100. Source

You need to ensure reliability for your application and operations by supporting reliable **task scheduling** for compute on GCP. Leveraging Google best practices, what should you do?

A. Using the Cron service provided by App Engine, publish messages directly to a message-processing utility service running on Compute Engine instances.

B. Using the **Cron service provided by App Engine**, publish messages to a **Cloud Pub/Sub topic**. Subscribe to that topic using a message-processing utility service running on Compute Engine instances.

C. Using the Cron service provided by Google Kubernetes Engine (GKE), publish messages directly to a message-processing utility service running on Compute Engine instances.

D. Using the Cron service provided by GKE, publish messages to a Cloud Pub/Sub topic. Subscribe to that topic using a message-processing utility service running on Compute Engine instances.

> Corn: Cron is the standard tool for scheduling recurring tasks on Unix systems.
>
> Both B & D work. Let's assume the Cron Service in D means CronJob. But D requires more infra cost while B is simpler and easier.

REF

101. Source

Your company is building a new architecture to support its data-centric business focus. You are responsible for setting up the network. Your company's mobile and web-facing applications will be deployed on-premises, and all data analysis will be conducted in GCP. The plan is to process and load 7 years of archived .csv files totaling 900 TB of data and then continue loading **10 TB of data daily**. You currently have an existing **100-MB internet connection**. What actions will meet your company's needs?

A. Compress and upload both archived files and files uploaded daily using the gsutil ג€"m option.

B. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish a connection with Google using a **Dedicated Interconnect or Direct Peering connection** and use it to upload files daily.

C. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish one Cloud VPN Tunnel to VPC networks over the public internet, and compress and upload files daily using the gsutil' ג€"'m option.

D. Lease a Transfer Appliance, upload archived files to it, and send it to Google to transfer archived data to Cloud Storage. Establish a Cloud VPN Tunnel to VPC networks over the public internet, and compress and upload files daily.

> 100-MB internet connection -> 27 hours

[REF]

102. Source

You are developing a globally scaled frontend for a legacy streaming backend data API. This API expects events in strict chronological order with no repeat data for proper processing. Which products should you deploy to ensure **guaranteed-once FIFO** (first-in, first-out) delivery of data?

A. Cloud Pub/Sub alone

B. Cloud Pub/Sub to **Cloud Dataflow**

C. Cloud Pub/Sub to Stackdriver

D. Cloud Pub/Sub to Cloud SQL

> Pub/Sub doesn't provide guarantees about the order of message delivery. Strict message ordering can be achieved with buffering, often using Dataflow.

REF

103. Source

Your company is planning to perform a lift and shift migration of their Linux RHEL 6.5+ virtual machines. The virtual machines are running in an on-premises VMware environment. You want to migrate them to Compute Engine following Google-recommended practices. What should you do?

A. 1. Define a migration plan based on the list of the applications and their dependencies. 2. Migrate all virtual machines into Compute Engine individually with Migrate for Compute Engine.

B. 1. Perform an assessment of virtual machines running in the current VMware environment. 2. Create images of all disks. Import disks on Compute Engine. 3. Create standard virtual machines where the boot disks are the ones you have imported.

C. 1. Perform an assessment of virtual machines running in the current VMware environment. 2. Define a migration plan, prepare a Migrate for **Compute Engine migration RunBook**, and execute the migration.

D. 1. Perform an assessment of virtual machines running in the current VMware environment. 2. Install a third-party agent on all selected virtual machines. 3. Migrate all virtual machines into Compute Engine.

> Migrate for Compute Engine organizes groups of VMs into Waves. After understanding the dependencies of your applications, create runbooks that contain groups of VMs and begin your migration!

REF

104. Source

You need to deploy an application to Google Cloud. The application receives traffic via **TCP** and reads and writes data to the filesystem. The application does **not support horizontal scaling**. The application process requires **full control** over the data on the file system because concurrent access causes corruption. The business is willing to accept a downtime when an incident occurs, but the application must be available 24/7 to support their business operations. You need to design the architecture of this application on Google Cloud. What should you do?

A. Use a managed instance group with instances in multiple zones, use Cloud Filestore, and use an HTTP load balancer in front of the instances.

B. Use a managed instance group with instances in multiple zones, use Cloud Filestore, and use a network load balancer in front of the instances.

C. Use an unmanaged instance group with an active and standby instance in different zones, use a regional persistent disk, and use an HTTP load balancer in front of the instances.

D. Use an **unmanaged instance group** with an active and standby instance in different zones, use a regional persistent disk, and use a **network load balancer** in front of the instances.

> TCP -> HTTPS load balance is not supported, eliminate A&C
>
> full control -> Cloud Firestore does not give full control, eliminate B

REF

105. Source

Your customer runs a web service used by e-commerce sites to offer product recommendations to users. The company has begun experimenting with a machine learning model on Google Cloud Platform to improve the quality of results. What should the customer do to improve their model's results over time?

A. Export Cloud Machine Learning Engine performance metrics from Stackdriver to BigQuery, to be used to analyze the efficiency of the model.

B. Build a roadmap to move the machine learning model training from Cloud GPUs to Cloud TPUs, which offer better results.

C. Monitor Compute Engine announcements for availability of newer CPU architectures, and deploy the model to them as soon as they are available for additional performance.

D. Save a **history of recommendations** and results of the recommendations in BigQuery, to be used as training data.

> To analyze the performance metrics and other data you need a ML system, you cannot do this by queries in BigQuery.
>
> Stackdriver monitors the applications and VMs and this data is used for training ML and the results of training are used in a new model of offers and recomendations or another actions.

106. Source

You are managing an application deployed on Cloud Run for Anthos, and you need to define a strategy for deploying new versions of the application. You want to evaluate the new code with a subset of production traffic to decide whether to proceed with the rollout. What should you do?

A. Deploy a new **revision** to Cloud Run with the new version. **Configure traffic percentage between revisions**.

B. Deploy a new service to Cloud Run with the new version. Add a Cloud Load Balancing instance in front of both services.

C. In the Google Cloud Console page for Cloud Run, set up continuous deployment using Cloud Build for the development branch. As part of the Cloud Build trigger, configure the substitution variable TRAFFIC_PERCENTAGE with the percentage of traffic you want directed to a new version.

D. In the Google Cloud Console, configure Traffic Director with a new Service that points to the new version of the application on Cloud Run. Configure Traffic Director to send a small percentage of traffic to the new version of the application.

> You can specify whether a new revision receives all, none, or some of the traffic, you can gradually roll out a new revision, you can split traffic between several revisions, and you can roll back from a revision. For more information, refer to Rollbacks, gradual rollouts, and traffic migration.

REF

107. Source

(Controversial issue A or D) I go D

You are monitoring Google Kubernetes Engine (GKE) clusters in a Cloud Monitoring workspace. As a Site Reliability Engineer (SRE), you need to **triage([ˈtriːɑːʒ],分流) incidents quickly**. What should you do?

A. Navigate the predefined dashboards in the Cloud Monitoring workspace, and then add metrics and create alert policies.

B. Navigate the predefined dashboards in the Cloud Monitoring workspace, create custom metrics, and install alerting software on a Compute Engine instance.

C. Write a shell script that gathers metrics from GKE nodes, publish these metrics to a Pub/Sub topic, export the data to BigQuery, and make a Data Studio dashboard.

D. Create a **custom dashboard** in the Cloud Monitoring workspace for each incident, and then **add metrics and create alert policies**.

> Legacy Logging and Monitoring was deprecated, ---> Coud Operations

REF

108. Source

You are implementing a single Cloud SQL MySQL second-generation database that contains business-critical transaction data. You want to ensure that the **minimum amount of data is lost** in case of catastrophic failure. Which two features should you implement? (Choose two.)

A. Sharding

B. Read replicas

C. **Binary logging**

D. **Automated backups**

E. Semisynchronous replication

> Point-in-time recovery (PITR) uses binary logs
>
> Automated backups are used to restore a Cloud SQL instance. A combination of automated backups and transaction logs are used to perform a point-in-time recovery.

REF-C REF-D

109. Source

You are working at a sports association whose members range in age from 8 to 30. The association collects a large amount of **health data**, such as sustained injuries. You are storing this data in BigQuery. Current legislation requires you to **delete such information** upon request of the subject. You want to design a solution that can accommodate such a request. What should you do?

A. Use a unique identifier for each individual. Upon a deletion request, delete all rows from BigQuery with this identifier.

B. When ingesting new data in BigQuery, run the data through the **Data Loss Prevention** (DLP) API to identify any personal information. As part of the **DLP scan**, save the result to Data Catalog. Upon a deletion request, query Data Catalog to find the column with personal information.

C. Create a BigQuery view over the table that contains all data. Upon a deletion request, exclude the rows that affect the subject's data from this view. Use this view instead of the source table for all analysis tasks.

D. Use a unique identifier for each individual. Upon a deletion request, overwrite the column with the unique identifier with a salted SHA256 of its value.

> NOT to delete the entire user records but specific data related to personal health data -----> Cloud Data Loss Prevention (DLP) uses information types—or infoTypes—to define what it scans for.

REF

110. Source

(Controversial issue A or D) I go A

Your company has announced that they will be outsourcing operations functions. You want to allow **developers to easily stage new versions of a cloud-based application** in the production environment and allow the **outsourced**

operations team to autonomously promote staged versions to production. You want to minimize the operational overhead of the solution. Which Google Cloud product should you migrate to?

A. **App Engine**

B. GKE On-Prem

C. Compute Engine

D. Google Kubernetes Engine

> GKE dose not support staged version.
>
> A is also the cheapest answer

[REF]

111. Source

Your company is running its application workloads on Compute Engine. The applications have been deployed in production, acceptance, and development environments. The production environment is business-critical and is used 24/7, while the acceptance and development environments are **only critical during office hours**. Your CFO has asked you to optimize these environments to achieve cost savings during idle times. What should you do?

A. Create a shell script that uses the gcloud command to change the machine type of the development and acceptance instances to a smaller machine type outside of office hours. Schedule the shell script on one of the production instances to automate the task.

B. Use **Cloud Scheduler** to trigger a **Cloud Function** that will stop the development and acceptance environments after office hours and start them just before office hours.

C. Deploy the development and acceptance applications on a managed instance group and enable autoscaling.

D. Use regular Compute Engine instances for the production environment, and use preemptible VMs for the acceptance and development environments.

> Cloud Scheduler, GCP's fully managed cron job scheduler, provides a straightforward solution for automatically stopping and starting VMs. By employing Cloud Scheduler with Cloud Pub/Sub to trigger Cloud Functions on schedule, you can stop and start groups of VMs identified with labels of your choice (created in Compute Engine).

REF

112. Source

You are moving an application that uses MySQL from on-premises to Google Cloud. The application will run on Compute Engine and will use Cloud SQL. You want to cut over to the Compute Engine deployment of the application with **minimal downtime and no data loss** to your customers. You want to migrate the application with minimal modification. You also need to determine the cutover strategy. What should you do?

A. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Create a mysqldump of the on-premises MySQL server. 4. Upload the dump to a Cloud Storage bucket. 5. Import the dump into Cloud SQL. 6. Modify the source code of the application to write queries to both databases and read from its local database. 7. Start the Compute Engine application. 8. Stop the on-premises application.

B. 1. Set up Cloud SQL proxy and MySQL proxy. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Stop the on-premises application. 6. Start the Compute Engine application.

C. 1. Set up Cloud VPN to provide private network connectivity between the Compute Engine application and the on-premises MySQL server. 2. Stop the on-premises application. 3. Start the Compute Engine application, configured to

read and write to the on-premises MySQL server. 4. **Create the replication configuration in Cloud SQL**. 5. Configure the source database server to accept connections from the Cloud SQL replica. 6. Finalize the Cloud SQL replica configuration. 7. When replication has been completed, stop the Compute Engine application. 8. Promote the Cloud SQL replica to a standalone instance. 9. Restart the Compute Engine application, configured to read and write to the Cloud SQL standalone instance.

D. 1. Stop the on-premises application. 2. Create a mysqldump of the on-premises MySQL server. 3. Upload the dump to a Cloud Storage bucket. 4. Import the dump into Cloud SQL. 5. Start the application on Compute Engine.

> minimal downtime ----> create an external database replica and synchronize the existing data to that replica
>
> two databases have different roles that are referred to in this document as primary and replica

REF

113. Source

Your organization has decided to **restrict the use of external IP addresses on instances to only approved instances**. You want to enforce this requirement across all of your Virtual Private Clouds (VPCs). What should you do?

A. Remove the default route on all VPCs. Move all approved instances into a new subnet that has a default route to an internet gateway.

B. Create a new VPC in custom mode. Create a new subnet for the approved instances, and set a default route to the internet gateway on this new subnet.

C. Implement a Cloud NAT solution to remove the need for external IP addresses entirely.

D. Set an Organization Policy with a constraint on **constraints/compute.vmExternalIpAccess**. List the approved instances in the allowedValues list.

> The constraint for controlling external IP address on VMs is `constraints/compute.vmExternalIpAccess`
>
> To use the constraint, you specify a policy with an allowedList of VMs that can have external IP addresses.

REF

114. Source

Your company uses the Firewall Insights feature in the Google Network Intelligence Center. You have several firewall rules applied to Compute Engine instances. You need to evaluate the efficiency of the applied firewall ruleset. When you bring up the **Firewall Insights page** in the Google Cloud Console, you notice that there are no log rows to display. What should you do to troubleshoot the issue?

A. Enable Virtual Private Cloud (VPC) flow logging.

B. Enable **Firewall Rules Logging** for the firewall rules you want to monitor.

C. Verify that your user account is assigned the compute.networkAdmin Identity and Access Management (IAM) role.

D. Install the Google Cloud SDK, and verify that there are no Firewall logs in the command line output.

> To see insights and usage metrics for firewall rules, you must enable Firewall Rules Logging for one or more firewall rules.

REF

115. Source

Your company has sensitive data in Cloud Storage buckets. Data analysts have Identity Access Management (IAM) permissions to read the buckets. You want to **prevent data analysts from retrieving the data in the buckets from outside the office network**. What should you do?

A. 1. Create a **VPC Service Controls** perimeter that includes the projects with the buckets. 2. Create an access level with the CIDR of the office network.

B. 1. Create a firewall rule for all instances in the Virtual Private Cloud (VPC) network for source range. 2. Use the Classless Inter-domain Routing (CIDR) of the office network.

C. 1. Create a Cloud Function to remove IAM permissions from the buckets, and another Cloud Function to add IAM permissions to the buckets. 2. Schedule the Cloud Functions with Cloud Scheduler to add permissions at the start of business and remove permissions at the end of business.

D. 1. Create a Cloud VPN to the office network. 2. Configure Private Google Access for on-premises hosts.

> VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services such as Cloud Storage and BigQuery.
>
> Create perimeters that protect the resources and data of services that you explicitly specify.

REF

116. Source

You have developed a non-critical update to your application that is running in a managed instance group, and have created a new instance template with the update that you want to release. To prevent any possible impact to the application, you **don't want to update any running instances**. You want any **new instances that are created by the managed instance group to contain the new update**. What should you do?

A. Start a new rolling restart operation.

B. Start a new rolling replace operation.

C. Start a new rolling update. Select the Proactive update mode.

D. Start a new rolling update. Select the **Opportunistic** update mode.

> Proactive mode ---> automated rolling update which means update will be applied to al the instances in the MIG. (disruptive)
>
> Opportunistic ---> Initiate the update manually on the selected instance or when the new instances are created.

REF

117. Source

Your company is designing its application landscape on Compute Engine. Whenever **a zonal outage** occurs, the application should be **restored in another zone** as quickly as possible with the latest application data. You need to design the solution to meet this requirement. What should you do?

A. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in the same zone.

B. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in **another zone in the same region**. Use the regional persistent disk for the application data.

C. Create a snapshot schedule for the disk containing the application data. Whenever a zonal outage occurs, use the latest snapshot to restore the disk in another zone within the same region.

D. Configure the Compute Engine instances with an instance template for the application, and use a regional persistent disk for the application data. Whenever a zonal outage occurs, use the instance template to spin up the application in another region. Use the regional persistent disk for the application data.

> Regional persistent disk is a storage option that provides synchronous replication of data between two zones in a region

REF

118. Source

(Controversial issue A or B or C) I go A

Your company has just acquired another company, and you have been asked to integrate their existing Google Cloud environment into your company's data center. Upon investigation, you discover that some of the RFC 1918 IP ranges being used in the new company' Virtual Private Cloud (VPC) overlap with your data center IP space. What should you do to enable connectivity and make sure that there are **no routing conflicts** when connectivity is established?

A. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and **apply new IP addresses** so there is no overlapping IP space.

B. Create a Cloud VPN connection from the new VPC to the data center, and create a Cloud NAT instance to perform NAT on the overlapping IP space.

C. Create a Cloud VPN connection from the new VPC to the data center, create a Cloud Router, and apply a custom route advertisement to block the overlapping IP space.

D. Create a Cloud VPN connection from the new VPC to the data center, and apply a firewall rule that blocks the overlapping IP space.

> IP overlap ---> apply new IP address
>
> RFC1918 ---> using VPN communication between two priovate IP addressees, eliminate B (Cloud NAT is used for outbound internet connections)
>
> blocking the overlapping IP space ---> NOT enable connectivity as per requirement

REF

119. Source

You need to **migrate Hadoop jobs** for your company's Data Science team **without modifying the underlying infrastructure**. You want to minimize costs and infrastructure management effort. What should you do?

A. Create a **Dataproc cluster** using **standard worker instances**.

B. Create a Dataproc cluster using preemptible worker instances.

C. Manually deploy a Hadoop cluster on Compute Engine using standard instances.

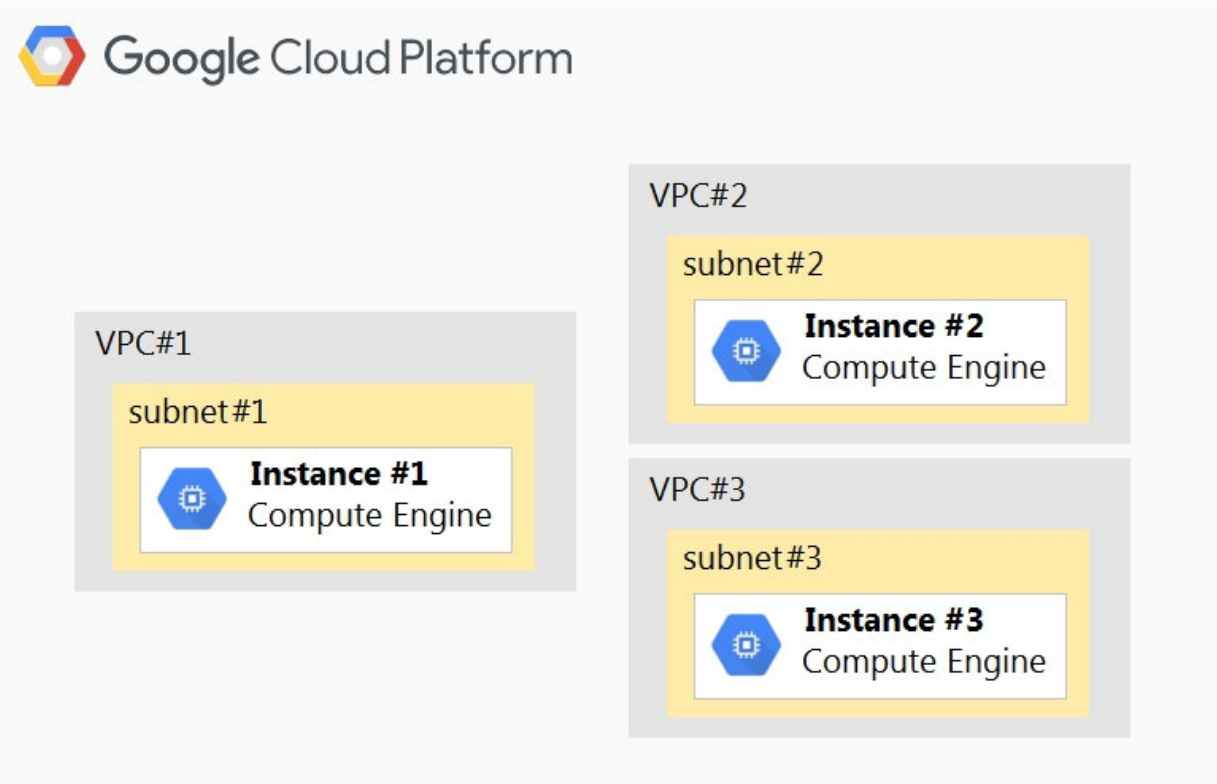
D. Manually deploy a Hadoop cluster on Compute Engine using preemptible instances.

> The primary workers can only be standard, where secondary workers can be preemtible.
>
> (preempt machines do not work standalone, they will only work in conjunction with standard machines.)

REF

120. Source

Your company has a project in Google Cloud with three Virtual Private Clouds (VPCs). There is a Compute Engine instance on each VPC. Network subnets do **not overlap** and must remain separated. The network configuration is shown below.



Instance #1 is an exception and must communicate directly with both Instance #2 and Instance #3 via **internal IPs**. How should you accomplish this?

A. Create a cloud router to advertise subnet #2 and subnet #3 to subnet #1.

B. Add two **additional NICs** to Instance #1 with the following configuration: ג€¢ NIC1 ג—‹ VPC: VPC #2 ג—‹ SUBNETWORK: subnet #2 ג€¢ NIC2 ג—‹ VPC: VPC #3 ג—‹ SUBNETWORK: subnet #3 Update firewall rules to enable traffic between instances.

C. Create two VPN tunnels via CloudVPN: 1 ¢€ג between VPC #1 and VPC #2. 1 ¢€ג between VPC #2 and VPC #3. Update firewall rules to enable traffic between the instances.

D. Peer all three VPCs: ג€¢ Peer VPC #1 with VPC #2. ג€¢ Peer VPC #2 with VPC #3. Update firewall rules to enable traffic between the instances.

> Cloud Router enables you to dynamically exchange routes between your Virtual Private Cloud (VPC) and on-premises networks, eliminate A
>
> No necessary for the connection between VPC#2 and VPC#3, eliminate C and D
>
> By default, every instance in a VPC network has a single network interface. Use these instructions to create additional network interfaces. Each interface is attached to a different VPC network, giving that instance access to different VPC networks in Google Cloud. You cannot attach multiple network interfaces to the same VPC network.

REF

121. Source

You need to deploy an application on Google Cloud that must run on a Debian Linux environment. The application requires extensive configuration in order to operate correctly. You want to ensure that you can install Debian distribution updates with minimal manual intervention whenever they become available. What should you do?

A. Create a Compute Engine instance template using the most recent Debian image. Create an instance from this template, and install and configure the application as part of the startup script. Repeat this process whenever a new Google-managed Debian image becomes available.

B. **Create a Debian-based Compute Engine instance**, install and configure the application, and use **OS patch management** to install available updates.

C. Create an instance with the latest available Debian image. Connect to the instance via SSH, and install and configure the application on the instance. Repeat this process whenever a new Google-managed Debian image becomes available.

D. Create a Docker container with Debian as the base image. Install and configure the application as part of the Docker image creation process. Host the container on Google Kubernetes Engine and restart the container whenever a new update is available.

> Repeat this process,eliminate A
>
> OS patch management -> apply operating system patches across a set of Compute Engine VM instances: Patch compliance reporting, Patch deploymen
>
> Overkill to update, eliminate C
>
> Restart the container, eliminate D k8s update

REF

122. Source

You have an application that runs in Google Kubernetes Engine (GKE). Over the last 2 weeks, customers have reported that a specific part of the application returns errors very frequently. You currently have no logging or monitoring solution enabled on your GKE cluster. You want to diagnose the problem, but you have **not been able to replicate the issue**. You want to cause minimal disruption to the application. What should you do?

A. 1. **Update** your GKE cluster to use Cloud Operations for GKE. 2. Use the **GKE Monitoring dashboard** to investigate logs from affected Pods.

B. 1. Create a new GKE cluster with Cloud Operations for GKE enabled. 2. Migrate the affected Pods to the new cluster, and redirect traffic for those Pods to the new cluster. 3. Use the GKE Monitoring dashboard to investigate logs from affected Pods.

C. 1. Update your GKE cluster to use Cloud Operations for GKE, and deploy Prometheus. 2. Set an alert to trigger whenever the application returns an error.

D. 1. Create a new GKE cluster with Cloud Operations for GKE enabled, and deploy Prometheus. 2. Migrate the affected Pods to the new cluster, and redirect traffic for those Pods to the new cluster. 3. Set an alert to trigger whenever the application returns an error.

> From GCP best practices for GKE we should rely on native logging capabilities. No need for additional solutions like Prometheus.

What is Prometheus

REF

123. Source

You need to deploy a stateful workload on Google Cloud. The workload can scale horizontally, but **each instance needs to read and write** to the same POSIX filesystem. At high load, the stateful workload needs to support up to 100 MB/s of writes. What should you do?

A. Use a persistent disk for each instance.

B. Use a regional persistent disk for each instance.

C. Create a **Cloud Filestore instance** and mount it in each instance.

D. Create a Cloud Storage bucket and mount it in each instance using gcsfuse.

> POSIX Portable Operating System Interface which defines both the system- and user-level application programming interfaces (API), along with command line shells and utility interfaces, for software compatibility (portability) with variants of Unix and other operating systems.
>
> Cloud Storage FUSE helps you make better and quicker use of Cloud Storage, but there is no concurrency control for multiple writers to a file, eliminate D. When multiple writers try to replace a file the last write wins and all previous writes are lost

REF

124. Source

Your company has an application deployed on Anthos clusters (formerly Anthos GKE) that is running multiple microservices. The cluster has both Anthos Service Mesh and Anthos Config Management configured. End users inform you that the application is responding very slowly. You want to **identify the microservice that is causing the delay**. What should you do?

A. Use the **Service Mesh visualization in the Cloud Console** to inspect the telemetry between the microservices.

B. Use Anthos Config Management to create a ClusterSelector selecting the relevant cluster. On the Google Cloud Console page for Google Kubernetes Engine, view the Workloads and filter on the cluster. Inspect the configurations of the filtered workloads.

C. Use Anthos Config Management to create a namespaceSelector selecting the relevant cluster namespace. On the Google Cloud Console page for Google Kubernetes Engine, visit the workloads and filter on the namespace. Inspect the configurations of the filtered workloads.

D. Reinstall istio using the default istio profile in order to collect request latency. Evaluate the telemetry between the microservices in the Cloud Console.

> The Anthos Service Mesh pages in the Google Cloud Console provide both summary and in-depth metrics, charts, and graphs that enable you to observe service behavior.

REF

125. Source

You are working at a financial institution that stores mortgage loan approval documents on Cloud Storage. Any change to these approval documents must be uploaded as a separate approval file, so you want to ensure that these documents **cannot be deleted or overwritten for the next 5 years**. What should you do?

A. Create a **retention policy** on the bucket for the duration of 5 years. Create a lock on the retention policy.

B. Create the bucket with uniform bucket-level access, and grant a service account the role of Object Writer. Use the service account to upload new files.

C. Use a customer-managed key for the encryption of the bucket. Rotate the key after 5 years.

D. Create the bucket with fine-grained access control, and grant a service account the role of Object Writer. Use the service account to upload new files.

> retention policy -> inreversible action.

REF

126. Source

Your team will start developing a new application using microservices architecture on Kubernetes Engine. As part of the development lifecycle, any code change that has been pushed to the remote develop branch on your GitHub

repository should be **built and tested automatically**. When the build and test are successful, the relevant microservice will be deployed automatically in the development environment. You want to ensure that all code deployed in the development environment follows this process. What should you do?

A. Have each developer install a pre-commit hook on their workstation that tests the code and builds the container when committing on the development branch. After a successful commit, have the developer deploy the newly built container image on the development cluster.

B. Install a post-commit hook on the remote git repository that tests the code and builds the container when code is pushed to the development branch. After a successful commit, have the developer deploy the newly built container image on the development cluster.

C. Create a Cloud Build trigger based on the development branch that tests the code, builds the container, and stores it in Container Registry. Create a **deployment pipeline** that watches for new images and deploys the new image on the development cluster. Ensure only the deployment tool has access to deploy new versions.

D. Create a Cloud Build trigger based on the development branch to build a new container image and store it in Container Registry. Rely on Vulnerability Scanning to ensure the code tests succeed. As the final step of the Cloud Build process, deploy the new container image on the development cluster. Ensure only Cloud Build has access to deploy new versions.

> automatically -> eliminate A,B
>
> Vulnerability Scanning, guarantee security not test, eliminate D

REF

127. Source

Your operations team has asked you to help diagnose a performance issue in a production application that runs on Compute Engine. The application is dropping requests(-> user may connect to this server) that reach it when under heavy load. The process list for affected instances shows a single application process that is consuming all available CPU, and **autoscaling has reached the upper limit of instances**. There is **no abnormal load** on any other related systems, including the database. You want to allow production traffic to be served again as quickly as possible. Which action should you recommend?

A. Change the autoscaling metric to agent.googleapis.com/memory/percent_used.

B. Restart the affected instances on a staggered schedule.

C. SSH to each instance and restart the application process.

D. **Increase the maximum number of instances** in the autoscaling group.

> A cannot solve the problem
>
> More resources can solve it.

[REF]

128. Source

You are implementing the infrastructure for a web service on Google Cloud. The web service needs to receive and store the data from 500,000 requests per second. The data will be queried later in **real time**, based on exact matches of a known set of attributes. There will be periods where the web service will not receive any requests. The business wants to keep costs low. Which web service platform and database should you use for the application?

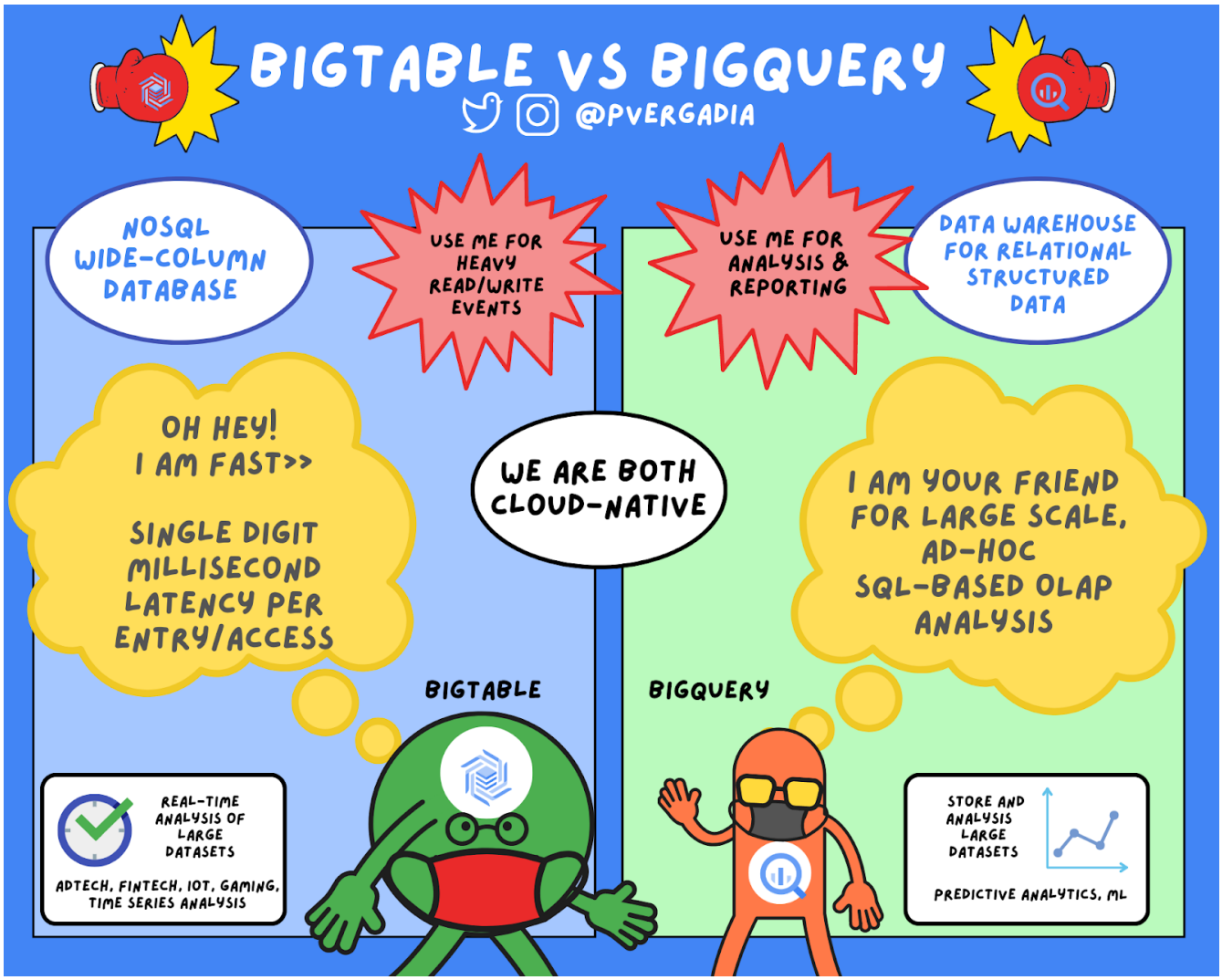
A. Cloud Run and BigQuery

B. **Cloud Run and Cloud Bigtable**

C. A Compute Engine autoscaling managed instance group and BigQuery

D. A Compute Engine autoscaling managed instance group and Cloud Bigtable

> Cost low is achieved by cloud Run.



129. Source

You are developing an application using different microservices that should remain internal to the cluster. You want to be able to configure each microservice with **a specific number of replicas**. You also want to be able to **address a specific microservice from any other microservice in a uniform way**, regardless of the number of replicas the microservice scales to. You need to implement this solution on Google Kubernetes Engine. What should you do?

A. **Deploy each microservice as a Deployment**. Expose the Deployment in the cluster using a Service, and use the **Service DNS** name to address it from other microservices within the cluster.

B. Deploy each microservice as a Deployment. Expose the Deployment in the cluster using an Ingress, and use the Ingress IP address to address the Deployment from other microservices within the cluster.

C. Deploy each microservice as a Pod. Expose the Pod in the cluster using a Service, and use the Service DNS name to address the microservice from other microservices within the cluster.

D. Deploy each microservice as a Pod. Expose the Pod in the cluster using an Ingress, and use the Ingress IP address name to address the Pod from other microservices within the cluster.

> Ingress is to expose HTTP and HTTPS routes from outside the cluster to services within the cluster.

graph LR; client([client])-. Ingress-managed
load balancer .->ingress[Ingress]; ingress-->|routing rule|service[Service]; subgraph cluster ingress; service-->pod1[Pod]; service-->pod2[Pod]; end classDef plain fill:#ddd,stroke:#fff,stroke-width:4px,color:#000; classDef k8s

fill:#326ce5,stroke:#fff,stroke-width:4px,color:#fff; classDef cluster fill:#fff,stroke:#bbb,stroke-width:2px,color:#326ce5; class ingress,service,pod1,pod2 k8s; class client plain; class cluster cluster;
REF

130. Source

Your company has a networking team and a development team. The development team runs applications on Compute Engine instances that contain sensitive data. The development team requires administrative permissions for Compute Engine. Your company requires all network resources to be managed by the networking team. The development team **does not want the networking team to have access to the sensitive data on the instances**. What should you do?

A. 1. Create a project with a standalone VPC and assign the Network Admin role to the networking team. 2. Create a second project with a standalone VPC and assign the Compute Admin role to the development team. 3. Use Cloud VPN to join the two VPCs.

B. 1. Create a project with a standalone Virtual Private Cloud (VPC), assign the Network Admin role to the networking team, and assign the Compute Admin role to the development team.

C. 1. Create a project with a **Shared VPC** and assign the Network Admin role to the networking team. 2. Create a second project without a VPC, configure it as a Shared VPC service project, and assign the Compute Admin role to the development team.

D. 1. Create a project with a standalone VPC and assign the Network Admin role to the networking team. 2. Create a second project with a standalone VPC and assign the Compute Admin role to the development team. 3. Use VPC Peering to join the two VPCs.

REF

131. Source

Your company wants you to build a highly reliable web application with a few public APIs as the backend. You don't expect a lot of user traffic, but traffic could spike occasionally. You want to leverage Cloud Load Balancing, and the solution must be cost-effective for users. What should you do?

A. Store static content such as HTML and images in Cloud CDN. Host the APIs on App Engine and store the user data in Cloud SQL.

B. Store static content such as HTML and images in a Cloud Storage bucket. Host the APIs on a zonal Google Kubernetes Engine cluster with worker nodes in multiple zones, and save the user data in Cloud Spanner.

C. Store static content such as HTML and images in Cloud CDN. Use Cloud Run to host the APIs and save the user data in Cloud SQL.

D. Store static content such as HTML and images in a **Cloud Storage bucket**. Use **Cloud Functions** to host the APIs and save the user data in Firestore.

> Cloud Run is serverless and more effective, eliminate A&B
>
> Cloud CDN: CDN stands for Content Delivery Network. A CDN is a geographically distributed network of PoPs (Points of Presence) that will deliver content based on location. For save money,elminate C.

REF

REF

132. Source

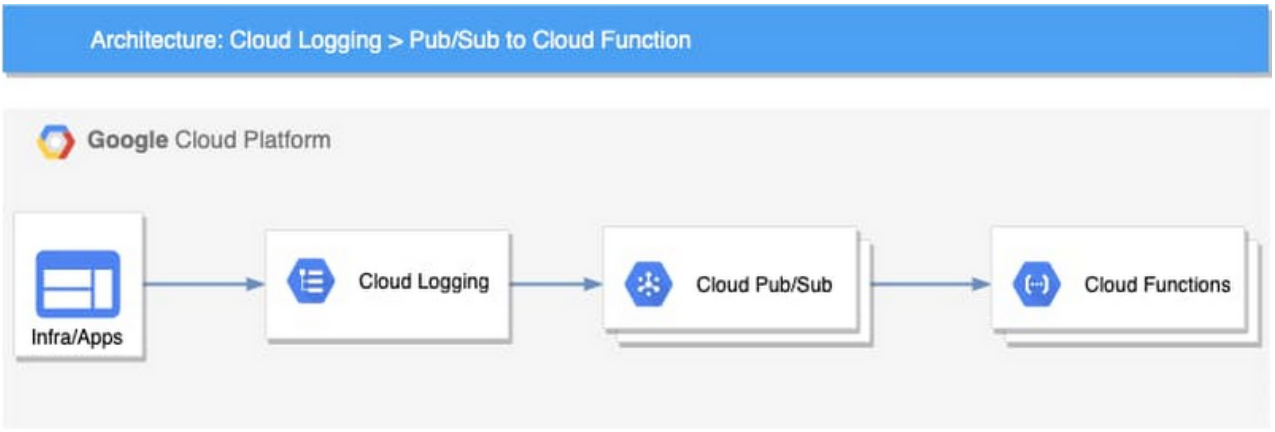
Your company sends all Google Cloud logs to Cloud Logging. Your security team wants to monitor the logs. You want to ensure that the **security team can react quickly** if an anomaly such as an unwanted firewall change or server breach is detected. You want to follow Google-recommended practices. What should you do?

A. Schedule a cron job with Cloud Scheduler. The scheduled job queries the logs every minute for the relevant events.

B. Export logs to BigQuery, and trigger a query in BigQuery to process the log data for the relevant events.

C. Export logs to a **Pub/Sub topic**, and trigger **Cloud Function** with the relevant log events.

D. Export logs to a Cloud Storage bucket, and trigger Cloud Run with the relevant log events.



REF

133. Source

You have deployed several instances on Compute Engine. As a security requirement, instances cannot have a public IP address. There is **no VPN connection** between Google Cloud and your office, and you need to **connect via SSH** into a specific machine without violating the security requirements. What should you do?

A. Configure Cloud NAT on the subnet where the instance is hosted. Create an SSH connection to the Cloud NAT IP address to reach the instance.

B. Add all instances to an unmanaged instance group. Configure TCP Proxy Load Balancing with the instance group as a backend. Connect to the instance using the TCP Proxy IP.

C. Configure **Identity-Aware Proxy (IAP)** for the instance and ensure that you have the role of IAP-secured Tunnel User. Use the gcloud command line tool to ssh into the instance.

D. Create a bastion host in the network to SSH into the bastion host from your office location. From the bastion host, SSH into the desired instance.

> Answer A is not valid because Cloud NAT is used for egress traffic when VMs do not have external IPs
>
> Answer B is not valid because the TCP proxy load balancer serves as a frontend and will not help to SSH directly into a VMs
>
> D is not valid because the security requirements state that instances shouldn't have public IPs, however setting up a bastion host will require assigning it a public IP. REF

REF

134. Source

Your company is using Google Cloud. You have two folders under the Organization: Finance and Shopping. The members of the development team are in a Google Group. The development team group has been assigned the Project Owner role on the Organization. You want to **prevent the development team from creating resources in projects in the Finance folder**. What should you do?

A. Assign the development team group the Project Viewer role on the Finance folder, and assign the development team group the Project Owner role on the Shopping folder.

B. Assign the development team group only the Project Viewer role on the Finance folder.

C. Assign the development team group the **Project Owner** role on the Shopping **folder**, and **remove** the development team group Project Owner role from the Organization.

D. Assign the development team group only the Project Owner role on the Shopping folder.

> Roles are always inherited, and there is no way to explicitly remove a permission for a lower-level resource that is granted at a higher level in the resource hierarchy.
>
> Eliminate A and B, overridden by the less-restrictive perimission on Organization level.
>
> Eliminate D, already the Organization level and does not remove the project owner permission on the other folder

REF

135. Source

You are developing your microservices application on Google Kubernetes Engine. During testing, you want to **validate the behavior** of your application in case a specific microservice should suddenly **crash**. What should you do?

A. Add a taint to one of the nodes of the Kubernetes cluster. For the specific microservice, configure a pod anti-affinity label that has the name of the tainted node as a value.

B. Use **Istio's fault injection** on the particular microservice whose faulty behavior you want to simulate.

C. Destroy one of the nodes of the Kubernetes cluster to observe the behavior.

D. Configure Istio's traffic management features to steer the traffic away from a crashing microservice.

REF

136. Source

Your company is developing a new application that will allow globally distributed users to upload pictures and share them with other selected users. The application will support millions of concurrent users. You want to allow developers to focus on just building code without having to create and maintain the underlying infrastructure. Which service should you use to deploy the application?

A. App Engine

B. Cloud Endpoints

C. Compute Engine

D. Google Kubernetes Engine

> App engine is fully managed service and developers don't need to worry about infrastructure.

REF

137. Source

Your company provides a recommendation engine for retail customers. You are providing retail customers with an API where they can submit a user ID and the API returns a list of recommendations for that user. You are responsible for the **API lifecycle** and want to ensure stability for your customers in case the API makes **backward-incompatible changes**. You want to follow Google-recommended practices. What should you do?

A. Create a distribution list of all customers to inform them of an upcoming backward-incompatible change at least one month before replacing the old API with the new API.

B. Create an automated process to generate API documentation, and update the public API documentation as part of the CI/CD process when deploying an update to the API.

C. Use a **versioning strategy for the APIs** that **increases the version number** on every backward-incompatible change.

D. Use a versioning strategy for the APIs that adds the suffix ג€DEPRECATEDג€ to the current API version number on every backward-incompatible change. Use the current version number for the new API.

> Sometimes it is necessary to make backwards-incompatible (or "breaking") changes to an API. These kinds of changes can cause issues or breakage for code that has dependencies on the original functionality.
>
> Google APIs use a versioning scheme to prevent breaking changes.

REF

138. Source

Your company has developed a monolithic, 3-tier application to allow external users to upload and share files. The solution cannot be easily enhanced and lacks reliability. The development team would like to re-architect the application to adopt microservices and a fully managed service approach, but they need to convince their leadership that the effort is worthwhile. Which advantage(s) should they **highlight** to leadership?

A. The new approach will be significantly less costly, make it easier to manage the underlying infrastructure, and automatically manage the CI/CD pipelines.

B. The monolithic solution can be converted to a container with Docker. The generated container can then be deployed into a Kubernetes cluster.

C. The new approach will make it easier to **decouple infrastructure** from application, develop and release new features, manage the underlying infrastructure,** manage CI/CD pipelines** and perform **A/B testing**, and scale the solution if necessary.

D. The process can be automated with Migrate for Compute Engine.

> decoupling, new features, CI/CD, A/B testing, scaling is the advantage so C

[REF]

139. Source

MARK Many questions and I am confused about the answer

Your team is developing a web application that will be deployed on Google Kubernetes Engine (GKE). Your CTO expects a successful launch and you need to ensure your application can handle the expected load of tens of thousands of users. You want to test the current deployment to **ensure the latency** of your application stays below a certain threshold. What should you do?

A. Use a **load testing tool to simulate** the expected number of concurrent users and total requests to your application, and inspect the results.

B. Enable autoscaling on the GKE cluster and enable horizontal pod autoscaling on your application deployments. Send curl requests to your application, and validate if the auto scaling works.

C. Replicate the application over multiple GKE clusters in every Google Cloud region. Configure a global HTTP(S) load balancer to expose the different clusters over a single global IP address.

D. Use Cloud Debugger in the development environment to understand the latency between the different microservices.

> K8S, 10,000 load, test latency -> simulate the situation -> A

[REF]

140. Source

Your company has a Kubernetes application that pulls messages from Pub/Sub and stores them in Filestore. Because the application is simple, it was deployed as a single pod. The infrastructure team has analyzed Pub/Sub metrics and discovered that the application cannot process the messages in real time. Most of them wait for minutes before being processed. You need to **scale the elaboration process** that is **I/O-intensive**. What should you do?

A. Use kubectl autoscale deployment APP_NAME --max 6 --min 2 --cpu-percent 50 to configure Kubernetes autoscaling deployment.

B. Configure a Kubernetes autoscaling deployment based on the subscription/push_request_latencies metric.

C. Use the --enable-autoscaling flag when you create the Kubernetes cluster.

D. Configure a Kubernetes **autoscaling deployment** based on the **subscription/num_undelivered_messages** metric.

[REF]

141. Source

Your company is developing a web-based application. You need to make sure that production **deployments are linked to source code commits and are fully auditable**. What should you do?

A. Make sure a developer is tagging the code commit with the date and time of commit.

B. Make sure a developer is adding a comment to the commit that links to the deployment.

C. Make the **container tag** match the source code commit hash.

D. Make sure the developer is tagging the commits with latest.

> Developer shouldn't tag or comment every commit with some specific data, like timestamps or something else. There might be an app version, but it's not mentioned. I'd go with C as it's an automated, error-less approach that answers the que

[REF]

142. Source

An application development team has come to you for advice. They are planning to write and deploy an HTTP(S) API using Go 1.12. The API will have a very **unpredictable workload** and must remain reliable during peaks in traffic. They want to minimize operational overhead for this application. Which approach should you recommend?

A. Develop the application with containers, and deploy to Google Kubernetes Engine.

B. Develop the application for **App Engine standard environment**.

C. Use a Managed Instance Group when deploying to Compute Engine.

D. Develop the application for App Engine flexible environment, using a custom runtime.

> Experiences sudden and extreme spikes of traffic which require immediate scaling.
>
> GAE is recommended for sudden spike and specific version of language

REF

143. Source

Your company is designing its data lake on Google Cloud and wants to develop different ingestion pipelines to collect **unstructured data** from different sources. After the data is stored in Google Cloud, it will be **processed in several data pipelines** to build a recommendation engine for end users on the website. The structure of the data retrieved from the source systems can change at any time. The data must be stored exactly as it was retrieved for reprocessing purposes

in case the data structure is incompatible with the current processing pipelines. You need to design an architecture to support the use case after you retrieve the data. What should you do?

A. Send the data through the processing pipeline, and then store the processed data in a BigQuery table for reprocessing.

B. Store the data in a BigQuery table. Design the processing pipelines to retrieve the data from the table.

C. Send the data through the processing pipeline, and then store the processed data in a Cloud Storage bucket for reprocessing.

D. Store the data in a **Cloud Storage bucket**. Design the processing pipelines to retrieve the data from the bucket.

> The data needs to be stored as it is retrieved. This would mean that any processing should be done after it is stored.

[REF]

144. Source

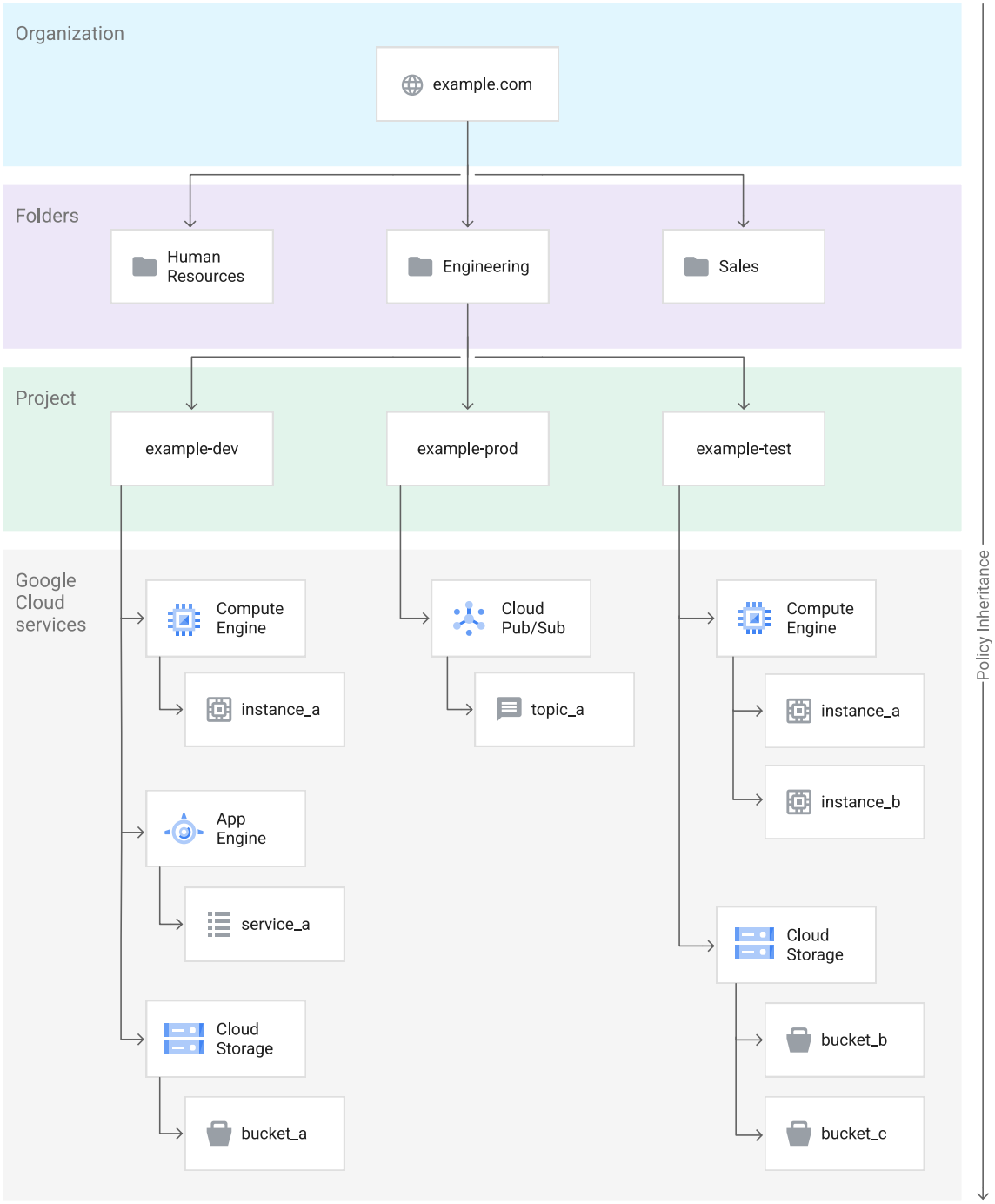
You are responsible for the Google Cloud environment in your company. Multiple departments need access to their own projects, and the members within each department will have the same project responsibilities. You want to structure your Google Cloud environment for **minimal maintenance and maximum overview of IAM permissions** as each department's projects start and end. You want to follow Google-recommended practices. What should you do?

A. Grant all department members the required IAM permissions for their respective projects.

B. Create a Google Group per department and add all department members to their **respective groups**. Create a folder per department and grant the respective group the required IAM permissions at the **folder level**. **Add the projects under the respective folders**.

C. Create a folder per department and grant the respective members of the department the required IAM permissions at the folder level. Structure all projects for each department under the respective folders.

D. Create a Google Group per department and add all department members to their respective groups. Grant each group the required IAM permissions for their respective projects.



[REF]

145. Source

MARK, I don't know the explanation

Your company has an application running as a Deployment in a Google Kubernetes Engine (GKE) cluster. You have separate clusters for development, staging, and production. You have discovered that the team is able to deploy a Docker image to the production cluster **without first testing the deployment in development and then staging**. You want to allow the team to have autonomy but want to prevent this from happening. You want a Google Cloud solution that can be implemented quickly with minimal effort. What should you do?

A. Configure a Kubernetes lifecycle hook to prevent the container from starting if it is not approved for usage in the given environment.

B. Implement a corporate policy to prevent teams from deploying Docker images to an environment unless the Docker image was tested in an earlier environment.

C. Configure **binary authorization policies** for the development, staging, and production clusters. Create attestations as part of the continuous integration pipeline.

D. Create a Kubernetes admissions controller to prevent the container from starting if it is not approved for usage in the given environment.

[REF]

146. Source

MARK, I don't know the explanation

Your company wants to migrate their 10-TB on-premises database export into Cloud Storage. You want to **minimize the time** it takes to complete this activity, the overall cost, and **database load**(->reading data directly from database is not recommendeds). The bandwidth between the on-premises environment and Google Cloud is **1 Gbps**. You want to follow Google-recommended practices. What should you do?

A. Develop a Dataflow job to read data directly from the database and write it into Cloud Storage.

B. Use the **Data Transfer appliance** to perform an offline migration.

C. Use a commercial partner ETL solution to extract the data from the on-premises database and upload it into Cloud Storage.

D. Compress the data and upload it with gsutil -m to enable multi-threaded copy.

> eliminate B --> Is Data Transfer appliance suitable for me
>
> Data size is greater than or equal to 10TB. Take more than one week to upload your data over the network
>
> D --> one day

[REF]

147. Source

Your company has an enterprise application running on Compute Engine that requires high availability and high performance. The application has been deployed on two instances **in two zones in the same region** in active-passive mode. The application writes data to a persistent disk. In the case of a single zone outage(中断), that data should be immediately made available to the other instance in the other zone. You want to maximize performance while **minimizing downtime and data loss**. What should you do?

A. 1. Attach a persistent SSD disk to the first instance. 2. Create a snapshot every hour. 3. In case of a zone outage, recreate a persistent SSD disk in the second instance where data is coming from the created snapshot.

B. 1. Create a Cloud Storage bucket. 2. Mount the bucket into the first instance with gcs-fuse. 3. In case of a zone outage, mount the Cloud Storage bucket to the second instance with gcs-fuse.

C. 1. Attach a **regional SSD persistent disk** to the first instance. 2. In case of a zone outage, force-attach the disk to the other instance.

D. 1. Attach a local SSD to the first instance disk. 2. Execute an rsync command every hour where the target is a persistent SSD disk attached to the second instance. 3. In case of a zone outage, use the second instance.

> Regional persistent disks provide synchronous replication of data between two zones in a region.

REF

148. Source

You are designing a Data Warehouse on Google Cloud and want to store sensitive data in BigQuery. Your company requires you to **generate the encryption keys outside of Google Cloud**. You need to implement a solution. What

should you do?

A. Generate a new key in Cloud Key Management Service (Cloud KMS). Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a new BigQuery dataset.

B. Generate a new key in Cloud KMS. Create a dataset in BigQuery using the customer-managed key option and select the created key.

C. Import a key in Cloud KMS. Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a new BigQuery dataset.

D. Import a key in Cloud KMS. Create a dataset in BigQuery using the **customer-supplied key** option and select the created key.

> Customers can use existing encryption keys that they manage with the Google Cloud, using the customer-supplied encryption keys feature.

REF

149. Source

Your organization has stored sensitive data in a Cloud Storage bucket. For regulatory reasons, your company must be able to **rotate the encryption key** used to encrypt the data in the bucket. The data will be processed in Dataproc. You want to follow Google-recommended practices for security. What should you do?

A. Create a key with Cloud Key Management Service (KMS). Encrypt the data using the encrypt method of Cloud KMS.

B. Create a key with Cloud Key Management Service (KMS). Set the encryption key on the bucket to the **Cloud KMS key**.

C. Generate a GPG key pair. Encrypt the data using the GPG key. Upload the encrypted data to the bucket.

D. Generate an AES-256 encryption key. Encrypt the data in the bucket using the customer-supplied encryption keys feature.

> Rotating keys(轮替密钥)
>
> Rotating keys requires the Cloud KMS Admin role (roles/cloudkms.admin).
>
> customer manage not customer key

REF

REF

150. Source

Your team needs to create a Google Kubernetes Engine (GKE) cluster to host a newly built application that requires access to third-party services on the internet. Your company does **not allow any Compute Engine instance to have a public IP address** on Google Cloud. You need to create a deployment strategy that adheres to these guidelines. What should you do?

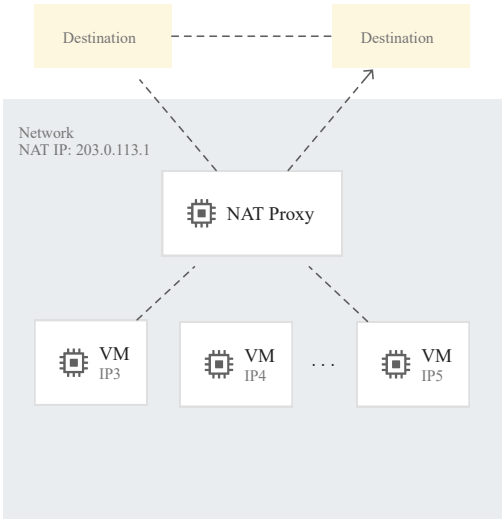
A. Configure the GKE cluster as a **private cluster**, and configure **Cloud NAT** Gateway for the cluster subnet.

B. Configure the GKE cluster as a private cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

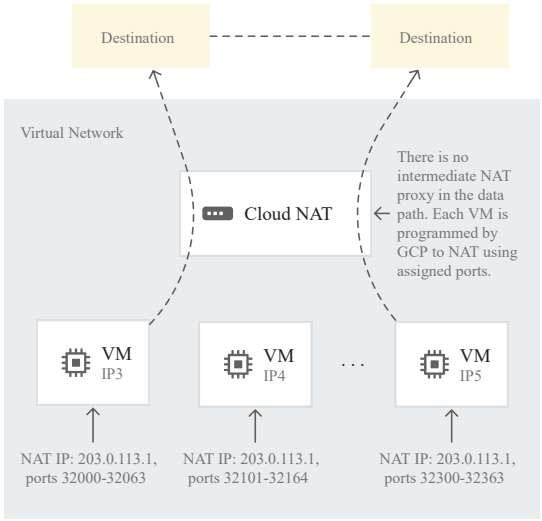
C. Configure the GKE cluster as a route-based cluster. Configure Private Google Access on the Virtual Private Cloud (VPC).

D. Create a Compute Engine instance, and install a NAT Proxy on the instance. Configure all workloads on GKE to pass through this proxy to access third-party services on the Internet.

> Cloud NAT (network address translation) lets certain resources without external IP addresses create outbound connections to the internet.



1. Typical NAT Proxies



2. Google Cloud NAT

REF

151. Source

Your company has a support ticketing solution that uses App Engine Standard. The project that contains the App Engine application already has a Virtual Private Cloud (VPC) network fully connected to the company's on-premises environment through a Cloud VPN tunnel. You want to enable the App Engine application to **communicate** with a **database that is running in the company's on-premises environment**. What should you do?

A. Configure private Google access for on-premises hosts only.

B. Configure private Google access.

C. Configure private services access.

D. Configure **serverless** VPC access.

REF

152. Source

Your company is planning to upload several important files to Cloud Storage. After the upload is completed, they want to verify that the uploaded content is **identical to what they have on-premises**. You want to minimize the cost and effort of performing this check. What should you do?

A. 1. Use Linux shasum to compute a digest of files you want to upload. 2. Use gsutil -m to upload all the files to Cloud Storage. 3. Use gsutil cp to download the uploaded files. 4. Use Linux shasum to compute a digest of the downloaded files. 5. Compare the hashes.

B. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Develop a custom Java application that computes CRC32C hashes. 3. Use gsutil ls -L gs://[YOUR_BUCKET_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

C. 1. Use gsutil -m to upload all the files to Cloud Storage. 2. Use gsutil cp to download the uploaded files. 3. Use Linux diff to compare the content of the files.

D. 1. Use gsutil -m to upload the files to Cloud Storage. 2. Use **gsutil hash -c FILE_NAME** to generate CRC32C hashes of all on-premises files. 3. Use gsutil ls -L gs://[YOUR_BUCKET_NAME] to collect CRC32C hashes of the uploaded files. 4. Compare the hashes.

> The hash command calculates hashes on a local file that can be used to compare with gsutil ls -L output. If a specific hash option is not provided, this command calculates all gsutil-supported hashes for the file.

REF

153. Source

You have deployed an application on Anthos clusters (formerly Anthos GKE). According to the SRE practices at your company, you need to be **alerted if request latency is above a certain threshold** for a specified amount of time. What should you do?

A. Install **Anthos Service Mesh** on your cluster. Use the Google Cloud Console to define a Service Level Objective (SLO), and create an alerting policy based on this **SLO**.

B. Enable the Cloud Trace API on your project, and use Cloud Monitoring Alerts to send an alert based on the Cloud Trace metrics.

C. Use Cloud Profiler to follow up the request latency. Create a custom metric in Cloud Monitoring based on the results of Cloud Profiler, and create an Alerting policy in case this metric exceeds the threshold.

D. Configure Anthos Config Management on your cluster, and create a yaml file that defines the SLO and alerting policy you want to deploy in your cluster.

> Service Level Objectives (SLOs) are a core tool in the Google service monitoring toolkit. SLOs can give you a concise and low-noise signal as to the overall health of your services.

REF

154. Source

Your company has a stateless web API that performs scientific calculations. The web API runs on a single Google Kubernetes Engine (GKE) cluster. The cluster is currently deployed in us-central1. Your company has expanded to offer your API to customers in Asia. You want to **reduce the latency** for users in Asia. What should you do?

A. Create a second GKE cluster in asia-southeast1, and expose both APIs using a Service of type LoadBalancer. Add the public IPs to the Cloud DNS zone.

B. Use a global HTTP(s) load balancer with Cloud CDN enabled.

C. Create a **second GKE cluster in asia-southeast1**, and use **kubemci** to create a global HTTP(s) load balancer.

D. Increase the memory and CPU allocated to the application in the cluster.

REF

155. Source

You are migrating third-party applications from **optimized on-premises** virtual machines to Google Cloud. You are unsure about the **optimum CPU and memory options**. The applications have a consistent usage pattern across multiple weeks. You want to optimize resource usage for the lowest cost. What should you do?

A. Create an instance template with the smallest available machine type, and use an image of the third-party application taken from a current on-premises virtual machine. Create a managed instance group that uses average CPU utilization to autoscale the number of instances in the group. Modify the average CPU utilization threshold to optimize the number of instances running.

B. Create an App Engine flexible environment, and deploy the third-party application using a Dockerfile and a custom runtime. Set CPU and memory options similar to your application's current on-premises virtual machine in the app.yaml file.

C. Create multiple Compute Engine instances with varying CPU and memory options. Install the Cloud Monitoring agent, and deploy the third-party application on each of them. Run a load test with high traffic levels on the application, and use the results to determine the optimal settings.

D. Create a **Compute Engine instance** with CPU and memory options **similar to** your application's current on-premises virtual machine. Install the Cloud Monitoring agent, and deploy the third-party application. Run a load test with normal traffic levels on the application, and follow the **Rightsizing Recommendations** in the Cloud Console.

> Cost-based recommendations: Recommends Compute Engine instances based on:
>
> - The current CPU and RAM configuration of the on-premises VM.
> - The average usage of this VM during a given period. To use this option, you must activate rightsizing monitoring with vSphere for this group of VMs and allow time for Migrate for Compute Engine to analyze usage.

REF

156. Source

Your company has a Google Cloud project that uses BigQuery for data warehousing. They have a VPN tunnel between the on-premises environment and Google Cloud that is configured with Cloud VPN. The security team wants to **avoid data exfiltration** by malicious insiders, compromised code, and accidental oversharing. What should they do?

A. Configure Private Google Access for on-premises only.

B. Perform the following tasks: 1. Create a service account. 2. Give the BigQuery JobUser role and Storage Reader role to the service account. 3. Remove all other IAM access from the project.

C. Configure **VPC Service Controls** and configure **Private Google Access**.

D. Configure Private Google Access.

> VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services such as Cloud Storage and BigQuery.
>
> You can configure private communication to Google Cloud resources from VPC networks that span hybrid environments with Private Google Access on-premises extensions.

REF

157. Source

You are working at an institution that processes medical data. You are migrating several workloads onto Google Cloud. Company policies require all workloads to run on physically separated hardware, and workloads from different clients must also be **separated**. You created a sole-tenant node(单租户节点) group and added a node for each client. You need to deploy the workloads on these **dedicated hosts**. What should you do?

A. Add the node group name as a network tag when creating Compute Engine instances in order to host each workload on the correct node group.

B. Add the node name as a network tag when creating Compute Engine instances in order to host each workload on the correct node.

C. Use node affinity labels based on the node group name when creating Compute Engine instances in order to host each workload on the correct node group.(not group name)

D. Use **node affinity labels** based **on the node name** when creating Compute Engine instances in order to host each workload on the correct node.

> Afinity should be set at node level, not node-group as every client has its own node in the group

REF

158. Source

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

A. Google Compute Engine unmanaged instance groups and Network Load Balancer

B. Google **Compute Engine managed instance groups with auto-scaling**

C. Google Cloud Dataproc to run Apache Hadoop jobs to process each test

D. Google App Engine with Google StackDriver for logging

REF

159. Source

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

A. Help the engineer to convert his websocket code to use HTTP streaming

B. Review the encryption requirements for websocket connections with the security team

C. Meet with the cloud operations team and the engineer to **discuss load balancer options**

D. Help the engineer redesign the application to use a distributed user session service that does not rely on websockets and HTTP sessions.

> Discuss Load Balancer Options. Global HTTP(S) load Balancer supports webSockets

REF

160. Source

The application reliability team at your company this added a debug feature to their backend service to send all server events to Google Cloud Storage for eventual analysis. The event records are at least 50 KB and at most 15 MB and are expected to peak at 3,000 events per second. You want to **minimize data loss**. Which process should you implement?

A. λ€¢ Append metadata to file body λ€¢ Compress individual files λ€¢ Name files with serverName λ€" Timestamp λ€¢ Create a new bucket if bucket is older than 1 hour and save individual files to the new bucket. Otherwise, save files to existing bucket.

B. λ€¢ Batch every 10,000 events with a single manifest file for metadata λ€¢ Compress event files and manifest file into a single archive file λ€¢ Name files using serverName λ€" EventSequence λ€¢ Create a new bucket if bucket is older than 1 day and save the single archive file to the new bucket. Otherwise, save the single archive file to existing bucket.

C. λ€¢ Compress individual files λ€¢ Name files with serverName λ€" EventSequence λ€¢ Save files to one bucket λ€¢ Set custom metadata headers for each object after saving

D. λ€¢ Append metadata to file body λ€¢ Compress individual files λ€¢ Name files with a **random prefix pattern** λ€¢ Save files to one bucket

> Longer randomized prefix provides more effective auto-scaling when ramping to very high read and write rates.

REF

161. Source

A recent audit revealed that a new network was created in your GCP project. In this network, a GCE instance has an SSH port open to the world. You want to **discover this network's origin**. What should you do?

A. Search for Create VM entry in the Stackdriver alerting console

B. Navigate to the Activity page in the Home section. Set category to Data Access and search for Create VM entry

C. In the Logging section of the console, **specify GCE Network as the logging section**. Search for the Create Insert entry

D. Connect to the GCE instance using project SSH keys. Identify previous logins in system logs, and match these with the project owners list

> Olny C focused on logging, the selection of network eventys, and the Create/Insert entry.

[REF]

162. Source

You want to make a copy of a production Linux virtual machine in the US-Central region. You want to manage and replace the copy easily if there are changes on the production virtual machine. You will deploy the copy as a new instance in a **different project** in the US-East region(**different region**). What steps must you take?

A. Use the Linux dd and netcat commands to copy and stream the root disk contents to a new virtual machine instance in the US-East region.

B. Create a snapshot of the root disk and select the snapshot as the root disk when you create a new virtual machine instance in the US-East region.

C. Create an image file from the root disk with Linux dd command, create a new virtual machine instance in the US-East region

D. Create a snapshot of the root disk, **create an image file in Google Cloud Storage from the snapshot**, and create a new virtual machine instance in the US-East region using the image file the root disk.

> eliminate B, because from snapshot can not use as a the root disk. You can created snapshot in one region. share snap shot with other region, create disk from snap shot and use in VM

REF

163. Source

Your company runs several databases on a single MySQL instance. They need to take backups of a specific database at **regular** intervals. The backup activity needs to complete as **quickly** as possible and cannot be allowed to impact disk performance. How should you configure the storage?

A. Configure a cron job to use the gcloud tool to take regular backups using persistent disk snapshots.

B. Mount a **Local SSD volume** as the backup location. After the backup is complete, use gsutil to move the backup to Google Cloud Storage.

C. Use gcsfise to mount a Google Cloud Storage bucket as a volume directly on the instance and write backups to the mounted location using mysqldump.

D. Mount additional persistent disk volumes onto each virtual machine (VM) instance in a RAID10 array and use LVM to create snapshots to send to Cloud Storage.

> When taking regular database backups, be careful not to consume too many persistent disk IOPS. Use the local SSD to stage your backups and then push them to a Cloud Storage bucket.

REF

164. Source

You are helping the QA team to roll out a new **load-testing tool** to test the scalability of your primary cloud services that run on Google Compute Engine with Cloud Bigtable. Which three requirements should they include? (Choose three.)

A. Ensure that the load tests **validate the performance of Cloud Bigtable**

B. Create a separate Google Cloud project to use for the **load-testing environment**

C. Schedule the load-testing tool to regularly run against the production environment

D. Ensure all third-party systems your services use is capable of handling high load

E. Instrument the production services to record every transaction for replay by the load-testing tool

F. Instrument the load-testing tool and the target services with **detailed logging and metrics collection**

> A --> Run your own typical workloads against a Bigtable cluster when doing capacity planning, so you can figure out the best resource allocation for your application.
>
> B --> test
>
> F --> gather logs and metrics in TEST environment for further scaling.

165. Source

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

A. Org viewer, project owner

B. **Org viewer, project viewer**

C. Org admin, project browser

D. Project owner, network admin

166. Source

Your company places a high value on being responsive and meeting customer needs quickly. Their primary business objectives are release **speed and agility**. You want to **reduce the chance of security errors** being accidentally introduced. Which two actions can you take? (Choose two.)

A. Ensure every code check-in is peer reviewed by a security SME

B. Use source code security analyzers as part of the CI/CD pipeline

C. Ensure you have stubs to unit test all interfaces between components

D. Enable **code signing** and a trusted binary repository integrated with your CI/CD pipeline

E. Run a **vulnerability security scanner** as part of your continuous-integration /continuous-delivery (CI/CD) pipeline

REF

167. Source

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

A. Add additional nodes to your Kubernetes Engine cluster using the following command: gcloud container clusters resize CLUSTER_Name λ€" -size 10

B. Add a tag to the instances in the cluster with the following command: gcloud compute instances add-tags INSTANCE - -tags enable- autoscaling max-nodes-10

C. **Update** the existing Kubernetes Engine cluster with the following command: gcloud alpha container clusters update mycluster - -enable- autoscaling - -min-nodes=1 - -max-nodes=10

D. Create a new Kubernetes Engine cluster with the following command: gcloud alpha container clusters create mycluster - -enable- autoscaling - -min-nodes=1 - -max-nodes=10 and redeploy your application

> eliminate A, manual scale, wasteful and an overhead.
>
> eliminate B, tagging is necessary for automation but does not address immediate ask.
>
> eliminate D, a running cluster not create a new one

How to update a cluster

168. Source

Your marketing department wants to send out a promotional email campaign. The development team wants to minimize direct operation management. They project a wide range of possible customer responses, from 100 to 500,000 click-through per day. The link leads to a simple website that explains the promotion and collects user information and preferences. Which infrastructure should you recommend? (Choose two.)

A. Use **Google App Engine to serve the website** and Google **Cloud Datastore** to store user data.

B. Use a Google Container Engine cluster to serve the website and store data to persistent disk.

C. Use a **managed instance group to serve the website** and Google **Cloud Bigtable** to store user data.

D. Use a single Compute Engine virtual machine (VM) to host a web server, backend by Google Cloud

> eliminate B, "Google Container Engine" does not exist,

[REF]

169. Source

Your company just finished a rapid lift and shift to Google Compute Engine for your compute needs. You have another 9 months to design and deploy a more **cloud-native** solution. Specifically, you want a system that is **no-ops and auto-scaling**. Which two compute products should you choose? (Choose two.)

A. Compute Engine with containers

B. **Google Kubernetes Engine with containers**

C. **Google App Engine Standard Environment**

D. Compute Engine with custom instance types

E. Compute Engine with managed instance groups

> A, D,E are incorrect as Compute Engine is a managed service

[REF]

170. Source

One of your primary business objectives is being able to trust the data stored in your application. You want to log all changes to the application data. How can you design your logging system to **verify authenticity of your logs**?

A. Write the log concurrently in the cloud and on premises

B. Use a SQL database and limit who can modify the log table

C. Digitally sign each **timestamp** and log entry and **store the signature**

D. Create a JSON dump of each log entry and store it in Google Cloud Storage

> To verify the authenticity of your logs if they are tampered with or forged, you can use a certain algorithm to generate digest by hashing each timestamp or log entry and then digitally sign the digest with a private key to generate a signature. Anybody with your public key can verify that signature to confirm that it was made with your private key and they can tell if the timestamp or log entry was modified. You can put the signature files into a folder separate from the log files. This separation enables you to enforce granular security policies.

[REF]