloud SDK to create the instance, and then use the –project flag to specify a new project.

Question 32: You are working as a developer at a tech company and recently set up a Deployment with 2 replicas in a Google Kubernetes Engine cluster that has a single preemptible node pool for one of your company's projects. After waiting for a few minutes, you use kubectl to check the status of your Pod and notice that one of them is still in Pending status. What could be the most likely cause for this issue?

A. Google Kubernetes Engine is experiencing an internal error that prevents the Pod from being scheduled.

B. The pending Pod is requesting a specific node or node with a specific label that does not exist in the cluster.

C. A firewall rule is blocking communication between the control plane and the node, preventing the Pod from being scheduled.

D. Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

Question 33: As an IT specialist in a software development company, you've recently set up the Google Cloud CLI on your workstation and configured the proxy. However, you're concerned that your proxy credentials might be recorded in the gcloud CLI logs. To prevent your proxy credentials from being logged, what action should you take?

A. Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

B. Disable logging for the entire gcloud CLI by issuing the command gcloud config set logging/verbosity none.

C. Create a .gcloudignore file in your home directory, and add the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD property names to it.

D. Provide values for CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD in the gcloud CLI tool configuration file.

Question 34: As an IT professional working in a company that uses Google Cloud, your application is currently running in a managed instance group (MIG). You've noticed some errors in Cloud Logging regarding one VM, where a process has become unresponsive. To quickly replace this problematic VM within the MIG, what should you do?

A. Update and apply the instance template of the MIG.

B. Enable autoscaling for the MIG based on CPU utilization.

C. Set the autohealing policy for the MIG to replace unhealthy instances automatically.

D. Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

Question 35: As a member of the IT department in a prominent software development company, you need to ensure that a production application deployed on Compute Engine remains safe from accidental deletion by employees clicking the wrong button. What measure should you take?

A. Disable the flag 'Delete boot disk when instance is deleted.'

B. Enable delete protection on the instance.

C. Disable live migrations for the instance.

D. Enable autohealing on the instance group.

Question 36: As a financial analyst at a technology company, you manage multiple Google Cloud projects for various departments, each linked to different billing accounts. In order to effectively predict and visualize future expenses across all projects, you want a unified view of all incurred costs, updated with new data as soon as possible. How should you proceed?

A. Visit the Cost Table page to get a CSV export and visualize it using Looker Studio.

B. Create a Google Cloud Function to consolidate costs from multiple projects periodically.

C. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio.

D. Export cost data from each billing account to a Google Sheet, and use the Google Sheets API to combine them for visualization

Question 37: As a software engineer in a reputable tech company, your team's application stores files on Cloud Storage using the Standard Storage class. The application only needs access to files created within the last 30 days. In order to automatically save costs on files that are not accessed by the application anymore, what should be your best course of action?

A. Enable object versioning on the storage bucket and add lifecycle rules to expire non-current versions after 30 days.

B. Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

C. Set a custom metadata key on the objects in the storage bucket to mark them for deletion after 30 days.

D. Enable Cloud CDN to cache objects in the bucket and allow 30-day expiration on the cached items.

Question 38: As a tech company that processes huge data from various clients every night, you currently use a large number of virtual machines (VMs) for

fault-tolerant batch workloads. However, the cost of these VMs is becoming a concern. What should be done to mitigate this issue without impacting the performance of the workloads?

A. Run a test using Cloud Run. If the test is successful, use N1 Standard VMs in the Cloud Run service when running future jobs.

B. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs.

C. Run a test using a managed instance group. If the test is successful, use N1 Standard VMs in the managed instance group when running future jobs.

D. Run a test using Google Compute Engine (GCE). If the test is successful, use preemptible N1 Highmem VMs when running future jobs.

Question 39: As an IT security specialist at a leading tech company, you are tasked with creating a custom IAM role for a GCP service that will be used in a production environment. This will be the first version of the custom role, and it is crucial to effectively communicate its status within your organization. How should you proceed?

A. Use permissions in your role that use the 'deprecated' support level for role permissions. Set the role stage to BETA while testing the role permissions.

B. Use permissions in your role that use the 'testing' support level for role permissions. Set the role stage to BETA while testing the role permissions.

C. Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

D. Use permissions in your role that use the 'deprecated' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

Question 40: You are working as a DevOps engineer at a software company and tasked with setting up a Jenkins installation to build and deploy source code for a new application. The goal is to automate the installation process in the most efficient and time-effective method possible. What should be your next step?

A. Create a new Kubernetes Engine cluster. Create a deployment for the Jenkins image.

B. Deploy Jenkins through the Google Cloud Marketplace.

C. Create a new Cloud Storage bucket, upload the Jenkins executable, and use it to deploy your application.

D. Create a new Dataproc cluster and use it to install Jenkins.

Question 41: As a software engineer in a gaming company, you've recently created a multiplayer mobile game hosted on Google Cloud. Users connect to the game using their smartphones via the Internet, and the game relies on

UDP packets to update the servers with player actions. To accommodate the growing user base, you've designed the game backend to scale over multiple virtual machines (VMs) and now need to expose the VMs through a single IP address. Which option should you implement?

A. Utilize Cloud Armor with the application servers to distribute traffic.

B. Configure an External Network load balancer in front of the application servers.

C. Configure an External HTTP(s) load balancer in front of the application servers.

D. Configure an External TCP Proxy load balancer in front of the application servers.

Question 42: As a software engineer working at a cybersecurity company, you have recently launched a new version of an application on Google App Engine. However, you identified a critical bug in the release and need to revert to the previous version without delay. What would be the most appropriate course of action to achieve this?

A. Stop the current version on the App Engine page, then restart the previous version. Use gcloud app migrations command to revert to the previous version. On the App Engine Services page of the GCP Console, delete the faulty version and select the prior version to be live. Use gcloud app versions command to switch to the previous version of the application.

B. Create a new App Engine instance and deploy the prior version, then route traffic to the new instance. Utilize storage service backups to restore the prior version to the App Engine. Revert the faulty code changes through Git, then deploy the resulting version to App Engine. On the GCP Console, choose GCP Datastore and rollback to an earlier snapshot to restore the application before the bug was released.

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

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

Question 43: As a security analyst in a multinational corporation, you need to determine when users were added to Cloud Spanner Identity Access Management (IAM) roles on your company's Google Cloud Platform (GCP) project. Which action should you take in the GCP Console?

A. Visit the Cloud Spanner section in the GCP Marketplace and review details.

B. Open the Cloud Pub/Sub console and create a new topic related to IAM roles.

C. Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

D. Go to the Cloud Functions console and create a function that monitors IAM roles in Cloud Spanner.

Question 44: As an IT consultant working in a software development company, you have a development project with appropriate IAM roles defined. You are now tasked with setting up a production project while maintaining the same IAM roles on the new project, ensuring to minimize the steps involved. What is the most effective approach to accomplish this goal?

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

B. Manually create the same IAM roles in the production project using gcloud iam roles create.

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

D. Use gcloud iam roles copy, specifying both the development and production projects as the source projects.

Question 45: You work for a company in the media industry, managing large files on an Apache web server that runs on a Compute Engine instance within your Google Cloud project. This project also hosts other applications. In order to monitor expenses, you need to ensure that you receive an email whenever the egress network costs for the server exceed 100 dollars in the current month, as calculated by Google Cloud. How should you proceed?

A. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

B. Set up a budget alert on the Compute Engine instances with an amount of 100 dollars, a threshold of 100%, and notification type of email.

C. Use the Cloud Logging Agent to export the Apache web server logs to Cloud Logging. Create a Cloud Function that uses BigQuery to parse the HTTP response log data in Cloud Logging for the current month and sends an email if the size of all HTTP responses, multiplied by current Google Cloud egress prices, totals over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

D. Create a billing export to a Google Cloud Storage bucket. Create a Cloud Function that reads the exported data, calculates the egress costs for the current month, and sends an email when the cost exceeds 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run daily.

Question 46: As a software engineer at a leading technology company, you have designed an application consisting of multiple microservices, with each one packaged in its own Docker container image. To deploy this application on Google Kubernetes Engine and enable individual scaling for each microservice, what action is required?

A. Create and deploy a Deployment per microservice.

B. Create and deploy a Bundle per microservice.

C. Create and deploy an App Engine Module per microservice.

D. Create and deploy a Job per microservice.

Question 47: As a software engineer in a technology company, you've completed testing for an App Engine application in a development environment. Your next step is to create a new project for the production environment. What action should you take?

A. Migrate the development environment to the production environment using a separate branch in your Version Control System.

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

C. Use Dataflow to copy the application code from one project to another for deployment.

D. Use the GCP Console to create a new project, and then manually copy the source code of the App Engine application.

Question 48: As a software developer in a tech company, you have been granted access to a Google Cloud project by receiving a JSON file containing a Service Account's private key. You've successfully installed the Cloud SDK on your system and need to use this private key for authentication when executing gcloud commands. What is the appropriate course of action you should take?

A. Place the private key file in the Cloud SDK installation directory and set the environment variable GOOGLE_APPLICATION_CREDENTIALS to its path.

B. Use the command gcloud auth activate-service-account and point it to the private key.

C. Use the command gcloud auth login and point it to the private key.

D. Use the command gcloud projects add-iam-policy-binding and point it to the private key.

Question 49: As an IT administrator at a software company, you are in charge of managing service accounts for various projects. You need to use a service account from a project named proj-sa to take snapshots of VMs operating in a different project called proj-vm. What action should you take to achieve this?

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

B. Add the service account email as a member in proj-vm without assigning any role.

C. Enable Google Cloud Storage JSON API in proj-vm and use the proj-sa service account JSON key for authentication.

D. Grant the service account the IAM Role of Compute Instance Admin in the project called proj-vm.

Question 50: You are working as a Cloud Engineer at a software company and need to permanently delete a Pub/Sub topic managed by Config Connector in your Google Cloud project. What should you do?

A. Use Firebase CLI to delete the topic resource.

B. Use Config Connector to manually remove the topic resource.

C. Use kubectl to delete the topic resource.

D. Use GCP Console to update the topic label managed-by-cnrm to false.

Practice Exam 17 Solutions

Solution to Question 1: D

The correct answer is D. You should execute the command: gcloud deployment-manager deployments update –config to update a deployment in Deployment Manager without causing resource downtime. This command allows you to update an existing deployment by specifying the new configuration file, while ensuring that resources are updated seamlessly to avoid any downtime.

Option A (gcloud deployment-manager resources delete –config) is incorrect because it will delete the specified resources within the deployment, which could lead to downtime while the resources are being recreated.

Option B (gcloud deployment-manager resources list –config) is also incorrect as it only lists the resources controlled by the deployment, without performing any actions to update or ensure no resource downtime.

Option C (gcloud deployment-manager resources update –config) is not correct because there is no 'resources update' command in gcloud. The correct command to update a deployment, as stated above, is "gcloud deployment-manager deployments update –config ", which ensures that resources are updated without causing any downtime.

Solution to Question 2: C

The most appropriate deployment method for this scenario is option C, deploying the container on Cloud Run. Here are the explanations why option C is the best choice and why other options will not work:

Option A: Deploy the container on GKE with cluster autoscaling and horizontal pod autoscaling enabled. - GKE (Google Kubernetes Engine) can be a suitable choice for deploying containerized applications. However, in this case, the application has a very low daily request volume, which means that the underlying infrastructure could be underutilized. Enabling cluster autoscaling and horizontal pod autoscaling would incorporate extra overhead and management that isn't necessary given the low volume of requests. GKE is typically used for applications with moderate-to-high traffic and complex deployment scenarios.

Option B: Deploy the container on Dataflow. - Dataflow is a managed service primarily designed for processing large-scale data, such as big data and data streaming pipelines. It is not tailored for deploying containerized applications with an HTTP endpoint. Therefore, using Dataflow for this purpose is not appropriate and would not be cost-effective.

Option C: Deploy the container on Cloud Run. - Cloud Run is a fully managed serverless compute platform for containerized applications. It automatically scales and handles incoming HTTP requests without the need for manual configuration or management of the underlying infrastructure. Cloud Run is an ideal choice for this scenario because it is designed for applications with low-to-

high traffic volumes, providing cost efficiency for the low daily request volume requirement, while also offering the scalability to accommodate any potential future growth.

Option D: Deploy the container on Dataproc with auto scaling enabled. - Dataproc is a managed service designed to handle Apache Hadoop and Apache Spark workloads. It is not meant for deploying containerized applications serving HTTP endpoints. Just like Dataflow, using Dataproc for this purpose would not be suitable and would incur unnecessary costs.

In conclusion, the most appropriate deployment method in this case is option C, deploying the containerized application on Cloud Run, as it provides the required functionality, cost-efficiency, and scalability for a low daily request volume application while minimizing overhead and management.

Solution to Question 3: C

The correct answer is C: Enable the Node Auto-Upgrades feature for your GKE cluster.

Enabling the Node Auto-Upgrades feature will ensure that the cluster consistently runs a supported and stable version of Kubernetes. This is because when the Node Auto-Upgrades feature is enabled, GKE automatically upgrades the nodes in the cluster to the latest supported and stable Kubernetes version. This not only keeps your cluster up-to-date but also ensures that you receive the latest security patches and bug fixes.

Here's why the other options are not suitable:

A. Create a custom node pool for your GKE cluster: A custom node pool allows you to create nodes with specific requirements, such as different machine types or additional resources. While this can be useful for customizing the applications running on your cluster, it does not inherently ensure that the cluster runs a supported and stable version of Kubernetes.

B. Enable the "Ingress" feature for your GKE cluster: The Ingress feature is used to create and manage an entry point for HTTP(S) traffic into your cluster. It does not, however, ensure that the cluster consistently runs a supported and stable version of Kubernetes. Ingress is related to network traffic management and has no influence on the underlying Kubernetes version.

D. Select the "Autoscaling" option for your GKE cluster: Autoscaling is a feature that automatically adjusts the number of nodes in a cluster based on the workload and resource demands. While this can help ensure that your cluster is adequately sized for its workload, it does not ensure that the cluster runs a supported and stable version of Kubernetes. Autoscaling is primarily concerned with scaling the number of nodes, not upgrading the Kubernetes version running on those nodes.

Solution to Question 4: D

The correct answer is D because it follows the Google-recommended practices for integrating Cloud Run with Cloud Pub/Sub. Here's an explanation for each step:

1. Creating a service account: Following the principle of least privilege, a dedicated service account should be created with the minimum permissions required to perform the task.
2. Giving the Cloud Run Invoker role to the service account: The Cloud Run Invoker role allows the service account to securely invoke Cloud Run applications. This role is essential for allowing the push endpoint to process messages from Cloud Pub/Sub.
3. Creating a Cloud Pub/Sub subscription: This step sets up the subscription using the service account created in step 1 and uses the Cloud Run application as the push endpoint to process the messages.

Options A, B, and C are not compliant with Google-recommended practices for the following reasons:

Option A: App Engine is not required for this setup, as Cloud Run can directly receive messages from Cloud Pub/Sub. Additionally, this creates unnecessary overhead and may result in greater latency when processing messages.

Option B: Cloud IoT Core is inappropriate for this use case, as it is specifically designed for integrating IoT devices with Google Cloud services and not for straightforward integration with Cloud Run. Furthermore, Cloud Run does not need a REST API to work with Cloud Pub/Sub; it can receive messages directly.

Option C: Although deploying the application on Cloud Run on GKE is a viable option in some cases, it is not necessary for this use case, as Cloud Run can directly receive messages from Cloud Pub/Sub. Deploying a separate container in the same Google Kubernetes Engine cluster to handle messages introduces additional management and complexity to the setup.

Solution to Question 5: A

The correct answer is A. Execute the Deployment Manager template using the "-preview" option in the same project and observe the state of interdependent resources. This is because the "-preview" option allows you to see a preview of the resources that will be created, modified, or deleted, without actually making any changes to the resources in the deployment. This gives you the fastest possible feedback regarding the state of the dependencies and whether the Deployment Manager template works as expected.

Option B is incorrect because adding real-time monitoring with Firebase is not specifically designed to solve dependency issues in Deployment Manager templates. Additionally, adding Firebase would complicate the template further and possibly introduce more errors.

Option C is incorrect because copying the template to a separate storage bucket and setting up object versioning would only track changes to the template over

time, rather than providing immediate feedback on the dependency of the resources used in the template.

Option D is incorrect because using a custom Cloud Function may not provide an accurate validation of the resource dependencies. It can also add complexity to the solution and require additional resources to maintain. The "-preview" flag simplifies the process and offers faster feedback to identify any discrepancies within the Deployment Manager template.

Solution to Question 6: B

The correct answer is B. Create a new project, enable the Compute Engine and Cloud SQL APIs in that project, and replicate the setup you have created in the development environment.

Here's why:

B is the only option that completely separates the development and production environments while adhering to Google's best practices for security, thereby ensuring that there are no network routes between the two environments, as per the security department's requirements.

Option A involves modifying the existing VPC to be a Shared VPC and sharing with the new project. However, this approach does not guarantee complete isolation between the development and production environments, which is a requirement in this case.

Option C suggests creating two new Cloud SQL instances in the existing project but separating them using firewall rules. This is not an ideal solution, as firewall rules can accidentally be misconfigured or bypassed. Using separate projects as in option B ensures a higher level of isolation and security.

Option D involves creating a new VPC for the production environment and connecting the two environments using VPC peering. This option does not adhere to the security department's requirement of prohibiting network routes between the two environments as VPC peering will create a direct network connection between the two environments. This option also does not follow Google's best practices for security, as VPC peering can introduce possible unintended network access.

Thus, option B is the most suitable course of action, as it adheres to the security requirements and Google's best practices by creating a completely separate project for the production environment, enabling the appropriate APIs, and replicating the development environment's setup.

Solution to Question 7: D

The correct answer is D, using the command line to run a 'dry run' query to estimate the number of bytes read before converting that bytes estimate to dollars using the Pricing Calculator.

Option A would not work as running the query in multiple parts and paying for each part separately does not help in estimating the cost beforehand. In fact, it may increase the total cost due to additional query processing, especially if the data is not properly partitioned or if each part involves complex operations.

Option B is not right because running the query using Cloud Dataflow does not directly address the problem of cost estimation. While Cloud Dataflow can help manage costs for BigQuery by processing and transforming data, it does not provide a cost estimation for running the query.

Option C is not accurate because the BigQuery UI, although it shows the amount of data processed in a query, does not provide an estimated cost without actually running the query. The UI shows the amount of data processed as a post-execution data point, which does not avoid costs stemming from running large queries in BigQuery.

Option D is the best choice because it allows you to estimate the cost without actually running the query. By running a dry run query using the command line, you can see the number of bytes that would be read if the query were executed. Once you have this information, you can use the Pricing Calculator to convert the bytes read into a cost estimation based on the on-demand pricing model. This allows you to understand the potential query cost upfront, helping you manage your budget and avoid unexpected charges.

Solution to Question 8: B

The correct answer is B. Add the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles.

The reason for choosing option B is that it follows Google's best practices for providing the appropriate level of access and security to the team of external auditors. By adding the auditors group to the 'logging.viewer' and 'bigQuery.dataViewer' predefined IAM roles, the auditors will have the necessary permissions to view logs and data in BigQuery, which is crucial for auditing purposes.

Option A is not the best choice because it involves adding individual user accounts to the roles rather than a group. Managing access for a group of auditors is easier when they are added to a group. Additionally, the 'logging.writer' role is not necessary for auditors as it permits writing logs, which is not required for their job.

Option C is also not ideal because it gives the auditors more privileges than they need. The 'bigQuery.jobUser' role allows them to run jobs, and the 'bigQuery.dataOwner' role grants them full access to datasets and tables, including the ability to modify or delete data. This is not in line with the principle of least privilege, which states that users should have only the minimum necessary permissions to do their job.

Option D is not suitable because it combines the 'bigQuery.viewer' role, which

is not necessary for auditors, with the 'logging.writer' role, which is also not required. The 'bigQuery.viewer' role allows users to view all resources in the project, including datasets, tables, and views, but it does not grant them access to the data itself. This is not sufficient for auditors who need to view the actual data for audits. Additionally, the 'logging.writer' role is not needed as auditors do not need to write logs.

In summary, option B is the correct answer as it follows Google's best practices for providing the appropriate level of access and security to a team of external auditors, while the other options do not meet the requirements or follow best practices.

Solution to Question 9: B

The correct answer is B. Let's explain why this is the most efficient and secure way to grant the required access to the operational team, and why the other options will not work.

Option A: Cloud Identity-Aware Proxy (IAP) is primarily used to control access to web applications, but it doesn't handle SSH access to Compute Engine instances. IAP for TCP forwarding could be used for SSH, but this adds operational complexity since you have to enable IAP for TCP forwarding on every administrative action. This is not operationally efficient for managing a large number of instances, therefore option A is not the best option.

Option B: This is the best option because it offers operational efficiency and secure authentication. By having each team member generate their own SSH key pair and add the public key to their Google account, it promotes good security practice by using unique keys. Additionally, individual access can be easily tracked since each member will have their own key. Granting the 'compute.osAdminLogin' role to the Google group means that the entire team will have administrative access to the instances in a convenient and manageable way.

Option C: Although this option creates restrictions using firewall rules and grants the 'compute.osAdminLogin' role, the major issue is giving the same private key to each team member. This poses a security risk, as it's difficult to distinguish between users and track individual access. There is also no easy way to revoke a specific user's access without revoking access for the entire team. Therefore, option C is not the optimal choice.

Option D: Similar to option C, this method involves sharing the same private key among team members, which poses the same security risks and is not optimal for controlling individual access. Additionally, setting the public key as a project-wide key could result in potential security vulnerabilities due to its wider accessibility.

In conclusion, option B is the most efficient and secure way to grant the required access to the operational team, as it ensures unique SSH key pairs for each individual member, making it easier to track access, maintain security and manage the team's administrative access to the servers.

Solution to Question 10: A

The correct answer is A. Use gcloud to expand the IP range of the current subnet.

Explanation:

A. Using gcloud to expand the IP range of the current subnet allows you to accommodate the additional 10 IP addresses needed for new VMs without disrupting the existing setup. This ensures that all VMs, both existing and new, can communicate with each other without additional routes. Expanding the IP range is the most appropriate solution considering the requirement of having no disruption within the current network architecture.

B. Creating a new project and using Shared VPC to share the current network with the new project is not appropriate in this scenario. This solution requires additional overhead and might lead to complexities in managing the resources. It also does not directly address the need for more IP addresses in the current subnet, which is the primary requirement.

C. Upgrading the VMs to larger machine types does not increase the number of available IP addresses in the subnet. This option doesn't address the issue directly and implies additional unnecessary costs for the company by upgrading the VMs to larger machine types that may not be required for their workloads.

D. Changing the subnet mask of the existing subnet to 255.255.255.224 might seem like a solution at first glance, but it's not a recommended approach. This method would require reconfiguring all devices' subnet masks in the network and could potentially cause a disruption in the existing setup. Moreover, it could also lead to downtime and hinder the seamless nature of communication required amongst the VMs.

In conclusion, Option A is the best option because it addresses the requirement of needing additional IP addresses in the current subnet without any disruptions or unnecessary overhead.

Solution to Question 11: B

The correct answer is B. The reason behind choosing this option is that creating a single custom VPC with 2 subnets, each subnet in a different region, and with different CIDR ranges allows the separation of production and testing workloads. This setup enables VMs in both subnets to communicate using Internal IPs without any additional routing configuration since subnets within the same VPC can communicate with one another regardless of their region.

Here is why the other options won't work:

A. This option involves creating a single custom VPC with 2 subnets in different zones within the same region. While this configuration does satisfy the requirement of having separate subnets with different CIDR ranges, locating subnets in different zones of the same region is not necessary. The question does not

state that the environments need to be in the same region, and the different regions can provide better separation of production and testing workloads.

C. Creating 2 custom VPCs, each with a single subnet, in the same region and with the same CIDR range is not a suitable option. This setup will not allow communication between VMs in each subnet without additional routing or peering configuration as they are in separate VPCs. Moreover, using the same CIDR range for both subnets might cause IP address overlapping issues.

D. Creating a single shared VPC with 2 subnets in different regions and with different CIDR ranges can be a valid option in some cases, but it is more complex and less appropriate than option B for the given requirements. Shared VPCs are primarily designed for managing resources across multiple projects, while the requirements in this scenario only involve production and testing workloads for multiple projects in the same organization. A custom VPC (option B) is better suited for these requirements and provides a simpler setup.

Solution to Question 12: D

The correct answer is D. Upload the image to Container Registry and create a Kubernetes Deployment referencing the image.

Explanation: To successfully deploy a Docker image on Google Kubernetes Engine (GKE), you need to follow these two steps:

1. Upload the Docker image to Google Container Registry (GCR): GCR is a private Docker container registry provided by Google Cloud Platform for storing and managing Docker images. Uploading your Docker image to GCR makes it accessible to GKE for deployment.

2. Create a Kubernetes Deployment referencing the image from GCR: A Kubernetes Deployment is a higher-level abstraction over pods that maintain a specified number of replica pods running using the referenced Docker image. By creating a Deployment, GKE can manage the application's lifecycle, scaling, and updates.

Reasons why the other options will not work:

A. Upload the image to Firestore and create a Kubernetes Service referencing the image: This option is incorrect because Firestore is a NoSQL database, not a container registry. Uploading the image to Firestore will not make it accessible to GKE for deployment. Additionally, creating a Kubernetes Service alone does not deploy the application; a Deployment is necessary for this purpose.

B. Upload the image to Compute Engine and create a Kubernetes Deployment referencing the image: This option is incorrect because Compute Engine is an Infrastructure-as-a-Service (IaaS) component of Google Cloud Platform, meant for virtual machines (VMs) management. It is not designed for storing and managing Docker images. Hence, uploading the Docker image to Compute Engine does not work.

C. Upload the image to Container Registry and create a Kubernetes Service referencing the image: While uploading the image to Container Registry is correct, creating a Kubernetes Service alone is not enough for deploying the Docker image. A Service is used for providing load balancing, networking, and exposing the deployed application. However, creating a Deployment is necessary for deploying the Docker image itself.

Solution to Question 13: D

The correct answer is D. Reserve the IP 10.0.3.21 as a static internal IP address using gcloud and assign it to the licensing server.

Explanation: Since the company does not want to change the application configuration, it is essential to ensure that the licensing server is reachable at the IP address 10.0.3.21. By reserving the IP address 10.0.3.21 as a static internal IP address and assigning it to the licensing server, you ensure that the application will be able to reach the licensing server at the expected IP address.

Here's why the other options are not suitable:

A. Creating a custom routing rule is not the best solution in this case because the application expects a direct connection to the licensing server. Routing traffic to a different IP address may not be feasible considering application design, and it may require additional configurations, increasing the complexity and potential points of failure.

B. Configuring the licensing server to listen to all IP addresses in the 10.0.3.0/24 subnet is not the most efficient solution, as it will not guarantee that the application will reach the licensing server at the expected IP address 10.0.3.21. Also, having the server listen on multiple IP addresses is unnecessary and may increase security and management overhead.

C. Using the IP 10.0.3.21 as a secondary IP address for the licensing server and assigning a primary IP address from the same subnet will not guarantee that the application will only connect to the secondary IP address. It may attempt to connect to the primary IP address instead, causing connectivity issues and potentially other unforeseen side effects.

In conclusion, reserving the IP 10.0.3.21 as a static internal IP address and assigning it to the licensing server (option D) is the best course of action, as it will ensure that the application can access its licensing server on the expected IP address. This method guarantees that the application continues functioning without any changes to its configuration or introducing unnecessary complexity.

Solution to Question 14: A

The correct answer is A. Add a bucket lifecycle rule that archives data with newer versions after 30 days to Nearline Storage.

The rationale for choosing option A is that the archiving solution needs to be cost-effective and must allow occasional access to previous versions of data.

Nearline Storage is designed for data that is accessed less frequently, making it cost-effective for storage but providing lower latency when accessing the data compared to Coldline Storage. Additionally, option A focuses on versioning, which is crucial for meeting the requirement of archiving previous versions of data.

Option B is not suitable because it involves moving data from multi-regional storage, which has higher storage costs and is meant for frequently accessed data. A cost-effective plan should aim to reduce storage costs by choosing the appropriate storage class.

Option C is not the best choice as well because it focuses on moving data from regional storage, which is designed for regular access and does not address the requirement of archiving previous versions of data.

Option D is not ideal because it suggests using Coldline Storage, which is designed for data that is rarely accessed. While it may provide cost savings for storage, it comes with a longer latency time for data retrieval. The requirement in this scenario mentions "occasional access" for reporting and updates, which implies the need for quicker data access than what Coldline Storage provides. Nearline Storage offers a better balance in terms of cost and access times for this use case.

Solution to Question 15: D

The answer should be D because setting up an export job for the first of the month and writing the export file to an Archive class Cloud Storage bucket meets the regulatory requirements. Archive class Cloud Storage ensures that the month-end copy of the Cloud SQL MySQL database is retained for three years with low cost and high durability. It is ideal for long-term, infrequent data access, like auditing purposes.

Option A is incorrect because Cloud SQL on-demand backups do not write backup files directly to Cloud Storage buckets. The backup process creates a new instance that uses the backup data, but it does not create a separate file that can be stored in a bucket.

Option B is incorrect because Cloud SQL automatic backup retention period is limited to a maximum of 365 days, which does not meet the three-year requirement. Additionally, this option wrongly suggests that you can save the automatic first-of-the-month backup to a Cloud Storage bucket, which is not possible.

Option C is incorrect because storing the backup file directly within the Cloud SQL MySQL database creates physical redundancy and takes up unnecessary space in the database instance. It is not a practical solution for managing backups.

The other options mentioned are not suitable because they involve using different Google Cloud services that do not provide a direct and efficient solution

for retaining a month-end copy of the Cloud SQL MySQL database. For example, Firestore, Bigtable, and BigQuery are primarily used for data analysis and processing, and they do not focus on long-term data retention. Cloud Function, Cloud Scheduler, Cloud Run, and Dataflow are used for processing and automation tasks rather than creating and retaining database backups.

Therefore, option D is the most suitable method for retaining a month-end copy of the database for three years for auditing purposes in compliance with regulatory policies.

Solution to Question 16: D

The correct answer is D because it directly addresses the issue of failed instance creation by providing a valid syntax in the instance template and resolving any conflicts by deleting persistent disks with the same name as instance names. This ensures the managed instance group can maintain the desired number of instances essential for supporting expected application traffic.

Option A is incorrect because enabling Shielded VMs on the instances is not relevant to the issue of instance creation failure due to invalid syntax. Shielded VMs provide security features, but they don't resolve the core issue of instance creation failure in the managed instance group.

Option B is incorrect because setting the minimum number of instances lower than the expected application traffic is a contradiction to the requirement of efficiently handling the traffic. Even if the instances are created using a valid syntax, it would not provide the required performance for the application, thus being ineffective in resolving the issue.

Option C is incorrect because modifying network settings specifically to allow instance creation traffic is unnecessary. The main issue is the presence of invalid syntax in the instance group and the potential conflict caused by persistent disks with the same name as instance names. Adjusting network settings does not address these concerns, making it an unhelpful solution.

Solution to Question 17: B

The correct answer is B: Organize the users in Cloud Identity into groups. Enforce multi-factor authentication in Cloud Identity.

Reasoning for B being the correct answer: As the company's personnel count increases from 100 to 1,000 employees, managing individual user accounts will become difficult and time-consuming. Organizing users into groups within Cloud Identity can help manage and control access to company resources effectively. Also, by enforcing multi-factor authentication (MFA) within Cloud Identity, the company adds an extra layer of security to protect its Google Cloud account, which is crucial as the number of users grows.

Reasoning for why other options are not ideal:

A: Turning on Google Cloud Directory Sync (GCDS) will help synchronize your

company's directory with Cloud Identity but skipping multi-factor authentication will expose your company to potential security risks. With the increasing number of employees, it is crucial to have MFA for added security.

C: Connecting Google Workspace to an on-prem LDAP server for user management and authentication would work but is not the most efficient or secure solution. This would require maintaining separate directories for Google Workspace and Google Cloud which can lead to potential inconsistencies and added complexity. Moreover, doing so would not take full advantage of the scalability and reliability provided by Cloud Identity.

D: Deploying a custom SSO (Single Sign-On) service using Cloud Functions and connecting it to Google Workspace could work, but it would unnecessarily complicate the authentication process. By doing so, the company would have to develop and maintain custom code, which might become difficult to manage with the growing number of employees. Relying on Google Cloud's built-in identity services would provide better scalability and security for your organization.

Solution to Question 18: D

The correct answer is D. Here's why:

A. This option is not the most efficient solution. Using a general-purpose machine type for the image rendering microservice, which requires more CPU time, can lead to underutilization of resources. Also, preemptible machine type nodes may not be ideal for other microservices as there is no guarantee of their availability.

B. Assigning a higher pod priority does not guarantee efficient resource utilization. The image rendering microservice with higher priority will still be using the same general-purpose machine type nodes, which might result in less efficient resource usage.

C. This approach doesn't cater to the specific needs of the image rendering microservice. Using general-purpose machines for the image rendering microservice will not efficiently utilize resources. On the other hand, the compute-optimized machine types might be overkill for the other microservices optimized for n2-standard types.

D. This is the best approach as it addresses the specific requirements of both types of microservices. Creating a node pool with compute-optimized machine type nodes for the image rendering microservice ensures efficient utilization of CPU resources. Meanwhile, using the node pool with general-purpose machine type nodes for the other microservices matches their optimization for n2-standard machine types, promoting overall efficiency in the Kubernetes Engine cluster.

Solution to Question 19: A

The answer should be A. Navigate to the project and then to the IAM section in the GCP Console. Review the members and roles.

Explanation for why option A is the best course of action:

Navigating to the IAM section of the GCP Console offers the most straightforward method to view and manage IAM users and roles. Within the IAM section, you will be able to view all members, their corresponding roles, and make any necessary modifications. IAM is specifically designed for the management of access and permissions within your GCP projects, making it the ideal choice.

Explanation for why other options will not work:

Option B: Navigating to the APIs & Services section in the GCP Console will not provide you with the necessary information about IAM users and roles assigned to the project. This section deals more with managing APIs and services used within the project and their respective quotas, but not with the user and role management required for this task.

Option C: Running "gcloud projects describe my-project" will provide you with general information about the project, but not specifically about IAM users and roles. The output does not include the list of users and their roles within the project, making this option insufficient for the task at hand.

Option D: Running "gcloud iam service-accounts list" will list the service accounts associated with your project. However, service accounts are not the same as IAM users and roles. Although service accounts can be used for authentication and authorization, they are not human users, and this command will not provide the required information about the IAM users and roles assigned to the project.

Solution to Question 20: B

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

Reason for choosing option B: Storing the database password in a Kubernetes Secret object is the best practice as it keeps the sensitive information secure and separate from the application's configuration. Secrets are specifically designed for managing sensitive data in Kubernetes and are more secure than plain text or other methods. Modifying the YAML file to populate the DB_PASSWORD environment variable from the Secret ensures that the sensitive information is securely injected into the running container.

Reasons for not choosing the other options:

Option A: Storing the database password inside a Cloud Storage bucket and using a Cloud Function to retrieve it during runtime adds extra complexity, latency, and potential points of failure. Additionally, it doesn't provide a clear security advantage over using Kubernetes Secrets, which are native to the Kubernetes environment and more suitable for this use case.

Option C: Storing the database password in the Compute Engine instance metadata and using a startup script to extract it is not as secure as storing it in a Secret object. Instance metadata can be accessed by any code running on the instance, making it more vulnerable to exploitation. Also, this approach is not as tightly integrated with Kubernetes, which makes it harder to manage.

Option D: Storing the database password in a file inside a Kubernetes persistent volume and using a persistent volume claim to mount the volume to the container is less secure compared to storing the password in a Secret object. Persistent volumes are designed for storing data that needs to be preserved across container restarts, not for securing sensitive data like passwords. Using a persistent volume for storing passwords makes it easier for unauthorized users to access the data, even if it is encrypted, because the decryption keys must be stored somewhere accessible, potentially exposing them to theft or misuse.

In summary, Option B is the best solution because it securely stores the database password inside a Secret object, adheres to Google-recommended practices, and simplifies management within the Kubernetes environment.

Solution to Question 21: D

The correct answer is D. Let's explain why this is the best option and why the other options will not work as efficiently.

Option A: Creating individual custom roles for Compute Engine, Cloud Functions, and Cloud SQL permissions in each project and assigning them to developers will require more maintenance effort, as you will need to manage multiple roles and assignments in each project. This approach can lead to potential inconsistencies and security vulnerabilities due to the increased complexity.

Option B: Assigning the default role of Editor to the Google group for each project in the Google Cloud organization may seem like an easier option, but it would grant developers more permissions than necessary, which is against the company's security policy. The Editor role allows access to most Google Cloud resources, which is excessive for the given scenario.

Option C: Enabling API access to Compute Engine, Cloud Functions, and Cloud SQL for all developers, without creating custom roles or assigning Google group permissions, is not a good option either. This approach would not provide any centralized control over the developers' permissions and could lead to security vulnerabilities if not managed correctly.

Option D is the best way to proceed because it streamlines the permission management process while adhering to the company's security policy. By adding all developers to a Google group in Cloud Identity, you can centrally manage the developers without having to manage individual access. Creating a custom role with Compute Engine, Cloud Functions, and Cloud SQL permissions at the Google Cloud organization level provides a uniform set of permissions across all Google Cloud projects. Finally, assigning this custom role to the Google group ensures that all developers have the same access, reducing the risk of

unauthorized access and human errors. This approach strikes the right balance between security and minimal effort.

Solution to Question 22: C

The correct answer is C. Give bigquery.dataViewer role to crm-databases-proj and appropriate roles to web-applications.

Explanation: The BigQuery datasets are stored in the crm-databases-proj, and the VMs in the web-applications project require access to these datasets. To achieve this, we can add the bigquery.dataViewer role to the crm-databases-proj, which allows read-only access to the datasets. Meanwhile, in the web-applications project, we can assign appropriate roles to the service accounts, enabling the VMs to communicate with the crm-databases-proj as needed.

Here's why the other options will not work:

A. Creating a new project to link crm-databases-proj and web-applications adds unnecessary complexity to the task and does not necessarily follow best practices. It also introduces the potential for future management issues, as it creates a new layer to maintain and monitor.

B. Disabling BigQuery API in the web-applications project and enabling it in crm-databases-proj with bigquery.dataViewer role will not provide the VMs in the web-applications project the necessary access to the BigQuery datasets. BigQuery API needs to be enabled for both projects to access the datasets.

D. Giving project owner roles of web-applications to crm-databases-proj can lead to excessive permissions being granted, which goes against the principle of least privilege. The best practice is to keep permissions to the minimum level possible. Just because a user needs access to BigQuery datasets, it does not mean they should have ownership permissions to the entire project.

Solution to Question 23: D

The best answer is D. Create a Billing account, associate a payment method with it, and provide all project creators with permission to associate that billing account with their projects.

Reasoning:

A. Granting all engineers permission to create their billing accounts for each new project would be an inefficient and ineffective approach. It can lead to multiple billing accounts, making it increasingly difficult for you to manage and monitor expenses across your team. Additionally, you would still require the engineers to use their credit cards to set up the billing accounts, defeating the purpose of your intention.

B. Requesting Google Cloud to provide a corporate credit card for the entire engineering team is not a viable option because the credit card should be issued by your company or financial institution, not Google Cloud.

C. Creating a billing account and associating it with a monthly purchase order (PO) is not an ideal solution because Google Cloud does not accept purchase orders for payment. They require a valid payment method, such as a credit card, to be associated with the billing account.

D. This option addresses your requirement most effectively. By creating a Billing account, associating a payment method with it, and providing all project creators with permission to associate that billing account with their projects, you centralize and streamline the process. It makes it easier for your engineering team to create new projects without needing their credit card details and enables you to track expenses more efficiently as everything goes through a single billing account.

Solution to Question 24: C

The correct answer is C. In the Google Cloud Platform Console, create a new billing account and set up a payment method.

Explanation:

By creating a new billing account and setting up a payment method within the Google Cloud Platform Console, the organization can effectively centralize the billing for all cloud-based projects. This approach eliminates the need for team members to use their personal credit cards and streamlines the reimbursement process.

Reasons why other options will not work:

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

This option is not advisable because it's not a secure method for providing sensitive payment information. Google Support does not typically request credit card details over the phone, and setting up payment methods should be done via the Google Cloud Platform Console.

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

Moving projects to the root Organization in the Resource Manager does not consolidate billing. It only helps to organize projects within the company's account structure. The billing and payment settings for each project would still need to be managed individually.

D. Create a billing account in the Google Cloud Console with the company's GCP-related expenses only.

This option does not directly address the issue of team members using their personal credit cards for project payments. It also does not mention how to set up a payment method or explain how to link existing projects to the new billing account. Additionally, limiting the account to GCP-related expenses does not necessarily ensure proper centralization of all cloud-based projects' billing.

Solution to Question 25: D

The correct answer is D: Create a Kubernetes Service of type NodePort for your application, and a Kubernetes Ingress to expose this Service via a Cloud Load Balancer.

Explanation for choice D: First, by creating a Kubernetes Service of type NodePort, you ensure that your application runs on a specific port on each node within your cluster. Then, by creating a Kubernetes Ingress, you automatically create a Google Cloud Load Balancer, which listens to incoming traffic and routes it to the appropriate backend service based on the specified NodePort and rules. By using Ingress, it is possible to easily configure your application to be accessible via HTTPS on a public IP address. This approach is best suited for deploying a highly available, scalable web application on Google Kubernetes Engine (GKE) with autoscaling enabled.

Reasons why other options do not work: Option A: Google Cloud Endpoints is mainly used for creating, deploying, and managing APIs on a global scale. Although it provides some level of security and authentication, it does not directly address the requirement of deploying a web application on GKE with autoscaling enabled. Also, deploying the application on a GCE instance does not make full use of the Kubernetes cluster and autoscaling capabilities.

Option B: Creating a Kubernetes Service of type LoadBalancer will automatically create a Google Cloud Load Balancer, which exposes your application to the public via an external IP address. However, this option does not mention enabling HTTPS, which is a requirement in the prompt. As a result, the application's public access would be insecure.

Option C: Google Cloud Storage buckets are primarily used for storing and managing unstructured data, like images and videos, not for deploying web applications. Cloud CDN is a content delivery network service, meant for caching static assets from your application, rather than directly serving the application itself. This approach is not suitable for deploying the required web application on GKE with autoscaling enabled.

Solution to Question 26: A

The best course of action in this scenario would be to change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 (Option A). Here's why:

Option A: By changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18, the number of available IP addresses will increase. The /20 subnet has 4096 addresses, while the /18 subnet has 16,384 addresses, allowing for more IP address allocation to the virtual machines without needing additional services or infrastructure. This directly addresses the issue of a shortage of primary internal IP addresses in your subnet.

Option B: Implementing Cloud VPN wouldn't solve the problem in this case. Cloud VPN is used to establish secure, encrypted connections between your

VPC network and resources beyond its perimeter, which doesn't address the current constraint of a limited number of IP addresses within the subnet itself.

Option C: Changing the subnet IP range from 10.0.0.0/20 to 10.0.0.0/22 would actually make the situation worse. The /22 subnet has only 1024 addresses, which would decrease the number of available IP addresses and further restrict the network capacity.

Option D: Configuring a NAT gateway for the virtual machines can help with outbound internet connectivity but doesn't resolve the issue of insufficient primary internal IP addresses in the subnet. NAT gateways are for providing IPv4 private instances (such as VMs) with internet access by translating their private IPs to public IPs. This doesn't affect the actual number of internal IP addresses in a subnet and doesn't solve the problem at hand.

In conclusion, the best course of action to accommodate the increasing demands in your custom mode VPC would be to change the subnet IP range from 10.0.0.0/20 to 10.0.0.0/18 (Option A).

Solution to Question 27: B

The correct answer is B. The reason for this is that you want to grant the external auditor access to your company's audit logs and data access logs. The role roles/logging.privateLogViewer meets this requirement since it allows the user to have read access to private logs, which includes both audit logs and data access logs. This role is designed specifically for this purpose and is a recommended choice in the Google Cloud Platform documentation.

Furthermore, you are also directed to ask the auditor to review the logs for changes to the Cloud IAM policy. Access to this information is also included in the roles/logging.privateLogViewer role.

Considering the other options: A. A custom role with logging.privateLogEntries.list permission does seem to allow the auditor to view the logs; however, it is not considered best practice to create a custom role unless there is a specific requirement for granular permissions that the predefined roles don't offer. Also, creating custom roles may often lead to security issues due to misconfigurations.

C. Assigning a custom role with logging.logEntries.list permission would not be suitable, as it only provides read access to public logs, not private logs like audit logs, and data access logs, which are the desired logs in this case.

D. Assigning a custom role with monitoring.logsWriter permission would not provide read access which the auditor needs for reviewing the logs. The role only allows for writing logs and not reading them. Additionally, the export of logs to Cloud Storage is not necessary for the auditor to perform the review, and this might cause potential security risks or additional work and costs.

Solution to Question 28: D

The correct answer is D: Add a new, GPU-enabled node pool to the GKE cluster.

Ask your ML team to add the cloud.google.com/gke-accelerator: nvidia-tesla-p100 nodeSelector to their pod specification.

Explanation:

Option A: Configuring your cluster to use only GPUs for all nodes by default is not an efficient solution. Since not all workloads in the cluster require GPU resources, this option increases the cost significantly and wastes resources.

Option B: Manually installing Nvidia Tesla P100 GPUs on the cluster's nodes is not a smart choice because it requires a lot of manual effort, increases the chances of configuration errors, and does not take advantage of GKE's ability to manage and scale node pools automatically.

Option C: Asking your ML team to use TPUs instead of GPUs for their training may not be a feasible option. Depending on the specific requirements of their machine learning workloads and existing tools, switching to TPUs could require significant changes in their workflows and introduce compatibility issues.

Option D: Adding a new, GPU-enabled node pool to the GKE cluster is the best solution. This approach minimizes effort, cost, and allows you to leverage GKE's automated scaling. By adding cloud.google.com/gke-accelerator: nvidia-tesla-p100 as a nodeSelector in the ML team's pod specification, you ensure that their resources are efficiently utilized only on the nodes with GPUs, leaving other nodes free to cater to different workloads. This approach keeps costs down, is easy to manage, and ensures optimal resource allocation.

Solution to Question 29: C

The most suitable course of action to ensure the infrastructure handles the failure of a single Compute Engine zone and avoids downtime while keeping costs low is option C: Create Compute Engine resources in us-central1-b. Balance the load across both us-central1-a and us-central1-b.

Here's why the other options will not work:

A. Use Cloud Pub/Sub with a regional endpoint to balance the load between VMs in us-central1-a and us-central1-b. Using Cloud Pub/Sub with a regional endpoint can help distribute messages between applications but does not address the issue of deploying an application on Compute Engine VMs in multiple zones for redundancy. This option does not ensure the application remains operational and able to handle the failure of a single zone.

B. Create a global Cloud Spanner instance and configure the VMs in us-central1-a and us-central1-b to share the same Spanner database. Creating a global Cloud Spanner instance might help with distributing your database globally, but it does not address the primary issue of having Compute Engine VM resources across multiple zones. While this option might be useful to improve database redundancy, it does not directly solve the problem of ensuring the application remains operational in the event of a single zone failure.

D. Perform regular backups of your application. Create a Cloud Monitoring Alert and be notified if your application becomes unavailable. Restore from backups when notified. Although performing regular backups and setting up Cloud Monitoring Alerts is a great practice, this option does not proactively handle single zone failure. You might still face downtime with this approach if the application becomes unavailable while you restore the backups. It is a reactive measure, rather than a proactive one.

Thus, option C is the best solution, as it ensures that you have Compute Engine resources in two different zones (us-central1-a and us-central1-b), allowing for load balancing and providing redundancy in case one of the zones fails, thus avoiding downtime and ensuring the application remains operational. This also helps in keeping costs low, as you're only adding resources in the same region but across different zones.

Solution to Question 30: B

The correct answer is B, "Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User." Here's an explanation for why this option is the best choice, and why the other options will not work.

Option A: Configure a Google Cloud Pub/Sub topic that allows the operations partner to send and receive messages related to instance maintenance. - This option is not ideal because Google Cloud Pub/Sub is a messaging service primarily used for asynchronous communication between applications and services. It does not provide direct access to Compute Engine instances or the ability to perform maintenance tasks on these instances.

Option B: Enable Cloud IAP for the Compute Engine instances, and add the operations partner as a Cloud IAP Tunnel User. - This is the best course of action because it allows the operations partner to securely access and maintain the Compute Engine instances. Cloud Identity-Aware Proxy (Cloud IAP) provides secure, context-aware access to applications and Compute Engine instances without the need for a traditional VPN. By enabling Cloud IAP for the Compute Engine instances and adding the operations partner as a Cloud IAP Tunnel User, the partner will have secure access to the instances without needing a Google Account.

Option C: Enable Cloud NAT and grant the operations partner access to the Cloud NAT gateway to allow traffic redirection. - This option is not suitable because Cloud NAT (Network Address Translation) is a Google Cloud service that provides private IP addresses to instances and other resources without direct external connectivity. Cloud NAT does not provide access to a Compute Engine instance's management console or the ability to manage installed tools within instances. Therefore, granting access to the Cloud NAT gateway will not help the operations partner with their maintenance responsibilities.

Option D: Use Cloud Identity Groups to create a group for the operations part-

ner and add their non-Google account emails to the group. - Although you can use Cloud Identity Groups as a way to manage access controls for the domain, this option alone will not allow the operations partner to access the Compute Engine instances without a Google Account. Furthermore, Cloud Identity Groups do not provide a mechanism for securing access to Compute Engine instances, unlike Cloud IAP, which is specifically designed for this purpose.

In conclusion, enabling Cloud IAP for the Compute Engine instances and adding the operations partner as a Cloud IAP Tunnel User (Option B) is the most appropriate course of action to provide secure access to the instances for maintenance purposes without requiring a Google Account.

Solution to Question 31: A

The correct answer is A: Using the Cloud SDK, create a new project, enable the Compute Engine API in that project, and then create the instance specifying your new project.

Here's why the other options will not work:

B. Enabling Kubernetes Engine API in the Cloud Console might be required for a Kubernetes cluster but is not necessary for creating a Compute Engine instance. Compute Engine instances are created using the Compute Engine API, not the Kubernetes Engine API, thus this option won't accomplish the task.

C. Creating a new instance using the Cloud SDK and the –project flag does not create a project. The –project flag is used to specify the project where you want to create the instance. Moreover, the option implies that the Compute Engine API will automatically be enabled when prompted by the Cloud SDK, but this isn't the case - you need to enable the API first before creating the instance.

D. Enabling the Compute Engine API in the Cloud Console is correct, but you cannot create an instance with the –project flag specifying a new project, as the project has not been created yet. You need to create a new project before using the –project flag in the Cloud SDK to specify where to create the instance.

Therefore, the best course of action is to follow option A - use the Cloud SDK to create a new project, enable the Compute Engine API for that project, and then create the Compute Engine instance specifying the newly-created project. This approach ensures that you have a new project with the necessary API enabled and a Compute Engine instance created within that project.

Solution to Question 32: D

The correct answer is D: Too many Pods are already running in the cluster, and there are not enough resources left to schedule the pending Pod.

Explanation: In this situation, you have created a Deployment with 2 replicas, which means you want to have 2 Pods running for that application. A Google Kubernetes Engine (GKE) single preemptible node pool, as the name suggests,

uses preemptible VMs. Preemptible VMs are lower-cost instances than regular VMs but can be terminated at any given time. The cluster will attempt to schedule and run the Pods but might not have enough resources to accommodate both Pods due to other running Pods consuming the available resources. This lack of resources is the most likely reason for the pending status in one of the Pods.

Reasons why other options are incorrect:

A. Google Kubernetes Engine experiencing an internal error that prevents the Pod from being scheduled is unlikely, as GKE is a highly reliable and stable platform. Any internal error would most likely affect other Pods or components in the cluster and not just a single Pod.

B. The pending Pod requesting a specific node or node with a specific label that does not exist in the cluster could be a potential issue but is less likely as you have already successfully deployed one replica, suggesting that the cluster's configuration in terms of node labels and selectors is suitable for the application you are deploying.

C. A firewall rule blocking communication between the control plane and the node, preventing the Pod from being scheduled, is also less likely. If this was the case, it would affect all Pods within the cluster and not just one specific Pod. Additionally, with at least one successfully deployed replica, it suggests there is no issue with the control plane-node communication.

Solution to Question 33: A

The correct answer is A. Set the CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD properties by using environment variables in your command line tool.

Explanation for A: By setting the proxy username and password via environment variables, you ensure that these credentials won't be persisted in any configuration files or logged by the gcloud CLI. This precaution helps maintain the security and confidentiality of your proxy credentials while still allowing the gcloud CLI to function with the proxy correctly.

Why other options won't work:

B. Disabling logging for the entire gcloud CLI might seem like a solution, but it's too extreme and might hinder your troubleshooting efforts. Completely disabling logging for all gcloud CLI operations can make it difficult to find issues when they arise. The goal is to prevent the proxy credentials from being logged, not disable the entirety of the log.

C. Creating a .gcloudignore file in your home directory is not effective, as the .gcloudignore file is used for ignoring files and directories when deploying Google Cloud Platform apps, not for preventing specific properties from being logged in the gcloud CLI.

D. Providing values for CLOUDSDK_PROXY_USERNAME and CLOUDSDK_PROXY_PASSWORD in the gcloud CLI configuration file will store these credentials in the config file, which is not a secure practice and can result in the proxy credentials being logged. By using environment variables instead (option A), you eliminate this concern and ensure the proxy credentials are not persisted in any configuration files or logged by the gcloud CLI.

Solution to Question 34: D

The correct answer is D. The gcloud compute instance-groups managed recreate-instances command allows you to specifically target and recreate the problematic VM within the managed instance group. This action ensures that the unresponsive process within the faulty VM is fixed swiftly without affecting the other instances. It also ensures that the new VM will inherit the most recent instance template.

Option A is incorrect because updating and applying the instance template of the MIG may affect all instances in the group. It won't immediately fix the current issues with the problematic VM. It requires a rolling update or instances recreation to take effect.

Option B is also incorrect as enabling autoscaling based on CPU utilization will not directly resolve the issue with the given VM. While autoscaling could help manage load across instances, it does not address a specific unresponsive process within one VM.

Option C may seem viable, but setting the autohealing policy for the MIG to replace unhealthy instances automatically only works if there's a specific health check that detects the unresponsiveness of the process in question. Moreover, autohealing generally takes longer to replace unhealthy instances compared to manually recreating the problematic VM using the gcloud command mentioned in option D.

Hence, the best and quickest solution to replace the problematic VM within the MIG is option D: Use the gcloud compute instance-groups managed recreate-instances command to recreate the VM.

Solution to Question 35: B

The correct answer should be B, "Enable delete protection on the instance," because this measure specifically focuses on preventing accidental deletion of the application.

Option A, disabling the flag 'Delete boot disk when instance is deleted,' would not protect the instance from accidental deletion. While this option ensures that the boot disk remains intact when the instance is deleted, it doesn't prevent deletion of the instance itself in the first place.

Option C, disabling live migrations for the instance, does not contribute to protecting the instance from accidental deletion. Live migrations refer to moving running virtual machine instances from one physical host to another without

any noticeable disruption. This feature helps to ensure high availability of applications and data, but has no bearing on protecting against instance deletion.

Option D, enabling autohealing on the instance group, is primarily a measure to maintain high availability of applications, ensuring that instances automatically restart when they experience issues or stop serving traffic. However, it does not prevent instances from being accidentally deleted by employees in the first place.

In conclusion, the best measure to take in order to protect the production application deployed on Compute Engine from inadvertent deletion is by enabling delete protection on the instance (Option B). This will prevent employees from accidentally deleting the instance, minimizing the risk of costly disruptions and downtime.

Solution to Question 36: C

The correct answer is C. Configure Billing Data Export to BigQuery and visualize the data in Looker Studio. This is the most effective method for predicting and visualizing future expenses across all projects because it provides a unified view of all incurred costs and updates rapidly with new data. BigQuery is designed for real-time data analysis and storage, which makes it suitable for handling the billing information from multiple Google Cloud projects. By exporting billing data to BigQuery, you enable the automatic integration of real-time data from all billing accounts, thereby streamlining the process and ensuring accuracy. Looker Studio, a data analytics and visualization tool, can then help present the data for easier interpretation and decision-making.

Option A is incorrect because the Cost Table page provides a CSV export, which is a one-time static data snapshot and does not update with new data automatically. Moreover, it may not provide an aggregated view of expenses from different billing accounts.

Option B is also incorrect because creating a Google Cloud Function to consolidate costs from multiple projects periodically would require custom coding, monitoring, and maintenance, which can be error-prone and not as efficient as using an integrated solution like BigQuery and Looker Studio.

Option D is incorrect because exporting cost data from each billing account to a Google Sheet and then using the Google Sheets API for visualization involves manual intervention and the risk of data inconsistencies. Additionally, Google Sheets may not be the best choice for handling large datasets and real-time analysis. Therefore, it is not an efficient way to manage and visualize financial forecasts for multiple Google Cloud projects and billing accounts.

Solution to Question 37: B

The best course of action for managing costs associated with the defined requirements is option B: Create an object lifecycle on the storage bucket to change the storage class to Archive Storage for objects with an age over 30 days.

Explanation for B: As the application only needs access to files created within the last 30 days, transitioning those older files to a more cost-effective storage class like Archive Storage will save costs. Archive Storage has lower storage costs but higher retrieval costs, which won't matter since the application isn't accessing those files anymore. By creating an object lifecycle rule on the storage bucket, this process will be automated, ensuring that only objects older than 30 days are moved to the Archive Storage class.

Reasons why other options are not suitable:

A. Object versioning is used for maintaining different versions of an object. Enabling object versioning and adding lifecycle rules to expire non-current versions after 30 days doesn't address the requirement of saving costs on files that are not accessed by the application anymore.

C. Setting a custom metadata key to mark objects for deletion after 30 days involves additional manual steps and doesn't scale well. Also, this approach may increase the risk of accidentally deleting important files that might be needed later and doesn't actually save costs.

D. Cloud CDN is used for caching content from backend services, improving the experience for users by serving content from a cache that is closer to the user. Enabling Cloud CDN and allowing 30-day expiration on cached items does not address the requirement of saving costs on files not accessed by the application anymore. Additionally, Cloud CDN serves cached content, whereas the primary concern is the costs associated with storing files on Cloud Storage.

Solution to Question 38: B

The answer should be B. Run a test using simulated maintenance events. If the test is successful, use preemptible N1 Standard VMs when running future jobs. The reason for choosing this option lies in its cost-effectiveness and ability to handle fault-tolerant batch workloads while not impacting performance. Preemptible VMs are cheaper than regular VMs because they can be terminated by the system if there is a resource contention. Since the company is dealing with fault-tolerant workloads, it can afford to use preemptible VMs, which will lead to cost savings without adversely affecting performance.

Option A is not a suitable choice because Cloud Run is designed for containerized applications and serverless workloads, not batch workloads. While it may reduce costs, using Cloud Run with VMs does not address the specific use case of fault-tolerant batch workloads. Additionally, N1 Standard VMs in Cloud Run service might not offer the desired cost savings.

Option C is not optimal because a managed instance group relies on regular VMs rather than preemptible VMs, which will not lead to significant cost savings compared to the current situation. While Managed Instance Groups provide scalability and fault tolerance, they might not offer the required cost savings without utilizing preemptible VMs.

Option D is not preferable because preemptible N1 Highmem VMs could be more expensive than preemptible N1 Standard VMs due to the additional memory capacity. Using preemptible VMs is a good strategy, but choosing Highmem VMs for batch workloads may not be necessary and will not provide optimal cost savings.

In conclusion, option B is the most appropriate choice, as it leverages preemptible VMs, which are designed for short-lived and fault-tolerant batch workloads, providing cost savings without impacting performance.

Solution to Question 39: C

The correct answer is C: Use permissions in your role that use the 'supported' support level for role permissions. Set the role stage to ALPHA while testing the role permissions.

Here's why the other options will not work effectively:

A. Using 'deprecated' support level permissions in your role is not a good practice because these permissions are outdated, and may pose security risks or compatibility issues. Additionally, setting the role stage to BETA is unnecessary as it implies that the role is almost production-ready, which contradicts the premise that it's the first version of the role.

B. Although setting the role stage to BETA is correct for testing purposes, using the 'testing' support level for role permissions is not recommended for a production environment. It indicates that the permissions are experimental and may not be stable or fully supported, which could lead to unexpected issues and vulnerabilities within your organization.

D. This option combines the incorrect aspects of both A and B. It suggests using 'deprecated' permissions, which can lead to security or compatibility problems, and setting the role stage to ALPHA, which is appropriate for early-stage testing but contradicts the use of deprecated permissions. Using deprecated support level for permissions in a custom IAM role is not a good practice, especially in the first version of the custom role.

Thus, the best approach is to use supported support level permissions to ensure stability and security, and set the role stage to ALPHA while testing, which effectively communicates the status of the custom role within the organization.

Solution to Question 40: B

The correct answer is B. Deploy Jenkins through the Google Cloud Marketplace.

Reasoning:

Option A: While creating a new Kubernetes Engine cluster and creating a deployment for the Jenkins image is a valid way to deploy Jenkins, this process could be more complex and time-consuming than deploying through the Google Cloud Marketplace. Google Cloud Marketplace offers ready-to-go development

stacks, solutions, and services to accelerate development, making it a more efficient and time-effective choice.

Option B: The Google Cloud Marketplace provides a quick and straightforward way of deploying services like Jenkins. By choosing this option, you can save time and effort during the setup process. The Google Cloud Marketplace offers a pre-configured Jenkins installation, which ensures seamless deployment with minimal manual intervention. This makes it the best choice for automating the installation process in the most efficient and time-effective way possible.

Option C: Creating a new Cloud Storage bucket and uploading the Jenkins executable is not an appropriate method for deploying Jenkins. Cloud Storage is designed for storing data, not for running applications. This method won't help you achieve your goal of automating the installation process in an efficient and time-effective way.

Option D: Creating a new Dataproc cluster is not suitable for installing Jenkins, as Dataproc is designed for running big data workloads rather than continuous integration and deployment like Jenkins. Furthermore, setting up a Dataproc cluster would be neither time-efficient nor an optimal way to automate the installation of Jenkins.

In summary, Option B (Deploy Jenkins through the Google Cloud Marketplace) is the best choice for automating the installation process in the most efficient and time-effective way possible. The other options are either more complex, time-consuming, or not designed for the specific task at hand.

Solution to Question 41: B

The correct answer is B. Configure an External Network load balancer in front of the application servers.

Explanation:

When dealing with UDP packets in a multiplayer mobile game, the best option to distribute traffic effectively and expose multiple VMs through a single IP address is to use an External Network load balancer.

Option B is suitable because External Network load balancers are designed to forward incoming traffic to respective VM instances by utilizing Layer-4 (Transport Layer) protocols such as UDP and TCP. Since the game relies on UDP packets for updating servers, this option is the most efficient and suitable choice for handling the required traffic.

Option A, utilizing Cloud Armor, is not suitable because it is primarily a security service that focuses on mitigating Distributed Denial of Service (DDoS) attacks and providing web application firewall features. It does not directly handle load balancing between VM instances.

Option C, configuring an External HTTP(s) load balancer, is not suitable because it operates at Layer-7 (Application Layer) and is designed to handle HTTP

and HTTPS traffic, not UDP packets. Thus, it cannot accommodate the game's requirements of handling UDP packets.

Option D, configuring an External TCP Proxy load balancer, is also not suitable because it operates at Layer-4 (Transport Layer) like the Network load balancer but only handles TCP traffic and not UDP traffic. Since the game relies on UDP packets, this option would not address the specific requirements.

Solution to Question 42: C

The most appropriate course of action to revert to the previous version without delay is Option C: On the App Engine Versions page of the GCP Console, route 100% of the traffic to the previous version.

Option C is the correct answer for the following reasons:

1. Routing 100% of the traffic to the previous version ensures that users are served by the stable version of the application immediately. App Engine allows you to manage different versions of your applications, so you can redirect traffic with minimal effort and no downtime.
2. This approach doesn't require any additional deployment which may delay the rollback process. Time is critical when dealing with an urgent issue, and this solution is the fastest way to revert to the previous version.

Option A is not the best course of action because: 1. Stopping the current version and restarting the previous version on the App Engine page is unnecessary since you can directly reroute traffic as mentioned in Option C. 2. Using gcloud app migrations or gcloud app versions commands are also unnecessary, as these are not the optimal ways to revert to a previous version. 3. Deleting the faulty version is not advisable since you might want to investigate the issue and apply fixes without permanently losing the related files.

Option B is not the best course of action because: 1. Creating a new App Engine instance adds extra complexity and resource use, as it requires another deployment to make the previous version live. 2. Reverting code changes through Git and deploying a new version will take more time than just rerouting traffic, which is undesirable in critical situations. 3. Restoring from storage service backups or GCP Datastore snapshots involves additional time and complexity, which is not ideal when you need a quick rollback.

Option D is not the best course of action because: 1. Deploying the original version as a separate application is unnecessary and creates an additional management overhead. It would be more efficient to use the versioning capabilities of App Engine and direct traffic to the desired version directly. 2. Splitting traffic between applications is a more complicated process compared to rerouting traffic within the same application using versions. Routing traffic to multiple applications comes with increased logistical challenges, which makes this option less preferable.

Solution to Question 43: C

The correct answer is C: Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles.

As a security analyst, your primary responsibility is to review and analyze logs to gather information regarding user activities. In the context of Google Cloud Platform (GCP), Stackdriver Logging, now known as Cloud Logging, is the tool to view and manage logs from GCP services, including Cloud Spanner and IAM.

Option C allows you to directly review administrative activity logs within the GCP Console, enabling you to filter and analyze these logs for specific IAM roles related to Cloud Spanner. This is the most efficient and accurate method to determine when users were added to those roles.

Option A suggests visiting the Cloud Spanner section in the GCP Marketplace. This will not help in tracking user activities as the Marketplace is primarily for discovering and deploying various GCP services, not for managing their access logs.

Option B is about creating a new Cloud Pub/Sub topic related to IAM roles. While Cloud Pub/Sub is a message queuing service for asynchronous communication between services, it is not suitable for tracking user activities. Creating a new topic will not provide the historical information needed to determine when users were added to IAM roles.

Option D proposes creating a Cloud Function to monitor IAM roles in Cloud Spanner. Though Cloud Functions can be used to create serverless functions that trigger on specific events, it would not provide retrospective data on when users were added to IAM roles. It might be helpful in monitoring future events but not for an existing GCP project with historical data.

Therefore, the most appropriate action to take is Option C: Go to the Stackdriver Logging console, review admin activity logs, and filter them for Cloud Spanner IAM roles, as it provides the relevant information needed for your investigation into user activity.

Solution to Question 44: C

The most effective approach to accomplish this goal is:

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

This is the most effective approach because it directly copies the IAM roles from the development project to the production project by specifying the production project as the destination. This avoids recreating the roles manually and ensures that the same IAM roles are set up in the production project with minimal steps.

Option A is not correct because it specifies the development project as the destination project, which means it would be copying the IAM roles within the same project rather than transferring them to the production project.

Option B is not ideal because manually creating the same IAM roles in the production project using gcloud iam roles create would be a longer and more error-prone process compared to directly copying the roles from the development project using the gcloud iam roles copy command.

Option D is not correct because specifying both the development and production projects as the source projects is invalid syntax for the gcloud iam roles copy command. The command requires a single source project and a single destination project to work properly.

Solution to Question 45: A

The correct answer is A. Export the billing data to BigQuery. Create a Cloud Function that uses BigQuery to sum the egress network costs of the exported billing data for the Apache web server for the current month and sends an email if it is over 100 dollars. Schedule the Cloud Function using Cloud Scheduler to run hourly.

Option A is the best solution because it directly targets the egress network costs and exports them to BigQuery, making it easier to analyze the data and calculate the total costs. Additionally, using a Cloud Function to check the costs and send an email when the threshold is exceeded is precise and efficient. Scheduling the Cloud Function to run hourly with Cloud Scheduler ensures that the system will be regularly monitored, and you will be notified in a timely manner if the egress costs surpass the limit.

Option B is not ideal because budget alerts are for overall budgets and don't specifically target egress network costs. Also, it doesn't provide a way to export the billing data to perform calculations on the usage related to the Apache web server alone.

Option C is not suitable because it focuses on Apache web server logs and HTTP responses, but it doesn't directly address the egress network costs. It would require additional calculations based on the current Google Cloud egress prices, making it a more complex solution than necessary.

Option D is not optimal because scheduling the Cloud Function that reads the exported data to run daily might not be as timely as running hourly, which could result in exceeding costs before the email notification is sent. Additionally, using Google Cloud Storage for billing exports is less efficient for data analysis and calculations compared to BigQuery.

Solution to Question 46: A

The correct answer is A. Create and deploy a Deployment per microservice.

An explanation for why other options will not work:

Option B: Creating and deploying a Bundle per microservice is incorrect because a "Bundle" is not a valid Kubernetes term or concept. The concept of a "bundle"

is not used within the Kubernetes ecosystem, and therefore it is not a valid way to deploy or manage microservices in Google Kubernetes Engine.

Option C: Creating and deploying an App Engine Module per microservice is incorrect because App Engine is a separate service from Google Kubernetes Engine. While App Engine also allows developers to deploy and manage applications, it is primarily focused on web applications, whereas Google Kubernetes Engine is specifically designed for containerized applications that use Docker images and Kubernetes.

Option D: Creating and deploying a Job per microservice is incorrect because Jobs in Kubernetes are used to run short-lived, one-time tasks, also known as batch processing. A Kubernetes Job will run to completion and then terminate, unlike Deployments that manage the desired state of the application continuously. Since microservices generally require long-running, scalable services, using Jobs for deploying them is not appropriate.

The correct answer, option A, is the best option because the Deployment is a Kubernetes resource specifically designed to automate the deployment, scaling, and management of applications, including containerized applications with microservices architecture. By creating a Deployment per microservice, you can easily manage and scale each microservice separately in Google Kubernetes Engine. Moreover, deployments ensure the desired number of replicas for your application are running, and they will manage any updates or rollbacks as needed.

Solution to Question 47: B

The correct answer is B: Use gcloud to create the new project, and then deploy your application to the new project.

Explanation:

As a software engineer, you must ensure the smooth transition from development to production while maintaining the code and environment consistency. Using the gcloud command-line tool is the best practice in this scenario because it allows you to create a new project directly, which maintains environment consistency, simplifies the deployment process, and ensures no unwanted changes affect the production environment.

Here's a brief explanation of why the other options are not appropriate:

Option A: Migrating the development environment to the production environment using a separate branch in your Version Control System is not an ideal solution. Although branching is helpful for code management, it doesn't create a new project in GCP, which is necessary for environmental isolation.

Option C: Dataflow is a GCP service used primarily for data transformation and processing tasks. It is not the right tool for creating new projects or deploying App Engine applications. Using Dataflow to copy the application code would not set up the new environment needed for the production infrastructure.

Option D: Using the GCP Console to create a new project and then manually copying the source code of the App Engine application would be a slow and error-prone process. Manually copying the application code can introduce inconsistencies between the development and production environments. The gcloud command-line tool automates this process and ensures consistency.

Solution to Question 48: B

The correct answer is B. Use the command gcloud auth activate-service-account and point it to the private key.

The reason B is correct is because the gcloud auth activate-service-account command is specifically designed for authenticating service accounts using their private key in JSON format. By using this command, you can set the active service account in your gcloud CLI, which will then be used for subsequent gcloud commands that require authentication.

Option A is incorrect. Although setting the environment variable GOOGLE_APPLICATION_CREDENTIALS to the path of the private key is an important step for application authentication, merely placing the private key in the Cloud SDK installation directory does not make it the active service account for gcloud commands. Also, the environment variable alone does not affect the gcloud authentication.

Option C is incorrect because the gcloud auth login command is meant for user authentication, not service account authentication. When you run this command, it'll prompt you to log in with your Google account, and it does not accept the private key as an input.

Option D is incorrect because the gcloud projects add-iam-policy-binding command is used to grant IAM roles to existing service accounts or users within a Google Cloud project. This does not authenticate the service account or set it as the active account for gcloud commands. The command should not be pointed to a private key. Instead, it requires the email address of the service account or user and the desired IAM role.

Solution to Question 49: A

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

Explanation: The task at hand requires the service account from proj-sa to have permissions to take snapshots of VMs operating in proj-vm. Snapshots involve creating backups of data stored in virtual machine instances, which falls within the scope of Compute Storage Admin permissions. By granting the service account the IAM Role of Compute Storage Admin in proj-vm, you give it the necessary privileges to perform the required task.

Here's why the other options will not work:

B. Add the service account email as a member in proj-vm without assigning

any role. Explanation: Simply adding the service account email as a member in proj-vm without assigning a role will not grant the necessary permissions to take snapshots of VMs. The service account needs to be assigned an appropriate IAM Role that grants it the required permissions.

C. Enable Google Cloud Storage JSON API in proj-vm and use the proj-sa service account JSON key for authentication. Explanation: Although enabling the Google Cloud Storage JSON API and using the proj-sa service account JSON key for authentication might help with storage-related tasks, it is not specifically focused on virtual machines and their snapshots. Granting proper IAM roles will be more effective in providing the specific permissions required.

D. Grant the service account the IAM Role of Compute Instance Admin in the project called proj-vm. Explanation: Although the Compute Instance Admin role provides several permissions regarding the management of virtual machine instances, it does not specifically grant the permissions needed to take snapshots of VMs. The Compute Storage Admin role is better suited for this particular purpose, as it allows for managing storage resources within the project, including snapshots.

Solution to Question 50: C

The correct answer is C. Use kubectl to delete the topic resource.

Explanation:

As a Cloud Engineer working with Config Connector in Google Cloud project, you need to be familiar with Kubernetes operations and the tools used for managing Kubernetes resources. Config Connector is a Kubernetes add-on that allows you to manage Google Cloud resources using Kubernetes configuration files and command-line tools. In this scenario, the Pub/Sub topic is managed by Config Connector, and Kubernetes-native tools should be used to interact with it.

Option A: Using the Firebase CLI to delete the topic resource is incorrect because Firebase CLI is a command-line tool to manage and deploy Firebase projects and services, which is not related to managing Pub/Sub topics with Config Connector in Google Cloud Project.

Option B: Using Config Connector to manually remove the topic resource is incorrect because Config Connector itself does not provide a dedicated tool to delete resources. Instead, you should use the Kubernetes tools like kubectl.

Option C: Using kubectl to delete the topic resource is the correct option. Since Config Connector manages the Pub/Sub topic as a Kubernetes resource, using kubectl command-line tool will allow you to delete the resource and Configuration Connector will take care of permanently deleting it afterwards. You can use the command like this: `kubectl delete [RESOURCE_KIND] [RESOURCE_NAME]`, where RESOURCE_KIND is the kind of Kubernetes object Config Connector

created for your Pub/Sub topic, and RESOURCE_NAME is the name of the Kubernetes object.

Option D: Using GCP Console to update the topic label managed-by-cnrm to false is incorrect because updating the label in GCP Console will not permanently delete the topic, nor stop Config Connector from managing the topic. In fact, it might cause synchronization issues between the GCP Console and Config Connector if labels are modified without proper kubectl commands.

Thus, the correct answer is C. Use kubectl to delete the topic resource, as it provides the required functionality for deleting Kubernetes resources managed by Config Connector in Google Cloud project.

Practice Exam 18

Question 1: You are working as a software developer for a gaming company and are responsible for creating a multi-player gaming platform that will store game information in a database. The company expects the application's popularity and user base to grow globally, so you need to ensure consistent performance without increasing management complexity. How should you design the database to maintain optimal gaming performance for users worldwide?

A. Use Cloud SQL database with cross-region replication to store game statistics in the EU, US, and APAC regions.

B. Use Cloud Storage with geographic redundancy to store game statistics structured in JSON format.

C. Use Cloud Spanner to store user data mapped to the game statistics.

D. Use Firebase Realtime Database to store game statistics with a master-master replication system for global consistency.

Question 2: As a software company looking to streamline the development process within the Google Cloud environment, you need to standardize the creation and management of multiple Google Cloud resources using Infrastructure as Code while minimizing the amount of repetitive code required. What approach should you take to achieve this?

A. Develop templates for the environment using HashiCorp Terraform.

B. Write custom Python code using the Google Cloud SDK to create and manage resources.

C. Create separate Google Cloud projects for each environment and replicate across projects.

D. Develop templates for the environment using Cloud Deployment Manager.

Question 3: You are working as a system administrator for a company that relies on Google Cloud Platform for its infrastructure. Your task is to find a dynamic way of provisioning virtual machines (VMs) on the Compute Engine, with the exact specifications contained in a dedicated configuration file while adhering to Google's recommended practices. Which method should you use?

A. Cloud Composer

B. Deployment Manager

C. Bigtable

D. Cloud Functions

Question 4: As an IT professional working at a company utilizing a hybrid cloud strategy with some applications deployed on Google Cloud, you've established a VPN tunnel to connect the company's on-premises network to your

VPC in Google Cloud. In order to ensure smooth connectivity between multiple Google Cloud applications and an on-premises database server, without having to modify each application's IP configuration when the database's IP changes, what solution should be implemented?

A. Create a private zone on Cloud DNS, and configure the applications with the DNS name.

B. Create an individual VPC peering connection for each application to your on-premises network.

C. Configure Firebase Realtime Database as a middle layer for the applications and the on-premises database.

D. Use a Global Load Balancer to distribute traffic between your on-premises database and a replica in Google Cloud.

Question 5: In your company, you have been using Cloud Spanner for managing the database, and one of the teams has reported read latency-related performance issues on a particular table. The table, which is accessed only by primary key from users, has the schema provided below. To resolve this issue, what action should you take?

A. Remove the profile_picture field from the table.

B. Optimize the table schema by normalizing the data.

C. Change the primary key to not have monotonically increasing values.

D. Enable caching on the Cloud Spanner instance.

Question 6: You are an IT specialist working in a finance company that deploys its applications on bare-metal servers located within its data center. Your company requires access to Google Cloud Storage for certain operations, but the security policies disallow public IP addresses or internet access for these servers. To comply with Google-recommended practices and provide access to Cloud Storage, what solution should you implement?

A. 6. Deploy a Kubernetes cluster on your on-premises servers using Anthos, then configure the application to access Cloud Storage using the Anthos Service Mesh.

B. 1. Using Cloud VPN or Interconnect, create a tunnel to a VPC in Google Cloud. 2. Use Cloud Router to create a custom route advertisement for 199.36.153.4/30. Announce that network to your on-premises network through the VPN tunnel. 3. In your on-premises network, configure your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com.

C. 1. Use Migrate for Compute Engine (formerly known as Velostrata) to migrate those servers to Compute Engine. 2. Create an internal load balancer (ILB) that uses storage.googleapis.com as backend. 3. Configure your new instances to use this ILB as proxy.

D. 7. Create a serverless VPC connector between your on-premises servers and a Google Cloud VPC, then use this connector to route all Cloud Storage requests from your servers via the VPC.

Question 7: You have recently taken up a job as a cloud consultant in a multinational company, and your first task is to configure the billing for a new Google Cloud customer within the organization. The customer wants to group resources that share common IAM policies. What should you do?

A. Use folders to group resources that share common IAM policies.

B. Set up a proper project naming structure to group IAM policies.

C. Use labels to group resources that share common IAM policies.

D. Use Cloud Pub/Sub to manage resources with common IAM policies.

Question 8: You are working in a well-established company that utilizes G Suite for efficient communication and collaboration amongst all its employees. Every employee in the organization possesses a G Suite account. If you wish to provide some G Suite users access to your Cloud Platform project, what is the appropriate course of action to take?

A. Grant them the required IAM roles using their G Suite email address.

B. In the GCP Console, set up an API key for each G Suite user, allowing access to the required resources.

C. In the GCP Console, create an Organization Policy restricting access to specific G Suite users by listing their email addresses.

D. In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group.

Question 9: As a software engineer in a tech company, you are responsible for maintaining a critical application. During a recent incident, you received user complaints about a particular error occurring frequently. Upon investigation, you found that a Service Account had insufficient permissions, causing the issue. You were able to fix the problem, but you want to be alerted if it happens again in the future. What should you do to achieve this?

A. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

B. In the Log Viewer, filter the logs on severity 'Error' and the name of the Service Account.

C. Configure Autoscaling policies to handle the error spikes.

D. Grant Project Owner access to the Service Account.

Question 10: As a software engineer working for a company that relies heavily on Google Cloud services, you're tasked with maintaining a Google Kubernetes

Engine (GKE) cluster called 'dev'. It's crucial for you to manage the GKE configuration via the command line interface (CLI) after installing the Cloud SDK. To make sure that any future CLI commands automatically target this specific cluster, what should you do?

A. Use the command gcloud config set project/cluster dev.

B. Create a file called config.json in the ~/.gcloud folder that contains the cluster name.

C. Use the command gcloud config set container/cluster dev.

D. Use the command gcloud container clusters set-cluster dev.

Question 11: As a database administrator in a growing tech company, you are tasked with selecting and configuring a cost-effective solution for relational data on Google Cloud Platform. The company currently manages a small set of operational data in one geographic location and requires support for point-in-time recovery. What should be your course of action?

A. Select Cloud SQL (PostgreSQL). Select the create failover replicas option.

B. Select Cloud SQL (MySQL). Choose the create read replicas option.

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

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

Question 12: As a software engineer at a leading tech company, you have developed Docker images for an application that will be hosted on Google Cloud. The company has decided to avoid managing the infrastructure related to this application, and it is your responsibility to ensure automatic scalability as the application grows more popular. What is the best course of action to achieve this goal?

A. Create and launch Cloud Dataflow jobs with the container image.

B. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

C. Deploy the application on Google Compute Engine with a Preemptible VM.

D. Upload Docker images to Cloud Storage, and use Cloud Build to deploy the application.

Question 13: As an IT specialist at a software company, your team has developed an update for a web application that is currently running on Cloud Run for Anthos. You need to evaluate this updated version with a specific percentage of the production users (canary deployment). What is the correct course of action?

A. Create a new version of the application in a separate Google Cloud Project and use VPC peering to route traffic between the two projects.

B. Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

C. Create a new service with the new version of the application. Add an HTTP Load Balancer in front of both services.

D. Create a new revision with the new version of the application. Add an HTTP Load Balancer in front of both revisions.

Question 14: As a software engineer in a tech company, you are tasked with managing a third-party application that will run on a Compute Engine instance. Your company already has other Compute Engine instances running with default configurations, and the application's installation files are stored on Cloud Storage. You need to access these files from the new instance without granting access to other virtual machines (VMs). What should you do?

A. Create a new service account and assign this service account to all instances. Grant the service account permissions on Cloud Storage.

B. Create a new service account and assign this service account to the new instance. Change the storage class of objects on Cloud Storage to Nearline storage.

C. Create the instance with the default Compute Engine service account. Grant the service account permissions on Cloud Storage.

D. Create a new service account and assign this service account to the new instance. Grant the service account permissions on Cloud Storage.

Question 15: As a network administrator in a tech company, you are managing multiple VPC-native Google Kubernetes Engine clusters in the same subnet. Your company's growth is causing the IPs available for the nodes to become exhausted, and you need to make sure the clusters can expand as needed. What action should be taken to ensure this?

A. Set up Cloud NAT for the GKE clusters to share IP addresses.

B. Expand the CIDR range of the relevant subnet for the cluster.

C. Configure the GKE clusters to use non-VPC-native network mode.

D. Add an alias IP range to the subnet used by the GKE clusters.

Question 16: As a network administrator at a large technology company, you've successfully established an LDAP server on Compute Engine that can be accessed via TLS through port 636 using UDP. To ensure clients can connect to it over that specific port, what action should you take?

A. Create a VPC peering connection to allow access to the LDAP server on port 636 using UDP. Enable the 'Allow Secure LDAP access over the Internet' option in the Compute Engine settings. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow ingress on TCP port 636 for that network tag. Create a Cloud VPN tunnel and configure

the LDAP server to be reachable only through the VPN. Create a firewall rule to allow ingress on UDP port 636 without specifying any specific network tags. Set the VM instance to use a shared VPC and enable ingress on UDP port 636 in the Shared VPC settings. Deploy an Identity-Aware Proxy for the LDAP server and allow access on UDP port 636 only for authorized users. Create a Cloud NAT gateway and configure it to allow access to the LDAP server on port 636 using UDP.

B. Add a network tag of your choice to the instance running the LDAP server. Create a firewall rule to allow egress on UDP port 636 for that network tag.

C. Add the network tag allow-udp-636 to the VM instance running the LDAP server.

D. Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

Question 17: You are an IT Project Manager at a growing software company, responsible for overseeing the data analysis processes. The company uses a data pipeline to ingest data into BigQuery via streaming, and your goal is to enable the Business Analysts to run custom SQL queries against the most up-to-date data in BigQuery. What is the most appropriate action to take?

A. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

B. Grant the BI team access to Google Sheets and configure a connected sheet with the respective BigQuery tables for them to query the data.

C. Create a dedicated BigQuery dataset for the BI team and provide them with DataViewer access.

D. Grant the BI team access to Cloud Pub/Sub to receive real-time data updates from the data pipeline, without querying BigQuery.

Question 18: As an employee in the financial department of a large corporation, you are tasked with migrating invoice documents stored on-premises to Cloud Storage. The documents have the following storage requirements:

• Documents must be kept for five years. • Up to five revisions of the same invoice document must be stored, to allow for corrections. • Documents older than 365 days should be moved to lower cost storage tiers.

To minimize operational and development costs while following Google-recommended practices, what should you do?

A. Enable retention policies on the bucket, use lifecycle rules to change the storage classes of the objects, set the number of versions, and delete old files.

B. Use Google Cloud SQL combined with Cloud Datastore to manage storage requirements and delete old files.

C. Enable lifecycle rules on the bucket and use Cloud Data Transfer Service to move your documents based on their metadata.

D. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

Question 19: As an IT specialist at a media transcription company, you are tasked with extracting text from audio files using the Speech-to-Text API. The audio files are pushed to a Cloud Storage bucket, and you need to set up a fully managed, serverless compute solution that requires authentication and adheres to Google's best practices. To streamline the process, you wish to automate the call to the API, submitting each file to the API as soon as it arrives in the bucket. How should you proceed?

A. Deploy a Compute Engine instance with a startup script that scans the bucket regularly and calls the Speech-to-Text API for each unprocessed file.

B. Trigger a Compute Engine instance group by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

C. Run a Kubernetes job to scan the bucket regularly for incoming files, and call the Speech-to-Text API for each unprocessed file.

D. Create a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

Question 20: As an IT administrator at a software company, you recently deployed an application on a single Compute Engine instance within your organization's cloud infrastructure. The application writes logs to disk and lately, users have been reporting errors with the application. In order to diagnose the issue and find a resolution, what is the most appropriate course of action to take?

A. Configure a health check on the instance and set a consecutive successes Healthy threshold value of 1.

B. Use Deployment Manager to re-deploy the application on a new instance.

C. Install and configure the Ops agent and view the logs from Cloud Logging.

D. Deploy a new version of the application using Cloud Functions.

Question 21: At your software development company, you are working on a project that utilizes a 3-tier solution running on Compute Engine. The current infrastructure configuration includes a service account associated with all instances within each tier. To meet project requirements, you must enable communication on TCP port 8080 between tiers as follows:

- Instances in tier #1 must communicate with tier #2.
- Instances in tier #2 must communicate with tier #3.

What steps should you take to enable the required communication between tiers?

A. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow TCP:8080 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP: 8080

B. 1. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.2.0/24) • Protocols: allow TCP: 8080 2. Create an egress firewall rule with the following settings: • Targets: all instances • Source filter: IP ranges (with the range set to 10.0.1.0/24) • Protocols: allow TCP: 8080

C. 1. Create an egress firewall rule with the following settings: • Targets: all instances with tier #1 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP:8080 2. Create an egress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #3 service account • Protocols: allow TCP: 8080

D. 1. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #2 service account • Source filter: all instances with tier #1 service account • Protocols: allow TCP:80 2. Create an ingress firewall rule with the following settings: • Targets: all instances with tier #3 service account • Source filter: all instances with tier #2 service account • Protocols: allow TCP:80

Question 22: You're working as a software engineer in a rapidly growing tech company that's developing an application to store relational data for clients worldwide. The company executives, including your CTO, are concerned about the scalability of the database solution, as the exact size of the user base is unknown. They're seeking a storage solution that can easily accommodate user growth with minimal changes to configuration settings. Which storage solution should you opt for?

A. Cloud Spanner

B. Cloud SQL

C. Cloud Storage

D. Cloud Bigtable

Question 23: You're working as a project manager in a software development company and need to add a new auditor to your Google Cloud Platform project. The auditor needs to have read access but must not be able to modify anything within the project. How can you configure the auditor's permissions?

A. Add the user to the IAM Billing Account Viewer role with project-wide permissions. Add the user's account to this role.

B. Create a custom role with view-only service permissions. Add the user's account to the custom role.

C. Select the built-in IAM project Viewer role. Add the user's account to this role.

D. Assign the user to the IAM BigQuery Data Viewer role with project-wide permissions. Add the user's account to this role.

Question 24: As a project manager at a software development company, you are responsible for ensuring that the DevOps team has full control over Compute Engine resources in the company's development project. However, they should not have permission to create or update any other resources in the project. To adhere to Google's recommendations for setting permissions for the DevOps team, what action should you take?

A. Create an IAM policy and grant all compute.instanceAdmin.* permissions to the policy. Attach the policy to the DevOps group.

B. Grant the basic role roles/editor to the DevOps group.

C. Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

D. Create a custom role at the project level and grant all compute.instance.* permissions to the role. Grant the custom role to the DevOps group.

Question 25: You are working as a network engineer for a tech company that recently deployed an application on a managed instance group in Compute Engine. This application accepts TCP traffic on port 389 and requires preserving the IP address of clients making requests. To expose the application to the internet using a load balancer, which method should you utilize?

A. Expose the application by using an external TCP Network Load Balancer.

B. Expose the application by using an external UDP Network Load Balancer.

C. Expose the application by using Google Cloud's Traffic Director.

D. Expose the application by using an internal TCP Network Load Balancer.

Question 26: As an IT expert working in a global company with a high-traffic application, you're tasked with reducing latency for SSL-encrypted TCP traffic on port 443 from clients worldwide. What type of load balancing would be the most suitable solution in this situation?

A. Backend Services Load Balancer

B. NAT Gateway Load Balancer

C. SSL Proxy Load Balancer

D. Cloud Armor Load Balancer

Question 27: As a data engineer at a financial services company, you have been tasked with configuring optimal data storage for files in Cloud Storage to minimize costs. These files are crucial for an analytics pipeline that operates continuously and serves users located in Boston, MA (United States). What should you do?

A. Configure dual-regional storage for the dual region closest to the users. Configure a Nearline storage class.

B. Configure regional storage for the region closest to the users. Configure a Standard storage class.

C. Configure dual-regional storage for the region furthest from the users. Configure an Archive storage class.

D. Configure multi-regional storage for the multi-region closest to the users. Configure a Nearline storage class.

Question 28: As a software engineer in your company, you've been tasked with creating a new billing account and linking it with an existing Google Cloud Platform project. What is the appropriate course of action?

A. Verify that you are Billing Administrator for the GCP project. Create a new billing account and update the existing project to link it to the new billing account.

B. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project.

C. Verify that you are Billing Administrator for the billing account. Update the existing project to link it to the existing billing account.

D. Verify that you are Billing Administrator for the billing account. Create a new project and link the new project to the existing billing account.

Question 29: You are working as an infrastructure engineer at a software company. The team responsible for maintaining the company's infrastructure has decided to make some updates and improvements. In order to ensure that the whole team is on the same page and following Google's recommended best practices, how should you share your proposed changes with your colleagues?

A. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in Cloud Source Repositories.

B. Apply the changes in a development environment, run gcloud compute instances list, and then save the output in a shared Storage bucket.

C. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

D. Use Deployment Manager templates to describe the proposed changes and store them in a Cloud Storage bucket.

Question 30: As an IT professional in a large company, you are tasked with configuring autohealing for network load balancing for a group of Compute Engine instances running in multiple zones, using the fewest possible steps. Your goal is to ensure re-creation of VMs if they are unresponsive after 3 attempts of 10 seconds each. What should you do?

A. Create a managed instance group and verify that autoscaling and autohealing settings are off

B. Create a managed instance group. Set the Autohealing health check to healthy (HTTP)

C. Create an HTTP load balancer with a backend configuration that references an existing instance group. Set the health check to healthy (HTTP)

D. Use a Cloud VPN to connect the instances and set the Autohealing health check to healthy (HTTP)

Question 31: As an IT manager in a tech company, you have been assigned to handle a web application on Compute Engine. Your goal is to ensure that your support team automatically receives notifications if users experience high latency for at least 5 minutes. Considering a solution recommended by Google with no development cost, what is the best course of action?

A. Use Cloud Armor to monitor and alert on high latency events in your Compute Engine instances.

B. Use the Cloud Monitoring dashboard to observe latency and take the necessary actions when the response latency exceeds the specified threshold.

C. Create an alert policy to send a notification when the HTTP response latency exceeds the specified threshold.

D. Export Cloud Monitoring metrics to Cloud Storage and use Data Studio to create a dashboard for monitoring latency.

Question 32: As a data engineer in a large construction equipment rental company, you're tasked with handling the vast amounts of data generated by sensors installed on the rented equipment. These sensors send event information every few seconds, such as engine status, distance traveled, and fuel level. Customers are billed based on the consumption data from these sensors. With high throughput expectations - up to thousands of events per hour per device - and the need to retrieve consistent data based on the event's timestamp, you must ensure that storing and retrieving individual signals are atomic. What solution would be the most suitable?

A. Use Cloud Pub/Sub to stream data and store it in Cloud Firestore.

B. Ingest the data into Cloud Bigtable. Create a row key based on the event timestamp.

C. Create a file in Google Sheets per device and append new data in it.

D. Ingest the data into Datastore. Store data in an entity group based on the device.

Question 33: As a software developer working in a tech company, you are tasked with creating an application that will run on Google Kubernetes Engine. Your team has chosen MongoDB as the most appropriate database system for the project, and you have been asked to deploy a managed MongoDB environment with a support SLA. What should be your next course of action?

A. Deploy MongoDB Atlas from the Google Cloud Marketplace.

B. Create a Cloud Dataproc cluster and use the MongoDB connector for Hadoop.

C. Use Cloud Datastore with the MongoDB API enabled.

D. Deploy a MongoDB container on Cloud Functions and trigger it with an event.

Question 34: As a project manager at a software development company, you want to establish a Google Kubernetes Engine cluster for an upcoming project. Ensuring node identity and integrity are verifiable is crucial, and the nodes must not be accessible from the internet. To minimize operational costs and adhere to Google's best practices, which approach should you choose?

A. Deploy a standard private cluster and enable workloads identity.

B. Deploy a private autopilot cluster.

C. Deploy a public App Engine cluster and enable shielded nodes.

D. Deploy a public regional cluster and enable shielded nodes.

Question 35: You are an IT manager at a manufacturing company and have been tasked with deploying a new Enterprise Resource Planning (ERP) system on Google Cloud to optimize production processes. The application requires the full database to be held in-memory for quick data access. Which configuration of resources on Google Cloud should you choose for this application?

A. Use Cloud Datastore with high read/write throughput.

B. Provision Compute Engine instances with local SSDs attached.

C. Deploy the application on Kubernetes Engine with memory optimized nodes.

D. Provision Compute Engine instances with M1 machine type.

Question 36: As a DevOps engineer at a tech company, you are tasked with setting up a Linux VM for your team that needs to connect to Cloud SQL. You have already created a service account with the required access permissions. To ensure that the VM utilizes this specific service account rather than the default Compute Engine service account, what action should you take?

A. Modify the VM's startup script to include the JSON Private Key for the service account and configure the VM to use it.

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

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

D. Use the gcloud CLI to set the service account as the default Compute Engine service account for the project.

Question 37: You are an IoT Engineer at a tech company that specializes in developing Internet of Things (IoT) applications. Your recent project involves constructing a data lake on Google Cloud to handle the data from millions of IoT sensors. These sensors continuously send structured and unstructured data to the cloud backend. To ensure a highly available and resilient architecture following Google's recommended practices, what step should you take?

A. Stream data to Pub/Sub, and use Cloud Functions to send data to BigQuery.

B. Stream data to Dataflow, and use Storage Transfer Service to send data to BigQuery.

C. Stream data to Dataflow, and use Dataproc to send data to Bigtable.

D. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

Question 38: As an employee at a prominent investment firm, you are tasked with managing the storage of audit log files for 3 years. The company utilizes hundreds of Google Cloud projects to operate its various financial services. To ensure the cost-effective retention of these crucial log files, which course of action should you recommend?

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

B. Utilize Cloud Functions to trigger on new log entries and store them in Cloud Spanner.

C. Create an export to the sink that saves logs from Cloud Audit to Firebase Realtime Database.

D. Implement a Cloud Run service that streams logs from Cloud Audit to Cloud Storage Nearline.

Question 39: As a software engineer working for a company with multiple clients, you have one Google Cloud Platform account running in the default region and zone and another account running in a non-default region and zone. You need to set up new Compute Engine instances for these two clients using the command line interface. What should you do to accomplish this task?

A. Create a configuration file for each account and use the –configuration flag when running gcloud command to start Compute Engine instances.

B. Use gcloud compute instances create [INSTANCE_NAME] with the –zone and –region flags to specify the desired zone and region for each account.

C. Create two configurations using gcloud config configurations create [NAME]. Run gcloud config configurations activate [NAME] to switch between accounts when running the commands to start the Compute Engine instances.

D. Create separate shell scripts for each account and specify the gcloud command to start Compute Engine instances with specific zone and region flags.

Question 40: As an IT engineer working in a radiology clinic, you are responsible for securely storing digital medical images in an on-premises data room. The clinic wants to utilize Cloud Storage for archival purposes and requires an automated process to upload new medical images to it. How should you design and implement this solution?

A. Create a Data Fusion pipeline to transfer medical images from the on-premises storage to Cloud Storage on a scheduled interval.

B. Create a Pub/Sub topic, and enable a Cloud Storage trigger for the Pub/Sub topic. Create an application that sends all medical images to the Pub/Sub topic.

C. Deploy a Dataflow job from the batch template, "Datastore to Cloud Storage." Schedule the batch job on the desired interval.

D. Create a script that uses the gsutil command line interface to synchronize the on-premises storage with Cloud Storage. Schedule the script as a cron job.

Question 41: You are working as a software engineer in a cloud computing company, and you have recently deployed an application to a single Compute Engine instance within the company's infrastructure. The application writes logs to disk, and users have begun to report errors within the application. In order to diagnose and resolve the issues, what action should you take?

A. Navigate to Cloud Logging and view the application logs.

B. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging.

C. Configure Cloud Pub/Sub to receive logs and analyze them externally.

D. Configure a Health Check on the instance and set a Low Healthy Threshold value.

Question 42: As a part of the IT team in the retail industry, your company experienced a recent security breach and now seeks to improve the monitoring of the Google Cloud environment, focusing on unanticipated firewall changes and instance creation. With a preference for simple solutions, what strategy should be implemented?

A. Turn on Google Cloud firewall rules logging, and set up alerts for any insert, update, or delete events.

B. Integrate Cloud Identity-Aware Proxy (IAP) with Cloud Monitoring to observe unauthorized access attempts and set up alerts for potential firewall changes and unexpected instance creation.

C. Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

D. Create custom monitoring dashboards using Grafana and integrate them with Google Cloud Monitor to visualize the changes in firewall and instance actions.

Question 43: As an IT manager at a software development company, you are in charge of an application that runs on multiple virtual machines within a managed instance group with autoscaling enabled. The policy is set to add more instances if their CPU utilization goes above 80% until either the group reaches its maximum limit of five VMs or until the CPU utilization drops to 80%. The initial delay for HTTP health checks against those instances is set to 30 seconds. However, it takes approximately three minutes for the virtual machine instances to become available for users. You've noticed that when autoscaling occurs, the instance group adds more instances than necessary to support the levels of end-user traffic. How should you properly maintain the instance group sizes when autoscaling?

A. Decrease the initial delay of the HTTP health check to 10 seconds.

B. Configure autoscaling based on memory utilization instead of CPU utilization.

C. Increase the instance group's maximum limit to 10.

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

Question 44: You are an IT manager at a financial services company and are responsible for creating an archival solution for the company's data warehouse using Cloud Storage. The company needs to access this archived data quarterly to meet regulatory requirements. Which cost-efficient storage option should you choose for this purpose?

A. Cold Storage

B. Durable Reduced Availability Storage

C. Datastore

D. Partner Interconnect

Question 45: As a data manager in a large financial company, you are responsible for overseeing the sensitive data stored in three Cloud Storage buckets, with data access logging enabled. To ensure the security of these buckets, you need to verify the actions of a specific user, including the addition of metadata

labels and which files have been accessed. To achieve this in the fewest possible steps, what action should you take?

A. Create a trace in Stackdriver to view the information.

B. Enable and configure Google Cloud Armor to view the logs.

C. Using the GCP Console, filter the Activity log to view the information.

D. Create a trace in Cloud Monitoring to view the information.

Question 46: As the CTO of a software development company, you manage a team of 10 developers working on various projects utilizing Google Cloud solutions. You've given each team member their own Google Cloud Project as a personal sandbox for experimenting and learning. To keep track of costs, you want to be notified if anyone exceeds $500 of spending per month in their individual sandbox environments. What should be your course of action?

A. Create a budget per project and configure budget alerts on all of these budgets.

B. Configure Google Cloud billing notification with a spending threshold of $500 per month on the Organization level.

C. Use Cloud Pub/Sub to notify you when developers are creating new resources in their sandbox projects.

D. Use Deployment Manager to track each sandbox project's resource usage and notify you when the cost reaches $500.

Question 47: You are working for a software company that develops applications for various industries. Your team has recently created an application targeting the healthcare industry, and it is packaged into a Docker image. Now, you need to deploy the Docker image as a workload on Google Kubernetes Engine. What should you do?

A. Upload the image to Container Registry and create a Kubernetes Service referencing the image.

B. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image.

C. Upload the image to Cloud Storage and create a Kubernetes DaemonSet referencing the image.

D. Upload the image to Artifact Registry and create a Kubernetes Service referencing the image.

Question 48: As a software engineer at a reputable tech company with three existing Google Cloud projects, you need to ensure that the Marketing department is billed solely for their Google Cloud services linked to a new campaign within their team. What steps should you take?

A. 1. Verify that you are assigned the Organization Administrator IAM role for your organization's Google Cloud account. 2. Assign quotas to Marketing department's project and manually calculate billing based on resource usage.

B. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud account. 2. Create a new Google Cloud Project for the Marketing department. 3. Set the default key-value project labels to department:marketing for all services in this project.

C. 1. Verify that you are assigned the Billing Administrator IAM role for your organization's Google Cloud Project for the Marketing department. 2. Link the new project to a Marketing Billing Account.

D. 1. Verify that you have the Billing Viewer IAM role for your organization's Google Cloud account. 2. Monitor the usage of the Marketing department's services and manually invoice them at the end of each month.

Question 49: As a network administrator for a company, you are tasked with creating a custom VPC with a single subnet that has the largest possible range. Which IP address range should you utilize for this subnet?

A. 203.0.113.0/24

B. 10.0.0.0/8

C. 192.168.1.0/24

D. 10.1.0.0/16

Question 50: You are working as a data analyst at a retail company, operating your data warehouse on BigQuery. A marketing agency that your company collaborates with offers to improve customer targeting by implementing a recommendation engine based on the data stored in your data warehouse. The marketing agency is also running their application on Google Cloud and manages resources in their own project. To implement this recommendation engine, they require access to the BigQuery dataset in your project. How should you provide the marketing agency with the necessary access to the dataset?

A. Create a Service Account in your own project, and grant this Service Account access to Cloud Storage in your project.

B. Ask the partner to create a Service Account in their project, and have them give the Service Account access to Compute Engine in their project.

C. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

D. Create a Service Account in your own project, and grant this Service Account access to BigQuery in your project.

Practice Exam 18 Solutions

Solution to Question 1: C

The correct answer is C. Use Cloud Spanner to store user data mapped to the game statistics.

Explanation: Cloud Spanner is designed specifically for globally scalable applications such as a multi-player gaming platform. It offers strong consistency across regions, high availability, and horizontal scalability without adding management complexity. This means that as the user base and the game's popularity grow worldwide, Cloud Spanner will continue to provide consistent performance without needing manual intervention for management.

Why the other options will not work:

A. Use Cloud SQL database with cross-region replication to store game statistics in the EU, US, and APAC regions: Although Cloud SQL with cross-region replication offers some degree of geographic redundancy, it might not provide strong consistency and latency mitigation needed for a global application like a gaming platform. Moreover, it can add management complexity as application demand grows over time.

B. Use Cloud Storage with geographic redundancy to store game statistics structured in JSON format: Cloud Storage is an object storage service optimized for storing unstructured data at scale. While it does offer geographic redundancy, it is not designed for real-time data storage and retrieval operations required for a multi-player gaming platform. It would also require significant processing overhead to maintain consistency in the stored game statistics.

D. Use Firebase Realtime Database to store game statistics with a master-master replication system for global consistency: While Firebase Realtime Database can be useful in real-time synchronization between clients, it does not scale horizontally for a global user base and throughput needs of a large-scale gaming application. Additionally, Firebase Realtime Database provides only eventual consistency, which is not ideal for maintaining optimal gaming performance for users worldwide.

In summary, Cloud Spanner is the best choice for designing a database that maintains optimal gaming performance for users worldwide due to its strong consistency, high availability, scalability, and low management complexity.

Solution to Question 2: D

The correct answer is D, Develop templates for the environment using Cloud Deployment Manager.

Here is the explanation for why the answer should be D and why other options will not work:

Option A: HashiCorp Terraform is a popular Infrastructure as Code (IaC) tool

that supports multi-cloud deployments, including Google Cloud. While it is a viable option for creating and managing resources in Google Cloud, it is not as natively integrated with the platform as Deployment Manager. Using a Google Cloud-native tool provides a tighter integration, better compatibility, and fewer potential issues.

Option B: Writing custom Python code using the Google Cloud SDK is not recommended because it requires significant time and effort to write, test, and maintain the custom code for resource management. This process would be more labor-intensive and error-prone compared to using an IaC tool such as Deployment Manager.

Option C: Creating separate Google Cloud projects for each environment and replicating across projects is not an efficient way to standardize the creation and management of resources, as it does not reduce the amount of repetitive code required. Also, managing multiple projects could become overly complicated and challenging to maintain over time.

Option D: Developing templates for the environment using Cloud Deployment Manager is the best approach because it is a Google Cloud-native IaC solution designed specifically for creating and managing resources in the Google Cloud environment. This tool allows you to describe the desired state of your infrastructure in declarative templates, enabling you to automate the creation and management process. Additionally, it supports the reuse of templates and the ability to create modular templates, which can help minimize repetitive code. This is why Option D is the correct choice for streamlining the development process and standardizing the management of multiple Google Cloud resources.

Solution to Question 3: B

The correct answer is B. Deployment Manager.

Explanation:

B. Deployment Manager is the ideal choice for provisioning virtual machines (VMs) on Google Compute Engine dynamically with the exact specifications detailed in a dedicated configuration file. Deployment Manager adheres to Google's recommended practices and allows you to manage your infrastructure through declarative templates and configuration files. It automates the deployment, management, and updates of your Google Cloud Platform resources, making it the best fit for this task.

Here's why other options are not appropriate:

A. Cloud Composer is a managed Apache Airflow service used to create, schedule, and manage complex pipelines. It is not specifically designed for provisioning VMs on Compute Engine and does not provide the functionality to maintain infrastructure declaratively.

C. Bigtable is a Google Cloud Platform service that provides a fully managed, scalable NoSQL database. It is used primarily for storing and managing large

amounts of data, and is not meant for provisioning and managing infrastructure resources like VMs.

D. Cloud Functions is a Google Cloud Platform service for running serverless applications by executing code in response to various events. While it can interact with other GCP services, it is not suitable for managing infrastructure in a dynamic, declarative way as required.

Solution to Question 4: A

The correct answer should be A - Create a private zone on Cloud DNS, and configure the applications with the DNS name.

Here's the explanation for why A should be the answer: By creating a private DNS zone in Cloud DNS and configuring the applications with the DNS name, you are allowing applications to resolve the database server's IP address automatically. When the database's IP changes, you only have to update the DNS record without modifying any application's IP configuration. DNS resolves the name to the new address, and the applications will continue connecting to the database server through the VPN tunnel.

However, the other options will not work, and here's why:

B. Creating individual VPC peering connections for each application would have a higher administrative overhead and will not solve the problem of applications having to update their IP configuration each time the database's IP changes. VPC peering is a network connection and not a DNS resolution mechanism, which is needed to handle changing IP addresses.

C. Configuring Firebase Realtime Database as a middle layer is not an ideal solution because it does not directly address the issue of handling changes to the database's IP. Firebase Realtime Database is a separate cloud-based NoSQL database, and configuring it as a middle layer would require significant changes in the existing applications' architecture.

D. Using a Global Load Balancer is not appropriate in this context because the database server is on-premises and the requirement is to ensure smooth connectivity without modifying each application's IP configuration when the database's IP changes. The Global Load Balancer is designed for distributing traffic between multiple instances of a service deployed in Google Cloud across regions and is not suited for on-premises database replication scenarios.

Solution to Question 5: C

The correct answer is C. Change the primary key to not have monotonically increasing values.

Explanation for the correct answer: C. Changing the primary key to not have monotonically increasing values is the most suitable action to resolve the read latency-related performance issue. In Cloud Spanner, having a primary key with monotonically increasing values can cause hotspotting issues. Hotspotting

happens when a specific area of a database becomes a bottleneck due to a significant concentration of read or write operations. By altering the primary key to have a more evenly distributed range of values, you can distribute the load evenly across the Cloud Spanner instance and prevent hotspotting, resulting in the reduced read latency.

Explanation for why other options will not work: A. Removing the profile_picture field from the table might help in reducing the storage size, but it will not solve the issue of read latency, as it doesn't address the potential hotspotting problem caused by the primary key design.

B. Normalizing the data can be useful for optimizing the table schema and reducing data redundancy, but it won't directly address the read latency issue reported by the team, which is more likely to be related to the primary key design causing hotspotting.

D. Enabling caching on the Cloud Spanner instance might improve the read performance for some use cases, but it won't solve the root cause behind the read latency issue, which is hotspotting caused by monotonically increasing primary key values. In fact, it might mask the actual issue and still result in poor performance during heavy read activity. Additionally, Cloud Spanner does not support caching explicitly; instead, it relies on its native optimizations to ensure performance.

Solution to Question 6: B

The best solution for this scenario is option B, and here's why:

Option B outlines a process for securely connecting your on-premises servers to Google Cloud Storage without having public IP addresses or internet access. By using Cloud VPN or Interconnect to create a secure tunnel between your on-premises network and a VPC in Google Cloud, your servers can access Google Cloud Storage without exposing them to the public internet. Additionally, using Cloud Router to create and advertise custom routes and configuring your DNS server to resolve *.googleapis.com as a CNAME to restricted.googleapis.com ensures secure access to required Google APIs without violating company security policies.

On the other hand, other options have shortcomings that make them unsuitable for this scenario:

Option A: Deploying a Kubernetes cluster on your on-premises servers using Anthos is not the most effective solution to meet the given requirements, as it can introduce unnecessary complexities related to managing Kubernetes and Anthos Service Mesh while not specifically addressing the security policies that restrict public IP addresses or internet access.

Option C: Migrate for Compute Engine involves migrating your on-premises servers to Google Cloud Compute Engine. This solution not only adds overhead in managing migration but also doesn't meet the requirements of your

existing security policies, as your applications are currently deployed on bare-metal servers within your own data center. Additionally, creating an ILB with storage.googleapis.com as backend may help with routing, but it doesn't address security concerns.

Option D: Creating a serverless VPC connector between your on-premises servers and a Google Cloud VPC cannot be directly used for bare-metal servers. It is designed to be used with Cloud Functions or Cloud Run services, which are serverless computing services. Thus, this solution does not satisfy the requirements of your current infrastructure setup.

In conclusion, option B is the most suitable solution for this scenario, as it ensures secure access to Google Cloud Storage without violating the company's security policies, whereas the other options do not effectively address the underlying concerns or introduce unnecessary complexities.

Solution to Question 7: A

The correct answer is A: Use folders to group resources that share common IAM policies.

Explanation for why the answer should be A: Folders are a powerful tool for organizing and managing resources in Google Cloud. They allow you to create a hierarchy of resources and manage access control policies according to organizational requirements. By grouping resources that share common IAM policies in folders, you can consolidate their access control management. This makes it easier to maintain and update IAM policies across these resources, ensuring proper access control is in place.

Explanation for why other options will not work:

B. A proper project naming structure may improve organization and visibility, but it will not help group resources that share common IAM policies. IAM policies are applied to resources within projects, so simply naming projects appropriately will not be sufficient for access control management.

C. Labels can be used to categorize and filter resources based on your organizational needs, but they do not have an impact on access control or IAM policies. While you can use labels to identify resources with similar characteristics, you cannot directly apply or manage IAM policies through labels.

D. Cloud Pub/Sub is a messaging service that allows communication between independent applications using published messages. It is not designed for organizing or grouping resources based on their IAM policies, nor does it provide functionality for managing access control. So, using Cloud Pub/Sub for this purpose is not appropriate and will not help configure billing or IAM policies effectively.

Solution to Question 8: A

The correct answer is A: Grant them the required IAM roles using their G Suite email address.

Explanation: Google Cloud Platform (GCP) provides Identity and Access Management (IAM) to control access to cloud resources effectively. In this scenario, as G Suite users already have their accounts, it makes sense to use their existing G Suite email addresses to assign them the required IAM roles. This way, you can grant access to your Cloud Platform project by ensuring their abilities are consistent with the Principle of Least Privilege, thus enabling efficient communication and collaboration.

Reasons why other options will not work: B. In the GCP Console, set up an API key for each G Suite user, allowing access to the required resources: API keys offer access to specific APIs but are not meant to control access to GCP resources or projects. IAM roles, on the other hand, help manage user access privileges more effectively.

C. In the GCP Console, create an Organization Policy restricting access to specific G Suite users by listing their email addresses: Organization policies allow you to set constraints on your resources across the organization, but they are not designed for managing access to specific projects or resources. Assigning IAM roles is a more appropriate approach.

D. In the G Suite console, add the users to a special group called cloud-console-users@yourdomain.com. Rely on the default behavior of the Cloud Platform to grant users access if they are members of this group: There is no default behavior for GCP to grant access based on G Suite group membership. While groups can be used in conjunction with IAM roles, there is no specific group that automatically provides Cloud Platform access. You still need to assign appropriate IAM roles to the users or groups to grant them access to your Cloud Platform project.

Solution to Question 9: A

The correct answer is A. Create a custom log-based metric for the specific error to be used in an Alerting Policy.

This is the best option because it allows you to set up a monitoring system that will trigger an alert when the specific error occurs, helping you catch the issue early and intervene in a timely manner. Creating a custom log-based metric for the specific error and using it in an Alerting Policy ensures precision in monitoring the exact problem that caused user complaints in the past.

The other options are not suitable for achieving the desired outcome:

B. In the Log Viewer, filter the logs on severity 'Error' and the name of the Service Account. - This option would only help you find the error in the logs when it has already occurred, but it does not provide any alerting mechanism. It's a useful approach to investigate a past issue but doesn't offer proactive monitoring.

C. Configure Autoscaling policies to handle the error spikes. - Autoscaling policies can help manage variable workloads, but they do not provide specific monitoring or alerting capabilities for a particular error. These policies are focused on adapting resource allocation in response to changing demands and not on detecting or resolving in-depth application issues.

D. Grant Project Owner access to the Service Account. - Giving the Service Account such a high level of access might resolve permission issues in the short term, but it might also introduce new security risks and vulnerabilities. Moreover, it does not address the need for an alerting system if the same error or a different problem happens in the future. It's important to adhere to the principle of least privilege, ensuring accounts have only the necessary access to fulfill their tasks.

Solution to Question 10: C

The correct answer is C: Use the command gcloud config set container/cluster dev.

Explanation:

A: The command `gcloud config set project/cluster dev` is incorrect because there is no "project/cluster" property in the Cloud SDK configuration. The correct property should be "container/cluster".

B: Creating a file called config.json in the ~/.gcloud folder is not the correct way to set the GKE cluster configuration. The Cloud SDK command-line tool provides commands for setting configurations, specifically the `gcloud config set` command.

C: By using the command `gcloud config set container/cluster dev`, you set the desired cluster as 'dev' for any future CLI commands automatically. This is the correct way to configure the Cloud SDK to target the specified GKE cluster.

D: The command `gcloud container clusters set-cluster dev` is incorrect because there is no "set-cluster" command for the "gcloud container clusters" category. To set the GKE cluster configuration, you must use the `gcloud config set` command with the proper property.

Solution to Question 11: D

The correct answer is D: Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected.

Explanation: The company's requirements are (1) a cost-effective solution for relational data on Google Cloud Platform, (2) support for point-in-time recovery, and (3) manageable within a single geographic location. Let's analyze each option:

A. Select Cloud SQL (PostgreSQL). Select the create failover replicas option. Failover replicas in Cloud SQL provide high availability for your database by

automatically rerouting traffic to one or more standby replicas in case the primary goes down. While it is a valuable feature, it does not fulfill the requirement of point-in-time recovery.

B. Select Cloud SQL (MySQL). Choose the create read replicas option. Creating read replicas in Cloud SQL allows you to horizontally scale MySQL instances, offload read traffic from primary instances, and distribute database workloads across replicas. However, this option does not specifically cater to the requirement of point-in-time recovery.

C. Select Cloud Spanner. Set up your instance with 2 nodes. Cloud Spanner offers horizontal scalability, global consistency, and strong transactional capabilities. However, it is not the most cost-effective solution and could be overkill for a small operational dataset confined to a single geographic location.

D. Select Cloud SQL (MySQL). Verify that the enable binary logging option is selected. (Correct answer) Cloud SQL for MySQL is a fully managed instance with built-in support for point-in-time recovery when binary logging is enabled. As a cost-effective solution, it satisfies the requirements for a small set of operational data in one geographic location. By enabling binary logging, it permits point-in-time recovery from any backup, providing the needed functionality for disaster recovery.

In conclusion, option D is the appropriate solution as it fulfills all the requirements of cost-effectiveness, point-in-time recovery, and manageability within a single geographic location.

Solution to Question 12: B

The correct answer is B. Upload Docker images to Artifact Registry, and deploy the application on Cloud Run.

Here's why option B is the best choice, and why the other options do not meet the requirements:

Option A: Create and launch Cloud Dataflow jobs with the container image. Cloud Dataflow is a fully managed service for data processing pipelines, and it is not meant for deploying and scaling containerized applications. Therefore, this option does not meet the requirements of automatic scalability and avoiding infrastructure management for the application.

Option B: Upload Docker images to Artifact Registry, and deploy the application on Cloud Run. This is the best choice because Cloud Run is a managed compute platform from Google Cloud that automatically scales containerized applications. By uploading the Docker images to Artifact Registry, you're providing a place to store and manage these images. Cloud Run lets you focus on writing code and not managing infrastructure, which is exactly what the company is looking for.

Option C: Deploy the application on Google Compute Engine with a Preemptible VM. Google Compute Engine allows you to run virtual machines, but

it doesn't automatically scale applications as needed. Additionally, preemptible VMs are short-lived instances that last up to 24 hours and can be terminated by Google at any time, which is not suitable for a growing, popular application.

Option D: Upload Docker images to Cloud Storage, and use Cloud Build to deploy the application. While Cloud Storage is a useful service for storing objects like Docker images, and Cloud Build can help you automate builds and deployments, this option still requires you to manage the infrastructure related to the application. In contrast, Cloud Run provides automatic scaling and reduces operational overhead, which is more appropriate for the company's requirements.

Solution to Question 13: B

The correct course of action for this scenario is Option B: Create a new revision with the new version of the application. Split traffic between this version and the version that is currently running.

Option B is the best choice because Cloud Run for Anthos allows you to create new revisions of your applications and manage traffic splitting between revisions. This allows you to perform canary deployments and gradually shift a percentage of your production users to the updated version of the application. This method enables you to monitor performance, identify potential issues, and make necessary adjustments before rolling out the update to all users.

Option A is not suitable because creating a new version of the application in a separate Google Cloud Project and using VPC peering to route traffic introduces unnecessary complexity and additional management overhead. This approach is not optimized for evaluating an updated version with only a specific percentage of users.

Option C is not optimal because creating a new service with the new version of the application, instead of a new revision, adds management complexity and requires additional infrastructure setup with an HTTP Load Balancer. This method does not take full advantage of Cloud Run for Anthos' revision and traffic-splitting features.

Option D is incorrect because although it involves creating a new revision for the updated version, adding an HTTP Load Balancer in front of both revisions is unnecessary and adds complexity. Cloud Run for Anthos provides traffic splitting directly between multiple revisions without requiring an external load balancer.

In conclusion, Option B is the most appropriate course of action to ensure a smooth canary deployment and evaluation process, leveraging the features provided by Cloud Run for Anthos.

Solution to Question 14: D

The correct answer is D because it ensures the new instance, and only the new instance, has access to the application files stored in Cloud Storage. Creating a

new service account and assigning it to the new instance means that this specific service account can be given permissions exclusively to access the required files in Cloud Storage. By doing this, access to the files is restricted to the new Compute Engine instance only, preventing unauthorized access from other VMs.

Option A is incorrect because assigning the new service account to all instances would allow every virtual machine to access the files, thus not limiting access to only the new instance.

Option B is incorrect because it includes changing the storage class to Nearline storage, which is unrelated to granting access to the application files or limiting VM access. Nearline storage is a low-cost storage class for infrequently accessed data, designed for long-term storage. It addresses data storage requirements, not access control.

Option C is incorrect because using the default Compute Engine service account would grant access to the entire Compute Engine instances using the default account, exposing the files to all instances rather than restricting access to the new instance only.

Solution to Question 15: B

The correct answer is B: Expand the CIDR range of the relevant subnet for the cluster.

Explanation: Since the company is growing, and the available IP addresses for the nodes are getting exhausted, the best solution is to expand the CIDR range of the subnet associated with the Kubernetes Engine clusters. Expanding the CIDR range will provide more IP addresses for nodes, allowing the company's clusters to expand as needed.

Why other options will not work:

A. Set up Cloud NAT for the GKE clusters to share IP addresses: Cloud NAT is used to enable private VM instances in a VPC network to access the internet and does not address the issue of increasing the number of available IP addresses for nodes in the cluster.

C. Configure the GKE clusters to use non-VPC-native network mode: Non-VPC-native network mode, also called as routes-based mode, has less scalability and flexible address management compared to VPC-native network mode. Switching to non-VPC-native network mode would limit cluster growth and affect the efficiency of the network.

D. Add an alias IP range to the subnet used by the GKE clusters: Alias IP ranges allow assigning multiple IP addresses to a single VM instance. This option does not address the core issue of providing more IP addresses for the nodes in the clusters, as the clusters need more dedicated IP addresses for growth and operations.

Solution to Question 16: D

The correct answer is D: Add a network tag of your choice to the instance. Create a firewall rule to allow ingress on UDP port 636 for that network tag.

Explanation:

Option D is the most suitable solution because it enables clients to connect to the server specifically over UDP port 636 with TLS. By adding a network tag to the instance running the LDAP server and creating a firewall rule that allows ingress on port 636 for that network tag, you effectively ensure connectivity while maintaining the security of the server.

Here is why the other options will not work:

Option A: This option suggests multiple steps, some of which are irrelevant or incorrect for the given scenario. Creating a VPC peering connection, using Cloud VPN or Cloud NAT, and deploying an Identity-Aware Proxy are unnecessary steps, as the question states that clients should be able to connect to the server directly over port 636 using UDP. Also, enabling 'Allow Secure LDAP access over the Internet' option or creating a firewall rule to allow ingress on TCP port 636 contradicts the requirement to use UDP port 636.

Option B: This option is not suitable because it focuses on egress traffic rather than ingress. The question asks for allowing clients to connect to the LDAP server, which requires allowing ingress traffic on UDP port 636.

Option C: While this option adds the network tag allow-udp-636, it does not mention any firewall rule allowing ingress on UDP port 636. Simply adding a network tag is not sufficient; the appropriate firewall rule must be implemented in order to allow clients to connect to the LDAP server on the specified port.

Solution to Question 17: A

The most appropriate action to take is A. Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team. This is because the primary objective is to enable the Business Analysts to run custom SQL queries against the most up-to-date data in BigQuery.

Reasons for other options not being suitable:

B. Grant the BI team access to Google Sheets and configure a connected sheet with the respective BigQuery tables for them to query the data. While connected sheets enable querying data in BigQuery, this option does not provide the flexibility, performance, and scalability of running native SQL queries directly in BigQuery. Letting the BI team query directly from BigQuery will leverage its full features and ensure they have real-time data.

C. Create a dedicated BigQuery dataset for the BI team and provide them with DataViewer access. Although this will give the team access to the data, the DataViewer role does not allow running custom SQL queries. Their access will be limited to viewing the data, which goes against the primary objective of enabling them to run queries.

D. Grant the BI team access to Cloud Pub/Sub to receive real-time data updates from the data pipeline, without querying BigQuery. This option is not appropriate because it does not allow the BI team to run custom SQL queries as required. Cloud Pub/Sub is used for message passing and is not suitable for querying data, while BigQuery is specifically designed for complex querying and analysis tasks.

Thus, the best option is A, which allows the BI team to have the proper permission to run custom SQL queries in BigQuery, leveraging real-time data and the platform's analytical capabilities.

Solution to Question 18: D

The correct answer is D. Here's why:

D. Enable object versioning on the bucket, use lifecycle conditions to change the storage class of the objects, set the number of versions, and delete old files.

This option meets all the requirements stated in the question. Object versioning will allow for storing 5 revisions of the same invoice document, lifecycle conditions will enable moving documents older than 365 days to lower cost storage tiers, and deleting old files will ensure that documents are kept for only five years. This approach follows Google-recommended practices and minimizes operational and development costs.

Here's why the other options won't work:

A. Enable retention policies on the bucket, use lifecycle rules to change the storage classes of the objects, set the number of versions, and delete old files.

This option doesn't mention object versioning, which is required to store up to five revisions of the same invoice document. Retention policies can't handle multiple revisions, making this option unsuitable for the requirements.

B. Use Google Cloud SQL combined with Cloud Datastore to manage storage requirements and delete old files.

This option introduces unnecessary complexity by using both Google Cloud SQL and Cloud Datastore. Additionally, it doesn't specify how to handle the storage of five revisions of the same invoice document and moving older documents to lower cost storage tiers.

C. Enable lifecycle rules on the bucket and use Cloud Data Transfer Service to move your documents based on their metadata.

This option doesn't address the requirement of storing up to five revisions of the same invoice document. Cloud Data Transfer Service is unnecessary, as you can use lifecycle conditions to change the storage class of the objects within the Cloud Storage itself.

Solution to Question 19: D

The correct answer is D: Create a Cloud Function triggered by Cloud Storage bucket events to submit the file URI to the Google Speech-to-Text API.

Here's why the other options are not suitable:

Option A: Deploying a Compute Engine instance with a startup script to scan the bucket regularly would not be the optimal choice. This method does not provide a serverless, fully managed solution as it would require manual maintenance and scaling of the Compute Engine instance. Additionally, it does not efficiently automate the process as it relies on scanning the bucket at fixed time intervals, which could lead to delays in processing files.

Option B: Triggering a Compute Engine instance group by Cloud Storage bucket events might seem like an efficient, automated option, but it does not meet the requirement of a serverless, fully managed solution. This method involves manual management and scaling of the Compute Engine instance group, which contradicts Google's best practices for a serverless compute solution.

Option C: Running a Kubernetes job to scan the bucket regularly involves using Kubernetes, which does not fit the requirement of a fully managed, serverless solution. Similar to option A, this approach would not efficiently automate the process as it relies on scanning the bucket at fixed time intervals, which could lead to delays in processing files.

Option D is the best choice because it employs a Cloud Function, which is a fully managed, serverless compute solution in Google Cloud. By triggering the function with Cloud Storage bucket events, you efficiently automate the process of submitting each arriving file to the Speech-to-Text API. This approach also requires authentication, as you'll need to use the API key or a service account for making the requests. Overall, it adheres to Google's best practices and fulfills all the requirements specified in the question.

Solution to Question 20: C

The correct answer is C: Install and configure the Ops agent and view the logs from Cloud Logging.

Explanation: Since the application is writing logs to the disk, the most appropriate course of action for diagnosing issues and finding resolutions is to use the available logs. Google Cloud Logging is specifically designed for aggregating and analyzing logs from various services within the Google Cloud Platform. By installing and configuring the Ops agent on the Compute Engine instance, you can efficiently collect and view the application's logs in Cloud Logging. This approach will provide you with the necessary information to identify and solve the reported errors.

Reasons why other options will not work:

A. Configure a health check on the instance and set a consecutive successes Healthy threshold value of 1: Health checks are useful for monitoring the availability and response of an application, but they don't provide detailed informa-

tion about the application's errors or logs. In this case, health checks are not sufficient to diagnose the issue.

B. Use Deployment Manager to re-deploy the application on a new instance: Redeploying the application on a new instance might not resolve the issue, as it does not help in understanding the cause of the errors in the first place. Firstly, you need to analyze the logs and diagnose the errors before making changes to the deployment configuration.

D. Deploy a new version of the application using Cloud Functions: Cloud Functions are used for deploying serverless applications and running event-driven code. Changing the application's deployment platform is not the most appropriate course of action to diagnose issues. Instead, it's better to focus on analyzing the application's logs and solving the errors reported by users.

Solution to Question 21: A

The correct answer is A, and here's why:

Option A sets up ingress firewall rules, targeting the specific service accounts for each tier, which allows communication between the respective tiers on the correct TCP port 8080. This directly addresses the project requirements of enabling communication between tier #1 to tier #2, and tier #2 to tier #3 using TCP port 8080, making it the best solution.

Option B is incorrect because it uses egress firewall rules which control the outbound traffic from instances rather than inbound traffic (ingress). Furthermore, it uses IP ranges rather than service accounts, which is less specific and might involve unnecessary instances.

Option C is incorrect because it also uses egress firewall rules, targeting each service account of the respective tiers. This still doesn't address the project requirement correctly, as they need to allow inbound (ingress) traffic between tiers.

Option D is incorrect because it uses ingress firewall rules, targeting each service account, to enable communication between tiers, but it allows traffic on TCP port 80 instead of the required TCP port 8080. This does not match the project requirements.

In conclusion, the answer should be A because it creates the correct ingress firewall rules to allow communication between the required tiers on TCP port 8080 and specifies service accounts as the targets and source filters. Other options either use the wrong types of firewall rules, the wrong port, or do not target the required service accounts accurately.

Solution to Question 22: A

The correct answer is A. Cloud Spanner.

The reasoning for choosing Cloud Spanner is as follows:

1. Scalability: Cloud Spanner is designed for applications that require strong consistency, high availability, and horizontal scalability. It is particularly well-suited for large-scale transactional workloads. As the size of the user base is unknown and the company wants a solution that can easily accommodate user growth, Cloud Spanner provides automatic sharding and load balancing, allowing the system to scale seamlessly, with no downtime or manual intervention.
2. Relational Data: The company is looking for a storage solution for relational data, and Cloud Spanner is a fully managed relational database. It combines the benefits of a traditional relational database management system (RDBMS) with the flexibility and scalability of NoSQL databases, making it the perfect choice for this scenario.

Now, let us look at why other options will not work:

B. Cloud SQL: Although Cloud SQL is a fully managed relational database service for MySQL, PostgreSQL, and SQL Server, it has limitations in terms of scalability compared to Cloud Spanner. It is designed to handle small to medium-sized applications and does not provide automatic sharding or load balancing, which makes it less suitable for an application that needs to accommodate unknown user growth.

C. Cloud Storage: Cloud Storage is primarily for storing and retrieving unstructured static objects like images, videos, and text files rather than relational data. Although it is highly scalable, it does not provide the relational data structure and consistency required for the company's application.

D. Cloud Bigtable: Cloud Bigtable is a fully managed NoSQL database service that provides high throughput and low latency, making it ideal for big data applications involving analytics and machine learning. However, it is not designed specifically for relational data, and it does not offer the strong consistency guarantees that Cloud Spanner does. Since the company requires a storage solution for relational data, Cloud Bigtable would not be the best choice.

In summary, due to its seamless scalability, consistency, and ability to handle relational data, Cloud Spanner is the most appropriate storage solution for the company's requirements.

Solution to Question 23: C

The correct answer is C. The auditor's permissions should be configured by selecting the built-in IAM project Viewer role and adding the user's account to this role.

Here's why the other options will not work:

Option A: IAM Billing Account Viewer role with project-wide permissions

The Billing Account Viewer role provides access solely to billing information. Although the auditor would have read access to billing data, they would not have

read access to other essential resources and configurations within the project, making this option insufficient for the desired read-only auditor capabilities.

Option B: Custom role with view-only service permissions

Creating a custom role with view-only service permissions might seem like a feasible option, but it is not necessary or efficient. The built-in IAM project Viewer role (Option C) already provides all required read-only permissions without the need to create a separate custom role, making Option B less ideal and less manageable for the project.

Option D: IAM BigQuery Data Viewer role with project-wide permissions

The BigQuery Data Viewer role is designed specifically for viewing data in BigQuery tables and datasets. Assigning this role would only give the auditor read access to BigQuery data while excluding other necessary read access permissions across different resources and services in the project. Therefore, this option does not fulfill the requirement of read access to the entire project without modification capabilities.

In conclusion, Option C is the best way to configure the auditor's permissions in a Google Cloud Platform project, as it provides all the necessary read-only permissions without allowing the user to modify anything within the project.

Solution to Question 24: C

The correct answer is C: Grant the basic role roles/viewer and the predefined role roles/compute.admin to the DevOps group.

Explanation:

Option A is not the recommended approach because it involves creating an IAM policy that explicitly grants all compute.instanceAdmin.* permissions. This is not a best practice, as Google provides predefined roles with efficient permission management to meet such requirements.

Option B is also not recommended since granting the roles/editor to the DevOps group will provide them with access to create and update other resources, which is against the desired constraints of not having permission to create or update any other resources in the project.

Option C is the recommended action because it adheres to Google's best practices for permission management. Granting the basic role roles/viewer ensures that DevOps team members can view all the resources within the project, while granting the predefined role roles/compute.admin provides them with full control over Compute Engine resources, as required.

Option D is not advised because it involves creating a custom role at the project level, which is not necessary considering the predefined roles available. Additionally, granting all compute.instance.* permissions might not offer the full control over Compute Engine resources the DevOps team requires.

In conclusion, Option C is the most suitable approach because it follows Google's recommended practices and provides the DevOps team with the necessary permissions to manage Compute Engine resources without allowing them to create or update other resources in the project.

Solution to Question 25: A

The correct answer is A: Expose the application by using an external TCP Network Load Balancer.

Explanation for choosing A: An external TCP Network Load Balancer is the most appropriate choice for this scenario because the application requires preserving the IP address of the clients making requests. TCP Network Load Balancers are designed to handle TCP traffic, like the one required by the application on port 389, and they are able to preserve the clients' source IP addresses, which is required for this use case. Additionally, an external load balancer is needed to expose the application to the internet.

Reasons for not choosing other options:

B. Expose the application by using an external UDP Network Load Balancer: An external UDP Network Load Balancer is not the right choice for this scenario because the application requires handling TCP traffic on port 389, not UDP traffic. UDP Load Balancers are designed to handle UDP traffic, which is not suitable for the application.

C. Expose the application by using Google Cloud's Traffic Director: Google Cloud's Traffic Director is not a suitable option in this case because it is typically used for service-to-service load balancing and advanced traffic control capabilities. It does not support exposing applications directly to the internet or preserving clients' source IP addresses as required.

D. Expose the application by using an internal TCP Network Load Balancer: While an internal TCP Network Load Balancer does handle TCP traffic, it is not suitable for this use case, as it is designed for internal traffic within a Virtual Private Cloud (VPC) network. The application needs to be exposed to the internet, which requires an external load balancer instead.

Solution to Question 26: C

The most suitable solution in this situation is C. SSL Proxy Load Balancer, and here's why:

C. SSL Proxy Load Balancer is specifically designed to handle SSL-based traffic, such as HTTPS, on port 443. It terminates the SSL connection from clients, decrypts the traffic, and then forwards it to the appropriate backend service. By doing this, the SSL Proxy Load Balancer takes care of the encryption and decryption process, ensuring lower latency and improved performance for clients worldwide. It also supports global request distribution and cross-regional load balancing, further enhancing user experience and ensuring consistent performance across the globe.

A. Backend Services Load Balancer is not the best choice because, while it does distribute traffic among backend instances, it doesn't provide any SSL offloading. This means that the decryption process still takes place on backend servers, contributing to higher latency and lower performance for SSL-encrypted traffic.

B. NAT Gateway Load Balancer is not the suitable solution, as it is used to enable instances in a VPC to access the internet without exposing their private IP addresses. This type of load balancer doesn't focus on reducing latency for SSL-encrypted traffic but rather deals with managing network address translation (NAT) for instances in a virtual private cloud (VPC).

D. Cloud Armor Load Balancer is an incorrect option because Cloud Armor is a security service that protects applications from Distributed Denial of Service (DDoS) attacks and other web-based threats. While it provides enhanced security, it's not meant to reduce latency specifically for SSL-encrypted traffic.

In conclusion, option C, SSL Proxy Load Balancer, is the most suitable solution for reducing latency for SSL-encrypted TCP traffic on port 443 from clients worldwide in a global high-traffic application.

Solution to Question 27: B

The correct answer is B: Configure regional storage for the region closest to the users. Configure a Standard storage class.

Explanation:

As a data engineer working for a financial services company with a continuous analytics pipeline and users located in Boston, MA (United States), the primary requirement is to ensure optimal data storage that minimizes costs while maintaining performance and latency.

A: This option suggests configuring dual-regional storage, which indeed provides higher availability, but it can be more expensive compared to regional storage. Also, Nearline storage class is designed for infrequently accessed data and has higher retrieval costs, making it unsuitable for a continuous analytics pipeline that requires regular access to the files.

B: This is the optimal choice because configuring regional storage for the region closest to the users minimizes latency and provides adequate redundancy and availability. The Standard storage class offers low-latency access and high throughput, making it suitable for frequently accessed data, such as the analytics pipeline in this scenario.

C: Configuring dual-regional storage for the region furthest from the users increases latency, negatively affecting the performance. Moreover, the Archive storage class is designed for long-term archiving and incredibly infrequent access, making it unsuitable for a continuous analytics pipeline.

D: Multi-regional storage is designed for geo-redundancy and high availability

across large geographical distances. It is not necessary for users located in a specific area like Boston, MA, and tends to be more expensive. Nearline storage class, as mentioned earlier, is unsuitable for frequently accessed data due to its higher retrieval costs.

Therefore, the best option is B, which ensures optimal data storage with low latency, adequate redundancy, and cost-effectiveness for a continuous analytics pipeline and users located in Boston, MA (United States).

Solution to Question 28: B

The correct answer is B. Verify that you are Project Billing Manager for the GCP project. Create a new billing account and link the new billing account to the existing project. This is because, as a software engineer, you need to check if you have the appropriate permissions to manage the billing aspects of the GCP project. The Project Billing Manager role allows you to create and manage billing accounts that can be linked to the projects.

Option A is incorrect because the Billing Administrator role focuses on managing the billing account itself, and not the linkage between the billing account and the GCP project. The key role you need here is the Project Billing Manager role.

Option C is incorrect because this option states that you should update the existing project to link it to the existing billing account, which is not the task given. The task requires you to create a new billing account and link it to the existing GCP project.

Option D is incorrect because it suggests creating a new project, which is not required in the given task. The task requires linking a new billing account to an existing GCP project, not creating a new project altogether.

Solution to Question 29: C

The correct answer is C. Use Deployment Manager templates to describe the proposed changes and store them in Cloud Source Repositories.

Explanation:

Option A and B are incorrect because they involve applying the changes in a development environment and running 'gcloud compute instances list' to save the output. While applying changes and testing them in a development environment is essential, simply saving the output of the listed instances does not provide the team with enough context or information about the proposed changes. Moreover, it is not a recommended best practice from Google.

Option C is the correct answer because Deployment Manager templates are per Google's best practices for managing infrastructure as code. By using Deployment Manager templates, you can describe the proposed changes to your infrastructure in a consistent, structured, and version-controlled format. Storing these templates in Cloud Source Repositories guarantees a centralized and

accessible location for your team to review and collaborate on the proposed changes.

Option D is incorrect because, although it involves using Deployment Manager templates to describe the proposed changes, storing them in a Cloud Storage bucket is not the best practice. While it might be accessible, Cloud Storage does not offer the same version control, collaboration, and code review features as Cloud Source Repositories. It is essential to use a proper source control system to manage infrastructure changes to maintain the infrastructure's history and provide collaborative features.

Solution to Question 30: B

The correct answer is B. Create a managed instance group. Set the Autohealing health check to healthy (HTTP).

Explanation: Option B is the best choice because it requires the fewest steps while also providing a solution that supports autohealing for network load balancing and re-creation of unresponsive VMs. By creating a managed instance group, you can take advantage of Google Cloud's built-in load balancing capabilities and easily configure autohealing for Compute Engine instances.

Since VMs are in multiple zones, a managed instance group is ideal as it can span across multiple zones. Setting the Autohealing health check to healthy (HTTP) ensures that the VMs that become unresponsive after 3 attempts of 10 seconds each are re-created.

Option A is incorrect because it suggests turning off autohealing settings, which contradicts the requirement of configuring autohealing.

Option C is incorrect because it involves creating an HTTP load balancer, but this does not directly address autohealing. Although the load balancer includes health checks, creating a separate HTTP load balancer is an additional step that is not necessary when a managed instance group allows you to directly configure autohealing.

Option D is incorrect because it suggests using a Cloud VPN, which is unrelated to configuring autohealing for network load balancing. Cloud VPN is meant for connecting on-premises networks with Google Cloud, and does not provide autohealing functionality. Furthermore, setting the Autohealing health check to healthy (HTTP) relies on the existence of a managed instance group, which is not mentioned in this option.

Solution to Question 31: C

The correct answer is C because it is the most efficient and automated way to achieve the goal of notifying the support team when users experience high latency for at least 5 minutes. By creating an alert policy, you can set the specific threshold for HTTP response latency and ensure that notifications are sent automatically when the threshold is exceeded. This allows the support

team to take prompt action and maintains a proactive approach to addressing latency issues.

Option A is incorrect because Cloud Armor is primarily designed for protecting web applications against DDoS attacks and implementing security policies for incoming traffic. It does not provide the ability to monitor and alert on high latency events in Compute Engine instances.

Option B is incorrect because the Cloud Monitoring dashboard is more focused on providing real-time visualizations and metrics, but it does not automatically send notifications when a particular metric, like latency, crosses a specified threshold. The support team would need to continually monitor the dashboard to spot any issues, which is not an efficient use of their time and resources.

Option D is incorrect because exporting Cloud Monitoring metrics to Cloud Storage and using Data Studio to create a dashboard would involve additional complexity and time-consuming manual processes. Furthermore, this approach does not provide any automated notifications, which is a key requirement in this scenario. Instead, setting up an alert policy directly within Cloud Monitoring is a more straightforward and efficient solution.

Solution to Question 32: B

The most suitable solution to handle the given scenario is option B: Ingest the data into Cloud Bigtable and create a row key based on the event timestamp.

Explanation:

Cloud Bigtable is designed to handle a high throughput of data, making it an ideal option for storing and processing the vast amounts of data generated by sensors every few seconds. By creating a row key based on the event timestamp, you ensure that the data is stored atomically and can be retrieved with consistency based on the timestamp. This setup accommodates the high throughput expectations and guarantees atomic storage and retrieval of individual signals.

Why other options will not work:

A. Cloud Pub/Sub for streaming data and storing it in Cloud Firestore is not ideal for this scenario. While Cloud Pub/Sub ensures reliable messaging, Cloud Firestore is not designed to store or handle high volumes of sensor data with time-series data like event timestamps. Firestore is better suited for hierarchical and real-time data.

C. Creating a file in Google Sheets per device and appending new data in it is an inefficient solution. Google Sheets is not designed to handle high throughput data and is not capable of managing the large volumes of data generated by thousands of events per hour per device. Besides, Google Sheets would significantly limit the processing, querying, and scalability of such data.

D. Ingesting data into Datastore and storing it in an entity group based on the device is not the optimal solution. While Datastore provides a NoSQL database

for web and mobile applications, it is not designed for handling high throughput time-series data like sensor events. Additionally, using entity groups might lead to contention issues, and Datastore could potentially become a performance bottleneck in this use case. Bigtable is a better option when dealing with high-volume, high-throughput, and time-series data.

Solution to Question 33: A

The correct answer to this question is A. Deploy MongoDB Atlas from the Google Cloud Marketplace.

Here's why the other options don't work and why option A is the most appropriate choice:

Option A: Deploy MongoDB Atlas from the Google Cloud Marketplace This is the best choice because MongoDB Atlas is a managed MongoDB service provided by the company behind MongoDB. It offers a complete solution for deploying, managing, and scaling MongoDB clusters, with an established support SLA (Service Level Agreement). By deploying MongoDB Atlas from the Google Cloud Marketplace, you can seamlessly integrate it with your Google Kubernetes Engine (GKE) application, ensuring a reliable and scalable database system for your project.

Option B: Create a Cloud Dataproc cluster and use the MongoDB connector for Hadoop This option is not ideal because Cloud Dataproc is primarily for running Apache Hadoop and Apache Spark workloads in the Google Cloud Platform. While you can connect Cloud Dataproc to MongoDB using the connector for Hadoop, this setup does not provide a managed MongoDB environment specific for your GKE application, nor does it guarantee a support SLA for your database.

Option C: Use Cloud Datastore with the MongoDB API enabled Cloud Datastore is a highly scalable NoSQL database offered by Google Cloud Platform. Although it has some similarities with MongoDB in terms of data modeling and querying, Cloud Datastore is a separate database system that only offers a limited compatibility mode with the MongoDB API. Enabling the MongoDB API in Cloud Datastore doesn't provide you with a fully-featured, managed MongoDB environment, nor does it have a dedicated support SLA for MongoDB.

Option D: Deploy a MongoDB container on Cloud Functions and trigger it with an event This option is impractical because Cloud Functions is a serverless compute platform that deals with executing individual functions in response to events rather than being designed to host and manage standalone containerized applications like a database system. Deploying a MongoDB container using Cloud Functions would not provide the reliability, scalability, and support SLA required for your project's database system.

In conclusion, the best course of action in this situation is to deploy MongoDB Atlas from the Google Cloud Marketplace to provide a managed MongoDB environment with a support SLA for your Kubernetes Engine application.

Solution to Question 34: B

The correct answer is B: Deploy a private autopilot cluster.

Explanation: As a project manager, your priorities are to ensure node identity and integrity, as well as to prevent nodes from being accessible from the internet while minimizing operational costs and adhering to Google's best practices. A private autopilot cluster is the best choice for this scenario because it has the following features:

1. A private cluster ensures that nodes are not assigned public IP addresses, preventing them from being accessed directly from the internet. This fulfills your requirement of keeping the nodes not accessible from the internet.
2. Autopilot clusters automatically iterate and maintain the node infrastructure. They minimize cluster management activities and optimize hardware resources, consequently reducing operational costs.
3. Autopilot clusters support shielded nodes that provide verifiable node identity and integrity. This feature matches your requirement of having verifiable node identity and integrity.
4. Autopilot clusters are designed in line with Google's best practices for cluster management and security.

Incorrect Options:

A. Deploy a standard private cluster and enable workload identity: Although this option provides private access to nodes, it won't minimize operational costs and doesn't ensure optimum performance, which can be achieved by using an autopilot cluster.

C. Deploy a public App Engine cluster and enable shielded nodes: This option contradicts your requirement of keeping the nodes inaccessible from the internet since it involves a public cluster. Additionally, App Engine is a different service that doesn't offer Kubernetes clusters.

D. Deploy a public regional cluster and enable shielded nodes: Similarly to option C, choosing a public cluster would expose the nodes to the internet. This does not align with your goal of keeping the nodes inaccessible from the internet.

Solution to Question 35: D

The correct answer is D, "Provision Compute Engine instances with M1 machine type." Here's why:

The main requirement specified in the question is that the full database must be held in-memory for quick data access. This means that you need a solution with a high amount of memory to ensure optimal performance.

Option D meets this requirement, as the M1 machine type is designed for memory-intensive workloads, with much higher memory-to-CPU ratios compared to other machine types. Therefore, M1 machine type instances would

provide the necessary resources for holding the full database in-memory and ensuring fast data access for the ERP system.

Now let's analyze why the other options are not suitable:

A. Cloud Datastore provides a NoSQL database which is good for high read/write throughput. However, it is not designed to hold the full database in-memory and does not guarantee instant access to all data. Therefore, it does not meet the primary requirement.

B. Provisioning Compute Engine instances with local SSDs attached is a good solution for disk-based databases that require high I/O performance. However, it does not allow you to hold the full database in-memory, which is the key requirement for this use case.

C. Deploying the application on Kubernetes Engine with memory-optimized nodes will indeed provide a reasonable amount of memory. However, Kubernetes Engine is a container orchestration platform; it is not the same as a Compute Engine instance. If the application is not containerized and designed to run in a Kubernetes environment, this option would require significant changes to the application architecture, which may not be feasible or optimal for the ERP system.

In conclusion, the most suitable option for this scenario is D, "Provision Compute Engine instances with M1 machine type," as it is specifically designed for memory-intensive applications and would allow the full database to be held in-memory for quick data access as required.

Solution to Question 36: B

The correct answer is B. When creating the VM via the web console, specify the service account under the 'Identity and API Access' section.

Reason: Specifying the service account at the VM creation step ensures that the newly created Linux VM will use the specific service account with the required access permissions to connect to Cloud SQL. The 'Identity and API Access' section in the Google Cloud Platform (GCP) web console allows you to configure the service account for the VM instance during its creation.

Option A is not the best practice because modifying the VM's startup script to include the JSON Private Key would make the credentials file more vulnerable to potential security breaches. This method also involves extra configuration steps in the startup script, which can be avoided using the recommended method (option B).

Option C is not recommended because storing the JSON Private Key file on the VM instance after it is created and configuring its path might not be secure. Additionally, this option requires unnecessary manual steps, such as SSH into the VM and saving the JSON key in the specified location. Option B ensures that the service account is properly configured at the instance creation time.

Option D is incorrect because setting the service account as the default Compute Engine service account for the project using the gcloud CLI would apply that service account to all Compute Engine instances in the project. This is not desired as the question specifically states that the Linux VM must use the newly created service account, rather than the default Compute Engine service account. Option B allows you to configure the service account for a specific VM, ensuring the flexibility of different instances with different service account configurations.

Solution to Question 37: D

The correct answer is D. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

Here's why D is the right answer and why other options will not work:

A. Stream data to Pub/Sub, and use Cloud Functions to send data to BigQuery.

This option is incorrect because it involves using Cloud Functions, which is not suitable for handling large-scale data ingestion and processing. Cloud Functions are primarily focused on event-driven use-cases and do not provide guaranteed performance, which could lead to the data pipeline becoming a bottleneck. Additionally, BigQuery is designed for analyzing structured data, whereas the scenario involves both structured and unstructured data, making this an unsuitable choice.

B. Stream data to Dataflow, and use Storage Transfer Service to send data to BigQuery.

This option is incorrect because it includes using Storage Transfer Service, which is designed for transferring data between cloud storage buckets or from on-premises to the cloud, not for streaming data between processing services. Furthermore, similar to option A, BigQuery is not suitable for handling both structured and unstructured data.

C. Stream data to Dataflow, and use Dataproc to send data to Bigtable.

This option is incorrect because it uses multiple data processing components (Dataflow and Dataproc), which would add unnecessary complexity to the architecture. Additionally, Bigtable is designed for handling time-series and NoSQL data, not necessarily the best fit for diverse IoT data storage.

D. Stream data to Pub/Sub, and use Dataflow to send data to Cloud Storage.

This option is correct because it follows Google's recommended architecture for a highly available and resilient data pipeline for IoT data processing. By using Pub/Sub, you can handle the continuous influx of structured and unstructured data, while ensuring reliable data ingestion. Dataflow is then used for processing and transforming the data, leveraging its autoscaling and fault-tolerant capabilities. Lastly, Cloud Storage is an ideal choice for storing structured

and unstructured data due to its cost-effectiveness, scalability, and durability, providing a robust data lake for the IoT application.

Solution to Question 38: A

The correct answer is A: Create an export to the sink that saves logs from Cloud Audit to a Coldline Storage bucket.

Explanation:

Option A is the most cost-effective and appropriate solution for retaining audit log files for three years. Coldline Storage is one of Google Cloud's storage classes and is designed specifically for infrequent access and long-term storage, which makes it perfect for storing audit log files for an extended period of time. By creating an export sink, you can easily save logs from Cloud Audit directly to a Coldline Storage bucket. This enables the company to retain these important files in a cost-efficient manner, while also fulfilling the 3-year retention requirement.

Option B: Utilizing Cloud Functions to trigger on new log entries and store them in Cloud Spanner is not the best option for this task. Cloud Spanner is a fully managed, mission-critical relational database service designed for high-performance transactions and strong consistency. It is more expensive and not specifically intended for long-term storage of infrequently accessed data like audit logs.

Option C: Creating an export to the sink that saves logs from Cloud Audit to Firebase Realtime Database is not advisable. Firebase Realtime Database is a NoSQL database built for real-time, high-frequency data updates and synchronization, not for long-term storage of infrequently accessed log files. Additionally, using this service for long-term log storage would incur unnecessary costs.

Option D: Implementing a Cloud Run service that streams logs from Cloud Audit to Cloud Storage Nearline is also not ideal. While Cloud Storage Nearline is designed for infrequent access and slightly longer retention periods than other storage classes, it has a minimum storage duration of 30 days. Coldline Storage, with a minimum storage duration of 90 days, is a more cost-effective and suitable storage class for retaining logs for three years.

In conclusion, Option A ensures cost-effective retention of audit log files by saving them in a Coldline Storage bucket specifically designed for infrequent access and long-term storage. The other options either propose expensive solutions, do not cater to the specific storage requirements, or go against the intended purpose of the storage services.

Solution to Question 39: C

The correct answer is C. Here's why:

Option A is incorrect because only creating a configuration file for each account

and using the –configuration flag is not enough to manage different accounts with different regions/zones effectively.

Option B is incorrect because it only specifies the zone and region flags when creating instances but does not manage different Google Cloud Platform accounts.

Option C is the correct answer. Creating two configurations using "gcloud config configurations create [NAME]" allows you to manage different accounts and their respective configurations separately. Running "gcloud config configurations activate [NAME]" before starting the Compute Engine instances helps switch between different accounts as needed, addressing the requirements of both clients.

Option D is incorrect because manually creating separate shell scripts to manage different accounts is an inefficient process and does not take advantage of gcloud's built-in ability to handle multiple configurations.

Solution to Question 40: D

The correct answer is D, and here is the explanation as to why it is the best choice and why the other options will not work:

Option A: Creating a Data Fusion pipeline to transfer medical images from the on-premises storage to Cloud Storage on a scheduled interval is not the right choice because Data Fusion is designed to process and transform structured and semi-structured data rather than efficiently transferring large binary files such as medical images. Additionally, Data Fusion is an expensive service that is more suitable for complex data integration tasks than simple file transfers.

Option B: Creating a Pub/Sub topic and enabling a Cloud Storage trigger for the Pub/Sub topic by creating an application to send all medical images to the Pub/Sub topic is not appropriate. Pub/Sub is intended for handling relatively smaller messages, not for transferring large binary files like medical images. Moreover, using Pub/Sub will not ensure efficiency and cost-effectiveness when transferring such large files.

Option C: Deploying a Dataflow job from the batch template, "Datastore to Cloud Storage", and scheduling the batch job on the desired interval is not suitable for the given scenario. First, the batch template is designed for importing/exporting Datastore entities, not for transferring large binary files. Second, Dataflow is a more expensive solution when compared to a simple data transfer method using scripts.

Option D (Correct): Creating a script that uses the gsutil command-line interface to synchronize the on-premises storage with Cloud Storage, and scheduling the script as a cron job, is the best solution for this use case. The gsutil tool is specifically designed for transferring and synchronizing files between the local file system and Cloud Storage. Besides, it can handle large binary files efficiently and offers an affordable solution to securely transferring these files to the cloud.

Moreover, scheduling the script as a cron job provides an automated process that satisfies the clinic's requirement.

Solution to Question 41: B

The correct option is B. Install and configure the Cloud Logging Agent and view the logs from Cloud Logging. The reason is that, by default, Google Cloud's Compute Engine instances do not automatically send logs to Cloud Logging. By installing and configuring the Cloud Logging Agent, you can enable log shipping from your application to Cloud Logging. This will allow you to easily view, search, and analyze the logs to diagnose and resolve the reported errors.

Option A is incorrect because merely navigating to Cloud Logging doesn't enable log shipping from the Compute Engine instance to Cloud Logging. The logs will not be available there unless the Cloud Logging Agent is installed and configured.

Option C is incorrect because configuring Cloud Pub/Sub to receive logs is an unnecessary and overly complex way to handle logs for a single application. Cloud Logging is the more appropriate service for log analysis and management in this scenario, especially since it provides built-in tools for log querying and alerting.

Option D is incorrect because a Health Check with a Low Healthy Threshold value would be used for monitoring the health of instances and potentially restarting unhealthy instances. It does not provide the means to diagnose and resolve application errors, which is the primary goal in this scenario. Health checks are used for automated service remediation, but they do not provide the required insight into log data to uncover the cause of the errors reported by users.

Solution to Question 42: C

The correct option is C: Use Cloud Logging filters to create log-based metrics for firewall and instance actions. Monitor the changes and set up reasonable alerts.

Explanation:

Option C addresses the main concerns of monitoring unanticipated firewall changes and instance creation while also being a simple solution. Cloud Logging filters allow you to specifically target log entries related to firewall and instance actions. By creating log-based metrics based on these filtered logs, you can effectively monitor and set up alerts to be informed about any unexpected changes in real-time.

Option A is incorrect because simply turning on Google Cloud firewall rules logging will only provide you with raw log data of all activity, and setting up alerts for any insert, update, or delete events may result in too many alerts, as not every event will be indicative of an issue.

Option B is incorrect because Cloud Identity-Aware Proxy (IAP) focuses on securing user access to applications, not monitoring for unanticipated firewall changes and instance creation. While IAP is useful for securing application access, it does not directly provide the desired monitoring and alerting capabilities for this specific scenario.

Option D is incorrect because it introduces unnecessary complexity by incorporating Grafana for custom monitoring dashboards. While Grafana is useful for creating elaborate dashboards, the scenario specifically asks for a simple solution to monitor firewall changes and instance creation. Moreover, integrating Grafana with Google Cloud Monitor will require additional setup that may not directly address the specific requirements of monitoring unanticipated firewall changes and instance creation.

Solution to Question 43: D

The correct answer should be D, and here's an explanation for why it's the best choice and why the other options wouldn't work:

Option A: Decreasing the initial delay of the HTTP health check to 10 seconds will not solve the problem. In fact, it could even make the situation worse. Since it takes about three minutes for the Virtual Machine instances to become available for users, having a shorter health check delay would cause the autoscaler to consider the new instances unhealthy because they haven't started yet. Therefore, it would add more instances than necessary.

Option B: Configuring autoscaling based on memory utilization instead of CPU utilization will not resolve the issue because the problem here is not related to the metric used for autoscaling; rather, it's related to the initial delay of the HTTP health check. The issue occurs because the health check is not delayed long enough for the instances to become available before autoscaler starts adding more instances.

Option C: Increasing the instance group's maximum limit to 10 also does not address the problem. This might temporarily alleviate the issue by preventing the group from hitting the maximum limit quickly, but it does not address the root cause of the problem: the initial delay of the HTTP health check.

Option D: Increasing the initial delay of the HTTP health check to 200 seconds (which is the correct answer and action) will allow the instances enough time to become available for users before the health check is done. This ensures that autoscaler does not add unnecessary instances. By giving the instances enough time to become fully functional, the instance group can maintain a more appropriate size and reduce any excessive scaling.

In conclusion, the best solution for properly maintaining the instance group sizes when autoscaling is to increase the initial delay of the HTTP health check to 200 seconds. This will give the instances enough time to become available before the health check is performed, helping prevent the addition of unnecessary instances and maintain a proper instance group size.

Solution to Question 44: A

The correct answer to this question is Option A: Cold Storage.

Reasoning:

A. Cold Storage: Cold Storage, often known as Nearline or Coldline storage in various cloud platforms, is designed specifically for data that is infrequently accessed, making it the ideal and cost-efficient option for a company that only needs to access its archived data quarterly. This storage class offers lower storage costs while still providing the required data durability and reliability needed for regulatory compliance.

B. Durable Reduced Availability Storage: While this option might offer lower costs, it sacrifices data durability and availability, making it unsuitable for a financial services company that has strict regulatory requirements. This option is more appropriate for use cases where the loss or unavailability of data is acceptable.

C. Datastore: Datastore is a NoSQL database that is designed for scalable, fully managed applications. It is not intended as a storage solution for archival purposes, especially when the company needs specific access and regulatory requirements to be fulfilled.

D. Partner Interconnect: Partner Interconnect refers to a high-speed, private connection between your on-premises data center and a cloud provider's network. This option is irrelevant for the company's archival storage needs since it deals with the connectivity between two locations and not the actual storage solution itself.

In conclusion, Cold Storage (Option A) is the most suitable and cost-efficient storage solution for the company's quarterly accessed data warehouse in accordance with the regulatory requirements. Options B, C, and D are either unsuitable for regulatory compliance, not designed for archival storage, or irrelevant to the actual storage needs of the company.

Solution to Question 45: C

The correct answer should be C: Using the GCP Console, filter the Activity log to view the information. This is because Google Cloud Platform's Activity log is specifically designed to record and store actions performed by users, such as the addition of metadata labels and file access in Cloud Storage buckets. Filtering the Activity log by the specific user will help you quickly verify the actions they have taken, fulfilling the requirement with the fewest possible steps.

The other options are not suitable for the following reasons:

A. Create a trace in Stackdriver to view the information: Stackdriver is now known as Cloud Operations, and Stackdriver Trace (or Cloud Trace) is a performance profiling tool primarily used to analyze latency in applications rather

than verifying user actions in Cloud Storage buckets. Thus, it does not meet the requirement.

B. Enable and configure Google Cloud Armor to view the logs: Google Cloud Armor is a security service that provides protection against Distributed Denial of Service (DDoS) and web attacks. It is not designed for monitoring or verifying user actions in Cloud Storage buckets and, therefore, does not meet the requirement.

D. Create a trace in Cloud Monitoring to view the information: As mentioned earlier, Tracing is a performance profiling tool, which is a part of Cloud Monitoring (formerly Stackdriver). Cloud Monitoring is usually used to track resource usage and uptime for applications, not for verifying user actions in Cloud Storage buckets. Therefore, this option does not meet the requirement.

Solution to Question 46: A

Answer A. Create a budget per project and configure budget alerts on all of these budgets. is the correct course of action. In this scenario, each developer has a personal sandbox environment which is an individual Google Cloud Project. Creating a budget for each project and configuring a budget alert at the $500 threshold ensures that you'll be notified if any developer exceeds this amount in monthly spending in their sandbox projects.

Option B. Configure Google Cloud billing notification with a spending threshold of $500 per month on the Organization level. is not optimal. It will not provide individual project spending limits; rather, it would track spending on the organization level, i.e., it will trigger when the total spending across all projects reaches $500 per month. It doesn't ensure separate spending limits for each sandbox.

Option C. Use Cloud Pub/Sub to notify you when developers are creating new resources in their sandbox projects. is not applicable in this situation. Although Cloud Pub/Sub can be used to notify you of new resources being created, it doesn't help in tracking the costs or spending of each project. This option will not allow you to set a spending limit for each sandbox environment.

Option D. Use Deployment Manager to track each sandbox project's resource usage and notify you when the cost reaches $500. is not suitable for this case. Deployment Manager is primarily used for creating and managing resources based on templates. It would require significant customizations and development effort to create a solution for tracking costs and sending notifications whenever the $500 limit is reached in each sandbox project. It is easier and more efficient to set up and manage budget alerts in the Google Cloud Console.

Solution to Question 47: B

The correct answer is B. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image. Here's why:

A. Upload the image to Container Registry and create a Kubernetes Service referencing the image. - This option is not correct because although Google Container Registry can store Docker images, Google now recommends using Artifact Registry for managing container images. Kubernetes Service alone is also not sufficient for deploying workloads, as Services are mainly for load balancing and handling network traffic.

B. Upload the image to Artifact Registry and create a Kubernetes Deployment referencing the image. - This is the correct answer because Artifact Registry is the recommended solution for storing and managing container images in Google Cloud. A Kubernetes Deployment is used to create and manage instances of a containerized application, while maintaining the desired number of replicas and automatically rolling out updates. This combination of Artifact Registry and Deployment is the right approach for deploying a Docker image as a workload on Google Kubernetes Engine.

C. Upload the image to Cloud Storage and create a Kubernetes DaemonSet referencing the image. - This option is not correct because Cloud Storage is primarily used for storing unstructured data like videos, images, or documents rather than container images. Furthermore, DaemonSets are for creating a single pod on each node in a cluster, which is useful for system level tasks, not for deploying regular application workloads that require scaling and rolling updates.

D. Upload the image to Artifact Registry and create a Kubernetes Service referencing the image. - This option is not correct because, although Artifact Registry is recommended for storing container images, Kubernetes Service alone does not deploy workloads. Its main purpose is to provide load balancing and network traffic management. A Kubernetes Deployment is needed to work alongside the defined Service for managing instances of the containerized application.

Solution to Question 48: C

The correct answer is C. Here's why:

Option A is not suitable because although verifying your Organization Administrator IAM role is an important step, assigning quotas and manually calculating billing based on resource usage is not an efficient way to ensure that the Marketing department is billed solely for their Google Cloud services. Furthermore, it can be prone to errors and delays.

Option B is partially correct, as you need to verify that you are assigned the Billing Administrator IAM role. However, creating a new project and setting labels for all services in the project will not guarantee that the Marketing department is billed solely for their Google Cloud services. Labels can help with filtering and reporting, but they will not segregate the billing by themselves.

Option C is the best approach because it ensures that you are assigned the Billing Administrator IAM role for the Marketing department's Google Cloud Project, which allows you to make changes to the billing settings. By linking

the new project to a Marketing Billing Account, you can be certain that the Marketing department will be billed solely for their Google Cloud services in this project. This keeps billing separate and manageable.

Option D is not suitable because having just the Billing Viewer IAM role will only allow you to view the billing information without the ability to modify it. Moreover, manually monitoring usage and invoicing the Marketing department at the end of each month is inefficient, error-prone, and not scalable.

Solution to Question 49: B

The optimal choice for creating a custom VPC with a single subnet and the largest possible IP address range is option B: 10.0.0.0/8.

Option B provides the widest range of available IP addresses due to the subnet mask /8. With /8, there are 24 bits available for hosts which results in 2^24 - 2 = 16,777,214 possible IP addresses. The 10.0.0.0/8 range is from 10.0.0.0 to 10.255.255.255, allowing a large number of hosts within the subnet. This range is a part of private IP addresses, and it is suitable for a company's internal network.

Option A: 203.0.113.0/24 has a subnet mask of /24 which leaves only 8 bits for hosts, resulting in 2^8 - 2 = 254 available IP addresses. The range is smaller and it's also a public IP block, meaning it's unsuitable for a private network.

Option C: 192.168.1.0/24 is a widely used private IP address range with a subnet mask of /24, allowing only 254 available IP addresses. Although it's private, the small range doesn't fit the requirement for the largest possible range.

Option D: 10.1.0.0/16 gives an address range of 10.1.0.0 to 10.1.255.255, with a subnet mask of /16, which leaves 16 bits for hosts. This results in 2^16 - 2 = 65,534 available IP addresses. Although it's a private IP address range and suits the network requirements, it's smaller than the /8 address range, making it a suboptimal choice.

To sum up, option B: 10.0.0.0/8 provides the largest possible IP address range from the given choices and is suitable for a private network. Therefore, it's the best option for a network administrator tasked with creating a custom VPC with a single subnet catering to the largest possible range.

Solution to Question 50: C

The correct answer is C. Ask the partner to create a Service Account in their project, and grant their Service Account access to the BigQuery dataset in your project.

Explanation:

In this scenario, your primary goal is to provide the marketing agency with access to the BigQuery dataset in your project. This enables the marketing agency to implement their recommendation engine using data from your data warehouse. Since the marketing agency is running their application on Google

Cloud and managing resources in their own project, it makes sense for them to create a Service Account in their project, which can then be granted the necessary access to the BigQuery dataset in your project. This ensures that only the marketing agency's application has access to the dataset, while maintaining a clear separation of responsibilities between the two projects.

Option A is incorrect because it suggests creating a Service Account in your own project and granting it access to Cloud Storage. This is not relevant to providing access to a BigQuery dataset, and it does not involve granting access to the marketing agency's application.

Option B is incorrect because it asks the partner to create a Service Account in their project, but then grants the Service Account access to Compute Engine in their project. This does not provide the necessary access to your BigQuery dataset for the marketing agency to implement their recommendation engine.

Option D is incorrect because it proposes creating a Service Account in your own project and granting access to BigQuery within your project. While this may grant access to the BigQuery dataset, it does not provide the necessary access control to the marketing agency's applications, potentially compromising security and ownership boundaries.

Practice Exam 19

Question 1: As a software engineer at a multinational company, you have been tasked with developing a globally distributed application using Cloud Spanner for data storage. In order to start setting up the Cloud Spanner instance, what is the first step you should take?

A. Create a new VPC network with subnetworks in all desired regions.

B. Set up Bigtable as the primary storage for the distributed application.

C. Enable the Cloud Datastore API for the project.

D. Enable the Cloud Spanner API.

Question 2: As a financial analyst at a tech company, you have developed a solution on Google Cloud incorporating numerous Google Cloud products. Your supervisor has requested that you calculate the projected monthly cost of implementing this solution. How should you proceed to deliver an accurate estimate?

A. Use only free tier resources in your solution and do not calculate any costs as it will be free.

B. Provision the solution on Google Cloud. Leave the solution provisioned for 1 week. Use Cloud Monitoring to determine the provisioned and used resource amounts. Multiply the 1 week cost to determine the monthly costs.

C. Visit pricing forums or community groups and ask other users to estimate the cost of your solution without using the pricing calculator.

D. For each Google Cloud product in the solution, review the pricing details on the products pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

Question 3: You work as a cloud engineer for a company where a team of data scientists occasionally requires access to a Google Kubernetes Engine (GKE) cluster that you manage. They need to utilize GPUs for certain long-running, non-restartable tasks. Your task is to minimize cost during this process. What approach should you take?

A. Manually add and remove GPU-enabled instances to the GKE cluster as needed.

B. Enable node auto-provisioning on the GKE cluster.

C. Create a node pool with regular VMs and GPUs attached to those VMs.

D. Launch GKE cluster in a shared VPC configuration for better resource management.

Question 4: As a software engineer in a tech company, you encounter an issue where your continuous integration and delivery (CI/CD) server is unable to

execute Google Cloud actions in a specific project due to permission issues. To ensure that the used service account has the right roles for the specific project, what should be your next course of action?

A. Verify if the billing account associated with the project is in good standing.

B. Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

C. Check the firewall settings in the VPC network configuration to ensure proper access.

D. Check if the needed API is enabled for the specific project in the Google Cloud console.

Question 5: You are working as a Cloud Engineer in a major software development company and have recently created a new project in Google Cloud using the gcloud command line interface (CLI) and linked a billing account. Now, you need to create a new Compute Engine instance for this project using the CLI. What prerequisite step should you perform to achieve this?

A. Enable the cloudresourcemanager.googleapis.com API.

B. Enable the compute.googleapis.com API.

C. Create a Cloud Run service in the project.

D. Create a Cloud Storage bucket in the project.

Question 6: As an IT administrator at a software company, you have two subnets (subnet-a and subnet-b) in the default VPC. The database servers run in subnet-a, while the application servers and web servers run in subnet-b. You are required to set up a firewall rule that only allows database traffic from the application servers to the database servers. What should be your best course of action?

A. Create service accounts sa-app and sa-db. • Associate service account sa-db with the application servers and the service account sa-app with the database servers. • Create an egress firewall rule to allow network traffic from source service account sa-db to target service account sa-app.

B. • Create service accounts sa-app and sa-db. • Associate service account sa-app with the application servers and the service account sa-db with the database servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

C. Create a network tags app-server and db-server. • Add the app-server tag to the database servers and the db-server tag to the application servers. • Create an egress firewall rule to allow network traffic from source network tag app-server to target network tag db-server.

D. Create a service account sa-app and a network tag app-server. • Add the service account sa-app to the application servers and the network tag app-server to the database servers. • Create an ingress firewall rule to allow network traffic from source VPC IP addresses and target the subnet-b IP addresses.

Question 7: You work for a software development company that has an application running on Compute Engine VM instances in a custom Virtual Private Cloud (VPC). Due to the company's security policies, only internal IP addresses are permitted on VM instances, and VM instances are not allowed to connect to the internet. You must ensure that the application can access a file hosted in a Cloud Storage bucket within your project. What action should you take?

A. Enable Private Google Access on the subnet within the custom VPC.

B. Deploy a Cloud NAT instance and route the traffic to the dedicated IP address of the Cloud Storage bucket.

C. Use Cloud Datastore instead of Cloud Storage, and enable Datastore Private Access.

D. Add storage.googleapis.com to the list of restricted services in a VPC Service Controls perimeter and add your project to the list of protected projects.

Question 8: As an IT specialist at a leading software company, you need to set up a single caching HTTP reverse proxy on GCP for a latency-sensitive client's website. The specific reverse proxy you're using consumes minimal CPU. You require a 30-GB in-memory cache and an additional 2 GB of memory for other processes. Your goal is to minimize cost while fulfilling these requirements. What's the most suitable approach to run this reverse proxy?

A. Create a Cloud Filestore with 32 GB of storage, and use it as the cache for the reverse proxy.

B. Run it on Compute Engine, and choose a custom instance type with 6 vCPUs and 32 GB of memory.

C. Deploy the reverse proxy on a Compute Engine instance with the instance type e2-highmem-16.

D. Create a Cloud Memorystore for Redis instance with 32-GB capacity.

Question 9: As a financial analyst in a tech company, you have created several resources across multiple Google Cloud projects for various departments. Each project is linked to a different billing account. In order to efficiently predict future expenses and present a comprehensive visualization of all costs to your team, you need to consolidate and include new cost data as quickly as possible. What should be your approach in this situation?

A. Create custom metrics for billing and track costs using Cloud Monitoring dashboards on a per-project basis.

B. Fill all resources in the Pricing Calculator to get an estimate of the monthly cost.

C. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

D. Set up a Google Sheets-based billing dashboard for each billing account and combine them manually.

Question 10: You are working as a developer in a software company, and you have been tasked with creating a code snippet that should run automatically whenever a new file is uploaded to a Cloud Storage bucket within the company's infrastructure. How should you deploy this code snippet to achieve this requirement?

A. Use Cloud Composer and configure a DAG to trigger the application using Pub/Sub.

B. Use Firebase Cloud Messaging and configure the bucket as a trigger resource.

C. Use Cloud Functions and configure the bucket as a trigger resource.

D. Use Cloud Run and configure the bucket as an event source using Cloud Pub/Sub.

Question 11: You are a cloud specialist working for a media company. The company requires you to establish a policy so that videos residing in a specific Cloud Storage Regional bucket are automatically transferred to Coldline after 90 days, and ultimately deleted after one year from their creation date. How should you configure the policy?

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

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

C. Use Google Data Studio to visualize the Age of objects in the bucket and manually apply the SetStorageClass and Delete actions accordingly.

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

Question 12: As a software engineer in a technology company, you developed an application that uses Cloud Spanner as a backend database in your firm's architecture. The application experiences very predictable traffic patterns, and you need to automate the process of scaling the number of Spanner nodes according to the traffic volume. What would be your approach to achieve this?

A. Configure Cloud Spanner to use Network Endpoints for automatic scaling based on traffic.

B. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

C. Create a Cloud Monitoring alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly.

D. Use Firebase Realtime Database instead of Cloud Spanner and enable automatic scaling with Cloud Functions for Firebase.

Question 13: As an IT professional working in a prominent e-commerce company, you need to update a web application that's currently deployed as a managed instance group, while also ensuring that it receives live web traffic without decreasing its available capacity. The application requires gradual deployment of a new version. What would be the best approach to achieve this?

A. Use Google Cloud Build to push the new app version to all instances in the managed instance group simultaneously.

B. Create a new instance template with the new application version. Update the existing managed instance group with the new instance template. Delete the instances in the managed instance group to allow the managed instance group to recreate the instance using the new instance template.

C. Perform a rolling-action start-update with maxSurge set to 0 and maxUnavailable set to 0.

D. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

Question 14: As a software developer in a reputable tech company, you have been tasked with deploying new features to an existing Cloud Run service in production. To ensure minimal risks and adhere to Google-recommended practices, you need a strategy that limits the number of affected customers in case of an outage, without adding any development or operational costs to them. What is the best approach to achieve this goal?

A. Deploy the new revision without any traffic allocation, and manually shift traffic when you're confident in the new revision's performance.

B. Gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

C. Deploy your application to a second Cloud Run service, and ask your customers to use the second Cloud Run service.

D. Send all customer traffic to the new revision, and roll back to a previous revision if you witness any problems in production.

Question 15: You are working as an IT specialist for a company operating in the healthcare industry, and your organization's infrastructure is on-premises with all machines running at maximum capacity. You've decided to burst to Google Cloud to tackle this issue, but it's crucial to ensure that the workloads on Google Cloud can directly communicate with the on-premises workloads using a private IP range. What should be your next course of action?

A. In Google Cloud, configure the VPC for VPC Network Peering.

B. In Google Cloud, configure the VPC for VPN tunneling using public IP addresses.

C. Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses.

D. Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Question 16: As a data engineer at a growing tech company, you have a Dataproc cluster running in a single Virtual Private Cloud (VPC) network within a single subnet that has a range of 172.16.20.128/25. Unfortunately, there are no private IP addresses available in the VPC network, and you need to add new VMs to communicate with your cluster using the least amount of steps. What action should you take?

A. Create a new GCP project with an additional VPC network and set up Shared VPC for the Dataproc cluster.

B. Create a new VPC network for the VMs. Enable VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network.

C. Increase the subnet's quota by submitting a request to GCP Support.

D. Add VMs with public IP addresses in the existing VPC network and configure firewall rules to allow communication between VMs and rest of the VPC.

Question 17: You are working as a data engineer in a tech company that specializes in processing time-series data. You've been tasked with constructing a pipeline using Google Cloud Platform services. Which combination of services should you use for the designated stages 1, 2, 3, and 4 in your pipeline?

A. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery

B. Cloud Pub/Sub, Cloud Dataflow, Cloud Spanner, Cloud Storage

C. Firebase Messages, Cloud Pub/Sub, Cloud Spanner, BigQuery

D. Cloud Pub/Sub, Cloud Dataproc, Cloud Storage, BigQuery

Question 18: As a software engineer in a company that heavily utilizes cloud services, you need to configure permissions for several Compute Engine instances, allowing them to write data into a specific Cloud Storage bucket while adhering to Google's recommended best practices. What is the most appropriate course of action to achieve this?

A. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/compute.read'

B. Create a service account and add it to the IAM role 'compute.admin' for that bucket.

C. Create a service account with an access scope. Use the access scope 'https://www.googleapis.com/auth/cloudkms'

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

Question 19: You are working with a technology company that has deployed an application on a Compute Engine instance. As a part of maintenance, an external consultant needs to access the Linux-based instance. The consultant has a VPN connection to your corporate network, but they don't have a Google account. What should be done in this situation?

A. Instruct the external consultant to generate an SSH key pair, and request the public key from the consultant. Add the public key to the instance yourself, and have the consultant access the instance through SSH with their private key.

B. Instruct the external consultant to use the gcloud compute ssh command line tool by using Identity-Aware Proxy to access the instance.

C. Instruct the external consultant to use Google Cloud SDK with their own Google account to access the instance.

D. Use Google Cloud IAM to create a temporary service account and provide the consultant with the JSON key file to access the instance.

Question 20: As a Cloud Administrator at a software company, you're responsible for hosting an application on a Compute Engine instance in a shared project with multiple teams. To ensure that other teams don't accidentally cause downtime on the application, which feature should you utilize?

A. Configure a firewall rule for the instance

B. Enable deletion protection on the instance.

C. Implement instance tags and labels

D. Enable autoscaling for the instance

Question 21: As a security analyst at a leading software company, it is crucial for you to grant a member of your security team visibility into vulnerabilities and other OS metadata for a specific Compute Engine instance that hosts a mission-critical application in your Google Cloud project. In order to successfully implement the security vulnerability management policy according to your company's requirements, what approach should you take?

A. Provide the security team member with roles/compute.instanceAdmin permission.

B. Use Cloud Data Loss Prevention (DLP) to scan the Compute Engine instance for vulnerabilities.

C. Create an organization policy to restrict access to specific Compute Engine instances.

D. • Ensure that the OS Config agent is installed on the Compute Engine instance. • Provide the security team member roles/osconfig.vulnerabilityReportViewer permission.

Question 22: As a software engineer at a major tech company, you are designing an application that will run in your organization's data center. The application will utilize Google Cloud Platform (GCP) services, such as AutoML. A service account with appropriate access to AutoML has been created for you. How can you enable authentication to the APIs from your on-premises environment?

A. Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.

B. Use gcloud to create a key file for the service account that has appropriate permissions.

C. Create a separate project for the on-premises application and use its default service account for authentication

D. Use OAuth 2.0 authentication code flow for on-premises application

Question 23: As a database administrator at a tech company, you have set up an instance of SQL Server 2017 on Compute Engine to explore its features for potential implementation within the company. Your goal is to connect to this instance in the most efficient way possible. What step should you follow?

A. Enable Windows authentication in the GCP Console. Verify that a firewall rule for port 3389 exists. Click the RDP button in the GCP Console and select "Connect using Windows Authentication".

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

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

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

Question 24: You are working as a cloud architect for a fintech company, and your team is responsible for deploying a single binary application on the Google Cloud Platform. To comply with company policies, you must use virtual machines directly and focus on operational efficiency and quick completion of

application scaling based on underlying infrastructure CPU usage. What should you do to achieve automatic scaling for the application?

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

B. Use Google App Engine flexible environment to deploy the application and configure dynamic scaling based on CPU usage.

C. Configure Google Cloud Run to automatically scale the application based on CPU usage.

D. Use Cloud Pub/Sub to create a subscription that triggers VM creation or deletion based on CPU usage.

Question 25: As a software engineer in a rapidly growing e-commerce company, you've been tasked with developing a backend service to handle and store transaction data from various mobile and web clients. The company anticipates a significant volume of worldwide transactions upon launching the platform. In addition, the business team will need to run SQL queries for data analysis purposes. How can you create a highly available and scalable data store to accommodate these requirements?

A. Migrate transaction data to Bigtable and run SQL queries using Apache Beam.

B. Create a multi-region Cloud Spanner instance with an optimized schema.

C. Create a multi-region Cloud SQL for PostgreSQL database with optimized indexes.

D. Create a multi-region Cloud SQL for MySQL database with no read replicas.

Question 26: As a cloud engineer working for a tech company, you receive a notification that your company's managed instance group has raised an alert due to the failure of new instance creation. To resolve the instance creation issue, what action should you take?

A. Create an instance template that contains valid syntax and add it to an existing instance group. Increase the instance count to generate new instances.

B. Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names.

C. Check the permissions of the service account being used by the instance group. Verify that the instance name and persistent disk name values are not the same in the template.

D. Verify that the instance template being used by the instance group contains valid syntax. Delete any persistent disks with the same name as instance names. Set the disks.autoDelete property to true in the instance template.

Question 27: Working at a software development company, you are tasked with building a web application that will be deployed on Google Cloud Platform. To ensure smooth updates, you want to test new releases on a small portion of real user traffic while directing the majority of users towards the stable version. What approach should you take for this process?

A. Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

B. Deploy the application on Kubernetes Engine and use a StatefulSet for each update. Configure traffic splitting through a Kubernetes Ingress to direct a small percentage of traffic to the new StatefulSet.

C. Deploy the application on Compute Engine. For each update, create a new instance template. Configure traffic splitting between instance groups using a load balancer.

D. Deploy the application on Kubernetes Engine. For a new release, update the deployment to use the new version.

Question 28: You're working as a Cloud Architect for a software development company that has decided to transition from an on-premises environment to Google Cloud. Your company has multiple development teams that rely on Cassandra environments for their backend databases, and each team needs an isolated development space within Google Cloud. Your goal is to ensure a swift and efficient migration with minimal technical support effort required. What should you do?

A. 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

B. 1. Use Cloud Firestore and create collections for each development team. 2. Configure security rules to isolate each team's access to their collections.

C. 1. Set up a Cloud Dataproc cluster and install Cassandra on it. 2. Configure the cluster for each development team to access their own isolated environment.

D. 1. Use Cloud Datastore as a replacement for Cassandra. 2. Set up separate projects for each development team to isolate their data.

Question 29: As a software engineer at a multinational company, you've developed an App Engine application within a Google Cloud Platform project for expanding your company's presence in the Asian market. Initially, the application was configured to be served from the us-central region. Now, your team decides to serve the application from the asia-northeast1 region instead. How should you proceed to achieve this?

A. Update the app.yaml file in the existing App Engine application to specify asia-northeast1 as the region, then redeploy the application.

B. Apply a forwarding rule in Google Cloud Load Balancer to redirect traffic from us-central to asia-northeast1 for the existing App Engine application.

C. Change the region property setting in the existing App Engine application from us-central to asia-northeast1.

D. Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application.

Question 30: As a network administrator in a growing technology company, you need to establish reliable VPN connectivity between a new VPC and a remote site. The connectivity must include dynamic routing, a shared address space of 10.19.0.1/22, and no overprovisioning of tunnels during a failover event. To set up a highly available Cloud VPN following Google-recommended practices, what should you do?

A. Use an automatic mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

B. Use a custom mode VPC network, use Cloud Router static routes, and use active/passive routing.

C. Use a custom mode VPC network, configure static routes, and use active/passive routing.

D. Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

Question 31: You are working as a system administrator at a tech company and need to confirm that a Google Cloud Platform service account was created at a specific time for auditing purposes. What should you do?

A. Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

B. Filter the Activity log to view the Data Access category. Filter the Resource type to Service Account.

C. Filter the Error Reporting logs to view the Configuration category. Filter the Resource type to Service Account.

D. Filter the Activity log to view the Configuration category. Filter the Resource type to Storage Bucket.

Question 32: You are working as a data architect at a leading tech company and have been tasked with migrating the company's on-premises data to Google Cloud. The company's data includes:

• 200 TB of video files in SAN storage • Data warehouse data stored on Amazon Redshift • 20 GB of PNG files stored in an S3 bucket

Your goal is to load the video files into a Cloud Storage bucket, transfer the data warehouse data into BigQuery, and load the PNG files into a second Cloud

Storage bucket. You are expected to follow Google-recommended practices and avoid writing any code for the migration. How should you proceed?

A. Use Storage Transfer Service for the video files, Dataproc for the data warehouse data, and Storage Transfer Service for the PNG files.

B. Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

C. Use Dataproc for the video files, BigQuery Data Transfer Service for the data warehouse data, and Cloud Pub/Sub for the PNG files.

D. Use Dataflow for the video files, Cloud Data Fusion for the data warehouse data, and Transfer Appliance for the PNG files.

Question 33: As a software engineer at a fintech company, you have developed a crucial application that will be used by the entire organization. It's essential to deploy this application on Kubernetes with maximum reliability. In order to provision a Kubernetes cluster and ensure adherence to Google-recommended practices, what action should be taken?

A. Create a GKE Autopilot cluster. Enroll the cluster in the preview release channel.

B. Create a GKE Autopilot cluster without enrolling in any specific release channel.

C. Create a regional GKE standard cluster. Enroll the cluster in the no-channel release setting.

D. Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

Question 34: As a DevOps engineer at a software development company, you are tasked with setting up a new Jenkins server for your team's project as quickly and efficiently as possible. What is the best approach you should take?

A. Deploy Jenkins as an API Gateway with an API key.

B. Use Firebase Hosting to deploy the Jenkins application.

C. Use GCP Marketplace to launch the Jenkins solution.

D. Try deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service.

Question 35: You are working in a software development company that operates a web application on Cloud Run for hundreds of clients. Some clients report that the initial web page of the application takes significantly longer to load compared to the following pages. In order to address this issue while adhering to Google's recommendations, what action should you take?

A. Change the Cloud Run memory allocation to a larger value.

B. Change the region for the Cloud Run service.

C. Update your web application to use the protocol HTTP/2 instead of HTTP/1.1.

D. Set the minimum number of instances for your Cloud Run service to 3.

Question 36: As an IT manager in a software development company, you recently found out that your development team is using numerous service account keys during their development process. To enforce short-lived service account credentials within the company while working on a long-term solution, you need to implement a Google-recommended process that meets these requirements:

• All service accounts that require a key should be created in a centralized project called pj-sa. • Service account keys should only be valid for one day.

Considering these requirements and your goal to minimize costs, what is the best approach to take?

A. Implement a Cloud Run job to purge all service account keys periodically. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours with an exception on pj-sa.

B. Use a custom App Engine task runner to rotate service account keys every day. Enforce an org policy to allow service account key creation with no exceptions across all projects.

C. Implement a Kubernetes CronJob to rotate all service account keys periodically. Disable attachment of service accounts to resources in all projects with an exception to pj-sa.

D. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

Question 37: As a developer at a rapidly growing software company, you're responsible for managing multiple Google Cloud projects efficiently. In order to make it easier for you to manage these projects using the Google Cloud SDK command line interface (CLI), what steps should you take?

A. 1. Use the default configuration for one project you need to manage. 2. Use gcloud init to update the configuration values when you need to work with a non-default project.

B. 1. Use a single configuration for all projects you need to manage. 2. Utilize labels and filters to differentiate between projects while managing resources.

C. 1. Create Google Cloud Storage buckets for each project you need to manage. 2. Use gcloud storage commands to manage and switch between the different projects.

D. 1. Create a configuration for each project you need to manage. 2. Activate the appropriate configuration when you work with each of your assigned Google Cloud projects.

Question 38: As a Google Cloud Platform (GCP) administrator in a multinational company, you're responsible for handling multiple projects and need to access all logs from the past 60 days across these projects. Your task is to efficiently explore and analyze the log contents, adhering to Google's recommended practices for obtaining combined logs. What should you do?

A. Create a Stackdriver Logging Export with a Sink destination to Cloud Storage. Create a lifecycle rule to delete objects after 60 days.

B. Configure a Cloud Scheduler job to read from Stackdriver and store the logs in BigQuery. Configure the table expiration to 60 days.

C. Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

D. Use Stackdriver Logging Viewer to export logs to Cloud SQL and set the retention policy for log data to 60 days.

Question 39: As a data analyst at a major tech company, you have been requested by the internal audit team to provide insight into the organization's use of data in Google Cloud, specifically focusing on which team members accessed data in Cloud Storage buckets. What is the most effective method to assist the auditors in obtaining the necessary information?

A. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage.

B. Assign the Data Loss Prevention API roles to the auditor for them to inspect the data.

C. Turn on Cloud Asset Inventory for the organization to track asset metadata.

D. Configure a Cloud Pub/Sub topic to stream logs related to Cloud Storage access.

Question 40: As a cloud administrator for a software company, you have recently been assigned to maintain a Google Cloud Platform project. To ensure maximum security, you want to review the list of users with the Project Owner role. What is the recommended course of action?

A. Use the command gcloud projects get-iam-policy to view the current role assignments.

B. Enable Stackdriver Monitoring for the project and review the logs for role changes.

C. Go to the IAM & admin page in the console and review the Service Accounts permissions.

D. Go to the Firebase Console and check the Authentication section for users who have been granted the Project Owner role.

Question 41: As a software engineer in a tech company, you have been tasked with setting up a Windows VM on Compute Engine for a new project. To ensure seamless remote access to the VM via RDP, what step should you take after the VM has been created?

A. After the VM has been created, download the JSON private key for the default Compute Engine service account. Use the credentials in the JSON file to log in to the VM.

B. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

C. When creating the VM, add metadata to the instance using 'windows-password' as the key and a password as the value.

D. After the VM has been created, use gcloud compute ssh to retrieve the login credentials for the VM.

Question 42: As a developer working in a tech company that uses multiple gcloud configurations, you need to efficiently examine the configured Kubernetes Engine cluster of an inactive configuration. What is the best method to accomplish this?

A. Use gcloud config set project and gcloud config get-value project to review the output.

B. Use gcloud config set compute/zone and gcloud config set compute/region to review the output.

C. Use kubectl get nodes to review the output.

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

Question 43: As an IT expert working for a cloud-based company, you need to use Deployment Manager to create a Google Kubernetes Engine cluster. Alongside this, you must create a DaemonSet in the kube-system namespace of the cluster using the same Deployment Manager deployment. Your solution should utilize the least number of services. What is the most efficient approach to achieve this?

A. Use the Deployment Manager Runtime Configurator to create a new Config resource that contains the DaemonSet definition.

B. Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

C. Add a Kubernetes ClusterRoleBinding in the Deployment Manager configuration that grants access to the kube-system namespace and references the DaemonSet in its rules.

D. Use the Deployment Manager to create a Cloud Build trigger which, when activated, deploys the DaemonSet to the kube-system namespace as part of the build process.

Question 44: As an IT specialist in a multinational company, you've been assigned a project involving a single Virtual Private Cloud (VPC) and a single subnetwork in the us-central1 region, where a Compute Engine instance is hosting an application. Your task is to deploy a new instance in the same project in the europe-west1 region, which requires access to the application. To ensure you adhere to Google-recommended practices, what steps should you take?

A. Use Google App Engine to deploy the new instance in europe-west1 and configure it to access the existing Compute Engine application in the us-central1 region.

B. Create a VPC and a subnetwork in europe-west1. Configure VPC peering between the two VPCs. Create the new instance in the new subnetwork and use the first instance's public address as the endpoint.

C. 1. Create a subnetwork in the same VPC, in europe-west1. 2. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

D. Use a third-party VPN solution to connect the existing subnetwork to a subnetwork in europe-west1. Create the new instance in the new subnetwork and use the first instance's private address as the endpoint.

Question 45: As a software engineer in a leading ecommerce company, you are tasked with transitioning your team's on-premises ecommerce application to a serverless Google Cloud solution. The application consists of a complex set of Python-based microservices running on Docker containers, with configurations managed using environment variables. How should you approach deploying your current application to the serverless Google Cloud solution?

A. Migrate the code to App Engine Standard Environment and deploy each microservice as separate services. Update the configurations and the required endpoints.

B. Use your existing continuous integration and delivery (CI/CD) pipeline. Use the generated Docker images and deploy them to Cloud Function. Use the same configuration as on-premises.

C. Use your existing CI/CD pipeline. Use the generated Docker images and deploy them to Cloud Run. Update the configurations and the required endpoints.

D. Use the existing CI/CD pipeline. Use the generated Docker images and deploy them to Compute Engine instances. Use the same configuration as on-premises.

Question 46: As an IT specialist at a software development company, you are in charge of configuring service accounts for an application that involves multiple projects. Your task is to grant access for Virtual machines (VMs) in the web-applications project to BigQuery datasets in the crm-databases project,

adhering to Google-recommended practices. How should you grant access to the service account in the web-applications project?

A. Grant "project owner" role to crm-databases and the web-applications project.

B. Grant "project owner" role to crm-databases and roles/bigquery.dataViewer role to web-applications.

C. Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

D. Grant "project owner" for web-applications appropriate roles to crm-databases.

Question 47: As a project manager in a tech company, you need to provide access to the billing report for your projects to the finance team without granting them extra permissions to the project. What is the appropriate action to take?

A. Add the group for the finance team to roles/billing viewer role.

B. Add the group for the finance team to roles/compute.viewer role.

C. Add the group for the finance team to roles/bigquery user role.

D. Add the group for the finance team to roles/container admin role.

Question 48: As a data analyst at a marketing company, you use Looker Studio to visualize a table from your company's data warehouse built on BigQuery. Data is appended throughout the day, and a daily summary is recalculated at night by overwriting the table. You've just noticed that the charts in Looker Studio aren't displaying correctly, and you need to investigate the issue. What step should you take to analyze the problem?

A. Verify Cloud Dataflow pipeline for any data ingesting issues in the Google Cloud platform.

B. Use the open source CLI tool, Snapshot Debugger, to find out why the data was not refreshed correctly.

C. Contact the Looker Studio support team for assistance in resolving the issue.

D. Use the BigQuery interface to review the nightly job and look for any errors.

Question 49: As a cloud engineer at a software development company, you are responsible for managing a fault-tolerant batch workload running every night on numerous virtual machines (VMs). However, the current cost of VMs has become a concern. What should you do to find a more cost-effective solution without compromising the workload's efficiency?

A. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs.

B. Run a test using App Engine Flexible environment. If the test is successful, migrate the workload to App Engine Flexible environment.

C. Run a test using simulated maintenance events. If the test is successful, use N2 Standard VMs when running future jobs.

D. Run a test using a managed instance group. If the test is successful, use N2 Standard VMs in the managed instance group when running future jobs.

Question 50: As a member of the IT department in a large corporation, your company relies on Active Directory for user identity management. In order to maintain control over Google accounts used by employees for all Google services, including Google Cloud Platform (GCP) organization, the company wants to utilize Active Directory as the source of truth for identities. What is the recommended course of action?

A. Create user accounts manually in Cloud Identity for each employee and assign them roles.

B. Ask each employee to create a Google account using self signup. Require that each employee use their company email address and password.

C. Set up a VPN connection between your on-premises network and GCP, then use Active Directory Domain Services in GCP to manage user accounts.

D. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

Practice Exam 19 Solutions

Solution to Question 1: D

The correct answer is D, "Enable the Cloud Spanner API."

Explanation: As a software engineer tasked with developing a globally distributed application using Google Cloud Spanner, the first step you should take is to enable the Cloud Spanner API. This is because Cloud Spanner is a fully managed relational database service built for global consistency and horizontal scalability. Enabling the API allows you to interact with the service and set up the necessary instances, databases, and tables for your application.

Why other options will not work:

A. "Create a new VPC network with subnetworks in all desired regions." While setting up a proper VPC network is important for implementing a globally distributed application, it is not the first step you should take. Before configuring the network, you need to enable the Cloud Spanner API to start using the desired database service.

B. "Set up Bigtable as the primary storage for the distributed application." Bigtable is not the correct storage method when using Cloud Spanner for data storage. Google Cloud Bigtable is a NoSQL database designed for low-latency, high-throughput data on a large scale, while Cloud Spanner is a fully managed relational database service optimized for global consistency and horizontal scalability. You should focus on enabling the Cloud Spanner API to implement the desired globally distributed application.

C. "Enable the Cloud Datastore API for the project." Enabling the Cloud Datastore API is not the right choice for this scenario, as it is not directly related to Cloud Spanner. Cloud Datastore is a highly scalable, fully managed NoSQL database designed for web and mobile applications, while Cloud Spanner is a fully managed relational database service designed for global consistency and horizontal scalability. Enabling the Cloud Spanner API is the correct first step in setting up the distributed application with the desired data storage.

Solution to Question 2: D

The correct answer is D. For each Google Cloud product in the solution, review the pricing details on the product's pricing page. Use the pricing calculator to total the monthly costs for each Google Cloud product.

Here's why D is the correct answer and why other options will not work:

Option A: Using only free tier resources in your solution would be unwise as Google Cloud resources are designed to accommodate varying needs and workloads. Depending on the scope, complexity, and needs of your solution, relying only on free tier resources could lead to insufficient infrastructure, performance issues, and limited features. Moreover, it would not provide your supervisor with an accurate cost projection for implementing the solution.

Option B: Provisioning the solution on Google Cloud and monitoring resource usage for just one week to estimate monthly costs is not a reliable method. Costs and resource consumption can vary significantly in different weeks or days, causing you to either underestimate or overestimate the actual costs. Also, leaving the solution provisioned for only one week is a short timeframe which may not capture variations in usage patterns and is not a full representation of monthly costs.

Option C: Visiting pricing forums or community groups and asking other users for cost estimates without using the pricing calculator is not a reliable, accurate, or professional method for estimating the monthly cost of implementing your solution. There are many factors that influence the cost of deploying a solution on Google Cloud, and different users may have different assumptions and experiences. The best source of information for calculating monthly costs accurately is the Google Cloud Pricing Calculator.

Option D (Correct Answer): For each Google Cloud product in the solution, it is crucial to review the pricing details on the product's pricing page to understand the cost structure, discounts, and special considerations. Then, use the Google Cloud Pricing Calculator, which is a built-in tool designed specifically for generating accurate cost estimates based on your solution's requirements and resource usage. This method directly applies the pricing information from Google Cloud and provides a comprehensive and reliable estimation of monthly costs to your supervisor, helping them make informed decisions about implementing the solution.

Solution to Question 3: B

The best approach in this scenario is to enable node auto-provisioning on the GKE cluster (Option B). The reason behind this choice is that node auto-provisioning automatically configures, adds or removes nodes based on actual load and requirements. By doing so, it optimizes resource usage and can minimize costs by using only the amount of resources needed at a given time. This also helps avoid under-provisioning or over-provisioning, which could negatively impact cost management. GPU-enabled instances are generated when required and removed when not in use, ensuring efficient use of resources.

Option A, manually adding and removing GPU-enabled instances on the GKE cluster, is not efficient as it would require human intervention. This increases the risk of delays and decreases flexibility, especially when the data scientists require access to GPUs on short notice or at irregular intervals. Moreover, manual management can lead to the inefficient use of resources and higher costs.

Option C, creating a node pool with regular VMs and GPUs attached to those VMs, would not be the best approach in this case. The reason being that GPUs attached to VMs will increase the cost and complexity of the solution. In addition, since the tasks to be executed are long-running and non-restartable, having them run on node pools could risk losing progress if something happens to the node or VM.

Option D, launching a GKE cluster in a shared VPC configuration for better resource management, might improve resource sharing between projects, but it would not directly help minimize cost during the process of utilizing GPUs for the specific tasks mentioned. Node auto-provisioning (Option B) would be more efficient in ensuring resource optimization and cost minimization in this particular scenario.

Hence, the ideal approach to minimize cost during the process of GPU usage in a GKE cluster would be to enable node auto-provisioning (Option B).

Solution to Question 4: B

The correct answer is B, and here's why:

Option B: Open the Google Cloud console, and check the Identity and Access Management (IAM) roles assigned to the service account at the project or inherited from the folder or organization levels.

This is the right course of action because permission issues are directly associated with the roles assigned to service accounts. By checking the roles assigned to the service account at the project, folder, or organization levels in the Google Cloud console, you can verify whether the service account has the necessary permissions to execute the CI/CD actions in the specific project. If the required roles are missing, you can fix the issue by adding the appropriate roles to the service account.

Reasons why other options will not work:

Option A: Verify if the billing account associated with the project is in good standing. While having a valid billing account is essential, it doesn't directly impact the permissions assigned to service accounts. The billing status might affect the functioning of some Google Cloud services, but it will not solve the permission issues you are experiencing.

Option C: Check the firewall settings in the VPC network configuration to ensure proper access. Firewall settings in the VPC network configuration are related to network access and traffic control rather than service account permissions. Although it's crucial to have proper firewall rules for your infrastructure, it won't solve the permission issues related to the CI/CD server and Google Cloud actions in the project.

Option D: Check if the needed API is enabled for the specific project in the Google Cloud console. APIs need to be enabled for your project to utilize specific Google Cloud services. However, your question relates to permission issues for a service account, which is not directly tied to API availability. Enabling a relevant API without proper roles assigned to the service account will not resolve your issue.

Solution to Question 5: B

The correct answer is B, Enable the compute.googleapis.com API, because it is

the API responsible for managing the Google Compute Engine resources within your Google Cloud project. It is required to have the Compute Engine API enabled before you can create, modify, or manage Compute Engine instances within the project.

Here is an explanation for why the other options will not work:

A. Enabling the cloudresourcemanager.googleapis.com API will not help in this case, because this API is related to managing Google Cloud resources and components such as projects, organizations, and folders. However, it doesn't specifically deal with Compute Engine instances and is not a prerequisite for creating one.

C. Creating a Cloud Run service in the project is not related to creating a new Compute Engine instance in the project. Cloud Run is a managed compute platform that enables you to run stateless containers and is suitable for microservices or event-driven workloads, while Compute Engine instances are Virtual Machines (VMs) that run on the Google Cloud infrastructure.

D. Creating a Cloud Storage bucket in the project is unrelated to creating a Compute Engine instance. Cloud Storage is designed for storing static objects like images, videos, or text files, while a Compute Engine instance is a VM-based resource that can be used for a variety of computing tasks, such as running applications, hosting web servers, or analyzing data.

Thus, option B is the appropriate prerequisite step for creating a new Compute Engine instance using the gcloud CLI in this situation.

Solution to Question 6: B

The correct answer is B, and here's why:

B. • Create service accounts sa-app and sa-db. • Associate service account sa-app with the application servers and the service account sa-db with the database servers. • Create an ingress firewall rule to allow network traffic from source service account sa-app to target service account sa-db.

This method allows for an efficient and clear configuration where the roles of the instances are specifically defined by service accounts. By creating an ingress firewall rule, we allow connections initiated by the application servers to be accepted by the database servers. This is the desired behavior as we want to ensure that only application servers can communicate with the database servers.

The other options are not suitable for the following reasons:

A. This option is incorrect because it creates an egress rule instead of an ingress rule. This rule will allow traffic leaving the application servers but does not ensure the database servers will accept the incoming connection.

B. This option is incorrect because it uses network tags instead of service accounts for defining the roles, which might lead to an unclear configuration.

Also, it creates an egress rule instead of an ingress rule, leaving open the receipt of traffic for the targeted instances.

C. This choice is incorrect because it mixes configuration elements (service accounts and network tags), making the setup less clear and difficult to maintain. Additionally, the ingress firewall rule uses VPC IP addresses as the source and targets subnet-b IP addresses, which might include web servers as well, resulting in an overly permissive configuration.

In conclusion, the best course of action is option B, which sets up clear configurations and follows the desired behavior of allowing only database traffic from the application servers to the database servers.

Solution to Question 7: A

The correct answer is A: Enable Private Google Access on the subnet within the custom VPC.

Explanation for A: Private Google Access allows VM instances with internal IP addresses to connect to various Google APIs and services, including Cloud Storage. This addresses your security policy requirements by only granting access to internal IP addresses and not allowing VM instances to connect to the internet. Hence, enabling this feature on the subnet within the custom VPC would allow your application to access the required files in the Cloud Storage bucket.

B is incorrect because deploying a Cloud NAT instance would provide VM instances with access to the internet. As per the company's security policies, VM instances cannot connect to the internet. Additionally, routing traffic to the dedicated IP address of the Cloud Storage bucket would require an external IP address, which is also not allowed by the security policy.

C is incorrect because using Cloud Datastore instead of Cloud Storage does not address the requirement to access a file in a Cloud Storage bucket. Cloud Datastore is a NoSQL database service for web and mobile applications and is not built for file storage, making it an incompatible solution for this scenario.

D is incorrect because adding storage.googleapis.com to the list of restricted services in a VPC Service Controls perimeter would further restrict access to Cloud Storage, while adding the project to the list of protected projects would only permit access to the restricted services within the project. The goal is to allow internal IP addresses to connect to the Cloud Storage bucket, which cannot be fulfilled by these actions.

Solution to Question 8: D

The most suitable approach to run this reverse proxy is option D: Create a Cloud Memorystore for Redis instance with 32-GB capacity.

Explanation: Option D is the best choice because it offers the necessary 30-GB in-memory cache and an additional 2 GB of memory for other processes, which

fulfill your project requirements. Cloud Memorystore for Redis is designed to provide fast and scalable in-memory caching, which is ideal for caching needs, especially for a latency-sensitive client's website. Additionally, it helps minimize costs while offering a fully managed Redis service without the need for manual configuration or maintenance. Redis is a popular caching solution, and using Cloud Memorystore ensures that you have a reliable and secure in-memory caching service.

Why other options will not work:

Option A: Creating a Cloud Filestore with 32 GB of storage is an inadequate choice for this case because Cloud Filestore is a managed file storage solution that is primarily meant for file sharing between instances and applications, not for caching HTTP reverse proxies. Also, it relies on disk storage, which will not provide the required low-latency caching capability compared to an in-memory cache like Redis.

Option B: Running the reverse proxy on a Compute Engine custom instance type with 6 vCPUs and 32 GB of memory seems like an option that "technically" fulfills the project's requirements. However, it increases management overhead and could incur higher costs than necessary for this particular use case. Since the reverse proxy consumes minimal CPU, using 6 vCPUs might result in underutilization of the allocated resources, which is not cost-effective. Moreover, Compute Engine instances require manual setup and management compared to a fully managed service like Cloud Memorystore for Redis.

Option C: Deploying the reverse proxy on a Compute Engine instance with the instance type e2-highmem-16 is not an optimal choice. This instance type is focused on high memory utilization workloads and may be overkill for the required 32-GB memory. Additionally, this instance type also has 16 vCPUs, which again could lead to underutilization of CPU resources and increased costs since the reverse proxy uses minimal CPU. Similar to Option B, using Compute Engine increases management overhead compared to a fully managed service like Cloud Memorystore for Redis.

In conclusion, Option D is the most suitable approach for your specific use case as it provides a managed in-memory caching solution tailored to your requirements while minimizing management overhead and costs.

Solution to Question 9: C

The correct answer is C. Configure Billing Data Export to BigQuery and visualize the data in Data Studio.

Here's why:

Option C allows you to efficiently consolidate the cost data across all your projects and billing accounts in a single place, BigQuery. BigQuery is a highly-scalable, serverless data warehouse solution that can handle large amounts of

data quickly. Furthermore, by using Data Studio, you can create dynamic, real-time visualizations of the data, making it easier to predict future expenses and present a comprehensive view of all costs to your team.

Option A, creating custom metrics for billing and tracking costs on a per-project basis, is not the best approach because it involves manually monitoring each project's dashboard. This can be time-consuming and might not give you a comprehensive view of the costs across all projects.

Option B, using the Pricing Calculator to get an estimate of the monthly cost, is not suitable because it requires manually inputting resource data for each project and only provides static estimations, while you need a dynamic solution to include new cost data quickly. Moreover, it's not possible to predict future expenses through such calculations.

Option D, setting up a Google Sheets-based billing dashboard for each billing account and combining them manually, may be a time-consuming and error-prone process, especially when there are several resources to manage. This approach is also not ideal for consolidating real-time data efficiently.

In summary, configuring Billing Data Export to BigQuery and visualizing the data in Data Studio (Option C) is the most efficient approach to handle the given situation as it offers a consolidated, real-time, and dynamic view of cost data from multiple Google Cloud projects. This enables you to effectively predict future expenses and present an easily understandable representation to your team.

Solution to Question 10: C

The correct answer is C. Use Cloud Functions and configure the bucket as a trigger resource. Cloud Functions is the ideal solution here because it is specifically designed for event-driven functionality and running small pieces of code in response to specific events. By configuring the Cloud Storage bucket as a trigger resource, you ensure that the code snippet will automatically run every time a new file is uploaded to the bucket.

Reasons for incorrect options:

A. Cloud Composer is mainly used for creating, scheduling, and orchestrating complex pipelines and workflows. It is not the best solution for a simple event-driven task, like running a code snippet in response to a file upload in a Cloud Storage bucket. Additionally, using a DAG (Directed Acyclic Graph) to trigger the application would make the solution overly complex for the given requirement.

B. Firebase Cloud Messaging is a messaging service primarily used for sending notifications and messages to users' devices, and it is not designed for executing code snippets or listening to events in Cloud Storage. Therefore, it is not an appropriate solution for this requirement.

D. Cloud Run is a serverless platform used for deploying and running containerized applications. Though it can be triggered by events in Pub/Sub, the primary use case for Cloud Run focuses on deploying and scaling web applications, rather than executing single-function code snippets in response to specific events. Cloud Functions is a more suitable solution for this requirement considering its ease-of-use, simplicity, and event-driven nature.

Solution to Question 11: D

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

Here's why:

Option A suggests using Age conditions with SetStorageClass and SetDeleted actions. However, there is no SetDeleted action available in Cloud Storage Object Lifecycle Management. The correct action is 'Delete'.

Option B uses CreationDate conditions instead of Age conditions. This approach is not suitable because the policy should be based on the age of objects, not their creation date, in order to apply the required actions after 90 days and 365 days.

Option C is not a suitable choice because it involves manual intervention and would not be practical in an automated and scalable solution. Google Data Studio is a reporting and visualization tool, and it is not designed to manage storage lifecycle policies.

Option D is the best choice for the following reasons: 1. It uses the Age conditions, which is the proper condition to apply actions based on the age of objects in the bucket. 2. It uses the SetStorageClass action for transferring objects to Coldline storage after 90 days. 3. It uses the Delete action for deleting objects after 365 days from their creation date. 4. This approach allows for a fully automated policy management without the need for manual intervention.

Solution to Question 12: B

The correct answer is B. Create a Cloud Monitoring alerting policy to send an alert to webhook when Cloud Spanner CPU is over or under your threshold. Create a Cloud Function that listens to HTTP and resizes Spanner resources accordingly.

Explanation:

Option B offers an automated solution for scaling Cloud Spanner according to the traffic volume, using Cloud Monitoring and Cloud Functions. By creating an alerting policy that sends an alert when the Cloud Spanner CPU exceeds or falls below a specified threshold, you ensure that the system reacts to changes in the traffic volume. Connecting this alert with a Cloud Function that listens

to HTTP and resizes Spanner resources accordingly will automate the scaling process. This solution aligns with the requirements of the question.

Why other options will not work:

A. Configure Cloud Spanner to use Network Endpoints for automatic scaling based on traffic: Cloud Spanner does not support automatic scaling using Network Endpoints. Network Endpoints are typically connected to Virtual Private Cloud (VPC) networks and are not designed for controlling and scaling Cloud Spanner resources.

C. Create a Cloud Monitoring alerting policy to send an alert to oncall SRE emails when Cloud Spanner CPU exceeds the threshold. SREs would scale resources up or down accordingly: While this option involves proactive monitoring, it relies on manual intervention by SREs to scale resources, which is not an automated solution as required in the question.

D. Use Firebase Realtime Database instead of Cloud Spanner and enable automatic scaling with Cloud Functions for Firebase: This option suggests changing the backend database and using Firebase Realtime Database, which is not mentioned in the question. Cloud Spanner is specifically mentioned as the backend database, and the question's objective is to find a solution to scale Cloud Spanner based on traffic volume, not to change the underlying database technology.

Solution to Question 13: D

The correct answer is D. Perform a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0.

Explanation:

Option A is incorrect because updating all instances simultaneously can lead to downtime, as the web application would not be available for users during the update process. This approach does not maintain the required availability and capacity.

Option B is not ideal because deleting the instances in the managed instance group before they are recreated using the new instance template poses the risk of decreasing the group's available capacity. This method does not sufficiently support a gradual deployment process or allow for live traffic without decreasing capacity.

Option C is incorrect because setting both maxSurge and maxUnavailable to 0 means that no extra instances will be created to maintain capacity during the update process, and no instances will be allowed to be unavailable during the update. This configuration will not result in any update at all.

Option D, performing a rolling-action start-update with maxSurge set to 1 and maxUnavailable set to 0, is the best approach. This method ensures a gradual rollout of the new version of the web application without compromising its capacity or availability to users. With maxSurge set to 1, an extra instance is

created during the update, helping to maintain overall capacity. With maxUnavailable set to 0, the process ensures that no instances will be unavailable during the update, providing uninterrupted service to live web traffic.

Solution to Question 14: B

The best approach to achieve this goal is option B, which is to gradually roll out the new revision and split customer traffic between the revisions to allow rollback in case a problem occurs.

This option ensures minimal risks by distributing the traffic between both the old and new revisions, giving you the ability to monitor and evaluate the new revision's performance with a smaller group of users. If any issues arise, you can quickly roll back to the previous stable version without impacting all users. This approach also adheres to Google's recommended practices for deploying changes in a production environment.

Option A requires manual traffic shifting, which increases the risk of human error and does not allow for the same level of monitoring and easy rollback as option B.

Option C is inefficient because it requires deploying to a second Cloud Run service and asking customers to use it. This solution could incur additional costs and burden for customers, which would contradict the goal of not adding any development or operational costs to them.

Option D is risky because it directs all customer traffic to the new revision without any evaluation or gradual rollout, potentially causing a large-scale failure if there are problems with the new revision. Rolling back immediately after detecting issues may still result in many customers being affected and could harm the company's reputation.

By choosing option B, you can ensure minimal risks and adhere to Google-recommended practices while limiting the number of affected customers in case of an outage, without adding any development or operational costs to them.

Solution to Question 15: D

The correct answer is D: Set up Cloud VPN between the infrastructure on-premises and Google Cloud.

Explanation: The main objective is to enable communication between the on-premises workloads and the Google Cloud workloads using a private IP range. The other options do not fulfill this requirement:

A. In Google Cloud, configure the VPC for VPC Network Peering: Network Peering is suitable for connecting VPC networks within Google Cloud or in other cloud providers. It does not support connecting to on-premises infrastructure using a private IP range.

B. In Google Cloud, configure the VPC for VPN tunneling using public IP addresses: This option does not use private IP ranges for communication be-

tween on-premises and Google Cloud workloads as the question requires. VPN tunneling using public IPs exposes data transmission to the public Internet.

C. Create bastion hosts both in your on-premises environment and on Google Cloud. Configure both as proxy servers using their public IP addresses: This option also doesn't use private IP ranges for communication. Bastion hosts are used for remote management and access control, not for privately connecting workloads across different environments.

Given the requirement to establish a secure and direct connection between on-premises and Google Cloud workloads using private IP ranges, option D is the best choice. Setting up Cloud VPN creates a secure connection between the two environments, allowing workloads to communicate with each other using private IP addresses. This approach meets the requirements of the healthcare industry, which typically has strict rules for privacy and security.

Solution to Question 16: B

The correct answer is B. Here is the explanation:

B. Creating a new VPC network for the VMs and enabling VPC Peering between the VMs' VPC network and the Dataproc cluster VPC network is the best option, as it allows the VMs and the Dataproc cluster to communicate with each other with minimal configuration and no need to use public IP addresses or create unnecessary resources.

A. Creating a new GCP project with an additional VPC network and setting up Shared VPC for the Dataproc cluster might work, but it involves a more complex configuration and additional management overhead. It is not the least amount of steps compared to VPC Peering (option B).

C. Increasing the subnet's quota by submitting a request to GCP Support will not work in this case, because the issue is about IP address availability within the VPC network, not about quota limits. Increasing quota won't create more IP addresses within the subnet range.

D. Adding VMs with public IP addresses in the existing VPC network and configuring firewall rules would technically allow communication between the VMs and the rest of the VPC. However, this is not recommended due to the additional security risks associated with using public IP addresses, and it still would not address the underlying issue of limited private IP addresses in the VPC network. Also, this option involves more steps than VPC Peering (option B).

Solution to Question 17: A

The correct answer is A. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery. Here's why:

In a time-series data processing pipeline, the key requirements are to ingest data from various sources in real-time, process and transform the data, store

the processed data for efficient retrieval, and perform analytics and visualization. Let's break down each of the options:

A. Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery:

1. Cloud Pub/Sub: This is an ideal service for ingesting real-time data from various sources, allowing for asynchronous messaging that can handle high throughput.
2. Cloud Dataflow: This is suitable for processing and transforming both batch and streaming data at scale. It provides a robust platform to handle the time-series data pipeline's processing requirements.
3. Cloud Bigtable: This is an excellent choice for storing time-series data as it is a scalable and high-performance NoSQL database service optimized for large analytical and operational workloads. It offers a low-latency storage solution for time-series data.
4. BigQuery: This is an enterprise data warehouse that enables fast SQL queries using the processing power of Google's infrastructure. It is perfect for analyzing and visualizing time-series data, making it an ideal end-stage service for the pipeline.

B. Cloud Pub/Sub, Cloud Dataflow, Cloud Spanner, Cloud Storage:

This option is not ideal because Cloud Spanner is primarily designed for relational, strongly consistent OLTP (Online Transaction Processing) workloads, which is not optimal for time-series data storage and retrieval. Additionally, Cloud Storage is an object storage service that doesn't provide an interactive querying layer, limiting its utility in the analytics and visualization phase.

C. Firebase Messages, Cloud Pub/Sub, Cloud Spanner, BigQuery:

This option doesn't work because Firebase Messages is a notification and messaging feature of Firebase, not a data ingestion service. The remaining services do not complement each other in the same way as the services in option A.

D. Cloud Pub/Sub, Cloud Dataproc, Cloud Storage, BigQuery:

This combination is not ideal because Cloud Dataproc is used for running Apache Spark and Hadoop clusters, which are more oriented towards batch processing. Time-series data analysis often requires both batch and real-time processing, making Cloud Dataflow a more suitable choice than Cloud Dataproc. Additionally, Cloud Storage lacks an interactive querying layer, limiting its utility for analytics and visualization.

In conclusion, option A (Cloud Pub/Sub, Cloud Dataflow, Cloud Bigtable, BigQuery) is the most suitable combination of services for constructing a time-series data processing pipeline using Google Cloud Platform as it aligns best with all the requirements across different stages of the pipeline.

Solution to Question 18: D

The most appropriate course of action to achieve the objective of configuring

permissions for Compute Engine instances to write data into a specific Cloud Storage bucket while adhering to Google's recommended best practices is option D: Create a service account and add it to the IAM role 'storage.objectCreator' for that bucket.

The reason why option D is the correct answer and other options will not work:

Option A: Creating a service account with an access scope and using the 'https://www.googleapis.com/auth/compute.read' scope is not appropriate because this scope grants read access to Compute Engine resources, but not write access to Cloud Storage buckets. The objective is to allow instances to write data into a specific Cloud Storage bucket.

Option B: Adding the service account to the IAM role 'compute.admin' for that bucket is not the best practice because it grants full administrative access to all Compute Engine resources. This is too broad and goes beyond the intended permission, which is only to allow instances to write data into the Cloud Storage bucket.

Option C: Creating a service account with an access scope and using the 'https://www.googleapis.com/auth/cloudkms' scope is not relevant because this scope grants access to manage encryption keys in Google Cloud KMS. This scope does not pertain to writing data into a Cloud Storage bucket.

Option D: Creating a service account and adding it to the IAM role 'storage.objectCreator' for that bucket is the most appropriate course of action because this role grants the permission to create (write) new objects within the specified bucket. This matches the intended permission, and follows the principle of least privilege, which is one of Google's recommended best practices for managing permissions in cloud environments.

In conclusion, option D fulfills the requirement of configuring permissions for Compute Engine instances to write data into a specific Cloud Storage bucket while adhering to Google's best practices.

Solution to Question 19: A

The correct answer is A, and here is why:

A. Instructing the external consultant to generate an SSH key pair and adding the public key to the instance allows them to access the instance through SSH with their private key. This method is the most suitable in this situation since the consultant doesn't have a Google account and already has a VPN connection to your corporate network. By using SSH keys, you provide the consultant with secure and controlled access without requiring them to create a Google account.

B. This option is not suitable because using the gcloud compute ssh command line tool with Identity-Aware Proxy would require the consultant to have a Google account. In this case, the consultant does not have a Google account, so this method is not appropriate.

C. This option is also not suitable because it requires the external consultant to have a Google account to access the instance with Google Cloud SDK. Since the consultant doesn't have a Google account, this method is not feasible.

D. Creating a temporary service account with Google Cloud IAM and providing the JSON key file is not recommended in this situation because it grants more permissions than necessary for the consultant. This approach could lead to unintended access to other resources in your Google Cloud account, which may present a security risk. Additionally, this method may not be suitable for the consultant's access needs since it involves credentials specific to Google Cloud services.

Therefore, the best option to provide the external consultant with access to the Compute Engine instance is A. Have the consultant generate an SSH key pair, add their public key to the instance yourself, and allow them to access the instance with their private key securely.

Solution to Question 20: B

The correct answer is B - Enable deletion protection on the instance.

Explanation: As a Cloud Administrator, the primary concern here is to prevent accidental downtime of the application due to actions from multiple teams sharing the project. Enabling deletion protection on the Compute Engine instance will ensure that the instance cannot be deleted without explicitly disabling this protection. This feature serves as an additional safety measure to prevent accidental deletion and consequently, the downtime of the application.

Why the other options do not work:

A. Configure a firewall rule for the instance - Firewall rules are primarily used to control incoming and outgoing network traffic to and from a Compute Engine instance. While it is essential to configure robust firewall rules, they don't directly prevent accidental downtime caused by other teams in a shared project.

C. Implement instance tags and labels - Tags and labels help in organizing, managing, and regulating access to Compute Engine resources. While they can assist with control and organization of instances, they don't offer specific protection against accidental deletions or downtime of the application.

D. Enable autoscaling for the instance - Autoscaling is a feature that automatically adjusts the number of instances in a managed instance group based on the current load and predefined scaling policies. While autoscaling could help manage instances efficiently, it does not directly prevent accidental downtime of the application caused by other teams' actions in a shared project.

Solution to Question 21: D

The correct answer is D. This approach involves two steps. Firstly, you need to ensure that the OS Config agent is installed on the Compute Engine instance.

The OS Config agent is responsible for managing package installations, applying OS patches, and collecting vulnerability information related to the operating system. By having the OS Config agent installed, you are enabling the collection of vulnerability and other OS metadata for the specific Compute Engine instance.

Secondly, providing the security team member roles/osconfig.vulnerabilityReportViewer permission allows them to access the vulnerability reports generated by the OS Config agent. This role grants read permission to the vulnerability reports, empowering the security team member to analyze these reports and implement the security vulnerability management policy as required.

The other options are not suitable for the given scenario:

Option A: Assigning roles/compute.instanceAdmin permission gives the security team member administrative access to the Compute Engine instance. While this might allow them to see some details about the instance, it does not specifically grant visibility into vulnerability reports nor ensures that OS metadata for the specific instance is collected. Furthermore, it might inadvertently grant them broader instance control, which is not the main objective.

Option B: Cloud Data Loss Prevention (DLP) is a separate service used for discovering, classifying, and protecting sensitive data. It does not have specific functionality for scanning Compute Engine instances for vulnerabilities or collecting OS metadata.

Option C: Creating an organization policy to restrict access to specific Compute Engine instances is a good practice for limiting access to critical resources. However, this approach does not address the primary objective of granting the security team member visibility into vulnerabilities or other OS metadata of the specific instance.

Solution to Question 22: B

The correct answer is B: Use gcloud to create a key file for the service account that has appropriate permissions.

Explanation:

Option B is the most appropriate solution for enabling authentication to GCP APIs in an on-premises environment. A service account with the appropriate access to AutoML has already been created for you, so the next step is to create a key file, which will be used for authentication. Using gcloud, you can create a JSON or P12 key file for the service account, which your on-premises application can then use to interact with the GCP AutoML services.

Option A is not the correct answer as Direct Interconnect is a solution for establishing a dedicated network connection between your data center and Google Cloud Platform. It doesn't directly address authentication for your on-premises applications but instead focuses on creating a faster and more reliable connection.

Option C is also incorrect since creating a separate project for the on-premises application is not necessary for authenticating the application to GCP services. In addition, using the project's default service account is not advisable due to security reasons. Utilizing the existing service account with appropriate permissions is the best practice.

Option D is not correct because using OAuth 2.0 authentication code flow is more suitable for user-level authentication and authorization. In this scenario, you are required to access a GCP service (AutoML), which can be achieved by using a service account and its key file to ensure programmatic access to APIs without involving user credentials.

Solution to Question 23: C

The correct answer is C because it provides the most efficient way to connect to the SQL Server 2017 instance on Compute Engine.

Option A is incorrect because it suggests enabling Windows authentication in the GCP Console and connecting using Windows Authentication via the RDP button. However, SQL Server 2017 on Compute Engine instances requires a Windows username and password to be set in the GCP Console.

Option B is incorrect because it suggests clicking the SSH button in the GCP Console instead of using an RDP client. SSH is used to connect to Linux-based instances, while RDP is meant for connecting to Windows-based instances. Since SQL Server 2017 runs on Windows, an RDP client should be used.

Option D is incorrect because it involves clicking the RDP button in the GCP Console, which is less efficient than directly using an RDP client. Although it may work, it is not the most efficient method of connecting to the instance.

In summary, installing an RDP client on the desktop and setting a Windows username and password in the GCP Console (Option C) offers the most efficient means of connecting to the SQL Server 2017 instance on Compute Engine.

Solution to Question 24: A

The correct answer is A: Create an instance template and use the template in a managed instance group with autoscaling configured.

Explanation for Answer A: Creating an instance template is the appropriate approach in this scenario, given the requirement to use virtual machines directly and focus on operational efficiency and quick scaling. Managed instance groups (MIGs) maintain a specified number of VMs based on an instance template. This satisfies the need to deploy the application using virtual machines directly. By configuring autoscaling within the MIG, the number of VMs will automatically scale based on the CPU usage as required.

Reasons why the other options will not work:

Option B: Google App Engine flexible environment is a Platform as a Service (PaaS) option, whereas the question specifically asks for the use of virtual ma-

chines directly. Furthermore, App Engine Flexible's application scaling is based on the number of request per second and not CPU usage.

Option C: Google Cloud Run is a container-based serverless platform and is not a suitable choice for this scenario, as it does not meet the requirement of using virtual machines directly.

Option D: Cloud Pub/Sub is an asynchronous messaging service used to send messages between independent applications. It is not designed to manage or control scaling of VMs based on CPU usage directly. Although it might be possible to create a complex solution by orchestrating VM creation and deletion using Pub/Sub, it would not be as efficient or straightforward as using a managed instance group with autoscaling configured.

Solution to Question 25: B

The correct answer is B. Create a multi-region Cloud Spanner instance with an optimized schema.

Explanation:

Option A: Migrate transaction data to Bigtable and run SQL queries using Apache Beam.

This option is incorrect because, although Bigtable can handle large amounts of data and is scalable, it is not a relational database and does not support SQL queries natively. While Apache Beam can be used to perform data processing, it is not an ideal solution for running SQL queries needed for data analysis by the business team.

Option B: Create a multi-region Cloud Spanner instance with an optimized schema.

This option is the best choice because Cloud Spanner is designed to be a highly available, globally distributed, and strongly consistent relational database service that supports SQL queries. By configuring it as a multi-region instance, you can ensure high availability, fault tolerance, and low latency for the worldwide transactions. Moreover, optimizing the schema will ensure the efficient handling of data and a better performance.

Option C: Create a multi-region Cloud SQL for PostgreSQL database with optimized indexes.

This option is incorrect because, although Cloud SQL for PostgreSQL is a managed relational database service that supports SQL queries, it does not provide the same level of scalability, global distribution, or strong consistency as Cloud Spanner. Creating a multi-region Cloud SQL instance can improve availability, but it would not be as efficient as Cloud Spanner in handling significant volumes of worldwide transactions.

Option D: Create a multi-region Cloud SQL for MySQL database with no read replicas.

This option is incorrect because, like Option C, Cloud SQL for MySQL does not provide the same level of scalability, global distribution, or strong consistency as Cloud Spanner. Moreover, not using read replicas would limit the capacity to handle read-heavy workloads during data analysis, leading to degraded performance.

In conclusion, Option B is the best answer as it provides a highly available, scalable, and globally distributed relational data store that meets the requirements of the rapidly growing e-commerce company while supporting the SQL queries needed for data analysis by the business team.

Solution to Question 26: B

The correct answer is B, "Create an instance template that contains valid syntax which will be used by the instance group. Delete any persistent disks with the same name as instance names."

Here's why the other options do not work:

Option A: This option suggests adding a new template to an existing instance group and increasing the instance count. Although creating a new instance template is part of the solution, adding it to an existing instance group with conflicting persistent disk names will not fix the issue. The existing instance group still needs to resolve the persistent disk name conflicts.

Option C: Checking the permissions of the service account being used by the instance group is not directly related to the failure of new instance creation due to persistent disk name conflicts. While it is essential to ensure that proper permissions are configured for the service account, this option does not address the root cause of the issue.

Option D: This option mentions verifying that the instance template contains valid syntax, which is a prerequisite for creating instances. However, simply deleting persistent disks with the same name as instance names may not be sufficient to fix the issue because newly created instances can still run into the same disk naming conflicts. Setting the disks.autoDelete property to true in the instance template will not help resolve the name conflicts as this property simply defines whether the disk should be deleted when the associated instance is deleted.

In summary, option B is the best course of action to resolve the issue, as it involves creating an instance template with valid syntax and deleting conflicting persistent disks with the same name as instance names, which allows the managed instance group to create new instances without any conflicts.

Solution to Question 27: A

The correct answer is A: Deploy the application on App Engine. For each update, create a new version of the same service. Configure traffic splitting to send a small percentage of traffic to the new version.

The answer A is the most suitable for this scenario because Google App Engine is designed specifically for building scalable web applications, and it natively supports traffic splitting between different versions of a service. This approach will enable you to test new releases on real user traffic while ensuring that the majority of users have a stable experience.

The other options do not provide the same level of control and ease:

B. Deploy the application on Kubernetes Engine and use a StatefulSet for each update. Configure traffic splitting through a Kubernetes Ingress to direct a small percentage of traffic to the new StatefulSet. This option is not ideal because StatefulSets are designed for managing stateful applications, not for managing multiple versions of an application. Implementing traffic splitting with Kubernetes Ingress would require manual configuration, and it may not be as efficient or straightforward as the traffic splitting feature provided by App Engine.

C. Deploy the application on Compute Engine. For each update, create a new instance template. Configure traffic splitting between instance groups using a load balancer. With Compute Engine, you have to manually set up and manage the infrastructure, traffic splitting, and load balancing. In addition, using instance templates and instance groups for version management may complicate your setup and maintenance processes. App Engine provides a more straightforward and efficient approach for this scenario.

D. Deploy the application on Kubernetes Engine. For a new release, update the deployment to use the new version. Though deploying the application on Kubernetes Engine offers scalability and flexibility, updating the deployment to use the new version would make it challenging to control traffic to specific percentages between the previous and new versions. It lacks the built-in, easy-to-use traffic splitting functionality provided by App Engine, which allows you to manage multiple versions of your application seamlessly.

Solution to Question 28: A

The correct answer is A, and here's why:

A: 1. Advise your developers to go to Cloud Marketplace. 2. Ask the developers to launch a Cassandra image for their development work.

This option is ideal for a quick and efficient transition to Google Cloud. By using the Cloud Marketplace, developers can launch a pre-configured Cassandra image tailored for their specific development needs, resulting in minimal technical support effort. Moreover, this approach provides an isolated development environment for each team.

Now let's look at why the other options would not work:

B: 1. Use Cloud Firestore and create collections for each development team. 2. Configure security rules to isolate each team's access to their collections.

This option would not be suitable because Cloud Firestore is a different type of database (NoSQL) as compared to Cassandra, and changing the database technology could lead to compatibility and performance issues when migrating the existing applications.

C: 1. Set up a Cloud Dataproc cluster and install Cassandra on it. 2. Configure the cluster for each development team to access their own isolated environment.

This option is not as efficient as using Cloud Marketplace, as setting up and configuring a Cloud Dataproc cluster would require more time and technical effort. Furthermore, Cloud Dataproc is primarily designed for running Apache Spark and Apache Hadoop workloads, not Cassandra.

D: 1. Use Cloud Datastore as a replacement for Cassandra. 2. Set up separate projects for each development team to isolate their data.

Similar to option B, this option would involve switching from Cassandra to Cloud Datastore, which is a different NoSQL database. This change could lead to compatibility and performance problems. Additionally, setting up separate projects for each development team would add unnecessary complexity to the migration process.

In conclusion, option A is the best choice in this scenario because it efficiently migrates the existing Cassandra environments to Google Cloud while providing isolated development spaces for each team with minimal technical effort.

Solution to Question 29: D

The correct answer to this question is D. Let's elaborate on why this is the best option, and why the other options will not work.

Option A: Update the app.yaml file in the existing App Engine application to specify asia-northeast1 as the region, then redeploy the application. This option does not work because, once an App Engine application is created within a region, its region cannot be changed by only updating the app.yaml file. The region stays the same throughout the lifetime of the application.

Option B: Apply a forwarding rule in Google Cloud Load Balancer to redirect traffic from us-central to asia-northeast1 for the existing App Engine application. This option is not correct because forwarding rules in Google Cloud Load Balancer are used to handle the traffic at the global or regional level, but they can't be used to change the region of an existing App Engine application. The Load Balancer serves traffic based on proximity; it doesn't change the underlying region of the application.

Option C: Change the region property setting in the existing App Engine application from us-central to asia-northeast1. This option is not valid because once an App Engine application is created in a specific region, it cannot be changed to another region by modifying the region property setting. The region of an application is set during its creation and remains the same throughout its lifetime.

Option D: Create a new GCP project and create an App Engine application inside this new project. Specify asia-northeast1 as the region to serve your application. This is the correct option because creating a new GCP project and a new App Engine application allows you to specify the desired region (asia-northeast1) for the new application. This ensures that the application is hosted and served from the Asia-based region as desired by the company. Once the new application is ready, traffic can be migrated over from the old (us-central) region to the new (asia-northeast1) region.

In summary, to serve the application from the asia-northeast1 region instead of the us-central region, you should proceed with option D, i.e., creating a new GCP project and deploying the new App Engine application with the desired region (asia-northeast1).

Solution to Question 30: D

The correct answer is D: Use a custom mode VPC network, use Cloud Router border gateway protocol (BGP) routes, and use active/passive routing.

Reasoning for answer D: It is specified in the question that the network administrator needs dynamic routing, a shared address space of 10.19.0.1/22, and no overprovisioning of tunnels during a failover event. A custom mode VPC network allows you to set up specific address spaces, like the shared address space of 10.19.0.1/22. Cloud Router BGP provides highly available, scalable, and dynamic routing control. Active/passive routing ensures that there are backup tunnels with no overprovisioning during failover events, which is one of the mentioned requirements.

Reasoning against other options:

A. Use an automatic mode VPC network, use Cloud Router BGP routes, and use active/passive routing: This option does not allow you to configure the specific shared subnet. Automatic mode VPC networks allocate subnets automatically, which means you cannot have a shared address space of 10.19.0.1/22.

B. Use a custom mode VPC network, use Cloud Router static routes, and use active/passive routing: Static routes do not offer dynamic routing, which does not fulfill the requirement for reliable VPN connectivity with dynamic routing.

C. Use a custom mode VPC network, configure static routes, and use active/passive routing: Again, this option uses static routes, which do not provide dynamic routing. This means it does not meet the requirement of dynamic routing for establishing reliable VPN connectivity between the VPC and the remote site.

Solution to Question 31: A

The correct answer is A: Filter the Activity log to view the Configuration category. Filter the Resource type to Service Account.

Explanation:

In this scenario, you need to confirm when a service account was created, i.e., you are looking for a configuration change within the Google Cloud Platform. Activity logs capture all operations performed on resources in your project, including changes in configuration. Hence, filtering the Activity log to view the Configuration category will present the relevant information.

Filtering by the Resource type to Service Account ensures you are specifically checking for service account creations, modifications, deletions, and other operations in the logs. This makes it easier to pinpoint the exact time the service account was created.

Why other options will not work:

B. Filtering the Activity log to view the Data Access category will not help in this scenario, as this category typically contains logs related to operations involving reading or writing of data. It does not include logs for service account creation.

C. Error Reporting logs are designed to provide data on errors and crashes occurring within an application rather than capturing service account creation events. Also, Error Reporting logs do not have a Configuration category.

D. Filtering the Activity log to view the Configuration category is correct, but choosing to filter the Resource type to Storage Bucket will only show activity logs related to storage buckets, not service accounts.

Solution to Question 32: B

The correct answer is B: Use Transfer Appliance for the videos, BigQuery Data Transfer Service for the data warehouse data, and Storage Transfer Service for the PNG files.

Why other options will not work:

A. Use Storage Transfer Service for the video files, Dataproc for the data warehouse data, and Storage Transfer Service for the PNG files. - While Storage Transfer Service can work for transferring the PNG files stored in an S3 bucket to a Google Cloud Storage (GCS) bucket, transferring 200 TB of video files from on-premises SAN storage to GCS using Storage Transfer Service may not be the best option in terms of speed and efficiency, especially in cases with limited network bandwidth. Transfer Appliance would be a better choice to handle this large amount of data efficiently. - Dataproc is a managed Hadoop and Spark service which is not designed for handling the migration of data warehouse data from Amazon Redshift to BigQuery. BigQuery Data Transfer Service would be a more suitable choice for such migration tasks.

C. Use Dataproc for the video files, BigQuery Data Transfer Service for the data warehouse data, and Cloud Pub/Sub for the PNG files. - Dataproc is not an appropriate choice for migrating video files to GCS, as it is a managed Hadoop and Spark service designed for specific data processing tasks rather than large-scale data migration. - Cloud Pub/Sub is a messaging service meant

for real-time communication between applications and services, making it unfit for transferring PNG files from an S3 bucket to a GCS bucket.

D. Use Dataflow for the video files, Cloud Data Fusion for the data warehouse data, and Transfer Appliance for the PNG files. - Dataflow is a managed service for stream and batch data processing, not for bulk data transfer of video files from SAN storage to GCS. The Transfer Appliance is a more suitable choice. - Although Cloud Data Fusion can be used for integrating, preparing, and managing data sets, using BigQuery Data Transfer Service is more efficient and follows Google-recommended practices for transferring data warehouse data from Amazon Redshift to BigQuery. - The Transfer Appliance is designed for transferring large volumes of on-premises data to GCS. In the case of the 20 GB of PNG files stored in an S3 bucket, the Storage Transfer Service suits the requirements better and less expensively.

Solution to Question 33: D

The correct answer is D: Create a GKE Autopilot cluster. Enroll the cluster in the stable release channel.

Here's why option D is the most appropriate:

Option D is the best choice since it utilizes the GKE Autopilot cluster, which automatically applies the best practices for running and managing Kubernetes clusters on Google Cloud. It provides enhanced reliability by automatically scaling and optimizing node pools, handling upgrades and maintenance, and using Google's secure infrastructure. Additionally, enrolling in the stable release channel ensures that the cluster receives the most reliable and thoroughly tested updates, considering the crucial nature of the application.

Here's why the other options would not work:

Option A: While it involves creating a GKE Autopilot cluster for best practices, enrolling in the preview release channel is not ideal for a crucial application. The preview channel contains pre-release versions with new features and updates, which may not be fully stable yet.

Option B: Creating a GKE Autopilot cluster without enrolling in any specific release channel is risky. Choosing a release channel, especially the stable release channel, allows access to updates that have been tested for stability and reliability to ensure the app runs smoothly.

Option C: Creating a regional GKE standard cluster and enrolling in the no-channel release setting would not be recommended for this scenario. First of all, using the GKE Autopilot cluster has distinct advantages in terms of features and best practices provided by Google. Secondly, the no-channel release setting skips important updates, which may lead to potential issues in the future.

Solution to Question 34: C

The correct answer is C. Use GCP Marketplace to launch the Jenkins solution.

Explanation:

Option A: Deploy Jenkins as an API Gateway with an API key. This option is incorrect because Jenkins is a continuous integration and continuous deployment (CI/CD) platform, not an API Gateway. Jenkins is not designed to manage APIs but to automate the building, testing, and deployment of applications in the software development process.

Option B: Use Firebase Hosting to deploy the Jenkins application. This option is also incorrect. Firebase Hosting is designed for hosting static web content and single-page web applications, while Jenkins is an advanced CI/CD platform with a wide range of plugins and integrations. Jenkins requires a runtime environment and server-based infrastructure to operate and manage builds and deployments. Firebase Hosting will not provide the necessary infrastructure to run Jenkins efficiently.

Option C: Use GCP Marketplace to launch the Jenkins solution. This is the correct answer. GCP Marketplace is Google Cloud Platform's marketplace for users to explore, deploy, and manage third-party cloud-native solutions easily. By using GCP Marketplace, you can quickly and efficiently launch a pre-configured and optimized Jenkins server. It ensures that the Jenkins server meets the desired security, performance, and scalability standards and is suitable for a DevOps engineer working in a software development company.

Option D: Try deploying Jenkins as a Cloud Identity-Aware Proxy (IAP) service. This option is not correct because Cloud Identity-Aware Proxy (IAP) is a security service for controlling access to applications running on Google Cloud Platform. It is not a hosting or deployment solution for applications like Jenkins. While IAP can be used to secure access to the Jenkins server after it has been deployed, deploying Jenkins as an IAP service is not the right approach to set up a Jenkins server.

In conclusion, to set up a new Jenkins server for your team's project quickly and efficiently, you should use GCP Marketplace to launch the Jenkins solution.

Solution to Question 35: D

The correct answer is D. Set the minimum number of instances for your Cloud Run service to 3.

Explanation: The issue of the initial web page taking significantly longer to load compared to the following pages indicates that the problem lies in the loading and initialization of the application instances. This is referred to as the "cold start" issue. In order to address this issue, Google recommends setting the minimum number of instances to a certain value. By setting the minimum number of instances for your Cloud Run service to 3, you ensure that there are always available instances to serve incoming requests, thus reducing the latency experienced by clients during the initial page load.

Now let's discuss why other options will not work:

A. Change the Cloud Run memory allocation to a larger value. Increasing the memory allocation might help to some extent in terms of performance, but it does not directly address the "cold start" issue. The larger memory allocation can also lead to increased costs for running the service without guaranteeing a significant improvement in the initial page load time for clients.

B. Change the region for the Cloud Run service. Changing the region might help to reduce network latency if the majority of the clients are located closer to the new region. However, it does not address the "cold start" issue and can also introduce complexities in managing resources in different regions.

C. Update your web application to use the protocol HTTP/2 instead of HTTP/1.1. While upgrading to HTTP/2 can offer some performance benefits such as multiplexing, server push, and header compression, it does not tackle the primary issue of "cold starts" and the initial loading time of the application instances. Moreover, adopting a new protocol may require significant changes in the existing web application, which might not be feasible in the short term.

In conclusion, option D – setting the minimum number of instances for your Cloud Run service to 3 – is the most suitable action to address the reported issue while adhering to Google's recommendations.

Solution to Question 36: D

The correct answer is D. Enforce an org policy constraint allowing the lifetime of service account keys to be 24 hours. Enforce an org policy constraint denying service account key creation with an exception on pj-sa.

Option A will not work because it involves the unnecessary use of Cloud Run to purge service account keys periodically, which could lead to additional costs. Moreover, the exception on pj-sa will not contribute to enforcing short-lived service account credentials.

Option B is not the best approach, as using a custom App Engine task runner to rotate service account keys every day is an inefficient method and may also result in added costs and management overhead. Furthermore, enforcing an org policy that allows service account key creation without any exceptions across projects is counterproductive to the goal of implementing short-lived service account credentials.

Option C is not the best choice, as implementation of a Kubernetes CronJob for rotating service account keys periodically might increase operational complexity and costs. Additionally, disabling the attachment of service accounts to resources in all projects would not contribute to the goal of enforcing short-lived service account credentials within the company.

Option D is the best approach, as it enforces short-lived service account credentials by setting an org policy allowing the lifetime of service account keys to be 24 hours, ensuring they expire and become useless after one day. In addition, by enforcing an org policy constraint to deny service account key creation with an

exception on the centralized project pj-sa, it meets the requirement and consolidates service account key management, while minimizing costs and operational complexity.

Solution to Question 37: D

The correct answer is D, and here's why:

When managing multiple Google Cloud projects using the Google Cloud SDK CLI, it is crucial to have a well-organized system to be efficient and avoid confusion between projects.

Option D provides the best approach to achieve this:

1. Creating a configuration for each project ensures that every project has its unique settings and environment. It avoids the overlapping of preferences and allows you to work on them independently, making your management more efficient.
2. Activating the appropriate configuration when working with each project allows you to easily switch between different projects without manually changing the settings. This not only saves time but also reduces the risk of errors due to incorrect settings.

Now, let's look at the other options and why they are not suitable:

Option A: Using the default configuration for one project and updating the configuration values using gcloud init when needed is not a good approach. Manually changing the settings every time you need to work with a non-default project is not only time-consuming but could also lead to mistakes due to human error.

Option B: Utilizing a single configuration for all projects and employing labels and filters to differentiate between projects can cause confusion. While labels and filters can help manage resources to some extent, they are not sufficient when it comes to managing configurations. Moreover, using a single configuration can cause clashes in settings and preferences when working on multiple projects.

Option C: Creating Google Cloud Storage buckets for each project and using gcloud storage commands to manage and switch between projects does not address the need for managing configurations. It only focuses on organizing storage and not the overall project configuration, making it an inefficient option for managing multiple projects using the Google Cloud SDK CLI.

In conclusion, Option D ensures that you can smoothly manage multiple Google Cloud projects using the Google Cloud SDK CLI by creating individual configurations for each project and activating the necessary configuration when working on a specific project. This approach saves time, reduces errors, and allows you to work efficiently across all your assigned projects.

Solution to Question 38: C

The correct answer is C: Create a Stackdriver Logging Export with a Sink destination to a BigQuery dataset. Configure the table expiration to 60 days.

Option A is not ideal because exporting logs to Cloud Storage is inefficient for analysis purposes. Cloud Storage is more suitable for archiving purposes, but not ideal for exploring and analyzing log data, as it would require additional steps to process the logs stored in the storage buckets.

Option B is not the best choice because using Cloud Scheduler for this purpose would require writing custom code to read logs from Stackdriver and storing them in BigQuery. Moreover, this approach doesn't adhere to Google's recommended practices for obtaining combined logs.

Option D is not appropriate because Stackdriver Logging Viewer doesn't have an option to directly export logs to Cloud SQL. Additionally, Cloud SQL is not the best solution for handling huge volumes of log data, and BigQuery is a more suitable option for analytics purposes.

Therefore, the best solution is Option C. By creating a Stackdriver Logging Export with a Sink destination to a BigQuery dataset, you'll be able to efficiently explore and analyze log data across multiple projects. Setting the table expiration to 60 days will also ensure that you're adhering to the retention policies.

Solution to Question 39: A

The most effective method in this scenario is A. Turn on Data Access Logs for the buckets they want to audit, and then build a query in the log viewer that filters on Cloud Storage. This approach directly targets the audit requirement by providing the internal audit team with detailed logs of data access events for the specific Cloud Storage buckets. They can analyze the logs conveniently using the log viewer query, which can be customized to focus only on the access events they are interested in.

Option B is not the right choice because Data Loss Prevention API focuses on identifying and preventing sensitive data exposure. Although it can help the organization detect and secure sensitive information in the cloud, it does not specifically offer data access logs for audit purposes.

Option C is also not applicable here, as Cloud Asset Inventory serves as a solution for discovering, understanding, and managing Google Cloud resources and policies at scale. It does not provide visibility into individual data access events in Cloud Storage.

Finally, option D is not the most effective choice because, although Cloud Pub/Sub can be used to stream logs, it requires additional components to set up and manage, such as subscribers to process the logs streamed to a topic. This approach may be more complex and time-consuming than simply turning on Data Access Logs and filtering logs using the log viewer, which better suits the auditor's needs for obtaining the necessary information about data access in Cloud Storage buckets.

Solution to Question 40: A

The correct answer is A: Use the command gcloud projects get-iam-policy to view the current role assignments.

Explanation for A: The gcloud projects get-iam-policy command allows you to view the existing IAM policy for a specific project, including the roles assigned to users and their corresponding email accounts. By using this command, you can quickly and efficiently find out who has the Project Owner role assigned to them, ensuring maximum security and proper role management.

Reasons why other options will not work:

Option B: Enabling Stackdriver Monitoring for the project and reviewing the logs for role changes is not the recommended course of action because it only helps track role changes and does not provide a quick and efficient way to review the list of users with the Project Owner role. You would need to sift through the logs, which can be time-consuming and may not provide an accurate assessment of all users with the assigned role.

Option C: Going to the IAM & admin page in the console and reviewing the Service Accounts permissions will not help in reviewing the list of users with the Project Owner role. Service accounts are used for applications and services, and while they can be assigned roles like users, focusing solely on them will not give you an accurate representation of human users with the Project Owner role.

Option D: Going to the Firebase Console and checking the Authentication section for users who have been granted the Project Owner role is not a recommended course of action because the Firebase Console manages user authentication for applications built on Firebase. It is not relevant to viewing role assignments or policies on the Google Cloud Platform.

Solution to Question 41: B

The correct answer is B. After the VM has been created, use gcloud compute reset-windows-password to retrieve the login credentials for the VM.

Here's why the other options will not work:

Option A: Downloading the JSON private key for the default Compute Engine service account and using the credentials to log in to the VM would not work because the JSON private key is used for authenticating applications and services to Google Cloud Platform services, not for logging into your VM instance via RDP. RDP requires a Windows username and password, which are not available from service account key files.

Option C: Adding metadata to the instance using 'windows-password' and a password as the value when creating the VM is not secure and is not the recommended method for setting up RDP access. Moreover, it is not an supported way to set passwords in Windows VMs on Compute Engine. Instead, you should

use the gcloud compute reset-windows-password command from option B to securely generate temporary passwords for logging in.

Option D: Using gcloud compute ssh to retrieve the login credentials for the VM would not work because gcloud compute ssh is used for connecting to Linux VM instances running in Compute Engine using SSH protocol, not for connecting to Windows VMs via RDP. Remote Desktop Protocol (RDP) is the standard protocol for Windows remote access, and to get the RDP credentials for a Windows VM on Compute Engine, you should use the gcloud compute reset-windows-password command as mentioned in option B.

Solution to Question 42: D

The correct answer is D, as using `kubectl config use-context` and `kubectl config view` will allow you to efficiently examine the configured Kubernetes Engine cluster of an inactive configuration. Here's why option D is correct and the other options are not suitable:

A. Use gcloud config set project and gcloud config get-value project to review the output. This option allows you to set and get the values of your project configuration settings. However, it does not focus specifically on Kubernetes Engine clusters or inactive configurations. The main goal here is to manage the project settings, not to review the Kubernetes configurations in detail.

B. Use gcloud config set compute/zone and gcloud config set compute/region to review the output. This option deals with setting the compute/zone and compute/region values in the gcloud configuration. While it may be useful in managing regions and zones, it does not target Kubernetes Engine clusters or inactive configurations directly.

C. Use kubectl get nodes to review the output. While this command is relevant to Kubernetes, as it returns information about the nodes within the active cluster, it does not focus on examining inactive configurations. Due to this limitation, this option does not fully address the main objective of this question.

D. Use kubectl config use-context and kubectl config view to review the output. This is the correct answer for this specific use case. The `kubectl config use-context` command allows you to switch to an inactive configuration (even if it's not currently active), while `kubectl config view` displays detailed information about the configurations, including the specified Kubernetes Engine cluster. This method enables you to efficiently review and examine the configurations you need, even if they are not in use at the moment.

Solution to Question 43: B

The correct answer is B: Add the cluster's API as a new Type Provider in Deployment Manager, and use the new type to create the DaemonSet.

Here's why:

Option A: Deployment Manager Runtime Configurator is primarily used for

storing configuration values and is not an appropriate solution for managing Kubernetes resources like DaemonSets. Additionally, using Runtime Configurator would unnecessarily introduce an extra service.

Option B: This approach allows you to use the Deployment Manager to directly interact with the Kubernetes API and manage everything within a single deployment, without introducing any additional services. By adding the Kubernetes cluster API endpoint as a new Type Provider, you can create the DaemonSet in the kube-system namespace during the same deployment process. This ensures minimal overhead and streamlined management.

Option C: While adding a Kubernetes ClusterRoleBinding could provide access to the kube-system namespace, this option doesn't actually address the need to create the DaemonSet using the same Deployment Manager deployment. Additionally, referencing the DaemonSet in the rules of ClusterRoleBinding is not the correct method for deploying and managing the DaemonSet.

Option D: Though the Cloud Build trigger could create and deploy the DaemonSet, it introduces an unnecessary service and complicates the deployment process by separating it from the main Deployment Manager configuration. This detracts from the goal of simplicity and efficiency.

In conclusion, Option B is the most efficient approach as it directly integrates with the Kubernetes API, manages the DaemonSet within a single deployment, and avoids introducing any additional services.

Solution to Question 44: C

The correct answer is C because it adheres to Google-recommended best practices for networking and communication between different regions within a single VPC. The following clarifies why the other options are not correct:

Option A: Although Google App Engine can be used to deploy applications in various regions, it is not a suitable solution for this particular use case. The task requires the deployment of a new Compute Engine instance, not an App Engine application. Additionally, App Engine applications automatically scale and are stateless, which may not be appropriate for the given application.

Option B: Creating a new VPC and using VPC peering adds unnecessary complexity to the project. This setup would require the instances to communicate over public internet, relying on their public addresses. Instead, it is best to keep the instances within the same VPC in different regions with private addressing to enhance security and reduce latency.

Option D: Using a third-party VPN solution is not recommended by Google as it involves additional configuration, complexity, and cost. Google Cloud's VPCs already offer secure and scalable options for inter-region communication. It is advisable to remain within the Google Cloud ecosystem and use their networking features, such as keeping both instances in the same VPC and using private addresses for communication.

Solution to Question 45: C

The correct answer is C. The reason for selecting this approach is because Cloud Run is specifically designed to run containerized applications and is a serverless solution, making it a good fit for migrating the existing Docker-based microservices. By using the existing CI/CD pipeline, you can maintain consistency and streamline the deployment process, reducing the chance of errors during the transition. Updating the configurations and required endpoints is necessary to ensure that the application adapts to its new environment on Google Cloud.

Option A is not suitable because App Engine Standard Environment does not support Python-based microservices running on Docker containers, making it difficult to migrate the application without significant refactoring. This may lead to increased costs, delayed delivery, and potential performance issues.

Option B is not appropriate because Cloud Functions is designed for running single-purpose, simple functions rather than complex sets of microservices. Additionally, Cloud Functions do not support Docker containers, which means you would need to rewrite your application logic to fit Cloud Functions' requirements, leading to increased costs and time spent refactoring.

Option D does not fit the requirement of transitioning to a serverless solution, as using Compute Engine instances implies managing virtual machines (VMs) and scaling them manually or through managed instance groups. This approach defeats the purpose of moving to a serverless architecture, which aims to abstract away infrastructure management and focus on application functionality.

Solution to Question 46: C

The correct answer is C: Grant roles/bigquery.dataViewer role to crm-databases and appropriate roles to web-applications.

Explanation: The question asks to grant access for VMs in the web-applications project to BigQuery datasets in the crm-databases project while adhering to Google-recommended practices. The Google-recommended practices involve following the principle of least privilege, which means giving the service accounts only the minimum required permissions to perform its tasks.

Reasons why other options will not work:

A. Grant "project owner" role to crm-databases and the web-applications project. This option would grant very broad permissions to both projects, violating the principle of least privilege. The "project owner" role has full control over all resources in the project, which is not necessary for the specific requirement of granting access to BigQuery datasets.

B. Grant "project owner" role to crm-databases and roles/bigquery.dataViewer role to web-applications. This option mistakenly grants "project owner" role to crm-databases, which again violates the principle of least privilege. Additionally, this approach grants the dataViewer role to the entire web-applications project instead of the specific service account, which is not following best practices.

D. Grant "project owner" role for web-applications appropriate roles to crm-databases. This option has two issues: Firstly, it implies granting "project owner" role to the web-applications project, which violates the principle of least privilege. Secondly, this option does not specify which appropriate roles to grant access to crm-databases, causing ambiguity and potentially a misconfiguration.

In conclusion, option C is the correct choice because it adheres to the principle of least privilege while granting the required permissions for the specific task. It assigns the roles/bigquery.dataViewer role to the crm-databases project, enabling the service account in web-applications to read the BigQuery datasets. Additionally, it states that appropriate roles should be granted to the web-applications project, ensuring that only the necessary permissions are assigned.

Solution to Question 47: A

The correct answer is A: Add the group for the finance team to roles/billing viewer role.

Here's why the answer should be A and why other options will not work:

A) Adding the group for the finance team to roles/billing viewer role grants the finance members access to the billing report without giving them additional permissions on the project. It is the right approach as it follows the principle of least privilege and provides exactly the level of permissions needed for the finance team.

B) Adding the group for the finance team to roles/compute.viewer role will grant them read-access to all Compute Engine resources, including virtual machine instances, disks, and metadata. However, it does not provide them access to billing reports, which is the primary requirement in this scenario.

C) Adding the group for the finance team to roles/bigquery user role grants the finance team members access to manage BigQuery data sets and run queries on them. While this could be useful for processing and analyzing data, it does not give direct access to billing reports as required.

D) Adding the group for the finance team to roles/container admin role grants them permissions to administer all GKE clusters resources. This is not relevant to providing access to billing reports and would give unnecessary additional permissions to the finance team that are not required for their job.

Solution to Question 48: D

The correct answer is D. Here's why:

D. Use the BigQuery interface to review the nightly job and look for any errors.

As a data analyst, you need to verify if there is any issue with the nightly job in the data warehouse (BigQuery) that recalculates the daily summary. The problem could be due to any errors or issues during the process of overwriting

the table. To investigate the issue, using the BigQuery interface to review the nightly job is the most appropriate and direct approach. You can look for errors, failed jobs, or other issues related to the data processing and loading.

Now let's analyze why other options will not work:

A. Verify Cloud Dataflow pipeline for any data ingesting issues in the Google Cloud platform.

While Cloud Dataflow is used for processing data in real-time or batch mode, it is not the correct choice in this context. As a data analyst working with Looker Studio and BigQuery, your focus should be on how data is processed and stored in the data warehouse. The data ingestion might not be directly under your control, and the issue you face is related to the recalculated daily summaries, not the data ingestion.

B. Use the open-source CLI tool, Snapshot Debugger, to find out why the data was not refreshed correctly.

Snapshot Debugger is used for debugging applications and not specifically for data analysis or data warehousing issues. In this situation, you need to analyze the problem within the context of BigQuery to understand possible issues with the nightly job running to recalculate daily summaries.

C. Contact the Looker Studio support team for assistance in resolving the issue.

While reaching out to Looker Studio support could be a viable option in some cases, it should not be your first step in investigating this particular issue. The problem is related to the BigQuery environment, which is responsible for recalculating daily summaries and overwriting the table. As a data analyst, you need to verify if any errors or issues occurred in the data warehouse before escalating the issue to Looker Studio support.

Solution to Question 49: A

The correct answer should be A, and here's why:

A. Run a test using simulated maintenance events. If the test is successful, use Spot N2 Standard VMs when running future jobs. This option is the most cost-effective and efficient solution. Spot N2 Standard VMs offer reduced costs in comparison to regular N2 Standard VMs while still providing the necessary computing power for batch workloads. By testing with simulated maintenance events, you can ensure that your workload remains fault-tolerant even with the sporadic nature of Spot VM de-allocations. If the test is successful, you can confidently use these cost-effective VMs for your nightly batch workloads without compromising efficiency.

Now, let's discuss why the other options are not suitable:

B. Run a test using App Engine Flexible environment. If the test is successful, migrate the workload to App Engine Flexible environment. App Engine Flexible environment is designed for web applications and APIs. It's not the

most suitable environment for batch workloads that run on numerous VMs. Additionally, the App Engine Flexible environment can be more expensive than traditional VM-based solutions.

C. Run a test using simulated maintenance events. If the test is successful, use N2 Standard VMs when running future jobs. This option may not significantly reduce the costs since it uses the regular N2 Standard VMs. The purpose of the simulated maintenance events is to test the fault-tolerance of the system on Spot VMs, so it doesn't make much sense to continue using regular N2 Standard VMs if the test proves successful.

D. Run a test using a managed instance group. If the test is successful, use N2 Standard VMs in the managed instance group when running future jobs. Managed instance groups can help maintain a robust and fault-tolerant workload, but they don't necessarily reduce the cost as they use regular N2 Standard VMs. Also, managed instance groups add complexity to the solution, which might not align with cost-efficiency goals. Option A still serves better in finding a more cost-effective solution.

Solution to Question 50: D

The recommended course of action for syncing Active Directory with Google accounts is option D. Use Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity.

Option D will work because GCDS synchronizes user identities, group memberships, and associated metadata between Active Directory and Cloud Identity effectively. By using GCDS, all the existing employees within the organization can be automatically synced to Cloud Identity at once, reducing manual errors and improving control over user accounts.

Option A suggests manually creating user accounts in Cloud Identity for each employee and assigning roles. This is not the most efficient approach, given that the company is large and relies on Active Directory. Manually creating each account would be time-consuming and error-prone, as well as difficult to manage and maintain consistency across multiple services.

Option B recommends asking each employee to create their own Google account using self signup with their corporate email and password. This approach is not ideal, considering the use of Active Directory as the source of truth for user identities should be maintained. Allowing employees to create their own accounts could lead to insufficient security, management, and monitoring of the accounts, and it doesn't provide a structured approach for integrating with GCP services.

Option C assumes establishing VPN connectivity between your on-premise network and GCP, and then using Active Directory Domain Services in GCP to manage user accounts. This approach is not recommended because it introduces additional complexity in managing user identities and might not provide seamless synchronization between Active Directory and Google services. GCDS is

specifically designed for syncing Active Directory and Google accounts, so it is better suited to this task than VPN connectivity.

In conclusion, option D, using Google Cloud Directory Sync (GCDS) to synchronize users into Cloud Identity, is the recommended approach for maintaining control over Google accounts within a large corporation that relies on Active Directory. GCDS provides an automated, secure, and efficient way to sync user accounts and metadata, ensuring consistency and reducing the risk of manual errors and management inefficiencies.

Practice Exam 20

Question 1: As a system administrator at a software company, you are responsible for setting up an SSH connection to a single Compute Engine instance for the dev1 team members. This instance is the only resource within the Google Cloud Platform project that the dev1 team should access. How should you proceed?

A. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

B. Create a Cloud SQL instance and grant the dev1 group the cloudsql.client role. Direct them to use the Cloud Shell to ssh to that instance.

C. Create a Cloud Storage bucket and grant the dev1 group the storage.objectAdmin role. Direct them to use the Cloud Shell to ssh to that instance.

D. Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.InstanceAdmin role. Direct them to use the Cloud Console to ssh to that instance.

Question 2: At your fast-growing startup company that relies heavily on nightly batch processing jobs taking around 2 hours to complete, you've been tasked with minimizing service costs while selecting and configuring compute resources for these jobs. What is the most cost-effective approach to accomplish this task?

A. Select Google Kubernetes Engine. Use node autoscaling with a minimum of zero and a maximum of five nodes.

B. Select Cloud Run with full CPU allocation and concurrency set to 1.

C. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types.

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

Question 3: You are working as a network administrator for a company that heavily relies on cloud-based applications. Your current project involves setting up a new application in a VPC behind a firewall for a client. The client is highly concerned about data egress and wants to minimize the number of open egress ports. How should you configure the firewall rules to address this concern?

A. Set up a high-priority (1000) rule that pairs both ingress and egress ports.

B. Use a VPN tunnel to manage egress traffic by allowing only specific ports.

C. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

D. Set up a single rule (1000) that allows only the appropriate egress ports and blocks all other ports.

Question 4: As a Cloud Administrator in a tech company, you are tasked with adding a group of new users to Cloud Identity. Some of these new users already have existing Google accounts. In order to follow Google's best practices and avoid conflicting accounts, what course of action should you take?

A. Tell the user that they must delete their existing account.

B. Invite the user to transfer their existing account.

C. Grant temporary access to another user's account until the conflict is resolved.

D. Tell the user to share their existing account credentials with the GCP admin to resolve the conflict.

Question 5: As a Database Administrator in a software company, you are tasked with granting access to three new employees so they can view and edit table data on a Cloud Spanner instance. What is the most appropriate course of action to achieve this?

A. Run gcloud iam roles describe roles/spanner.viewer –project my-project. Add the users to the role.

B. Run gcloud projects add-iam-policy-binding my-project –member user:email@example.com –role roles/spanner.databaseUser.

C. Run gcloud iam roles describe roles/spanner.databaseUser. Add the users to a new group. Add the group to the role.

D. Run gcloud iam roles describe roles/spanner.viewer –project my-project. Add the users to a new group. Add the group to the role.

Question 6: You are working for a company in the finance industry that deals with a significant amount of unstructured data in various file formats. Your team needs to conduct ETL transformations on this data, making it accessible on Google Cloud to facilitate processing by a Dataflow job. Which method should you employ?

A. Upload the data to Cloud Storage using the gcloud storage command.

B. Upload the data to Cloud Functions using the gcloud functions deploy command.

C. Upload the data to Cloud Run using the gcloud run deploy command.

D. Upload the data into Cloud SQL using the import function in the Google Cloud console.

Question 7: As a cost optimization specialist for a large technology company, you've been tasked with minimizing GCP service expenses for a specific depart-

ment. You need to efficiently deactivate all configured services in an existing GCP project. What should be your course of action?

A. 1. Verify that you are assigned the Project Billing Administrator IAM role for this project. 2. Locate the project in the GCP console, click on billing and pause billing for the project.

B. 1. Verify that you are assigned the Cloud Engineering IAM role for this project. 2. Switch to the project in the GCP console, locate the resources, and disable their APIs.

C. 1. Verify that you are assigned the Security Administrator IAM role for this project. 2. Switch to the project in the GCP console, locate the resources and revoke access to them.

D. 1. Verify that you are assigned the Project Owners IAM role for this project. 2. Locate the project in the GCP console, click Shut down and then enter the project ID.

Question 8: As a financial analyst in a software development company, you are tasked with analyzing Google Cloud Platform service costs from three separate projects within the organization. Your goal is to create service cost estimates by service type, daily and monthly, for the next six months using standard query syntax. What approach should you take to complete this task?

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

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

C. Export your bill to a Cloud Storage bucket, and then import into Firestore for analysis.

D. Export your bill to a Cloud Storage bucket, and then import into Cloud Datastore for analysis.

Question 9: As a software developer working for a rapidly growing tech company, you have been tasked with developing an application that will be deployed on Google Kubernetes Engine. The application consists of both critical components that must always be available, as well as non-critical components that can afford to experience downtime. In order to efficiently manage costs while ensuring availability, how should you configure the Google Kubernetes Engine cluster?

A. Create a cluster with a single node-pool by using Preemptible VMs. Label the fault-tolerant Deployments as preemptible_true.

B. Create a cluster with both a Spot VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the Spot VM node pool and the fault-tolerant deployments on the node pool by using standard VMs.

C. Create a cluster with both a Shielded VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Shielded VM node pool.

D. Create a cluster with both a Spot VM node pool and a node pool by using standard VMs. Deploy the critical deployments on the node pool by using standard VMs and the fault-tolerant deployments on the Spot VM node pool.

Question 10: In your technology company that specializes in data analytics, you rely on the Google Cloud Platform and specifically use BigQuery for data warehousing purposes. The data science team in your company is quite dynamic and sometimes experiences frequent changes in its structure, with only a handful of team members. To ensure the members are able to perform queries while following Google's recommended practices, what course of action should you take?

A. 1. Create an IAM entry for each data scientist's user account. 2. Assign the BigQuery dataViewer user role to the group.

B. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery jobUser role to the group.

C. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery admin user role to the group.

D. 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery dataEditor user role to the group.

Question 11: As a database administrator in a rapidly growing tech company, you are tasked with managing a Cloud Spanner instance to ensure optimal query performance. Your company's production environment runs in a single Google Cloud region, and you need to enhance its performance as quickly as possible, adhering to Google's best practices for service configuration. What action should you take?

A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

B. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. Use database query statistics to identify queries that result in high CPU usage, and then rewrite those queries to optimize their resource usage.

C. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 75%. If you exceed this threshold, add nodes to your instance.

D. Increase the percentage of high priority CPU utilization threshold to 85% and create an alert in Cloud Monitoring to check for performance degradation.

Question 12: You are working as a cloud administrator in a large enterprise that has recently acquired a smaller company with its own Google Cloud organization. Your responsibility is to ensure that the Site Reliability Engineers (SREs) in your company have the same project permissions in the acquired company's organization as they do in your own organization. What action should you take to achieve this?

A. In the Google Cloud console for your organization, select Create role from selection, and choose destination as the startup company's organization.

B. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

C. In the Google Cloud console for your organization, select Create role from selection, and choose destination as the startup company's project in your organization.

D. Use the gsutil iam copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

Question 13: As a financial analyst at a large tech firm, you are responsible for managing the GCP costs for your company. Your company has recently acquired another organization that also has hundreds of projects and its own billing account. You have been tasked with consolidating all GCP costs for both organizations onto a single invoice, starting from tomorrow. What would be the most appropriate approach to achieve this task?

A. Configure both billing accounts to send email notifications to the finance team whenever a new invoice is issued.

B. Configure your company's billing account to access the acquired company's billing data using IAM roles.

C. Create a custom report in the GCP Console that shows the combined costs of both companies' GCP projects and use that as the invoice.

D. Link the acquired company's projects to your company's billing account.

Question 14: As a security analyst at a tech company, you are conducting a routine security review and need to determine who has the authorization to view information within your Google Cloud Project. What should be your next course of action?

A. Enable Data Catalog for data resource mapping.

B. Review the IAM permissions for any role that allows for data access.

C. Check the Access Transparency Logs for unusual activities.

D. Review the Bucket Policy Only settings for your storage buckets.

Question 15: You are working as an IT specialist for a tech company, and you have a Google Compute Engine instance hosting a critical production application. Your manager wants you to set up a system that sends an email notification when the instance consumes more than 90% of its CPU resources for over 15 minutes, using Google services. How should you proceed?

A. 1. Create a consumer Gmail account. 2. Write a script that monitors the CPU usage. 3. When the CPU usage exceeds the threshold, have that script send an email using the Gmail account and smtp.gmail.com on port 25 as SMTP server.

B. 1. Create a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it. 2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

C. 1. In Cloud Logging, create a logs-based metric to extract the CPU usage by using this regular expression: CPU Usage: ([0-9] {1,3})% 2. In Cloud Monitoring, create an Alerting Policy based on this metric. 3. Configure your email address in the notification channel.

D. 1. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Set up a Cloud Function to monitor the instance's CPU usage. 3. Trigger an email notification using Cloud Pub/Sub when the CPU usage exceeds the threshold.

2. Use Stackdriver Debugger to monitor the instance's CPU usage. 3. Set up an email notification channel to receive alerts when the CPU usage exceeds the threshold.

3. Configure a Cloud Scheduler job to monitor the instance's CPU usage. 2. If the CPU usage exceeds the threshold, set up a Cloud Task to send an email notification.

4. Use the Google Cloud Console to manually monitor the instance's CPU usage. 2. Set up a Google Groups mailing list to receive email notifications when the CPU usage exceeds the threshold.

5. Create a Cloud Monitoring Workspace and associate your GCP project with it. 2. Monitor the CPU usage using a built-in Cloud Monitoring agent. 3. Enable Google Workspace email notifications and configure alerts to be sent when the CPU usage exceeds the threshold.

6. Use a Cloud Run instance to monitor the CPU usage of the Compute Engine instance. 2. Set up a Cloud Storage bucket to store the results. 3. Configure email notifications for high CPU usage using Cloud Pub/Sub.

7. Use Google Kubernetes Engine to monitor the Compute Engine instance's CPU usage. 2. If the CPU usage exceeds the threshold, create a log entry in Google Cloud Logging. 3. Configure Cloud Logging to send email notifications for high CPU usage events.

8. Set up a Cloud Identity-Aware Proxy to monitor the CPU usage of the Compute Engine instance. 2. Configure the Identity-Aware Proxy to send email notifications after the CPU usage remains above the threshold for more than 15 minutes.

Question 16: As an IT manager in a rapidly growing tech company, you need to designate a team member to create and manage all service accounts for Google Cloud projects. To provide the minimum necessary access for this employee, which role should you assign them?

A. Add the user to roles/iam.serviceAccountOperator role.

B. Add the user to roles/iam.serviceAccountAccessManager role.

C. Add the user to roles/iam.roleAdmin role.

D. Add the user to roles/iam.serviceAccountAdmin role.

Question 17: As a data analyst at a tech company, you need to send all the logs from all the company's Compute Engine instances to a BigQuery dataset called platform-logs for further analysis. You have already installed the Cloud Logging agent on all the instances and want to minimize cost. What should you do?

A. 8. Use Logstash to generate a pipeline that pulls logs from Compute Engine instances and sends them to the platform-logs dataset in BigQuery. 9. Grant BigQuery Data Editor role to the service account used by Logstash.

B. 1. Create a Cloud Function that has the BigQuery User role on the platform-logs dataset. 2. Configure this Cloud Function to create a BigQuery Job that executes this query: INSERT INTO dataset.platform-logs (timestamp, log) SELECT timestamp, log FROM compute.logs WHERE timestamp > DATE_SUB(CURRENT_DATE(), INTERVAL 1 DAY) 3. Use Cloud Scheduler to trigger this Cloud Function once a day.

C. 1. In Cloud Logging, create a filter to view only Compute Engine logs. 2. Click Create Export. 3. Choose BigQuery as Sink Service, and the platform-logs dataset as Sink Destination.

D. 4. Create a Dataflow job to stream logs from Compute Engine instances to Cloud Storage. 5. Create a Cloud Storage Transfer Service job to move the logs from Cloud Storage to BigQuery dataset platform-logs daily.

Question 18: As a developer for a software company, you are tasked with building a product utilizing Google Kubernetes Engine (GKE). In the single cluster, each client has a Pod running, allowing them to execute arbitrary code within their designated Pod. To ensure optimal isolation between clients' Pods, what action should you take?

A. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

B. Use Cloud Armor to configure security policies for each customer's Pod.

C. Create a separate GKE cluster for each of your customers to run their Pods.

D. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

Question 19: As a project manager in a leading software company, you're responsible for overseeing the transfer of a crucial batch process from an on-premises server to the cloud. This process typically takes approximately 30 hours to complete, occurs on a monthly basis, and requires a restart if it happens to be interrupted. The task can also be carried out offline. Your ultimate goal is to ensure a smooth transition to the cloud with minimal costs. What course of action should you take?

A. Host the workload on a Cloud Storage bucket and use Pub/Sub for event-driven processing.

B. Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

C. Migrate the workload to a Google Kubernetes Engine cluster with Pre-emptible nodes.

D. Migrate the workload to a Compute Engine Preemptible VM.

Question 20: As a cloud administrator in a software development company, you need to set up application performance monitoring on Google Cloud projects A, B, and C as a single pane of glass for your team to simultaneously monitor CPU, memory, and disk usage. What should you do?

A. Set up Google Kubernetes Engine for projects A, B, and C with a single dashboard.

B. Create a custom Cloud Functions service to gather metrics data from projects A, B, and C.

C. Enable API, create a workspace under project A, and then add projects B and C.

D. Enable API and then share charts from project A, B, and C.

Question 21: As a data analyst at a growing company, you're currently using an on-premises data analytics set of binaries that processes data files in memory for 45 minutes every midnight. The sizes of those data files range from 1 gigabyte to 16 gigabytes. Your company has decided to migrate this application to Google Cloud with minimal effort and cost. What should be your recommended approach?

A. Upload the code to Cloud Functions. Use Cloud Scheduler to start the application.

B. Create a container for the set of binaries and use Cloud Scheduler to start the processing on AI Platform every midnight.

C. Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

D. Create a container for the set of binaries. Use Cloud Scheduler to start an App Engine job for the container.

Question 22: As a network engineer in a leading software development company, you are tasked with load balancing an instance group that serves a public web application over HTTPS. The company wants the load balancer to terminate the client SSL session while adhering to Google-recommended practices. What approach should you take?

A. Configure an external TCP proxy load balancer.

B. Configure an internal TCP load balancer.

C. Configure an HTTP(S) load balancer.

D. Configure an internal HTTPS load balancer.

Question 23: As a cloud engineer at a tech company, you are tasked with generating a list of enabled Google Cloud Platform APIs for a GCP project called "my-project" using the gcloud command line in Cloud Shell. How should you proceed?

A. Run gcloud config set project my-project, and then run gcloud compute networks describe default.

B. Run gcloud init to set the current project to my-project, and then run gcloud services list –available.

C. Run gcloud projects list to get the project ID, and then run gcloud services list –project .

D. Run gcloud init to set the current project to my-project, and then run gcloud services describe my-project.

Question 24: You are working as a Cloud Engineer at a company utilizing Google Cloud Platform for both production and development projects. You are tasked with creating an automated process to list all compute instances in these projects daily. How should you accomplish this?

A. Install Stackdriver Logging Agent on each instance, and use a daily log export to get a list of compute resources.

B. Go to Cloud Shell and export this information to Cloud Storage on a daily basis.

C. Create two configurations using gcloud config. Write a script that sets configurations as active, individually. For each configuration, use gcloud compute instances list to get a list of compute resources.

D. Create a Cloud Function that runs daily using Cloud Scheduler and uses gcloud compute instances list to get a list of compute resources for both projects.

Question 25: As an engineer working in a tech company, you have been utilizing Google Cloud on your personal credit card for various projects, and the company has been reimbursing these expenses. To streamline the process, the company is planning to move the charges to their monthly billing. What is the most appropriate action to take in this situation?

A. Use Google Cloud Pub/Sub to send billing notifications to your finance team.

B. Generate a billing report from the Google Cloud Console and email it to your finance department monthly.

C. Change the billing account of your projects to the billing account of your company.

D. Create a separate Google Cloud account for your company and manually transfer your projects.

Question 26: As a software engineer in a tech company, you are using a developer laptop with Cloud SDK installed on Ubuntu from the Google Cloud Ubuntu package repository. You need to test your application locally on your laptop using Cloud Datastore. What should you do?

A. Use the gcloud datastore export command to export data and then import it to your local Datastore emulator.

B. Set up a Firebase Realtime Database and use it instead of Cloud Datastore for your application.

C. Install the cloud-datastore-emulator component using the gcloud components install command.

D. Export Cloud Datastore data using gcloud datastore export.

Question 27: As a member of a tech company, you've been assigned a new Google Cloud project with a billing account where you will manage the creation of instances, set up firewalls, and store data in Cloud Storage while adhering to Google-recommended practices. What is the appropriate course of action?

A. Deploy instances and set firewall rules using default settings without enabling any APIs in the Google Cloud console.

B. Open the Google Cloud Console and manually create instances, set firewalls, and store data in Cloud Storage without enabling any APIs.

C. Use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs.

D. Use the gsutil cp command to interact with Cloud Storage without enabling the storage-api.googleapis.com first.

Question 28: As a software engineer working in a company that specializes in image processing, you are managing multiple microservices in a Kubernetes Engine cluster. One microservice is responsible for rendering images and demands a large amount of CPU time compared to its memory requirements. The other microservices are workloads optimized for n1-standard machine types. Your goal is to optimize the cluster so that all workloads utilize resources as efficiently as possible. What should you do?

A. Increase the number of replicas for the image rendering microservice without changing machine types.

B. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

C. Disable autoscaling for the entire cluster and allocate fixed resources to the image rendering microservice.

D. Use memory-optimized machine type nodes for the image rendering microservice and compute-optimized machine type nodes for the other microservices.

Question 29: You are a data manager working in a company that relies heavily on digital storage. You have been tasked with setting up Object Lifecycle Management for objects stored in storage buckets used by your team. Your team members typically write the objects once and access them frequently over a 30-day period. After 30 days, these objects are rarely read unless required for special purposes. The objects need to be stored for three years and the company wants to minimize storage costs. How should you configure the storage policy?

A. Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

B. Set up a policy that uses Coldline storage for 30 days, then moves to Nearline for one year, and then moves to Archive storage for two years.

C. Set up a policy that uses Standard storage for 30 days, then moves to Coldline for two years, and then moves to Archive storage for one year.

D. Set up a policy that uses Nearline storage for 30 days and then moves to Coldline storage for three years.

Question 30: As a DevOps engineer at a growing tech company, you are tasked with scaling an existing application running in Google Kubernetes Engine (GKE) that currently consists of multiple pods running on four GKE n1“standard”2 nodes. You need to deploy additional pods requiring n2“highmem”16 nodes without causing any downtime. What action should you take?

A. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

B. Create a new Deployment with a nodeSelector specifying n2-highmem-16 nodes and deploy the new pods.

C. Use Kubernetes horizontal pod autoscaling and specify machine type n2-highmem-16 during deployment.

D. Create a new Cluster Autoscaler with n2-highmem-16 nodes and deploy the additional pods.

Question 31: As a software engineer at a tech company, you've been tasked with migrating a crucial on-premises application that requires 96 vCPUs to the Google Cloud Platform (GCP) to ensure it operates in a similar environment. What should be your course of action?

A. Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations.

B. Adjust the VM's vCPU configuration after its creation using the GCP Console.

C. Use App Engine Standard Environment to host the application.

D. When creating the VM, use machine type n1-standard-96.

Question 32: As a software engineer at a tech company, you developed an application on your personal laptop utilizing Google Cloud services with Application Default Credentials for authentication. Everything runs smoothly on your laptop, but now you need to transfer this application to a Compute Engine virtual machine (VM) and establish authentication following Google's suggested practices and minimal modifications. What should you do?

A. Create an OAuth2.0 client ID for the application running on the Compute Engine VM and store the client secret in a secure file.

B. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.

C. Create a new Google account with appropriate access for Google services and use its credentials in a Compute Engine VM.

D. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Question 33: As a cybersecurity team member of a company in the finance industry, you are tasked with logging all read or write operations, including metadata and configuration read operations, of a Bigtable instance containing three nodes storing personally identifiable information (PII) data. This information must be logged within your company's Security Information and Event Management (SIEM) system. How should you proceed to accomplish this task?

A. Use Stackdriver to create a custom dashboard to monitor the Bigtable instance and send alerts to your SIEM system.

B. • Navigate to Cloud Monitoring in the Google Cloud console, and create a custom monitoring job for the Bigtable instance to track all changes. • Create an alert by using webhook endpoints, with the SIEM endpoint as a receiver.

C. • Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.

D. • Navigate to the Audit Logs page in the Google Cloud console, and enable Admin Write logs for the Bigtable instance. • Create a Cloud Functions instance to export logs from Cloud Logging to your SIEM.

Question 34: As a team lead at a software development company, you are responsible for managing a GCP project and wish to delegate access to your team members so they can efficiently manage buckets and files in Cloud Storage. Following Google-recommended practices, which IAM roles should you assign to your colleagues?

A. Storage Object Creator

B. Cloud Functions Admin

C. Storage Object Admin

D. Storage Admin

Question 35: You are working as a network administrator for a tech company that uses Google Cloud. You are asked to configure Cloud DNS to direct home.mydomain.com, mydomain.com, and www.mydomain.com to the IP address of the company's Google Cloud load balancer. What is the best approach to achieve this?

A. Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively. Most Voted

B. Create one NS record to point mydomain.com to the load balancer, and create two NS records to point WWW and HOME to mydomain.com respectively.

C. Create one AAAA record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

D. Create one SOA record to point mydomain.com to the load balancer, and create two A records to point WWW and HOME to mydomain.com respectively.

Question 36: As a web developer at a fast-growing IT company, you are tasked with creating a secure website with autoscaling based on the compute instance CPU load for a client. Your aim is to enhance performance by storing static content in Cloud Storage. Which resources should be utilized to distribute the user traffic effectively?

A. An external network load balancer pointing to the backend instances to distribute the load evenly. The web servers will forward the request to the Cloud Storage as needed.

B. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

C. A combination of Cloud Functions and Firebase Hosting to manage the website, and a URL map to target the requests for the static content to the Cloud Storage backend.

D. An external HTTP(S) load balancer with managed SSL for the backend service and an additional Cloud Pub/Sub integration for distributing the requests for the static content to the Cloud Storage backend.

Question 37: As a software engineer at a tech company, you are tasked with managing an application that runs on Google Kubernetes Engine (GKE) with cluster autoscaling enabled. This application exposes a TCP endpoint and has several replicas. You also have a Compute Engine instance situated in the same region but on a different Virtual Private Cloud (VPC) called gce-network, which has no overlapping IP ranges with the first VPC. Your objective is to enable the Compute Engine instance to connect to the GKE application while minimizing the effort involved. What should be your course of action?

A. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Add an annotation to this service: cloud.google.com/load-balancer-type: Internal 3. Peer the two VPCs together. 4. Configure the Compute Engine instance to use the address of the load balancer that has been created.

B. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Set the service's externalTrafficPolicy to Cluster. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

C. 1. In GKE, create a Service of type LoadBalancer that uses the application's Pods as backend. 2. Configure a VPN between the two VPCs. 3. Configure the Compute Engine instance to use the address of the load balancer that has been created.

D. 1. In GKE, create a Service of type ClusterIP that uses the application's Pods as backend. 2. Peer the two VPCs together. 3. Configure the Compute Engine instance to use the address of the ClusterIP that has been created.

Question 38: As a financial manager in a technology company, you are responsible for managing the budget for Compute Engineer services among three Google Cloud Platform projects that the company has. All three projects are linked to a single billing account. How should you properly set a budget alert for the usage of Compute Engineer services on one of these projects?

A. Verify that you have owner role at the organization level. Select the associated billing account and create a budget and alert for the appropriate project.

B. Verify that you are the project billing administrator. Select the associated billing account and create a budget for Compute Engine only.

C. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

D. Verify that you are the project administrator. Select the associated billing account and create a budget for the appropriate project with additional padding for potential overruns.

Question 39: As a software developer in a growing e-commerce company, you need to create and maintain a copy of a custom Compute Engine virtual machine (VM) to handle the anticipated surge in application traffic due to an upcoming business acquisition. What is the recommended course of action to achieve this?

A. Create a Google Kubernetes Engine cluster from your base VM. Create your instances from that cluster.

B. Create a custom Compute Engine image from a snapshot. Create your instances from a Cloud Storage bucket.

C. Create a custom Compute Engine image from your base VM. Create your instances from that image.

D. Create a custom Compute Engine image from a snapshot. Create your instances from that image.

Question 40: You recently started working as a Cloud Engineer in a multinational company and set up the Google Cloud CLI on your new work laptop. Before executing the gcloud compute instances list command to view the existing instances of your organization, which of the following actions must be performed? (Choose two.)

A. Run gcloud compute instances create to create a new instance before listing existing instances.

B. Run gcloud config set compute/zone $my_zone to set the default zone for gcloud CLI.

C. Install the Google Cloud SDK for Python to use the gcloud CLI.

D. Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI.

Question 41: As an IT specialist at a tech company, you're responsible for managing a virtual machine that currently has 2 vCPUs and 4 GB of memory. However, it is consistently running out of memory. To resolve this issue, you decide to upgrade the virtual machine to have 8 GB of memory. What should you do?

A. Stop the VM, increase the memory to 8 GB, and start the VM.

B. Enable Datastore mode for automatic memory allocation.

C. Resize the boot disk to 8 GB and restart the VM.

D. Enable autoscaling to increase the memory automatically.

Question 42: As a software engineer in a fast-paced tech company, you're responsible for deploying a newly developed application that consists of multiple microservices on Google Kubernetes Engine (GKE). To accommodate future growth, you need to ensure the cluster can scale as more applications are deployed without requiring manual intervention each time. How should you proceed?

A. Use Google App Engine instead of GKE to automatically scale the application.

B. Use Google Cloud Run instead of GKE and create multiple replicas of the application to provide automatic scaling.

C. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

D. Deploy the application on GKE, and add a HorizontalPodAutoscaler to the deployment.

Question 43: You are working as an IT specialist at a major corporation that recently completed the acquisition of a smaller company. As part of the integration process, you are responsible for merging the IT systems, including the smaller company's production Google Cloud project. Your goal is to transfer this project into your corporation's organization with minimal effort while ensuring that the billing is redirected to your company. What is the best course of action to achieve this?

A. Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization.

B. Use the gcloud command-line tool to create snapshots of Compute Engine virtual machines in the startup's project, then deploy those snapshots in your organization's project.

C. Decrypt the startup's Google Cloud Storage Service Account Key, share it with your organization, and grant Google Cloud Storage accounts the required permissions in the new organization.

D. Create a VPC Network Peering between the startup's Google Cloud project and your organization's project, then configure Billing Export to send billing data from the startup's project to your organization's project.

Question 44: As an IT manager in a software development company, you need to set up 10 Compute Engine instances for optimal availability even during maintenance. The instances must automatically restart if they crash, and should

be highly available, including during system maintenance. How should you configure the setup?

A. Create an instance group for the instances. Configure the instances to use an instance template with an attached Persistent Disk. Set 'On-host maintenance' to Migrate VM instance.

B. Create an instance template for the instances. Set the 'Automatic Restart' to off. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

C. Create an instance template for the instances. Set 'Automatic Restart' to off. Set 'On-host maintenance' to Terminate VM instances. Add the instance template to an instance group.

D. Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

Question 45: As a data engineer at a rapidly growing technology company, you have a massive 5-TB AVRO file stored in a Cloud Storage bucket. The company's data analysts are proficient only in SQL and require access to the data stored in this particular file. Your task is to find a quick and cost-effective solution for completing their request.

A. Create a Hadoop cluster and copy the AVRO file to NDFS by compressing it. Load the file in a hive table and provide access to your analysts so that they can run SQL queries.

B. Create a Cloud Dataproc cluster to process the AVRO file and store the results in a Cloud Spanner database for analysts to query.

C. Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

D. Configure Cloud Dataflow to read the AVRO file and write the data into Cloud Firestore for SQL querying.

Question 46: You are working as a software developer at a tech company and are responsible for updating an application hosted in an App Engine environment. You have been instructed to test the new version with only 1% of users before transitioning the entire application to the new version. What is the best approach to achieve this goal?

A. Create a new network in VPC and deploy the new version of your application in App Engine, then use GCP Console to split traffic.

B. Deploy the new version of your application in a separate project within App Engine and then use GCP Console to split traffic.

C. Deploy a new version of your application in Cloud Functions and then use GCP Console to split traffic.

D. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current version and newly deployed versions accordingly.

Question 47: As a developer in a retail company, you are tasked with transferring the company's internal application for managing transactional orders to the cloud. The application is used exclusively by employees at the headquarters and requires strong consistency, fast queries, and ACID guarantees for multi-table transactional updates. The first version of the application was implemented in PostgreSQL. To ensure a smooth transition with minimal code changes, which database would be most appropriate for this task?

A. Firestore

B. Cloud SQL

C. Cloud Spanner

D. Datastream

Question 48: As an IT specialist at a software development company, you are responsible for managing the Google Cloud resources for various teams. The sales team has a project named Sales Data Digest with the ID acme-data-digest. You now need to set up a similar system for the marketing team, but their resources must be organized separately from the sales team. What is the appropriate action to take?

A. Utilize Cloud Composer to build a pipeline that transfers data from acme-data-digest to the Marketing team's resources.

B. Create a separate organization for the Marketing team and migrate the acme-data-digest project there.

C. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

D. Clone the acme-data-digest project and rename it to acme-marketing-data-digest, then grant Marketing team access.

Question 49: As a project manager at a software development company, you oversee the organization and billing administration. The engineering team holds the Project Creator role within the organization. Your goal is to prevent the engineering team from linking projects to the billing account, allowing only the finance team to do so without granting them permission to make other changes to projects. How can you achieve this?

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

B. Give the finance team only the Compute Network User role on the organization.

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

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

Question 50: You work as a network administrator for a company operating in the finance industry. The company has workloads running on both Google Compute Engine and on-premises. The facility's Google Cloud Virtual Private Cloud (VPC) is connected to the WAN through a Virtual Private Network (VPN). To deploy a new Compute Engine instance and guarantee no public Internet traffic can be routed to it, what should you do?

A. Create a firewall rule to only allow traffic from Google Cloud VPC.

B. Create the instance without a public IP address.

C. Create a route on the VPC to route all traffic to the instance over the VPN tunnel.

D. Create the instance with a public IP address and use Cloud NAT.

Practice Exam 20 Solutions

Solution to Question 1: A

The correct answer is A: Set metadata to enable-oslogin=true for the instance. Grant the dev1 group the compute.osLogin role. Direct them to use the Cloud Shell to ssh to that instance.

Explanation: As a system administrator, your goal is to set up an SSH connection for the dev1 team members to access a single Compute Engine instance, which is the only resource within the Google Cloud Platform (GCP) project. The dev1 team doesn't need any other permissions in the project.

Option A is the best choice because it follows the principle of least privilege, which means giving the dev1 team members the minimum permissions necessary to accomplish their tasks. By setting the metadata to enable-oslogin=true for the instance, you enable Google's OS Login, which provides centralized user management for SSH connections. Granting the dev1 group the compute.osLogin role allows them to log in to the instance using SSH. Directing them to use the Cloud Shell to SSH to the instance lets them access the resource without setting up additional software or exposing their private keys.

Options B and C are incorrect because they involve granting access to different GCP services, Cloud SQL, and Cloud Storage, respectively, which are unrelated to the requirement of setting up an SSH connection to a Compute Engine instance.

Option D is not the best choice because granting the dev1 group the compute.InstanceAdmin role would provide them with excessive permissions to manage instances, not just SSH access. This role would allow them to create, modify, and delete instances in the project, which exceeds the requirement of only accessing a single Compute Engine instance.

Solution to Question 2: D

The most cost-effective approach for your fast-growing startup that relies on nightly batch processing jobs is to select option D. This involves using Compute Engine with preemptible VM instances of the appropriate standard machine type. Here's why:

D. Select Compute Engine. Use preemptible VM instances of the appropriate standard machine type:

- Compute Engine offers a variety of machine types that can be customized to fit the exact needs of your batch processing tasks, ensuring that you only pay for resources you need.
- Preemptible VM instances provide significant cost savings (up to 80%) compared to regular instances. Since your batch processing jobs run nightly and have a 2-hour duration, using preemptible instances will minimize service costs considerably.

- Though preemptible instances may be terminated at any time due to system demands, your 2-hour batch-processing jobs can be easily restarted without significant impact on your business workflow.

Now, let's see why other options will not work.

A. Select Google Kubernetes Engine. Use node autoscaling with a minimum of zero and a maximum of five nodes:

- While node autoscaling helps optimize resource usage, the Google Kubernetes Engine (GKE) platform usually has additional overhead and management costs compared to Compute Engine.
- GKE is more optimal for containerized applications that need constant autoscaling and management features. For your nightly batch processing jobs, GKE is not the most cost-effective solution.

B. Select Cloud Run with full CPU allocation and concurrency set to 1:

- Cloud Run is designed to manage and scale containerized applications automatically. By setting concurrency to 1, you'll limit the cost-effectiveness of Cloud Run.
- Cloud Run uses a pay-per-use pricing model. For your case, where tasks run continuously for 2 hours, Compute Engine with preemptible instances will provide better cost savings.

C. Select Google Kubernetes Engine. Use a three-node cluster with micro instance types:

- Though micro instances are cheaper than standard machine types, they have significantly reduced CPU and memory resources, which may negatively impact your batch processing jobs' performance and completion time.
- Similar to option A, GKE introduces additional overhead and management costs. Compute Engine with preemptible instances will offer better cost optimization for your specific use case.

In conclusion, option D (Compute Engine with preemptible VM instances) is the most cost-effective approach to run your nightly batch processing jobs while minimizing service costs for your fast-growing startup company.

Solution to Question 3: C

The correct answer is C: Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

Explanation:

Option A is not suitable because setting up a high-priority (1000) rule that pairs both ingress and egress ports will not minimize the number of open egress ports. Such a rule would allow access to many unnecessary egress ports, which goes against the client's requirements.

Option B, using a VPN tunnel to manage egress traffic by allowing only specific ports, does not address the firewall rule configuration directly. A VPN can encrypt and secure data transmission but does not inherently minimize the number of open egress ports in the firewall configuration.

Option C is the most appropriate choice because it strictly manages the egress traffic by putting a low-priority rule (65534) that blocks all egress alongside a high-priority rule (1000) that allows only the necessary ports. This way, only approved egress ports will be open, and all others remain blocked, fulfilling the client's requirement.

Option D, setting up a single rule (1000) that allows only the appropriate egress ports and blocks all other ports, is incorrect because the firewall may not automatically block all other non-specified ports, creating a potential security risk. It is imperative to have two separate rules with different priorities to ensure that the firewall effectively blocks undesired egress ports while allowing the required ones.

Solution to Question 4: B

The correct answer is B: Invite the user to transfer their existing account. This is the ideal course of action as it complies with Google's best practices for managing accounts in Cloud Identity.

Inviting users to transfer their existing accounts ensures that their personal data, settings, and files are preserved. It also streamlines access to the company's resources while avoiding conflicting account issues. Once the invitation is accepted and the transfer is completed, the new user will be part of the organization's Cloud Identity, allowing them to access the company's designated resources.

Option A is not advisable because it requires users to delete their existing accounts, which can result in loss of important data, files, and settings. Google's best practices emphasize preserving user's personal information and streamlining the process of adding new users to an organization.

Option C is not suitable, as granting temporary access to another user's account is a security risk. It does not address the issue of conflicting accounts and can result in unauthorized access to sensitive information or system resources.

Option D is inappropriate and against security best practices. Sharing account credentials compromises the security of the user's information and can lead to unauthorized access, data breaches, and a lack of clear responsibility tracking. Google recommends keeping personal account information confidential.

In summary, the best course of action when adding new users to Cloud Identity with existing Google accounts is Option B: Invite the user to transfer their existing account. This approach aligns with Google's guidelines, retains personal data, and avoids potential conflicts that could arise with other options.

Solution to Question 5: C

The correct answer is C. The reason why this is the most appropriate course of action is because it involves describing the 'roles/spanner.databaseUser' role, which grants permissions to both view and edit table data on a Cloud Spanner instance. By adding the new employees to a group and then adding the group to the 'roles/spanner.databaseUser' role, you ensure that all their access requirements are satisfied.

Option A is incorrect because it describes the 'roles/spanner.viewer' role instead of the 'roles/spanner.databaseUser' role. The 'roles/spanner.viewer' role only grants viewing permissions, which means the employees will not have the ability to edit table data.

Option B is also incorrect as it only adds a single user to the 'roles/spanner.databaseUser' role, rather than all three new employees. Though this role is appropriate for the required permissions, it is not efficient to manually add each user one by one.

Option D is incorrect because, similar to Option A, it describes the 'roles/spanner.viewer' role. This role only allows the users to view the table data but does not grant them access to edit the data. Thus, it will not fulfill the complete requirement.

In conclusion, the best course of action is to choose Option C, as it provides the necessary permissions to both view and edit table data in the Cloud Spanner instance for all new employees by utilizing an efficient process.

Solution to Question 6: A

The correct answer is A - Upload the data to Cloud Storage using the gcloud storage command.

Option A is the right choice because Google Cloud Storage is designed to store, access, and manage unstructured data in a variety of formats. It is a highly flexible, scalable, and durable solution that ensures data accessibility across different Google Cloud Services. Additionally, it is completely compatible with Dataflow, which will allow seamless processing of the transformed ETL data.

Option B - Upload the data to Cloud Functions using the gcloud functions deploy command is not appropriate for this scenario. Cloud Functions focus on event-driven applications and triggering code execution in response to specific events. It is not designed to store large volumes of unstructured data or to facilitate Dataflow processing.

Option C - Upload the data to Cloud Run using the gcloud run deploy command is not suitable for this situation. Cloud Run is a service that enables you to run stateless containers without managing the underlying infrastructure. While it is great for deploying and running applications, it is not designed to store and manage large amounts of unstructured data for ETL and Dataflow processing.

Option D - Upload the data into Cloud SQL using the import function in the Google Cloud console is not the right choice because Cloud SQL is a relational

database service that is primarily designed for structured data, unlike the unstructured data mentioned in the question. Furthermore, it is not optimized to serve as a source for ETL transformations and Dataflow processing like Cloud Storage.

Solution to Question 7: D

The correct answer is D. Here's why the other options won't work and why D should be chosen:

A. Pausing billing for the project doesn't deactivate all the configured services. It only stops billing for the project, but the services will still run. To minimize expenses, you need to shut down the services rather than just pausing the billing.

B. Cloud Engineering IAM role is not a predefined role in GCP. Moreover, just disabling APIs for resources doesn't guarantee deactivation of all configured services, as some services might still function partially or generate expenses.

C. The Security Administrator role's primary responsibility is to manage the security of the project assets and resources, not for cost optimization. Revoking access to resources would only limit their usage and not deactivate the services. This doesn't guarantee cost minimization for the GCP services.

D. The correct course of action is to have the Project Owners IAM role, which gives you the necessary permissions to manage a project's resources and cost settings. By shutting down the project using the GCP console and entering the project ID, you will deactivate all configured services in one go, ensuring the most efficient cost optimization. This option is ideal for minimizing GCP service expenses for the department.

Solution to Question 8: B

The correct answer is B: Export your bill to a BigQuery dataset, and then write time window-based SQL queries for analysis. This approach is most suitable for a financial analyst because it allows for efficient and scalable querying of large datasets using a standard SQL syntax. BigQuery is a serverless, highly-scalable, and cost-effective multi-cloud data warehouse designed for business agility. By exporting your Google Cloud Platform service costs to BigQuery, you can leverage its powerful capabilities to analyze and create reports on service cost estimates by service type, daily and monthly, for the upcoming six months.

Here is why the other options will not work effeciently:

Option A: Export your transactions to a local file, and perform analysis with a desktop tool. This approach might work for a small dataset, but it is not well-suited for large and complex datasets. It is often resource-intensive, slow, and may face challenges when dealing with large amounts of data coming from multiple projects within the organization.

Option C: Export your bill to a Cloud Storage bucket, and then import into Firestore for analysis. While Firestore is a powerful NoSQL database, it is de-

signed for real-time data synchronization and not for complex analytical queries with SQL syntax. Using Firestore for this task would likely result in inefficient data processing and lack the standard query syntax your goal requires.

Option D: Export your bill to a Cloud Storage bucket, and then import into Cloud Datastore for analysis. Similar to option C, Cloud Datastore is a NoSQL database and does not support standard SQL syntax for analyzing data. Moreover, it is less suitable for large-scale analytical processing compared to BigQuery. Thus, this option would not allow you to accomplish your goal effectively.

Solution to Question 9: D

The correct answer is D because it provides an efficient and cost-effective way to manage both critical and non-critical components of the application while maintaining the necessary availability.

Option A is not the best choice because using only one node-pool with Preemptible VMs for the entire cluster would make both critical and non-critical components subject to sudden termination, which is not ideal for ensuring the availability of critical components.

Option B is not suitable as it suggests deploying critical deployments on the Spot VM node pool, which can be terminated on short notice due to fluctuating market prices and user demand. This would not ensure the required availability for critical components.

Option C is not appropriate because Shielded VMs are designed primarily for security, focusing on integrity and data protection. This choice does not provide an efficient way to manage costs, as both node pools would use standard VMs, and the additional security features of Shielded VMs would not contribute to the cost-efficiency needs of the non-critical components.

In contrast, option D recommends using both a Spot VM node pool and a node pool with standard VMs. By deploying critical components on the standard VM node pool, it ensures their availability and consistent performance by providing stable VMs. Simultaneously, the non-critical components can be deployed on Spot VM node pools, which are cost-efficient as they utilize unused resources that can be reclaimed when not in high demand. As a result, option D is the most appropriate choice for managing costs and ensuring availability for the different components of the application.

Solution to Question 10: B

The correct answer is B: 1. Create a dedicated Google group in Cloud Identity. 2. Add each data scientist's user account to the group. 3. Assign the BigQuery jobUser role to the group.

Explanation:

Answer B follows the best practice of creating a dedicated Google group in

Cloud Identity, which allows for easier management of users and their access permissions. By adding each data scientist's user account to the group, you centralize access control and efficiently manage permissions as the team structure changes. Assigning the BigQuery jobUser role to the group enables them to run queries, which is the primary requirement for the data science team.

Reasons why other options are not correct:

Option A: This option suggests managing individual users instead of utilizing a dedicated group. This can become inefficient and challenging when dealing with frequent personnel changes. Additionally, it assigns the dataViewer role, which only allows the users to view data but not execute queries.

Option C: Although this option correctly proposes creating a dedicated Google group and adding user accounts, it assigns the BigQuery admin user role. Granting the admin user role would give the data scientists unnecessary permissions that go beyond the scope of their tasks, violating the principle of least privilege.

Option D: Similar to option C, this option appropriately forms a dedicated Google group in Cloud Identity and adds user accounts to the group. However, the BigQuery dataEditor role would grant data scientists access to edit, delete, and insert data, which exceeds the required permissions for performing queries. Therefore, it is not the best course of action for managing the data science team's access.

Solution to Question 11: A

The correct answer is A. Create an alert in Cloud Monitoring to alert when the percentage of high priority CPU utilization reaches 65%. If you exceed this threshold, add nodes to your instance.

Explanation for Answer A: As a database administrator, ensuring optimal query performance is one of your primary responsibilities. By creating an alert in Cloud Monitoring at the 65% high priority CPU utilization threshold, you are taking a proactive approach towards performance monitoring. Once the threshold is exceeded, adding nodes to the Cloud Spanner instance scales horizontally to enhance performance, directly addressing the issue at hand and adhering to Google's best practices.

Reasons why the other options will not work:

Option B: While identifying and optimizing inefficient queries are generally good practices, rewriting queries may not provide immediate results, especially if the root cause of the high CPU usage is traffic growth. Additionally, deploying and testing the optimized queries in a production environment may take time, leaving the system underperforming throughout the process.

Option C: Creating an alert at the 75% CPU utilization threshold is risky. By the time the threshold is reached, the system might be under significant load, leading to reduced performance. Adding nodes at a higher threshold gives lesser

buffer for managing sudden surges in traffic and can result in performance degradation when the system is under stress.

Option D: Increasing the high priority CPU utilization threshold to 85% is not advisable for a rapidly growing tech company. Operating continually near the 85% threshold may cause severe performance issues, as there isn't much room left for handling unexpected traffic growth or temporary spikes in demand. This can result in a sluggish system and poor user experience, which is against Google's best practices for service configuration.

Solution to Question 12: B

The correct answer is B. Use the gcloud iam roles copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination.

Explanation: The goal is to ensure that the Site Reliability Engineers (SREs) in your company have the same project permissions in the acquired company's organization as they do in your own organization. The gcloud iam roles copy command allows you to copy IAM roles within and across organizations, which fits the requirement perfectly. By providing the Organization ID of the startup company's Google Cloud Organization as the destination, you are ensuring that the permissions are transferred appropriately.

Reasons why other options will not work:

A. In the Google Cloud console for your organization, select Create role from selection, and choose destination as the startup company's organization. This option refers to creating a new IAM role using the Google Cloud console, rather than copying an existing role. Additionally, choosing a destination in this method is not supported. You must use the gcloud command-line tool to copy roles across organizations.

C. In the Google Cloud console for your organization, select Create role from selection, and choose destination as the startup company's project in your organization. This option also refers to creating a new IAM role using the Google Cloud console, which is not the requirement. Plus, choosing a project in your organization as the destination will not provide the necessary permissions in the acquired company's organization.

D. Use the gsutil iam copy command, and provide the Organization ID of the startup company's Google Cloud Organization as the destination. This option is incorrect because gsutil is a command-line tool for Google Cloud Storage, not for IAM roles. It cannot be used to manage IAM roles or copy them between organizations.

Solution to Question 13: D

The most appropriate approach to achieve this task of consolidating all GCP costs for both companies onto a single invoice would be option D: Link the acquired company's projects to your company's billing account.

Option D allows for full integration and consolidation of GCP costs and billing. By linking all projects from the acquired company to your company's billing account, both organizations' costs will be combined and billed together on one invoice. This simplifies the process and ensures that starting from tomorrow, your finance team only needs to handle a single invoice to manage all GCP costs.

Option A does not consolidate the costs onto a single invoice. Instead, it only sends notifications about two separate invoices to the finance team. This would provide the team with information on costs, but it doesn't make handling the invoices and payments any easier.

Option B grants your company's billing account access to the acquired company's billing data. While this might give your finance team an overview of the billing data, it does not merge the costs onto a single invoice or streamline the billing process.

Option C suggests creating a custom report in the GCP Console, which shows the combined costs of both companies' GCP projects. However, this would be more of a workaround and manual solution. It does not involve any actual consolidation of the GCP costs on the billing level, and it doesn't automatically generate a single invoice.

In conclusion, option D is the most appropriate approach as it allows for true consolidation and simplification of the billing process, streamlining the finance team's work and enabling them to manage both companies' GCP costs with a single invoice.

Solution to Question 14: B

The correct answer is B - Review the IAM permissions for any role that allows for data access.

Reasoning: The primary task of a security analyst is to determine who has the authorization to view information. In a Google Cloud Project, the Identity and Access Management (IAM) service is responsible for managing access control and defining user roles and permissions. Reviewing the IAM permissions for any role that allows data access will help you determine who has the authorization to view the information within the project.

Why the other options will not work:

A. Enable Data Catalog for data resource mapping: Data Catalog is a service focused on data discovery and metadata management. It does not manage user access and permissions. Enabling it may help you organize and understand your data resources better, but it does not directly solve the problem of identifying who has access to those resources.

C. Check the Access Transparency Logs for unusual activities: Access Transparency Logs provide an audit trail of actions performed on your resources by Google Cloud Support and Engineering. While these logs can help identify

potential security risks and unauthorized access by third parties, they do not directly list user access permissions within your project.

D. Review the Bucket Policy Only settings for your storage buckets: Bucket Policy Only settings, also known as "Uniform Bucket-Level Access," apply to storage buckets within Google Cloud Storage. They govern the management of objects stored within the buckets and who can access them. While reviewing these settings is important for some security use cases, it is insufficient to provide a complete understanding of access authorizations for your entire Google Cloud Project. Focusing only on storage buckets would leave other resources like VMs, databases, and other services out of the scope of your security review.

Solution to Question 15: B

The correct answer should be B, and here's why:

Option B: 1. Create a Cloud Monitoring Workspace and associate your Google Cloud Platform (GCP) project with it. 2. Create a Cloud Monitoring Alerting Policy that uses the threshold as a trigger condition. 3. Configure your email address in the notification channel.

This is the correct option because it utilizes Google's native monitoring services to create an alerting policy that triggers based on a specific threshold (CPU usage exceeding 90% for over 15 minutes). Configuring the email address in the notification channel ensures that an email will be sent whenever the alert is triggered.

Other options will not work for the following reasons:

Option A: This option lacks proper integration with Google Cloud services and relies on a consumer Gmail account. Additionally, it does not provide an efficient or reliable way to monitor the CPU usage on Google Compute Engine instances.

Option C: This option relies on Cloud Logging, which is not designed for monitoring CPU usage and would not be accurate or efficient for tracking this specific metric.

Option D: It overcomplicates the solution by using unnecessary components such as Cloud Functions and Cloud Pub/Sub. Monitoring the CPU usage can be done directly with Cloud Monitoring.

Options E, F, G, and H: These options utilize various Google Cloud services that are not intended for monitoring CPU usage on Compute Engine instances. These solutions do not make use of Cloud Monitoring, which is the most appropriate service for this specific requirement.

In conclusion, option B is the correct choice because it uses Cloud Monitoring to create an Alerting Policy based on specific CPU usage criteria, ensuring that notifications will be sent when the threshold is exceeded.

Solution to Question 16: D

The correct answer is D: Add the user to roles/iam.serviceAccountAdmin role. As an IT manager, you should adhere to the principle of least privilege, which involves providing the minimum level of access necessary to perform a specific job function. The roles/iam.serviceAccountAdmin role offers the exact permissions needed to create and manage service accounts for Google Cloud projects. This role allows the user to create, update, and delete service accounts, as well as create and manage keys. It protects your company's data and ensures that the team member can perform their tasks without any unnecessary access to other resources.

Now let's discuss why the other options are not suitable:

A. Add the user to roles/iam.serviceAccountOperator role - The roles/iam.serviceAccountOperator role allows the user to act as (i.e., impersonate) a service account, but it does not provide the necessary permissions to create and manage service accounts themselves. It is more appropriate when you need somebody to just use the service accounts, but not create or manage them.

B. Add the user to roles/iam.serviceAccountAccessManager role - The roles/iam.serviceAccountAccessManager role is designed to provide permissions to manage service account access control, not to create or manage the service account themselves. It is more relevant for cases where you need someone to control who can access the existing service accounts, but not manage the accounts themselves.

C. Add the user to roles/iam.roleAdmin role - The roles/iam.roleAdmin role allows the user to create, update, and delete custom roles within a project. This role is not specifically tailored to managing service accounts; it gives broader access to all roles within a project, which is unnecessary and goes against the principle of least privilege.

In conclusion, by assigning the user to roles/iam.serviceAccountAdmin role (option D), you will be providing the minimum necessary access for creating and managing service accounts while adhering to the principle of least privilege.

Solution to Question 17: C

The correct answer is C, which involves creating an export in Cloud Logging to filter and export Compute Engine logs directly to the platform-logs dataset in BigQuery.

Option A is not the most cost-effective solution, as it requires the use of Logstash (an open-source, server-side data processing pipeline) to pull logs from Compute Engine and send them to BigQuery. This approach might result in additional costs and higher maintenance, as it requires a separate Logstash setup to manage the log pipeline.

Option B is inefficient and more complicated than necessary, as it requires creating a Cloud Function to be triggered by Cloud Scheduler once a day to execute

the BigQuery job. It's also limited to daily updates, meaning analysis won't be done in real-time.

Option D involves using Dataflow to stream logs from Compute Engine to Cloud Storage and then using the Cloud Storage Transfer Service to move the logs to the platform-logs dataset in BigQuery daily. This solution introduces extra steps and costs (from Cloud Storage and Dataflow usage) that can be avoided by directly exporting the logs from Cloud Logging.

In summary, option C is the most cost-effective and efficient solution for sending logs from the company's Compute Engine instances to the platform-logs dataset in BigQuery for further analysis.

Solution to Question 18: D

The best answer to this question is D, as it best meets the requirements of ensuring optimal isolation between clients' Pods while still running in a single cluster.

D. Create a GKE node pool with a sandbox type configured to gvisor. Add the parameter runtimeClassName: gvisor to the specification of your customers' Pods.

Explanation: gVisor is a container runtime that adds an isolation boundary between the application and the host kernel. In this case, gvisor ensures that there is optimal isolation between different clients' Pods. By creating a GKE node pool with gvisor sandbox and specifying the runtimeClassName parameter in the Pod specifications, you can make sure that each client's Pod will run in an isolated environment.

Reasons why other options will not work:

A. Use Binary Authorization and whitelist only the container images used by your customers' Pods.

Explanation: Binary Authorization is a feature that ensures only verified and authorized container images are deployed within a GKE cluster. While this can be helpful for security purposes, it does not address the need for optimal isolation between clients' Pods.

B. Use Cloud Armor to configure security policies for each customer's Pod.

Explanation: Cloud Armor is designed to protect applications from DDoS attacks and other malicious traffic. Though it is a great tool for securing and controlling access to your applications, it does not address the specific requirement of optimal isolation between the clients' Pods running in a single cluster.

C. Create a separate GKE cluster for each of your customers to run their Pods.

Explanation: Although creating separate GKE clusters for each customer would provide strong isolation between them, it deviates from the requirement of hav-

ing all clients running their Pods in a single cluster. This approach can also lead to increased management overhead and cost inefficiencies.

Solution to Question 19: B

The correct answer is B: Migrate the workload to a Compute Engine VM. Start and stop the instance as needed.

Explanation:

Given the nature of the batch process, which runs for 30 hours and requires a restart if interrupted, you should be looking for a solution that ensures high availability and control over when the process is started or stopped. You also want to minimize costs since it occurs on a monthly basis and can be carried out offline.

Option B meets these requirements. Google Compute Engine VMs offer high availability and a highly customizable environment. With the ability to start and stop the instance as needed, it allows for better control over resource utilization, ensuring the workload is completed without interruption and that you are not incurring unnecessary costs when the process is not running.

Here's why the other options won't work:

Option A - Hosting the workload on a Cloud Storage bucket and using Pub/Sub for event-driven processing isn't suitable in this scenario as it requires a restart upon interruption, and the typical event-driven architecture may lead to significant delays in restarts, resulting in failure to meet deadline or additional costs.

Option C - Migrating the workload to a Google Kubernetes Engine cluster with Preemptible nodes isn't ideal for this scenario. Preemptible nodes are short-lived and only live for a maximum of 24 hours, meaning they will likely be terminated before the 30-hour batch process is completed, causing it to be interrupted and requiring a restart.

Option D - Migrating the workload to a Compute Engine Preemptible VM isn't suitable either. Preemptible VMs are terminated after a maximum of 24 hours, and instances can also be terminated earlier if resources are needed by Google Cloud. This increases the likelihood of an interrupted process, which would require a restart, causing delays and additional costs.

In conclusion, the best course of action is to migrate the workload to a Compute Engine VM and start and stop the instance as needed (Option B) to ensure a smooth transition to the cloud with minimal costs.

Solution to Question 20: C

The correct answer is C: Enable API, create a workspace under project A, and then add projects B and C.

Explanation:

Setting up application performance monitoring requires a solution that allows the team to simultaneously monitor CPU, memory, and disk usage across all projects. Google's Cloud Monitoring, when set up with a workspace, provides a single pane of glass for monitoring and managing multiple Google Cloud projects.

A - While Google Kubernetes Engine (GKE) is great for containerized applications, it doesn't cover the needs of this question. GKE provides a single dashboard for monitoring Kubernetes clusters, but it doesn't help monitor other resources in Google Cloud projects. Therefore, this option is not sufficient for the given scenario.

B - Creating a custom Cloud Functions service would require developing, deploying, and maintaining additional code. This might be a viable solution in some cases but is not necessary as Google Cloud Monitoring already provides the desired functionality out of the box. It would result in a more complex and harder-to-maintain solution than needed.

D - Enabling API and sharing charts from project A, B, and C can help with some visibility, but it doesn't create a single pane of glass for monitoring all resources across the projects. Furthermore, sharing charts doesn't provide the same level of functionality and centralization as a Cloud Monitoring workspace would.

In conclusion, by enabling the API and creating a workspace under project A, and then adding projects B and C, you will have a single pane of glass for simultaneously monitoring CPU, memory, and disk usage across all three projects. This solution leverages the Cloud Monitoring functionality provided by Google Cloud Platform, making it the best option for the given scenario.

Solution to Question 21: C

The correct answer is C: Lift and shift to a VM on Compute Engine. Use an instance schedule to start and stop the instance.

Explanation for C: Given that your company wants minimal effort and cost for migrating the on-premises data analytics set of binaries, lifting and shifting the application to a VM on Google Cloud's Compute Engine is a suitable approach. The VM can be set up to have the required resources to handle the data file sizes, and you can use an instance schedule to automatically start and stop the instance daily at midnight to save costs.

Why A is not suitable: Cloud Functions is not suited for applications that require a long execution time, especially 45 minutes, since they come with a maximum execution timeout. This makes it a poor choice for the scenario mentioned.

Why B is not suitable: AI Platform is designed for machine learning and AI workflows rather than general data processing tasks, making it a less cost-effective

and efficient option for the scenario. Additionally, it involves creating and managing containers, which might not align with the "minimal effort" requirement.

Why D is not suitable: App Engine is more suitable for web applications and microservices rather than data processing tasks, making it a less efficient option for the case. Also, like option B, it entails creating and managing containers, which adds unnecessary complexity to the migration.

Solution to Question 22: C

The correct answer is C, "Configure an HTTP(S) load balancer."

The reason why option C is the best approach is that an HTTP(S) load balancer not only supports HTTPS traffic but also provides SSL termination for the client SSL session. As per Google-recommended practices, using an HTTP(S) load balancer ensures that the appropriate performance, reliability, and security features are implemented.

Here's why the other options are not suitable:

A. Configure an external TCP proxy load balancer: An external TCP proxy load balancer only supports TCP traffic and does not terminate SSL for client sessions. While it may work for load balancing, it does not adhere to the requirement of terminating the client SSL session.

B. Configure an internal TCP load balancer: An internal TCP load balancer is used for balancing traffic within the private network and does not terminate SSL for client sessions. As a public web application requires an externally-facing load balancer, this option is not appropriate.

D. Configure an internal HTTPS load balancer: An internal HTTPS load balancer does not exist in the Google Cloud Platform (GCP) offerings. Load balancers that support HTTPS traffic are either external HTTP(S) load balancers or SSL proxy load balancers; there is no internal version available for this requirement.

In conclusion, to fulfill the task of load balancing an instance group serving a public web application over HTTPS with client SSL session termination, configuring an HTTP(S) load balancer is the appropriate approach, following Google-recommended practices.

Solution to Question 23: C

The correct answer is C: Run gcloud projects list to get the project ID, and then run gcloud services list –project .

Here's why C is correct and other options will not work:

Option A: Running `gcloud config set project my-project` will set the active project to "my-project," but running `gcloud compute networks describe default` will only describe the default network in the project, not

the enabled APIs. This command has nothing to do with listing APIs, so it doesn't solve the task.

Option B: Running `gcloud init` will let you set the current project to "my-project"; however, running `gcloud services list --available` will show you all the available GCP APIs, not the enabled ones for your specific project. Hence, it doesn't help you generate a list of enabled APIs for "my-project."

Option C: This is the correct approach because you first run `gcloud projects list` to get the project ID. Then, with that ID, you run `gcloud services list --project <project ID>` to get a list of enabled Google Cloud Platform APIs for the specific project. This direct command gives you the exact information you're looking for.

Option D: Although you can set the current project to "my-project" with `gcloud init`, running `gcloud services describe my-project` will not list the enabled APIs because `describe` is used for individual API descriptions, not for listing all enabled APIs for a project.

In conclusion, to successfully generate a list of enabled Google Cloud APIs for the "my-project" GCP project, you should proceed with option C by running `gcloud projects list` to find the project ID and `gcloud services list --project <project ID>` to get the enabled APIs list.

Solution to Question 24: C

The correct answer is C. This is because creating two configurations using gcloud config provides the ability to define settings, such as project properties, separately for production and development projects. You can then easily switch between configurations as needed. Writing a script to activate the configurations individually and using gcloud compute instances list to query all compute resources for each project will provide a daily list of instances.

Option A is incorrect, as the primary function of the Stackdriver Logging Agent is to collect and transfer logs, not to provide a list of compute instances. Although log exports can be useful for monitoring resource usage and other pertinent information, they are not designed to provide a daily inventory of compute resources.

Option B is also incorrect because Cloud Shell is an interactive shell environment in a web browser and is not designed for automated processes. While exporting information to Cloud Storage is an option, automating it via Cloud Shell is not the appropriate method for this task.

Option D is not entirely correct because Cloud Functions are typically used for lightweight and event-driven tasks. While using Cloud Scheduler to trigger a Cloud Function to run daily is possible, it does not provide an efficient way of managing and aggregating the information from both the production and development projects. Thus, option C is the most suitable solution for this task.

Solution to Question 25: C

The most appropriate action to take in this situation is option C: Change the billing account of your projects to the billing account of your company.

Option C is the correct answer because it directly addresses the problem of expenses on personal credit card and the company reimbursement process. By changing the billing account of your projects to the company's billing account, you would effectively move the payment responsibility from your personal account to the company. This streamlines the process by eliminating the need for reimbursement and ensures accurate tracking of expenses for the finance department.

Option A is incorrect because Google Cloud Pub/Sub is a messaging service used for real-time as well as asynchronous messaging between components of your applications. While it could potentially be used for sending billing notifications, it does not address the issue of moving charges from your personal credit card to the company's billing account.

Option B is not suitable because generating a billing report and emailing it to the finance department merely provides them with the information related to the expenses incurred, but it does not resolve the underlying payment responsibility issue. You would still be using your personal credit card and the company would have to reimburse you.

Option D is not the best solution because creating a separate Google Cloud account for the company and manually transferring your projects would be a cumbersome process. Not only it may pose the risk of errors during the transfer, but it also adds unnecessary complexity and overhead. Instead, simply updating the billing account associated with your existing projects would be a more efficient and direct approach while keeping all the project configurations intact.

Solution to Question 26: C

The correct answer is C. Install the cloud-datastore-emulator component using the gcloud components install command.

Explanation:

As a software engineer, it is crucial to test your applications locally before deploying them in a real environment, as it allows you to catch and fix any bugs or issues before they affect users. In this scenario, you need to emulate the application's interaction with Cloud Datastore locally on your developer laptop.

Option C is the best choice because it allows you to install the cloud-datastore-emulator, a tool specifically designed to replicate Cloud Datastore's functionality locally. This enables you to perform tests accurately and effectively, without needing to access the actual Cloud Datastore in a live environment.

Option A is not the right choice because it suggests using the gcloud datastore

export command followed by importing the data to your local Datastore. Although it would help you have the data locally, it doesn't create the emulated environment necessary for proper testing.

Option B proposes setting up a Firebase Realtime Database to use it instead of Cloud Datastore. While both are related to data storage, they are different products with distinct use cases. Firebase Realtime Database is designed for real-time applications and provides synchronization across devices, whereas Cloud Datastore is optimized for more general data storage needs. Replacing Cloud Datastore with Firebase Realtime Database might not be suitable for your application's requirements and would not accurately emulate the Cloud Datastore behavior.

Option D is not the correct answer because exporting Cloud Datastore data using gcloud datastore export does not provide you with a local environment to test your application. It simply exports your data from the live Cloud Datastore, but it doesn't create an emulator for local testing.

In conclusion, the best approach for your scenario is to install the cloud-datastore-emulator component using the gcloud components install command, as suggested in Option C. This provides you with an accurate emulation of Cloud Datastore, allowing you to test your application effectively on your local developer laptop.

Solution to Question 27: C

The correct answer is C, and here's why:

In this scenario, you are required to manage the creation of instances, set up firewalls, and store data in Cloud Storage while following Google-recommended practices. In order to achieve this, you should enable the necessary APIs before performing these tasks on the Google Cloud platform.

Option C states that you should use the gcloud services enable compute.googleapis.com command to enable Compute Engine and the gcloud services enable storage-api.googleapis.com command to enable the Cloud Storage APIs. Following this approach allows you to properly enable the required APIs, which is the recommended practice by Google. This ensures that you can effectively manage instances, firewalls, and storage according to Google guidelines.

Options A and B do not follow Google-recommended practices, as they suggest operating without enabling the necessary APIs. By not enabling APIs, you may encounter issues or limitations while working with instances, firewalls, and Cloud Storage.

Option D recommends using the gsutil cp command to interact with Cloud Storage without enabling the storage-api.googleapis.com API first. This is also not a good approach, as attempting to interact with Cloud Storage without

enabling the appropriate API may cause unexpected errors or limitations during your project.

In summary, the appropriate course of action for managing instances, firewalls, and storage in a Google Cloud project while adhering to Google-recommended practices is to enable Compute Engine and Cloud Storage APIs using the gcloud services enable commands provided in option C. This ensures a proper setup that allows you to effectively work with the required resources.

Solution to Question 28: B

The correct answer is B. Create a node pool with compute-optimized machine type nodes for the image rendering microservice. Use the node pool with general-purpose machine type nodes for the other microservices.

Explanation:

The image rendering microservice requires more CPU time relative to memory, and the other microservices are optimized for n1-standard machine types (general-purpose machine types). By creating a separate node pool with compute-optimized machine type nodes for the image rendering microservice, it allows the microservice to efficiently utilize the available CPU resources to perform its tasks. The general-purpose machine type nodes can be used for the other microservices as they are optimized for those types of workloads.

Option A is not an efficient solution because increasing the number of replicas for the image rendering microservice without changing machine types will not address the underlying CPU resource constraint. This may lead to underutilization of resources and can increase costs.

Option C is not optimal as it suggests disabling autoscaling for the entire cluster, which would limit the ability to dynamically allocate resources based on workload demands. Allocating fixed resources to the image rendering microservice might lead to wasted resources when that microservice is not actively processing images.

Option D is not suitable because using memory-optimized machine type nodes for the image rendering microservice would not provide the needed CPU resources as they are optimized for memory-intensive workloads, not CPU-intensive tasks. On the other hand, compute-optimized machine type nodes for the other microservices could lead to unnecessary cost increases and inefficient resource utilization since they are optimized for n1-standard machine types.

In conclusion, answer B is the most efficient and cost-effective method for optimizing the Kubernetes Engine cluster considering the given workloads. It ensures that each microservice has access to the appropriate resources based on their specific requirements.

Solution to Question 29: A

The correct answer is A: Set up a policy that uses Standard storage for 30 days and then moves to Archive storage for three years.

Reasoning for answer A: This option best aligns with the team's usage pattern and the company's objective to minimize storage costs. In this configuration, the team can work efficiently with the objects in Standard storage for the first 30 days when they are frequently accessed. After 30 days, the objects move to Archive storage, which provides the lowest storage cost for long-term data retention. This choice ensures that the objects are stored for the required three years and minimizes the overall cost for the company.

Reasoning for other options:

B. This option is not the ideal choice as there are unnecessary transitions between Coldline and Nearline storages. The objects are rarely accessed after 30 days, so they can be transitioned directly to Archive storage which offers the lowest storage cost for long-term storage.

C. This option is not suitable as it involves moving to Coldline storage after 30 days and then transitioning to Archive storage after two years. It would be more cost-effective to move the objects directly to Archive storage after 30 days, as they are rarely accessed. Coldline storage has a higher cost per gigabyte compared to Archive storage.

D. This option is also not appropriate because Nearline storage is more expensive than Standard storage, and Coldline storage is costlier than Archive storage. In this case, the company would be paying extra for both the frequently accessed and the infrequently accessed storage periods, which is not a cost-effective solution given the usage pattern and storage requirements.

Solution to Question 30: A

The correct answer is A. Create a new Node Pool and specify machine type n2-highmem-16. Deploy the new pods.

Explanation:

Option A: Creating a new Node Pool with the n2-highmem-16 machine type allows you to add a new set of nodes specifically with the resources required by the additional pods. Deploying the new pods on this Node Pool ensures that the existing application running on the n1-standard-2 nodes is not affected, permitting seamless scaling without causing downtime.

Option B: Creating a new Deployment with a nodeSelector specifying n2-highmem-16 nodes would not work because, in this scenario, the GKE cluster does not currently have any n2-highmem-16 nodes. Thus, the new pods will not be deployed, and the scaling requirement will not be met.

Option C: Using Kubernetes horizontal pod autoscaling does not resolve the issue because it focuses on adding or removing pods based on a specific metric, such as CPU usage or memory consumption. It doesn't handle the deployment

of new pods on specific machine types. Furthermore, you cannot specify a machine type during deployment, as this is a GKE feature, not a Kubernetes one.

Option D: Creating a new Cluster Autoscaler with n2-highmem-16 nodes does not directly address the scaling requirement, as it deals with automatically adjusting the size of the node pool based on the current resource needs of all the pods. Though it may eventually add nodes of the desired type, doing so is not a direct, immediate solution, and it may take time to scale out depending on the configured options. Additionally, it does not ensure a separate pool for the new pods, which could still cause an impact on the existing application without proper isolation.

Solution to Question 31: D

The correct answer is D - When creating the VM, use machine type n1-standard-96.

Explanation:

The question states that the application requires 96 vCPUs and needs to operate in a similar environment as the current on-premises setup. The only option that guarantees 96 vCPUs is D, which suggests using a machine type of n1-standard-96. Selecting this machine type in the VM creation process ensures the application will have the necessary resources in the Google Cloud Platform environment.

Reasons why other options will not work:

A. Start the VM using Compute Engine default settings, and adjust as you go based on Rightsizing Recommendations:

This approach doesn't guarantee the application will have 96 vCPUs from the beginning, as the default settings may have a lower amount of vCPUs. Moreover, adjusting based on Rightsizing Recommendations will require time and monitoring, which could lead to performance issues or downtime if the application lacks the necessary resources.

B. Adjust the VM's vCPU configuration after its creation using the GCP Console:

Adjusting the vCPU configuration after the VM is created might result in VM downtime as resizing a VM instance requires the VM to be stopped. Also, there's no guarantee that the initial vCPU configuration will provide the required 96 vCPUs, which could impact the application's performance.

C. Use App Engine Standard Environment to host the application:

App Engine Standard Environment isn't suitable for an application that requires 96 vCPUs because it is designed for smaller applications with automatic scaling. For large-scale applications that need specific resource requirements, using Google Compute Engine with custom VM configurations is more appropriate.

Solution to Question 32: D

The correct answer is D. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

Explanation:

Option A is incorrect because creating an OAuth2.0 client ID and storing the client secret in a file requires additional modifications to the application and goes against Google's recommended practices for authentication on a Compute Engine VM. Instead, Google suggests using Application Default Credentials, which simplifies the process and provides better security for your application.

Option B is incorrect as it involves storing credentials in a config file and deploying it with the application. This creates a risk of exposing the credentials, leading to potential security issues. Storing credentials this way is also not recommended as it doesn't follow Google's best practices.

Option C is incorrect as creating a new Google account and using its credentials in a Compute Engine VM goes against best practices. Instead of creating a new Google account, it is recommended to use service accounts with specific roles and permissions for use with Google services in a Compute Engine VM instance.

Option D is the best solution because it involves minimal modifications to the application and follows Google's recommended practices. Assigning the appropriate access for Google services to the service account used by the Compute Engine VM allows the application to use Application Default Credentials, which would automatically detect and authenticate your application running on the VM. This approach maintains both simplicity and security in the authentication process, while ensuring that the application builds on the pre-existing authentication setup on the personal laptop.

Solution to Question 33: C

The correct answer is C, and here's why:

Option C: • Navigate to the Audit Logs page in the Google Cloud console, and enable Data Read, Data Write, and Admin Read logs for the Bigtable instance. • Create a Pub/Sub topic as a Cloud Logging sink destination, and add your SIEM as a subscriber to the topic.

By choosing option C, you can achieve your task of logging read or write operations, metadata, and configuration read operations for the Bigtable instance. The Audit Logs in Google Cloud will handle these logging requirements, and enabling Data Read, Data Write, and Admin Read logs ensures that all relevant activity is logged. Using a Pub/Sub topic as a Cloud Logging sink destination guarantees the real-time and reliable transfer of data to the SIEM system, making it the best choice to accomplish the goal.

Here's why the other options don't work:

Option A: Use Stackdriver to create a custom dashboard to monitor the Bigtable instance and send alerts to your SIEM system.

Stackdriver, now known as Cloud Monitoring, is suitable for monitoring metrics and performance data. However, it doesn't provide the required granular audit logging for storing personally identifiable information (PII) data in the SIEM system. Thus, this option isn't efficient for this task.

Option B: • Navigate to Cloud Monitoring in the Google Cloud console and create a custom monitoring job for the Bigtable instance to track all changes. • Create an alert by using webhook endpoints, with the SIEM endpoint as a receiver.

Similar to Option A, Option B also relies on Cloud Monitoring, which doesn't offer the detailed audit logging required for PII data storage. While webhook alerts help monitor the Bigtable metrics, they can't provide the granularity of data needed for your company's Security Information and Event Management system.

Option D: • Navigate to the Audit Logs page in the Google Cloud console, and enable Admin Write logs for the Bigtable instance. • Create a Cloud Functions instance to export logs from Cloud Logging to your SIEM.

This option is inadequate because enabling just the Admin Write logs won't provide full coverage of read or write operations and metadata and configuration read operations needed for PII data. Also, using Cloud Functions for exporting logs adds complexity and is less efficient compared to the Pub/Sub method provided in option C.

In conclusion, option C is the best choice for accomplishing the task of logging read or write operations, metadata, and configuration read operations within your company's Security Information and Event Management system.

Solution to Question 34: D

The correct answer is D. Storage Admin.

Explanation: As a team lead managing a Google Cloud Platform (GCP) project, you may need to delegate access to team members so that they can efficiently manage your company's buckets and files within Cloud Storage. To do this, you must assign them the appropriate IAM roles that follow Google's recommended practices.

D. Storage Admin: This IAM role is the most suitable for your purpose, as it allows your team members to have the necessary permissions to manage buckets and files within Cloud Storage. Storage Admins can create, delete, set up access controls, configure bucket lifecycle and versioning policies, add and remove labels, and manage objects within the databases. This role will provide a comprehensive level of access to fulfill their responsibilities while maintaining control over data management.

Other options:

A. Storage Object Creator: This IAM role allows users to create objects within a bucket, but it does not provide permissions for deleting objects or managing buckets. Thus, it would not be sufficient for team members to efficiently manage your Cloud Storage.

B. Cloud Functions Admin: This IAM role allows users to manage Google Cloud Function resources. However, it is unrelated to Cloud Storage bucket and file management. Therefore, it would not be suitable for your team members to manage your Cloud Storage.

C. Storage Object Admin: This IAM role grants permissions to read, create, and delete objects within a bucket, but it does not include permissions for managing bucket configurations, such as setting up access controls, configuring bucket lifecycle and versioning policies, and managing object metadata. Although this role permits data management to some extent, it falls short of the comprehensive access that the Storage Admin role provides.

In conclusion, the best IAM role for your colleagues to manage your Cloud Storage efficiently would be Storage Admin, ensuring that they have all necessary permissions without compromising control over the data.

Solution to Question 35: A

The correct answer is A: Create one A record to point mydomain.com to the load balancer, and create two CNAME records to point WWW and HOME to mydomain.com respectively.

An A (Address) record is used to map a domain to the IP address of the server. In this case, the question asks you to point home.mydomain.com, mydomain.com, and www.mydomain.com to the IP address of the Google Cloud load balancer. Thus, creating one A record for mydomain.com and pointing it to the load balancer is the right approach.

After creating the A record for mydomain.com, you can point the subdomains (home and www) to it by creating two CNAME (Canonical Name) records. CNAME records are used to map aliases or subdomains of a domain to the canonical domain. In this case, by creating CNAME records for WWW and HOME and pointing them to mydomain.com, you establish an alias relationship between the subdomains and the primary domain, which is directed to the load balancer.

The other options are not suitable because:

B. NS (Name Server) records are used to delegate a domain or subdomain to a specific set of DNS servers. This configuration is not required in this scenario, as you only need to map the domain and subdomains to the load balancer's IP address.

C. AAAA records are used to map a domain to anIPv6 address, whereas the

question asks you to map the domain and subdomains to the IP address of the Google Cloud load balancer, which is more likely an IPv4 address.

D. SOA (Start of Authority) records contain administrative information about the domain, such as primary name server and email address of the responsible party. Creating an SOA record to point the domain to the load balancer is not the correct approach as SOA records are not used for mapping domains to IP addresses.

Solution to Question 36: B

The correct answer is B, and here's why:

An external HTTP(S) load balancer with a managed SSL certificate is essential to distribute the load among the backend compute instances effectively. It can process high amounts of user traffic, ensuring the website remains accessible and performs well. Having a managed SSL certificate also ensures the site is secure for users.

The URL map that targets the requests for static content to the Cloud Storage backend is crucial in this scenario. It will make static content, like images or scripts, readily available from Cloud Storage and offload the work from the compute instances. This setup will improve the website's performance and reduce the load on the backend servers.

Option A is not suitable because an external network load balancer is not designed to manage HTTP(S) traffic and does not offer the same level of flexibility and features as an HTTP(S) load balancer.

Option C is not optimal because Cloud Functions and Firebase Hosting are meant for serving dynamic content and not dedicated to handling autoscaling of compute instances based on CPU load with Cloud Storage integration.

Option D is not the best choice because the integration of Cloud Pub/Sub is unnecessary for distributing requests for static content to Cloud Storage. The URL map in the external HTTP(S) load balancer is sufficient to accomplish this task without adding complexity to the architecture.

Therefore, Option B, which utilizes an external HTTP(S) load balancer with a managed SSL certificate and a URL map for Cloud Storage backend, is the ideal solution for the given scenario.

Solution to Question 37: A

The correct answer to this question is option A, and here's why:

A. In option A, we create an internal LoadBalancer service in GKE with the necessary annotation (cloud.google.com/load-balancer-type: Internal) to ensure that it is not exposed to the internet. This LoadBalancer service allows the Compute Engine instance to reach the GKE application, as it balances traffic among the Pods' backend. By peering the two VPCs, we establish a direct connection between the networks for both the Compute Engine instance and the

GKE cluster, maintaining network security. Finally, we configure the Compute Engine instance to use the load balancer's address to access the GKE application. This approach is optimal because it minimizes the effort and maintains a secure and direct connection within the VPCs.

B. Option B is incorrect as it does not address the issue of connecting separate VPCs. The service that would be created would be an external LoadBalancer, which is unnecessary for our use case, as we aim to keep the connection internal to the VPCs.

C. Option C involves setting up a VPN between the two VPCs. Although this does establish a connection between them, it adds unnecessary complexity and overhead to the solution, as VPC peering from option A is simpler and more efficient.

D. Option D uses a ClusterIP service, which is not accessible outside of the GKE cluster. Even after peering the VPCs, the Compute Engine instance wouldn't be able to access the GKE application since ClusterIP is only reachable within the cluster. A LoadBalancer service (as in option A) is required to expose the application correctly.

In conclusion, option A is the most suitable course of action, as it provides a secure and direct connection between the Compute Engine instance and the GKE application while minimizing the effort involved.

Solution to Question 38: C

The correct answer is C. Verify that you are the project billing administrator. Select the associated billing account and create a budget and alert for the appropriate project.

The reason this is the best option is that you first need to have the project billing administrator role to manage budgets for specific projects. Once you have verified your role, you can then create a budget and set alerts specifically for the Compute Engineer services' usage in that project. This ensures that you're managing the budget at the level of usage you want, providing better visibility and control.

Option A is incorrect because having owner role at the organization level doesn't necessarily require that you manage budgets for individual projects. Roles should be assigned based on the specific responsibilities they carry, in this case, the project billing administrator.

Option B is incorrect because it only suggests creating a budget for Compute Engine services, without setting up an alert. Setting up a budget without alerts will not help monitor and control usage effectively, potentially missing overruns and unexpected costs.

Option D is incorrect because being a project administrator does not give you the necessary permissions to manage the billing account. Project administrators

manage the overall project configurations, not the billing-related tasks. Moreover, just creating a budget with padding for potential overruns is not enough – setting alerts will help ensure you are notified when the budget is approaching its limit or if any unexpected costs arise.

Solution to Question 39: D

The correct answer is D: Create a custom Compute Engine image from a snapshot. Create your instances from that image. This is the most efficient way to create and maintain a copy of a custom Compute Engine virtual machine because it allows for the creation and scaling of instances using a custom source image based on the snapshot.

Here is why other options will not work:

A. Creating a Google Kubernetes Engine (GKE) cluster from your base VM does not address the problem of creating a copy of your VM to handle increased traffic. GKE is a managed container orchestration solution and specifically designed for deploying, scaling, and managing containerized applications rather than virtual machines.

B. Creating a custom Compute Engine image from a snapshot is a good start, but creating instances from a Cloud Storage bucket is not the recommended practice. This method is much less efficient in managing and scaling instances as it relies on fetching the source from a bucket, rather than having a dedicated image readily available for instance creation.

C. Creating a custom Compute Engine image from your base VM seems like a viable option, but it does not provide the same level of data consistency as creating an image from a snapshot. Snapshots capture a point-in-time state of the VM, ensuring data consistency; therefore, creating a custom image from a snapshot is a more reliable approach to handle increased application traffic.

Solution to Question 40: D

The correct answer should be D because it is necessary to authenticate the gcloud CLI with your Google Cloud Platform (GCP) credentials before performing any operations, such as listing compute instances. It ensures that you have the required permissions to access and manage resources within your organization's GCP project.

D. Run gcloud auth login, enter your login credentials in the dialog window, and paste the received login token to gcloud CLI: This step authenticates your CLI session and associates it with your GCP account. It is a necessary step because it enables the gcloud CLI to access resources within your project based on your permissions. Without this authentication, the gcloud CLI would not have access to your organization's GCP resources.

The other options are not necessary or relevant in this situation:

A. Run gcloud compute instances create to create a new instance before listing

existing instances: This step is not required because you can list existing instances without creating a new one. Creating a new instance is not related to viewing the list of existing instances.

B. Run gcloud config set compute/zone $my_zone to set the default zone for gcloud CLI: Setting the default zone is not required before listing instances because you can view all the instances across all zones for a project. Setting the default zone is only useful when you want to interact with resources within a specific zone frequently.

C. Install the Google Cloud SDK for Python to use the gcloud CLI: Since you have already set up the Google Cloud CLI on your work laptop, installing the Google Cloud SDK for Python is not necessary. The gcloud CLI is part of the Google Cloud SDK, and once it is installed, you don't need additional SDKs or libraries to use it.

Solution to Question 41: A

The correct answer is A. Stop the VM, increase the memory to 8 GB, and start the VM.

Explanation for why A is the correct answer: The issue mentioned in the question is related to memory, and not the number of vCPUs or the size of the boot disk. The virtual machine is consistently running out of memory, which means it needs more memory to function efficiently. To upgrade the memory of a virtual machine, you need to stop the VM first, then increase its memory, and finally start the VM again. This process allows the virtual machine to recognize the new memory configuration and utilize the increased memory space.

Reasons why other options will not work:

B. Enable Datastore mode for automatic memory allocation. Datastore mode is related to storage, not memory. Datastore mode can be useful for automatic storage allocation, but it cannot solve the problem of a virtual machine running out of memory.

C. Resize the boot disk to 8 GB and restart the VM. Resizing the boot disk will increase the available storage space, not the memory. The issue mentioned in the question is related to memory and not storage, so resizing the boot disk will not resolve the problem.

D. Enable autoscaling to increase the memory automatically. Autoscaling is used to automatically scale the number of instances or virtual machines in a cloud environment based on demand. It is not used for increasing the memory of a specific virtual machine. Moreover, enabling autoscaling could lead to additional costs and complexity in managing the environment but would not solve the issue of the virtual machine running out of memory.

Solution to Question 42: C

The correct answer is C. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool.

Here's why C is the best choice and why the other options don't work:

A. Use Google App Engine instead of GKE to automatically scale the application. Although Google App Engine (GAE) provides automatic scaling, it's not based on the Kubernetes architecture and does not support deploying microservices on Google Kubernetes Engine. The requirements clearly state the need for deploying microservices on GKE, so this option does not fit the project's needs.

B. Use Google Cloud Run instead of GKE and create multiple replicas of the application to provide automatic scaling. Google Cloud Run is a serverless environment for containerized applications, and although it provides automatic scaling, it's not designed to work directly with GKE. Additionally, switching to Cloud Run would require changes to how the application is deployed and managed, whereas the required solution is to use GKE and manage scaling within that environment.

C. Create a GKE cluster with autoscaling enabled on the node pool. Set a minimum and maximum for the size of the node pool. This option is the correct choice because it addresses the requirements of deploying the microservices application on GKE and allows the cluster to scale without manual intervention. By enabling autoscaling on the node pool, additional nodes will be added or removed automatically as required, based on the minimum and maximum size configurations. This approach keeps the cluster size optimized and accommodates future growth as more applications are deployed.

D. Deploy the application on GKE, and add a HorizontalPodAutoscaler to the deployment. Adding a HorizontalPodAutoscaler to the deployment would only handle the scaling of pods within the existing cluster, but it wouldn't handle the scaling of the actual GKE cluster itself. This means that as more applications are deployed, manual intervention would still be required to manage and scale the cluster to accommodate the increased workload. Hence, this option doesn't fulfill the requirement of automatically scaling the GKE cluster as the application grows.

Solution to Question 43: A

The correct answer is A, "Use the projects.move method to move the project to your organization. Update the billing account of the project to that of your organization."

Here is the explanation for why this answer is correct and why the other options will not work:

A. Moving the project to your organization using the projects.move method is the most efficient way of transferring the smaller company's Google Cloud project. Once in your organization, you can easily update the billing account

to ensure it is billed to your company. This method requires minimal effort and directly addresses the task at hand.

B. Option B is not the best solution because taking snapshots of Compute Engine virtual machines and deploying them in your organization's project only addresses the virtual machines aspect of the IT systems. It does not cover other components such as databases, application services, and storage, nor does it address the billing redirection to your company. This approach requires more effort and does not achieve the primary goal.

C. Option C focuses on Google Cloud Storage Service Account Keys, which is only a small part of the entire IT systems. Sharing these keys and granting permissions in the new organization does not move the project or ensure billing redirection. Additionally, this option increases the risk of exposing sensitive data and may lead to security-related issues.

D. Creating a VPC Network Peering between the two projects in option D does not solve the problem. This approach only establishes a network connection between the two projects but does not merge the IT systems or redirect the billing to your organization. Configuring Billing Export will only share the billing data between the projects without changing the billing responsibility.

In summary, option A is the best course of action because it directly moves the smaller company's project into your corporation's organization, allowing you to update the billing account efficiently while ensuring minimal effort. The other options do not address the primary goal and would require more work without achieving the desired outcome.

Solution to Question 44: D

The correct answer is option D: Create an instance template for the instances. Set the 'Automatic Restart' to on. Set the 'On-host maintenance' to Migrate VM instance. Add the instance template to an instance group.

Explanation:

Option A suggests creating an instance group and attaching a Persistent Disk to an instance template. However, it does not mention setting the 'Automatic Restart' feature. This is crucial for ensuring that instances will restart if they crash, which is required for high availability.

Option B suggests setting the 'Automatic Restart' to off. Disabling this feature would mean that instances will not automatically restart if they crash, affecting the availability of the instances during maintenance or system errors.

Option C has a similar problem as option B, where it suggests disabling the 'Automatic Restart' feature. Additionally, this option sets 'On-host maintenance' to Terminate VM instances, which can affect the availability of instances during maintenance.

Option D is the best choice because it creates an instance template and configures the instances to automatically restart if they crash, ensuring high availability. Furthermore, it sets 'On-host maintenance' to Migrate VM instance, which allows the instances to be migrated to another host during maintenance, ensuring that they remain available during system maintenance. Finally, adding the instance template to an instance group enables the IT manager to manage and scale the instances more easily.

Solution to Question 45: C

The optimal answer is C: Create external tables in BigQuery that point to Cloud Storage buckets and run a SQL query on these external tables to complete your request.

The reason for choosing this option is because BigQuery is a fully managed, serverless and cost-effective data warehouse that is designed to help data analysts run SQL queries on large datasets. In addition, BigQuery allows you to create external tables pointing to data stored in Cloud Storage buckets, which means you don't have to copy or move the AVRO file, making the process faster overall. Thus, choosing BigQuery as the solution perfectly caters to the analysts' proficiency in SQL and the company's need for a quick and affordable solution.

The other options are not ideal for the following reasons:

A. Creating a Hadoop cluster and performing the steps mentioned in Option A is not only time-consuming, but it is also not cost-effective. Besides, configuring and managing a Hadoop cluster adds additional complexity that is unnecessary, considering the simpler and more effective solution provided by BigQuery without involving clusters or copying the file.

B. Option B suggests creating a Cloud Dataproc cluster and then storing results in a Cloud Spanner database. Although Cloud Dataproc is a managed Hadoop and Spark service, it requires more processing steps and is more expensive due to the creation of an additional cluster and the use of Cloud Spanner, a globally scalable and highly available database service. BigQuery, on the other hand, offers a more straightforward and efficient solution.

D. Using Cloud Dataflow to read the AVRO file and write data into Cloud Firestore poses similar disadvantages as the other options mentioned. Cloud Firestore is primarily a NoSQL database designed for real-time updates, and cannot natively support SQL queries. While it might be possible to configure the system to adapt to SQL queries, your data analysts might face difficulties compared to the simpler and more efficient solution provided by BigQuery. Additionally, the processing and writing involved in this option makes it slower and less cost-effective.

Solution to Question 46: D

Answer: D. Deploy a new version of your application in App Engine. Then go to App Engine settings in GCP Console and split traffic between the current

version and newly deployed versions accordingly.

Explanation: The best approach for achieving the goal of testing the new version with only 1% of users before transitioning the entire application to the new version is option D.

Option D is the correct answer because deploying a new version of your application in App Engine and then using GCP (Google Cloud Platform) Console to split traffic between the current version and the newly deployed version is in line with the requirements and utilizes the built-in features of App Engine. This approach avoids the need for additional resources, ensures proper scaling, and keeps the deployment process simple and efficient.

Option A is an incorrect approach because creating a new network in VPC (Virtual Private Cloud) requires additional resources and does not relate to the App Engine environment. Moreover, splitting traffic will not be as straightforward as in option D.

Option B is not the best approach either because deploying the new version of your application in a separate project within App Engine will make it harder to manage and track updates between the projects. Transitioning the application to the new version may not be seamless, and traffic-splitting becomes more complex than in option D.

Option C is incorrect because deploying a new version of your application in Cloud Functions will not be suitable for an application hosted in an App Engine environment. Cloud Functions is designed for small, single-purpose functions. Besides, the traffic-splitting feature is not applicable to Cloud Functions since it's specific to App Engine.

In conclusion, option D is the best approach to achieve the goal of testing the new version with a limited number of users before transitioning the entire application to the new version. It is efficient, easy to manage, and takes advantage of the built-in capabilities of App Engine.

Solution to Question 47: B

The most appropriate choice for this task is B. Cloud SQL, and here is the explanation for why other options will not work:

B. Cloud SQL: Cloud SQL is a managed relational database service that runs fully managed versions of MySQL, PostgreSQL, and SQL Server databases. Since the company's internal application was initially implemented in PostgreSQL and requires strong consistency, fast queries, and ACID guarantees for multi-table transactional updates, Cloud SQL is an excellent fit. Moving to Cloud SQL for PostgreSQL would require minimal code changes, and it would satisfy all the requirements of the application. Thus, Cloud SQL is the most appropriate choice for this task.

A. Firestore: Firestore is a NoSQL document database designed for scalable, real-time applications. However, it is not ideal for this scenario as it doesn't

provide ACID guarantees for multi-table transactional updates. Also, transitioning from a relational database (PostgreSQL) to a NoSQL database could require significant code changes, which is not the goal in this case. Hence, Firestore is not the best choice.

C. Cloud Spanner: Cloud Spanner is a globally distributed, horizontally scalable relational database service, but it is often overkill for smaller applications that do not require such scalability. While it is designed to provide strong consistency and ACID guarantees, transitioning to Cloud Spanner from PostgreSQL can be more involved than just switching to Cloud SQL, making it more complicated and expensive than necessary for the given use case.

D. Datastream: Datastream is a real-time data change capture and replication service, not a database itself. It is primarily used for streaming data between databases and other services for real-time analytics and event-driven architectures. In this scenario, the company needs a database to manage transactional orders. Datastream doesn't fulfill this requirement, making it a non-viable option.

In conclusion, B. Cloud SQL is the best choice for the company's internal application as it supports the original PostgreSQL implementation, provides strong consistency, fast queries, minimal code changes, and ACID guarantees for multi-table transactional updates.

Solution to Question 48: C

The correct answer is C. Create another project with the ID acme-marketing-data-digest for the Marketing team and deploy the resources there.

Explanation:

Option A is incorrect because Cloud Composer is primarily used for building, scheduling, and monitoring data processing workflows, rather than organizing resources. While you could use Cloud Composer to transfer data, it doesn't address the need for a separate organization for the Marketing team's resources.

Option B is incorrect because creating a separate organization is not necessary in this scenario. Organizations in Google Cloud represent high-level containers for projects, and are usually more helpful for grouping multiple projects under the same company and enforcing consistent policies. In this case, we only need to create a separate project for the Marketing team, not an entire organization.

Option C is the correct answer because creating another project with a different ID (acme-marketing-data-digest) allows you to separate the resources for each team, while still maintaining a link to the original project's structure and resources. This ensures the Marketing team's resources are organized separately from the Sales team, as required.

Option D is incorrect because cloning the acme-data-digest project and renaming it to acme-marketing-data-digest might create conflicts or confusion, especially if any dependencies or linked resources are associated with the original

project. Instead, creating a new project ensures that the two teams' resources are separately managed and prevents any unintended consequences of duplicating a project. Additionally, simply granting the Marketing team access to the cloned project does not address the need for separated resource organization.

Solution to Question 49: A

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

Option A is the best choice as it gives the finance team the ability to link projects to the billing account without providing them with the ability to make other changes to the project. The Billing Account User role allows users to view the billing account and perform necessary tasks, while the Project Billing Manager role allows users to link projects to the billing account.

Option B is incorrect because the Compute Network User role only allows users to manage networking resources like firewalls and routers. This role does not enable the finance team to manage billing or link projects to the billing account.

Option C is not appropriate because assigning the engineering team the Billing Account User role on the billing account and the Project Billing Manager role on the organization would give the engineering team the permissions to manage billing, which is exactly what you are trying to prevent.

Option D is also incorrect, as giving the finance team the Project Owner role on the organization grants them much broader permissions to manage projects and resources, exceeding the scope of tasks that must be limited to linking projects to the billing account. The Project Owner role would give the finance team permissions to change various settings and configurations, which is not the intended purpose in this scenario.

Solution to Question 50: B

The correct answer is option B: Create the instance without a public IP address.

Explanation: By creating the Compute Engine instance without a public IP address, you ensure that it is not accessible from the public internet. This guarantees that no traffic intended for achieving the instance can be routed to it via the internet. Instead, traffic to the instance will only be possible through the VPC, further secured by the VPN connection.

Why the other options are incorrect:

Option A: Create a firewall rule to only allow traffic from Google Cloud VPC. This option is insufficient because, while it restricts incoming traffic to the VPC, it doesn't prevent the instance from having a public IP address. With a public IP address, the instance can still be exposed to the internet, which goes against the goal of ensuring no internet traffic can be routed to it.

Option C: Create a route on the VPC to route all traffic to the instance over the VPN tunnel. Creating a route on the VPC to route all traffic to the instance

over the VPN tunnel only focuses on controlling the route of traffic within the VPC and does not address the potential exposure of the instance to public internet traffic. It is still possible that the instance might have a public IP address, allowing unwanted traffic to reach it.

Option D: Create the instance with a public IP address and use Cloud NAT. Using Cloud NAT in this scenario is counterproductive, as the goal is to prevent any public internet traffic. Cloud NAT translates the private IP addresses of instances to a public address to allow access to the internet. By providing the instance with a public IP address and using Cloud NAT, you would be enabling the instance to access the internet and potentially expose it to unwanted traffic.