Google Cloud PCA exam sample questions:

1. EHR Healthcare experienced unauthorized access in their Kubernetes application due to compromised credentials. You want to establish a secure connection between on-premises and GKE, meet regulatory compliance, and integrate with EHR's existing identity provider. You do not want to use Cloud VPN. What should you do?
    a. Use service account keys to authenticate workloads running on GKE.
    b. Establish a Cloud VPN tunnel and restrict access using firewall rules.
    c. Implement Workload Identity Federation integrated with the existing identity provider.
    d. Create long-lived service account credentials and distribute them securely.

    Answer: C

2. For this question, refer to the EHR Healthcare case study.
    You are designing the technical architecture for hybrid connectivity between EHR's on-premises environment and Google Cloud.
    You want to follow Google-recommended practices for mission-critical healthcare applications. Considering the EHR Healthcare business and technical requirements, what should you do?
    a. Configure two VPN connections from on-premises to Google Cloud and make sure the VPN devices on-premises are in separate locations.
    b. Configure two Partner Interconnect connections in one metro and make sure the Interconnect connections are placed in different edge availability domains.
    c. Configure Direct Peering between EHR Healthcare and Google, and make sure you are peering at least two Google locations.
    d. Configure two Dedicated Interconnect connections in one metro and two connections in another metro and make sure the Interconnect connections are placed in different metro zones.

    Answer: D

3. For this question, refer to the EHR Healthcare case study. You are define the technical architecture for securely deploying workloads to Google Kubernetes Engine (GKE). You also need to ensure that only verified containers are deployed using Google-recommended best practices. What should you do?
    a. Enable Binary Authorization on GKE, and sign containers as part of the CI/CD pipeline.
    b. Configure Artifact Registry to use vulnerability scanning to confirm there are no vulnerabilities before deploying the workload.

c. Configure Artifact Registry to only allow trusted service accounts and deploy containers from the registry.
d. Configure Jenkins to utilize Kritis to cryptographically sign containers as part of a CI/CD pipeline.

Answer: B

4. For this question, refer to the Cymbal Retail case study. Cymbal wants to connect their on-premises systems to Google Cloud while maintaining secure and manageable communication between on-premises and cloud environments. You want to follow Google's recommended approach. What should you do?
    a. Use Google Cloud's VPC peering to connect Cymbal's on-premises systems to Google Cloud.
    b. Configure a Cloud VPN gateway and establish a VPN tunnel. Use firewall rules to restrict access to specific resources, IP addresses, and ports.
    c. Configure a static VPN connection using SSH tunnels to connect on-premises systems to Google Cloud.
    d. Use a bastion host to provide secure access to Google Cloud from Cymbal's on-premises systems.

    Answer: B

5. For this question refer to the EHR Healthcare case study. EHR Healthcare recently experienced unauthorized access to their Kubernetes-based applications due to compromised credentials, resulting in a security breach. You need to secure access between their on-premises systems and Google Kubernetes Engine (GKE) while maintaining regulatory compliance and integrating with EHR's existing identity provider. What should you do?
    a. Establish a secure VPN tunnel between the on-premises network and the GKE VPC, and implement strict firewall rules to restrict access based on source IP addresses and ports.
    b. Deploy an OpenID Connect (OIDC) identity provider in GKE, and integrate with Active Directory for centralized authentication and fine-grained authorization controls.
    c. Create a service account with minimal permissions for each application running in GKE, and distribute the credentials securely to the on-premises systems.
    d. Configure Workload Identity Federation with Active Directory to enable authentication and authorization for applications across both Kubernetes environments.

    Answer: D

6. For this question, refer to the EHR Healthcare case study. Due to the high Infrastructure administration costs, you want to migrate the legacy relational database systems to Google Cloud. You need to maintain the strict uptime requirements and have limited in-house expertise. What should you do?
    a. Backup and restore the databases to Cloud SQL instances with minimal changes.
    b. Set up database replication to Cloud SQL instances using native database tools, and incrementally switch applications to use the replicas.
    c. Leverage AlloyDB to migrate the on-premises databases.
    d. Use the Database Migration Service (DMS) to migrate the MySQL databases to Cloud SQL.

    Answer: D

7. For this question, refer to the EHR Healthcare case study You are designing the Google Cloud network architecture for Google Kubernetes Engine (GKE) and want to follow Google best practices. Considering the EHR Healthcare technical requirements, what should you do to reduce the attack surface?
    a. Use a public cluster with firewall rules and Virtual Private Cloud routes.
    b. Use a private cluster with a public endpoint with authorized networks configured.
    c. Use a private cluster with a private endpoint with authorized networks configured.
    d. Use a public cluster with authorized networks enabled and firewall rules configured.

    Answer: C

8. For this question, refer to the EHR Healthcare case study to ensure that EHR's use of Google Cloud will pass an upcoming audit. What should you do??
    a. Use GKE private clusters for all Kubernetes workloads
    b. Verify EHR's product usage against the list of complia Google Cloud compliance page.
    c. Use Firebase Authentication for EHR's user-facing ap
    d. Implement Prometheus to detect and prevent security web-based applications.

    Answer:

9. For this question, refer to the EHR Healthcare case study. You are [partially obscured] customer portal team. The application servers have increased [partially obscured] is having timeout errors. You recently incorporated Pub/Sub architecture, and the application is not logging any Pub/Sub [partially obscured] want to improve publishing latency. What should you do?

a. Create a backup Pub/Sub message queue.
b. Retrieve from a Pub/Sub subscriber pull model to a push model.
c. off Pub/Sub message batching.
d. Increase or decrease the Pub/Sub Total Timeout retry value.

Answer: c

10. For this question, refer to the Cymbal Retail case study. Cymbal plans to migrate their existing on-premises systems to Google Cloud and implement AI virtual agents to handle customer interactions. You need to provision the compute resources that can scale for the AI-powered virtual agents. What should you do?
    a. Configure Cloud Build to call AI Applications (formerly Vertex AI Agent Builder)
    b. Deploy a Google Kubernetes Engine (GKE) cluster with autoscaling enabled
    c. Create a single, large Compute Engine VM instance with a high CPU allocation
    d. Use Cloud SQL to store the customer data and product catalog

    Answer: B

11. For this question, refer to the Cymbal Retail case study, Cymbal has a centralized project that supports large video files for Vertex AI model training. Standard storage costs have suddenly increased this month, and you need to determine what you should do?
    a. Investigate if the project owner moved from dual-region storage to region storage.
    b. Investigate if the project owner moved from multi-region storage to region storage.
    c. Investigate if the project owner disabled a soft-delete policy on the bucket holding the video files.
    d. Investigate if the project owner enabled a soft-delete policy on the bucket holding the video files

    Answer: B

12. For this question, refer to the Cymbal Retail case study. Generative AI models require high-performance storage for temporary files generated during training and inference. These files are ephemeral and frequently accessed and modified. You need to select a storage solution that minimizes latency and maximizes performance for generative AI workloads. What should you do?
    a. Use a Cloud Storage bucket in the same region as your virtual machines. Configure lifecycle policies to delete files after processing.
    b. Use Filestore to store temporary files.

c. Use performance persistent disks.
d. Use Local SSDs attached to the VMs running the generative AI workloads.

Answer: D

13. For this question, refer to the Cymbal Retail case studies project. Cymbal wants you to design a cloud first data storage infrastructure for the product catalog modernization project. You want to ensure efficient data access and high availability for the Cymbal's web application and virtual agents while minimizing operational costs. What should you do?
    a. Use Spanner for the structured product data, and BigTable images.
    b. Use AlloyDB for structured product data, and Cloud Storage images.
    c. Use Cloud Storage for structured product data, and BigQuery images.
    d. Use Filestore for the structured product data, and Cloud Storage images.

    Answer: confusing question as if D was Firestore then it would be Firestore but now its Filestore so ans is C

14. You are developing a retail application on Vertex AI that use the __age model to give customers real-time product recommendation. ____ code, images, audio, and video prompts to communicate with customer and to minimize the application's latency to ensure a responsive and ___ence. What should you do?
    a. Enable streaming responses from the model to process the output in real time.
    b. Avoid using system instructions to prevent overly long response
    c. Increase the temperature parameter.
    d. Avoid using the max_output_tokens parameter to prevent overly responses.

    Answer: A

15. Your team plans to use Vertex Al to develop and deplo dels for various use cases for fraud detection, product recom tomer chun prediction. You want to enhance the security post Workbench environment by restricting data exfiltration. What should you do?
    a. Enable VPC Flow Logs to monitor network traffic to and from ____ services and to identify suspicious activity.
    b. Enable Private Google Access for the VPC network to allow V services to access public Google services without traversing the internet.
    c. Create a service perimeter and include ml.googleapis.com and document.googleapis.com as protected services.
    d. Create a service perimeter and include aiplatform.googleapis.com and notebooks.googleapis.com as protected services.

Answer: D

16. You have an application that uses Vertex Al Feature Store. It serve product features for real-time recommendations. You want to improve(maximize) performance and health of the application. You need to understand the o---- of a request. What should you do?
    a. Measure the Latency of your requests
    b. Observe the Request size in your featurestore
    c. Track the online serving throughput of your requests
    d. Monitor the queries per second for your featurestore

    Answer: D

17. _____ us-west1 region. A new regulatory man____ to implement and document a business continuity plan (BCP). This p_____ that the EHR application can be fully recovered and operational in a ___ geographical region with a recovery time objective (RTO) of two hours and Recovery Point Objective (RPO) of 15 minutes. You need to design a disaster recovery plan that meets these strict BCP requirements. What should you do?
    a. Deploy active managed instance groups (MIGs) in both us-east1 and us-west1, fronted by a global external HTTP(S) Load Balancer, Fo_____ database, use a cross-region read replica in us-east1, and rely on balancer health checks to automatically fail over all traffic during ___
    b. Use Terraform to define the application's compute infrastructure. disaster, configure the Cloud SQL database in us-west1 to use region read replica in us-east1, build the environment in us-east1 ___ promote the replica
    c. Take daily snapshots of the Compute Engine disks and Cloud SQL database. Copy these snapshots to a Cloud Storage bucket in us-__ During a disaster, manually restore the virtual machines (VMs) and database from the latest snapshots.
    d. Deploy a regional MIG in us-west 1 for high availability, and rely on___ Google Cloud SLA to ensure the region remains online

    Answer: B terraform

18. A financial services company is decommissioning one of its on-premises ____ters. As part of this initiative, the company needs to perform a one-time migration of _ TB of historical transaction archives to a Cloud Storage bucket for long-term retention. The data center's internet egress is 1 Gbps, which is shared with critical business operations. You must complete the secure data transfer within a 60-day window to meet the decommissioning deadline. What should you do?

a. Use Storage Transfer Service to create an agent-based transfer job that moves the data from the on-premises file servers directly to the Cloud Storage bucket.
b. Write a script that uses the gcloud storage cp -parallel command to upload the data in chunks over the public internet during off-peak hours.
c. Provision a Partner Interconnect connection with a 10 Gbps capacity to accelerate the data transfer, and then use Storage Transfer Service.
d. Order a Transfer Appliance, copy the data to the appliance using your high-speed local network, and ship it back to Google to upload the data into your Cloud Storage bucket.

Answer: D

19. A retail company's most critical application is its online payment pr. The business has a requirement that the system must be able to sur e zonal outage while minimizing cost. You need a design solution the a zonal failure. What should you do?
    a. Deploy the application in an active-active configuration using manage instance groups (MIGs) in two different regions, fronted by a global ex HTTP(S) Load Balancer and backed by a multi-regional database like Spanner.
    b. Deploy the application on a regional MIG to provide high availability acr multiple zones in the primary region.
    c. Configure the regional MIG to use only Spot VMs to aggressively minim operational costs while maintaining high availability
    d. Deploy the application on Compute Engine instarices across multiple regions, and rely on daily snapshots for recovery to achieve the lowest possible cost

    Answer: B

20. Your company is running AI/ML workloads on graphics processing units (GPUs) within Google Kubernetes Engine (GKE). These workloads are deployed across production and development projects, with the production environment being business critical and operating 24/7. You need to ensure that the GPU capacity is always available during scaling events, without being limited by overall GPU availability. You also need the ability to shift unused GPU capacity from production to development projects as needed. You want to follow Google-recommended best practices. What should you do?
    a. Create a reservation in the production project, and then create a separate reservation in the development project to secure capacity
    b. Create a reservation in the production project, and then transfer the reservation to the development project when needed

c. Create an owner project with shared reservations, and then configure the production project and development project as consumer projects to consume capacity.
d. Create a shared reservation in the production project, and then add the development project as a consumer project to move capacity when needed.

Answer: D

21. A global media company is launching a new web application. The application backend is hosted on Compute Engine in us-central1 and serves both static assets (images, CSS, and JavaScript) and dynamic, user-specific content from a Cloud SQL database in the same region. Early user feedback from Europe and Asia indicate significant page load delays due to slow loading static content. You need to design a solution that minimizes latency for all global users accessing the static content. What should you do? Choose 2 answers
    a. Create Cloud SQL read replicas in regions in Europe and Asia, and direct all database read traffic from those continents to their local replica
    b. Use a regional external Network Load Balancer in us-central1 to better distribute the incoming global traffic.
    c. Deploy the application frontend service to Compute Engine managed instance groups in regions in Europe and Asia. Use a global external HTTP(S) Load Balancer to route user traffic to the nearest region.
    d. Vertically scale the Compute Engine instances in us-central1 by increasing their machine size
    e. E. Enable Cloud CDN for the backend service that serves the static assets, and configure it as part of a global external HTTP(S) Load Balancer

    Answer: C and E

22. You are setting up a new regional environment for your business re on to migrate more than 2 TB of data from the us-central1 region to the utheast1 region. The transfer should occur as quickly as possible. If the t errupted, the operation must resume where it left off and copy only new or m bjects. What should you do?
    a. Utilize Storage Transfer Service (STS) to migrate objects to the destinat bucket in the target region. Once the transfer is complete, delete the orig source bucket objects
    b. Leverage Cloud Composer to orchestrate a data pipeline that copies obje from the source bucket to the destination bucket.
    c. Use the gcloud storage rsync-recursive command to replicate the source bucket to a new target bucket in the us-west1 region.
    d. Use the gcloud storage cp command to copy the objects. Be careful to manage potential naming conflicts to ensure data integrity.

Answer: C

23. You are developing a deep learning model that requires access to large volumes of media data currently stored in Cloud Storage. The model is to be executed on multiple VM instances with GPUs attached. You need to interact with the data as if it were on the local file system to minimize code complexity and cost. What should you do?
    a. Copy the data from Cloud Storage to Filestore, and then mount the Filestore volume as a local file system on your VM instances.
    b. Use the gcsfuse command line tool to mount the Cloud Storage bucket as a local file system, and perform read/write operations in your code using standard file system semantics.
    c. Create a shared persistent disk, attach the disk to your VM instances, and load data from the Cloud Storage bucket.
    d. Use the gsutil command line tool to download the data to your VM instances.

    Answer: B

24. A large, multinational corporation is migrating to Google Cloud: The company has several distinct business units: Finance, Marketing, and Research and Development (R&D). The central security team has mandated governance requirements for each business unit:

    Finance: Must be restricted to deploying resources only in specific, compliant regions (us-central1 and europe-west2). Access to their projects must be tightly controlled by a dedicated finance-admins group.

    Marketing: Needs separate environments for production and development, with different teams managing each environment.

    R&D: Requires maximum flexibility to experiment with new services but must be completely isolated to prevent any impact on production systems.

    Global Auditing: A central compliance team requires read-only access to view all resources across the entire company for auditing purposes.

    You need to design a resource hierarchy that enforces these security policies at scale according to the Google Cloud Well-Architected Framework while providing the correct level of autonomy for each business unit. What should you do?
    a. Create a single project for each department. Apply the resource location policy directly to the Finance project. Grant the compliance team the roles/browser role on each project individually.
    b. Place all projects directly under the Organization node. Use network tags and service accounts to enforce security boundaries between the different department workloads. Apply the resource location Organization Policy on the Finance project.

c. Create separate Google Cloud Organizations for each department (Finance, Marketing, and R&D). Grant the compliance team the roles/viewer role for each organization.
d. Create a folder for each department under the root Organization node. Apply the resource location Organization Policy on the Finance folder. Within the Marketing folder, create separate projects for mktg-prod and mktg-dev. Grant the compliance team the roles/viewer role at the Organization level

Answer: D

25. Your organization is going to migrate applications to Kubernetes and use managed cloud services to deploy applications. Your team is new to Kubernetes and wants to quickly onboard engineers. You want to reduce operational overhead, so engineering team can focus on developing consumer requirements instead of maintaining the infrastructure. What should you do?
    a. Package your application into a Docker image, and deploy it to Kubernetes on Compute Engine.
    b. Leverage Cloud Build to create a container image, and deploy it automatically to Kubernetes on Compute Engine.
    c. Assess application and dependencies for containerization. Develop a migration strategy for deployment to GKE in Standard mode.
    d. Assess application and dependencies for containerization. Develop a migration strategy for deployment to GKE in Autopilot mode

    Answer: D

26. Your organization uses Google Kubernetes Engine (GKE) and Amazon Elastic Kubernetes Service (EKS) to manage a complex Kubernetes environment across multiple cloud providers. You need to deploy a solution that streamlines configuration management, enforces security policies, and ensures consistent application deployment across all of the environments. You want to follow Google-recommended practices. What should you do?
    a. Deploy Kustomize for configuration customization, Config Sync with multiple Git repositories, and a script to enforce security policies
    b. Leverage Argo CD for GitOps-based continuous delivery and Open Policy Agent (OPA) for policy enforcement, and develop a controller for multi-cluster configuration management.
    c. Utilize Config Sync as part of GKE to synchronize configurations from a centralized repository, and utilize Policy Controller to enforce policies using OPA Gatekeeper.

d. Deploy Crossplane for managing cloud resources as Kubernetes objects, FluxCD for GitOps-based configuration synchronization, and Kyverno for policy enforcement

Answer: B

27. Your company runs a critical, revenue-generating ecommerce application that is served by a regional managed instance group (MIG) behind an external HTTP(S) Load Balancer. The operations team is currently overwhelmed with low-priority notifications and is starting to ignore alerts. Your team's service level objective (SLO) is to maintain 99.9% availability, which is measured by the ratio of successful requests (2xx status codes) to total requests. You want to minimize noise from non-critical events and ensure that the team is only notified of issues that are actionable and threaten the SLO. What should you do?
    a. Create log-based alerts for only the WARN and ERROR log entries generated by the application to ensure that no potential issue is missed
    b. Configure alerts based on predictive metrics. Use the instance count of the MIG as the primary metric to trigger an alert
    c. Implement an error budget policy based on the availability of the SLO. Create a "page" alert that triggers only when the rate of burn of the error budget predicts a full exhaustion within the next 24 hours
    d. Focus on cause-based alerts, creating alerting policies with thresholds for the Compute Engine instances, including CPU utilization, memory usage, disk I/O, and network traffic

    Answer: C

28. You manage a highly distributed, hybrid- and multi-cloud IT environment, and your developers rely heavily on Prometheus for their workflows. You need a cloud-based, highly scalable, low-maintenance enterprise solution that supports Prometheus Query Language (PromQL) queries, quick metric viewing, and efficient issue diagnosis. What should you do?
    a. Set up Cloud Monitoring as a single pane of glass across multi-cloud environments.
    b. Build a SaaS-based, Prometheus-compatible solution to display metrics for each cloud in a customizable way.
    c. Enable Google Cloud Managed Service for Prometheus to monitor and alert on your workloads at scale.
    d. Deploy a Prometheus operator in your existing Kubernetes and Serverless setup across multi-cloud environments.

    Answer: D

29. You are designing the storage architecture for a financial analytics platform. The platform ingests and stores terabytes of transactional data daily, which is used for both real-time fraud detection and long-term historical analysis. Transaction data from the last 30 days must be accessible with very low latency for the fraud detection engine. Data older than 30 days is accessed infrequently for quarterly reports, where retrieval times of a few seconds are acceptable. All data must be retained for five years to meet compliance regulations. You need to design a solution as cost-effective as possible. What should you do?
    a. Store all transaction data in a Cloud Storage bucket using the Standard storage class for the entire five-year retention period.
    b. Ingest all data into BigQuery using time-partitioned tables, and rely on BigQuery's automatic long-term storage pricing for data older than 90 days
    c. Configure a Cloud Storage bucket with an Object Lifecycle Management policy to transition data from the Standard class to the Archive class after 30 days.
    d. Configure a Cloud Storage bucket with an Object Lifecycle Management policy to transition data from the Standard class to the Coldline class after 30 days.

    Answer: D

30. You are designing the storage architecture for a financial analytics platform. The platform ingests and stores terabytes of transactional data daily, which is used by both real-time fraud detection and long-term historical analysis. Transaction data from the last 30 days must be accessible with very low latency for the fraud detection engine. Data older than 30 days is accessed infrequently for quarterly reports, where retrieval times of a few seconds are acceptable. All data must be retained for five years to meet compliance regulations. You need to design a solution as cost-effective as possible. What should you do?
    a. Store all transaction data in a Cloud Storage bucket using the Standard storage class for the entire five-year retention period.
    b. Ingest all data into BigQuery using time-partitioned tables, and rely on BigQuery's automatic long-term storage pricing for data older than 90 days.
    c. Configure a Cloud Storage bucket with an Object Lifecycle Management policy to transition data from the Standard class to the Archive class after 30 days.
    d. Configure a Cloud Storage bucket with an Object Lifecycle Management policy to transition data from the Standard class to the Coldline class after 30 days.

Answer:

31. You are migrating a large, on-premises application to Google plication consists of several interconnected virtual machines. You wa etailed migration plan to ensure a smooth migration with minimal effort understand the existing environment, identify dependencies, and estima ownership (TCO) in the cloud. What should you do?
    a. Use Config Connector to declare the desired state of your Google resources in Kubernetes-style manifests.
    b. Use the Google Cloud Migration Center to perform an automated discovery and assessment of the on-premises environment.
    c. Use the Google Cloud pricing calculator to input the specifications o on-premises servers and receive a TCO estimate.
    d. Write a custom script to query the vSphere API for virtual machine information and then import it into BigQuery for analysis

    Answer: B

32. You are migrating a critical, on-premises, three-tier ecommerce application to Google Cloud. The application has tightly coupled dependencies between its web, application, and database tiers. The business has strict performance and availability requirements and is concerned about the risks associated with an "all-at-once" migration. You want to follow Google-recommended practices to create a migration plan that systematically addresses application dependencies and validates post-migration performance before the final production cutover. What should you do?
    a. Use dependency mapping to group application components into waves, create a phased migration plan, and incorporate performance testing for each wave
    b. Prioritize the establishment of a high-bandwidth, low-latency Cloud Interconnect connection, and then plan to migrate the database servers first
    c. Redesign the application to be cloud-native using microservices before migration to eliminate dependencies and simplify workload testing
    d. Plan a "lift and shift" migration for all application tiers to be executed simultaneously over a single weekend to minimize downtime

    Answer: A

33. To improve governance and security, your organization has structured the Google Cloud environment using folders for different business units. Each business unit folder has subfolders for development, staging, and production environments, which must comply with internal security controls:
    * Production workloads must be protected from direct internet ingress by default unless explicitly tagged

* The application must be accessible to customers over HTTPS

You need to design a scalable and enforceable model that blocks internet ingress traffic to the production folders while selectively allowing direct HTTPS traffic to the necessary virtual machines. You must also ensure that individual project teams cannot overwrite these controls once they are implemented for all current and future production projects. What should you do?

a. Mandate the application teams to deploy a Terraform module to create VPC firewall rules in each project that deny ingress and allow HTTPS.
b. At each production folder, use an organization policy to block all external IPs and require teams to use external HTTPS load balancers.
c. At the organization root, apply a hierarchical firewall policy to deny all ingress except for HTTPS to tagged VMs.
d. At each production folder, apply a hierarchical firewall policy to deny all ingress except for HTTPS to tagged VMs.

Answer: D

34. You are designing the access control strategy for a new system that will store highly sensitive financial reports in a series of Cloud Storage buckets. Each bucket holds a specific type of sensitive data. Your company uses Google Workspace, and all employee roles are managed through Google Groups. The design must allow members of these groups to access only the reports they are authorized to see. The company's governance policy has two additional, critical requirements:

* All access must be directly tied to an employee's corporate identity for clear audit trails
* The access model must be simple to operate and scalable.

What should you do?

a. Generate and distribute time-limited signed URLs to grant users temporary per-object access
b. Maintain fine-grained access control, and use default object ACLs to grant the required permissions to the Google Groups
c. Enable uniform bucket-level access on the buckets, and grant predefined Storage IAM roles to the Google Groups
d. Grant the IAM role roles/storage.objectAdmin to all authorized Google Groups to simplify permission management.

Answer: D

35. The entire question and options from the image are as follows:

A large enterprise is building a file processing pipeline. The pipeline ingests the raw

files, which are then accessed by a fleet of Compute Engine virtual machines (VMs) in a single region for parallel processing. These VMs need concurrent, low-latency read and write access to a single storage solution that delivers the highest possible performance to minimize the overall processing time. What should you do?

a. Create a Regional Persistent Disk and attach it to all VMs in multi-writer mode.
b. Create a Filestore Zonal instance in each zone where the VMs are. Mount the Filestore file share on each Compute Engine VM.
c. Create a Filestore Enterprise instance in the same region as the VMs. Mount the Filestore file share on each Compute Engine VM.
d. Use a multi-region Cloud Storage bucket to store the files.

Answer: C

36. Your company has hired an external auditing firm to perform a company audit. Your company's governance policy requires that external auditors be managed via a single Google Group that is granted temporary read-only access to a Cloud Storage bucket named audit-evidence-bucket. Access must be traceable to the individual auditor's identity and be active only for the duration of the audit engagement, which runs the entire month of October. You need a secure access control strategy that avoids administrative overhead and complies with your company's governance policy. What should you do?

a. Use Cloud Scheduler to run a Cloud Run functions script that adds the IAM binding of roles/storage.objectViewer to the Google Group on October 1 and another that removes the IAM binding on November 1.
b. Apply an IAM policy binding that grants the roles/storage.objectViewer role to the Google Group. Configure this binding with a time-based IAM Condition that automatically grants access from October 1 to November 1.
c. Use Workforce Identity Federation to map the auditors' group to the Google Group. Bind the roles/storage.objectViewer role to this Google Group. Configure a 1-month session duration on the provider.
d. Create a service account, and grant it the roles/storage.objectViewer role on the bucket. Generate and share Signed URLs for each object in the bucket with an expiration date of November 1.

Answer: B

37. You are deploying a highly confidential data processing workload on Google Cloud. Your company's compliance framework mandates that cryptographic keys used for encrypting data at rest must be generated and stored exclusively within a validated Hardware Security Module (HSM). You want to use a fully integrated Google Cloud

managed service to handle the lifecycle and usage of these keys. What should you do?

a. Use Customer-Supplied Encryption Keys (CSEK) by providing your on-premises generated key with each API request.
b. Configure Cloud External Key Manager (Cloud EKM) to connect to your on-premises HSM.
c. Create a new key in Cloud Key Management Service (Cloud KMS) with the HSM protection level.
d. Import your on-premises HSM key material into a Cloud KMS key with the SOFTWARE protection level.

Answer: B

38. You are designing a new insurance claims processing application deployed on Google Kubernetes Engine (GKE). Your company's compliance requires a complete and non-repudiable audit trail for all administrative actions. Your application must capture who deploys a new container image, who changes the GKE cluster's configuration, and who interacts with running pods or Kube secrets using kubectl. What should you do?

a. Activate the Security Command Center Premium tier to analyze GKE and detect threats, vulnerabilities, and misconfigurations in real time.
b. Deploy a DaemonSet to every node in the GKE cluster that runs a log agent to collect and forward all container logs to Cloud Logging.
c. Enable GKE Audit Logging to send Kubernetes API server logs to Cloud Logging, and ensure Cloud Audit Logs are enabled for the project.
d. Enable Binary Authorization on the GKE cluster, and create a policy that requires all deployed container images to be signed by a trusted attestor.

Answer: C

39. Your company is building containerized applications as part of its CI/CD pipeline. To improve the security and maintainability of the build process, you need to:
* Identify potential vulnerabilities within your container images
* Generate verifiable metadata about the builds for auditing and compliance
* Create a comprehensive inventory of your application's dependencies
What should you do?

a. Use Cloud Build to build container images, and then trigger Artifact Analysis on images pushed to Artifact Registry.
b. Use Cloud Build to build container images, trigger Binary Authorization, and use Cloud Asset Inventory for tracking and analysis.
c. Use Cloud Build to build container images, trigger Binary Authorization, and use Security Command Center for tracking and analysis,

d. Use Cloud Build to build container images, push the images to Artifact Registry, and use Security Command Center for tracking and analysis.

Answer: D

40. Your team is developing a new application using a microservice architecture on Kubernetes Engine. As part of the development lifecycle:
* Any code change that is pushed to the remote develop branch on your git repository should be built and tested automatically.
* When the builds and tests 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.

1. 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.

2. After a successful commit, have the developer deploy the newly built container image on the development cluster.

b.

1. 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.

2. After a successful commit, have the developer deploy the newly built container image on the development cluster.

c.

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

d.

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

Answer: C

41. Your company uses the Firewall Insights feature in the Google Cloud console. You have several firewall rules applied to compute instances. You need to evaluate the efficiency of the applied firewall rules. When you open up the Firewall Insights page in the Google Cloud console, you notice there are no log rows to display. What should you do to troubleshoot the issue?
    a. Enable Firewall Rules Logging for the firewall rules you want to evaluate.
    b. Enable Virtual Private Cloud (VPC) flow logging.
    c. Verify that your user account is assigned the compute.networkViewer Identity and Access Management (IAM) role.
    d. Install the Google Cloud SDK, and verify that there are no Firewall Insights errors in the command line output.

Answer: A

42. You are using a GitHub repository for your application's source code and you want to set up an efficient and secure continuous deployment process to build and deploy the application to Cloud Run whenever a pull request is merged. What should you do?
    a. Create a workflow using GitHub Actions to build and deploy the application to Cloud Run once a pull request is merged. The workflow will use a service account key checked in with your source code for deployment purposes
    b. Create a GitHub webhook trigger in Cloud Build. Once a pull request is merged, trigger Cloud Build to build a container image and save it to Artifact Registry. Use Config Sync to deploy the application to Cloud Run.
    c. Create a GitHub Enterprise trigger in Cloud Build. Once a pull request is merged, trigger Cloud Build to build and deploy the application to Cloud Run. Save the deployment credential to Secret Manager.
    d. Connect your repository using the Cloud Build GitHub app. Create a trigger in Cloud Build. Once a pull request is merged, trigger Cloud Build to build and deploy the application to Cloud Run.

Answer: A

43. Your ecommerce platform uses a regional Cloud SQL for PostgreSQL database to store critical order information. The business requests a recovery time objective (RTO) of less than 10 minutes and a recovery point objective (RPO) of 15 minutes to ensure business continuity in the event of a full regional outage. You design a disaster recovery strategy for the Cloud SQL database that meets the business's strict RTO and RPO requirements. Your design must avoid operational complexity. What should you do?

a. Use Database Migration Service to continuously replicate the database to another instance in a different region. In a disaster, redirect application traffic to the replica.
b. Schedule hourly automated backups of the Cloud SQL instance to a multi-regional Cloud Storage bucket. In a disaster, restore the latest backup to a new instance in a different region.
c. Configure the Cloud SQL instance with a cross-region read replica. In a disaster, promote the read replica to a standalone, primary instance.
d. Configure the primary instance for high availability (HA). In the event of a regional outage, trigger a failover to the standby instance.

Answer: C

44. Your product team is building a critical, customer-facing application on Cloud. The development team wants to use Spanner for their database to take advantage of its horizontal scalability and low operational overhead. However, the FinOps team is concerned about the direct monthly cost of Spanner and proposes using a self-managed PostgreSQL database on Compute Engine VMs instead. You need to resolve this conflict and ensure the project moves forward with an architecturally sound database choice that balances technical requirements with financial constraints. What should you do?
    a. Provide the development team with a reference architecture for deploying a highly available PostgreSQL cluster on a regional managed instance group (MIG).
    b. Suggest using Cloud SQL for PostgreSQL as a compromise to get a fully managed service at a lower cost than Spanner.
    c. Cite the reliability and performance optimization pillars of the Google Cloud Well-Architected Framework to formally justify the use of Spanner.
    d. Develop a total cost of ownership (TCO) analysis that includes operational overhead, and present it in a workshop to facilitate a decision.

Answer: D

45. You need to build a continuous delivery pipeline for a containerized application in Google Cloud. You want to run all your tests in the pipeline to improve your application's quality. What should you do?
    A.

    1. Run unit tests in the developer's local environment before committing and pushing the code to a central repository.
    2. After the code is pushed, trigger Cloud Build to build the application container and deploy the container to a testing environment, and run integration tests.

3. If the integration tests are successful, deploy the container to your production environment and run acceptance tests.

B.

1. After the developers push the code to a central repository, trigger Cloud Build to build the application container. Then run unit tests.
2. If unit tests are successful, deploy the container to a testing environment and run integration tests.
3. If the integration tests are successful, deploy the container to a production environment and run acceptance tests.

C.

1. Automatically run unit tests in a local environment once the code is changed. If all tests are successful, build a container.
2. Trigger Cloud Build to deploy the container to a testing environment, and run integration tests and acceptance tests.
3. If all tests are successful, tag the code as production ready. Trigger Cloud Build to build and deploy the container to the production.

D.
1. After the developers push the code to a central repository, trigger Cloud Build to run unit tests. If all unit tests are successful, build the application container and push it to a central registry.
2. Trigger Cloud Build to deploy the container to a testing environment and run integration tests and acceptance tests.
3. If all tests are successful, deploy the application to the production environment and run the smoke tests.

Answer: C

46. You are leading a large-scale Google Cloud implementation project. Your development teams need to deploy applications, but they lack deep expertise in cloud-native patterns. This leads to inconsistent and insecure deployments, such as GKE clusters without proper logging and overly permissive IAM roles. You need to create a system that empowers these teams to deploy complete, pre-approved application patterns in a self-service manner. The system must ensure security and compliance by default while maintaining high developer velocity and avoiding manual approval bottlenecks. What should you do?

a. Use a combination of organization policies to restrict resource configurations and IAM recommender to periodically suggest improvements.
b. Create a central Cloud Monitoring dashboard and a set of custom alerts that fire whenever a non-compliant resource is detected.
c. Enforce a mandatory CI/CD pipeline using Cloud Build that requires every Terraform deployment to be reviewed and approved before the Terraform apply step can run.
d. Use Service Catalog to define, govern, and offer a portfolio of approved products. Include Terraform scripts into Service Catalog items.

Answer: C

47. You are planning to migrate your on-premises compute to Google Cloud. You want to follow Google-recommended practices to get a cost estimate for running these workloads in Google Cloud. What should you do?
    a. Use the Google Cloud pricing calculator, and input the estimated usage to generate a cost estimate.
    b. Engage with a Google Cloud partner to perform a comprehensive assessment and provide a customized cost estimate.
    c. Leverage Cloud Asset Inventory to gather data and generate a cost estimate.
    d. Gather data about your current environment, and leverage Google Cloud Migration Center to generate a cost estimate.

Answer: D

48. You are deploying a critical application with a stateless, containerized frontend on Cloud Run and a Cloud SQL for PostgreSQL backend. The application experiences unpredictable traffic spikes, and the business requires the ability to immediately roll back a failed deployment to the last known good state. You need to apply a deployment strategy that aligns with Site Reliability Engineering (SRE) principles for both the application code and the database schema updates, while meeting the business's requirements. What should you do?
    a. A. Use a single CI/CD pipeline that first applies database schema changes and then deploys the new Cloud Run revision
    b. Package the database schema migration script within the container to be executed on every container startup before the application process begins
    c. Configure the CI/CD pipeline to use the latest container tag for deployments, with database schema changes applied manually as needed

d. Separate CI/CD pipelines for database schema migrations from application deployments. When deploying a new Cloud Run revision, use gradual traffic split

Answer: D

49. You are designing a central, automated infrastructure deployment process for your organization using Terraform and Cloud Build. The security team prohibits the use of long-lived, static service account keys in any CI/CD pipeline. Additionally, while developers can propose infrastructure changes for peer review, they must not have permissions to directly apply changes in the production project. You need to design a secure and automated workflow for applying Terraform changes that meets the security team's requirements and ensures proper governance. What should you do?
    a. A. Create a privileged service account and store its JSON key in Secret Manager. Configure the Cloud Build pipeline to fetch this key during execution to authenticate Terraform.
    b. B. Configure the Cloud Build pipeline to use service account impersonation. Set up a trigger that automatically runs terraform apply when a pull request is merged.
    c. C. Configure the pipeline to only run terraform plan. After a pull request is approved, have an authorized developer run terraform apply from a secured workstation.
    d. D. Use service account impersonation in Cloud Build. Configure the pipeline to run terraform plan on pull requests, and require manual approval before running terraform apply.

Answer: B

50. You created a Cloud Monitoring dashboard for your dev environment to real-time application metrics. The Ops team wants a similar dashboard to monitor production environment. You want to minimize time and effort as you assist the Op team with their dashboard request. What should you do?
    a. Share your dashboard and send the shared dashboard URL to the Ops team.
    b. Export your dashboard to a JSON file and share it with the Ops team.
    c. Create a shared document and list every step you performed to create the dashboard. The Ops team can use the document to build their own dashboard.
    d. Grant viewer permission to the Ops team in your project so they can recreate the charts in their dashboard from the console.

Answer: A

51. You are designing the observability strategy for a new microservices app running on Google Kubernetes Engine (GKE). The application consists of multiple services (e.g., frontend, orders, payments). During load testing, you observe an error in the frontend service's logs, but you cannot find the corresponding logs in the downstream services to investigate the root cause because the logs are not correlated. You need to implement a solution that allows you to follow a single user request across all microservices involved in the transaction. The solution must not require developers to manually add correlation logic to their application code. What should you do?
    a. Require developers to generate a unique correlation-id at the frontend, and manually add it as a field to every log message in all services
    b. Implement Cloud Trace by ensuring the traceparent header is propagated between microservice calls to link logs to a single trace
    c. Create custom metrics in Cloud Monitoring for error counts in each service and correlate incident spikes using a shared dashboard.
    d. Configure all containers to write logs to STDOUT/STDERR, and then filter logs by pod name and timestamp in the Logs Explorer

Answer: B

52. Your organization has a significant amount of log data stored in Cloud Logging. The data engineering team is accustomed to using SQL for analysis and wants the ability to create insightful dashboards for visualizing log trends and patterns. You want to follow the recommendations of the Google Cloud Well-Architected Framework to provide a solution for the data engineering team. What should you do?
    a. Create a log sink, and export the data to BigQuery using Pub/Sub. Run queries and visualize the data with Cloud Monitoring dashboards.
    b. Enable log analytics and run queries in Cloud Monitoring. Visualize the data using Vertex AI workbench.
    c. Enable log analytics and run queries in the linked log dataset in BigQuery. Visualize the data with Looker Studio dashboards.
    d. Create a log sink, and export the data to a storage bucket. Create an external table in BigQuery for the data in the bucket. Run queries and visualize the data with Cloud Monitoring dashboards.

Answer: C

53. Your company has an application deployed on Anthos clusters that is running 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 Anthos Config Management to create a NamespaceSelector selecting the relevant cluster namespace. On the Google Cloud console page for Google Kubernetes Engine, view the workloads and filter on the namespace. Inspect the configurations of the filtered workloads.
b. Reinstall Istio using the default Istio profile in order to collect request latency. Evaluate the telemetry between the microservices in the Google Cloud console.
c. Use the Service Mesh visualization in the Google Cloud console to inspect the telemetry between the microservices.
d. 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.

Answer: C

54. The operations team in your company wants to save Cloud VPN log events for the year. You need to configure the cloud infrastructure to save the logs. What should you do?
    a. Set up a filter in Cloud Logging and a topic in Pub/Sub to publish the logs
    b. Set up a Cloud Logging Dashboard titled Cloud VPN Logs, and then add a chart that queries for the VPN metrics over a one-year time period
    c. Set up a filter in Cloud Logging and a Cloud Storage bucket as an export target for the logs you want to save
    d. Enable the Compute Engine API, and then enable logging on the firewall rules that match the traffic you want to save.

Answer: C

55. For this question, refer to the EHR Healthcare case study. Due to the growing partnerships with new insurance providers, EHR Healthcare needs a solution to automate the creation of secure Google Cloud environments for each provider. You need to automate the provisioning and management of these secure environments, ensure that each provider's environment is consistently configured and managed, and provide a consistent user experience across all providers. What should you do?
    a. Develop custom Cloud Run functions to automate the provisioning of new Google Cloud environments. Incorporate security measures and pre-defined configurations within the functions to ensure consistency and protection.
    b. Leverage Google Kubernetes Engine (GKE) for workload deployments. Use cluster autoscaling and node auto-provisioning features to scale the cluster based on resource usage.

c. Provision and configure each new environment and resources through the Google Cloud console.
d. Utilize Infrastructure as Code (IaC) tools, such as Terraform, to define and manage infrastructure configurations.

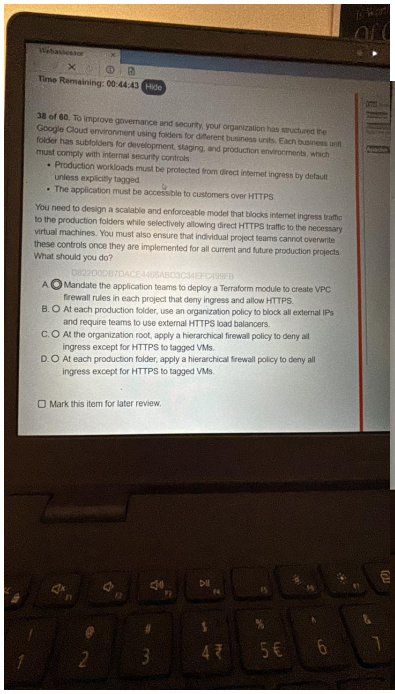
Answer: D

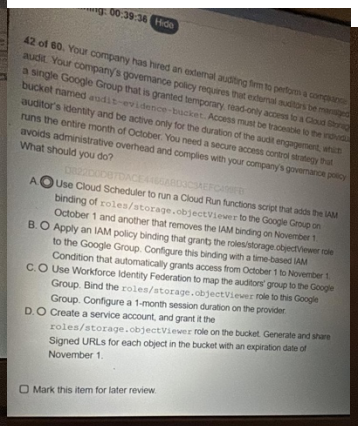
56. Your company wants to optimize Google Cloud costs for their development and staging environments. These environments are workstations used by developers Monday through Friday, 9:00 AM to 6:00 PM local time. Currently, the environments run on a fleet of n1-standard-4 Compute Engine instances that operate 24/7, leading to a high monthly cost for resources that are idle more than 70% of the time. You need to implement a solution that significantly reduces the monthly cost of these non-production environments without impacting the development team's productivity during work hours. What should you do?
    a. Upgrade all instances to the N2 machine series.
    b. Schedule the virtual machines to start and stop to match your team's work schedule.
    c. Re-architect the environments to run on a regional managed instance group (MIG) with autoscaling enabled.
    d. Purchase three-year committed use discounts (CUDs) for the existing n1-standard-4 instances.

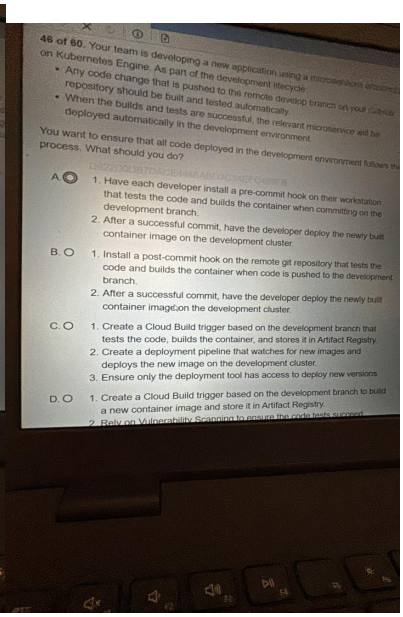
Answer: B

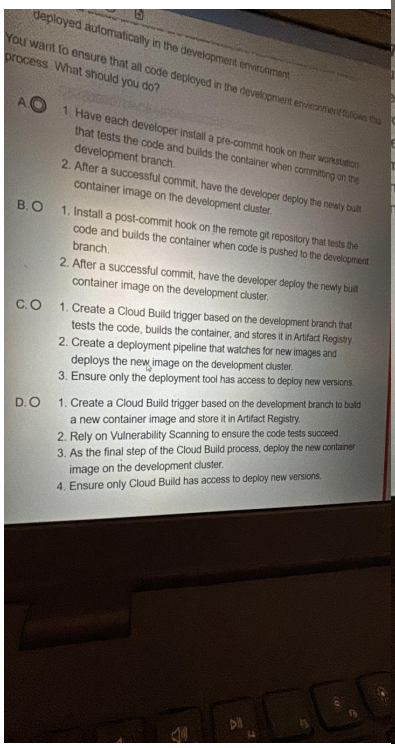
57. Your company is expanding its AI-powered operations nationwide and has chosen accelerator-based compute for the AI workloads. The batch image processing workloads are not time-sensitive and can tolerate interruptions. You need to rapidly deploy cost-effective accelerator nodes for these batch tasks, ensuring rapid deployment and data persistence when necessary. What should you do?
    a. Deploy spot VMs with local SSD to reduce time for bursty workloads
    b. Deploy standard VMs with configured accelerators and attached persistent disks.
    c. Deploy Cloud Run functions with ephemeral local SSD
    d. Deploy spot VMs with attached persistent disks and implement checkpoint mechanisms.

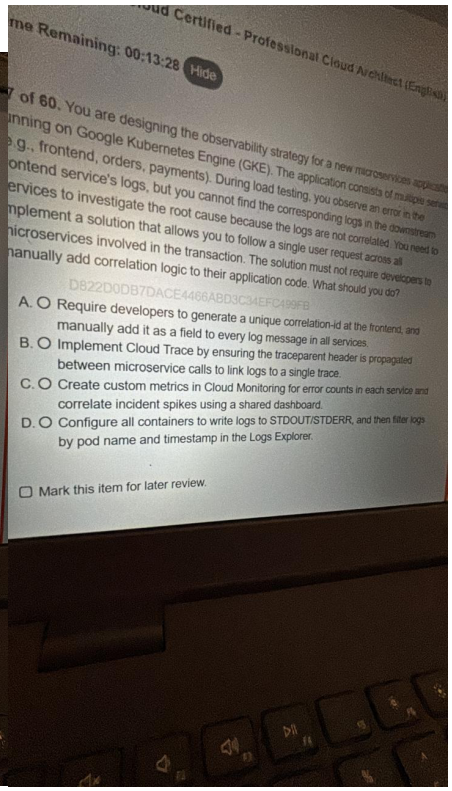
Answer: D

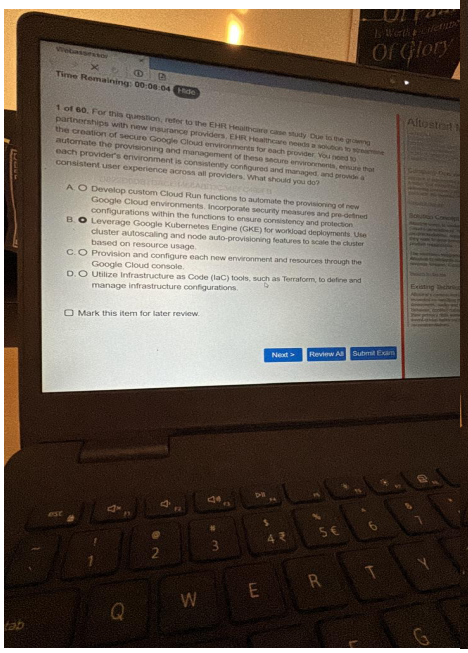

Time Remaining: 00:44:43 Hide
38 of 60. To improve governance and security, your organization has structured the Google Cloud environment using folders for different business units. Each business unit folder has subfolders for development, staging, and production environments, which must comply with internal security controls.
• Production workloads must be protected from direct internet ingress by default unless explicitly tagged.
• The application must be accessible to customers over HTTPS.
You need to design a scalable and enforceable model that blocks internet ingress traffic to the production folders while selectively allowing direct HTTPS traffic to the necessary virtual machines. You must also ensure that individual project teams cannot overwrite these controls once they are implemented for all current and future production projects. What should you do?
A. Mandate the application teams to deploy a Terraform module to create VPC firewall rules in each project that deny ingress and allow HTTPS.
B. At each production folder, use an organization policy to block all external IPs and require teams to use external HTTPS load balancers.
C. At the organization root, apply a hierarchical firewall policy to deny all ingress except for HTTPS to tagged VMs.
D. At each production folder, apply a hierarchical firewall policy to deny all ingress except for HTTPS to tagged VMs.
Mark this item for later review.

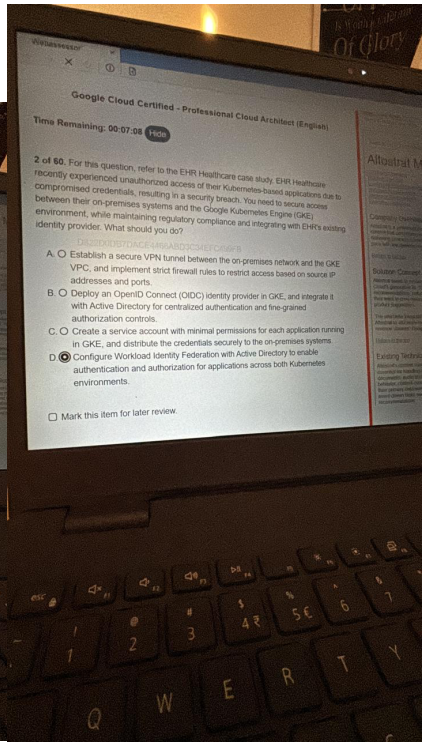

42 of 60. Your company has hired an external auditing firm to perform a compliance audit. Your company's governance policy requires that external auditors be granted access to a single Google Group that is granted temporary, read-only access to a Cloud Storage bucket named audit-evidence-bucket. Access must be traceable to the individual auditor's identity and be active only for the duration of the audit engagement, which runs the entire month of October. You need a secure access control strategy that avoids administrative overhead and complies with your company's governance policy. What should you do?
A. Use Cloud Scheduler to run a Cloud Run functions script that adds the IAM binding of roles/storage.objectViewer to the Google Group on October 1 and another that removes the IAM binding on November 1.
B. Apply an IAM policy binding that grants the roles/storage.objectViewer role to the Google Group. Configure this binding with a time-based IAM Condition that automatically grants access from October 1 to November 1.
C. Use Workforce Identity Federation to map the auditors' group to the Google Group. Bind the roles/storage.objectViewer role to this Google Group. Configure a 1-month session duration on the provider.
D. Create a service account, and grant it the roles/storage.objectViewer role on the bucket. Generate and share Signed URLs for each object in the bucket with an expiration date of November 1.
Mark this item for later review.

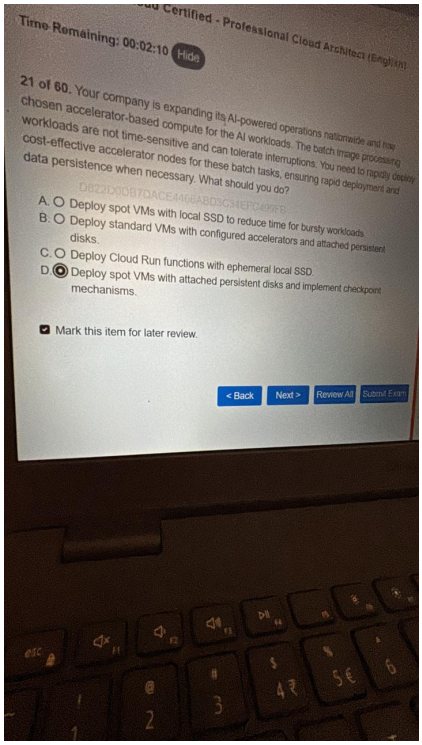

46 of 60. Your team is developing a new application using a microservices architecture on Kubernetes Engine. As part of the development lifecycle:
• Any code change that is pushed to the remote develop branch on your cutover repository should be built and tested automatically.
• When the builds and tests 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 the process. What should you do?
A. 1. 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.
2. After a successful commit, have the developer deploy the newly built container image on the development cluster.
B. 1. 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.
2. After a successful commit, have the developer deploy the newly built container image on the development cluster.
C. 1. Create a Cloud Build trigger based on the development branch that tests the code, builds the container, and stores it in Artifact Registry.
2. Create a deployment pipeline that watches for new images and deploys the new image on the development cluster.
3. Ensure only the deployment tool has access to deploy new versions
D. 1. Create a Cloud Build trigger based on the development branch to build a new container image and store it in Artifact Registry.
2. Rely on Vulnerability Scanning to ensure the code tests succeed.


deployed automatically in the development environment.
You want to ensure that all code deployed in the development environment follows the process. What should you do?
A. 1. 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.
2. After a successful commit, have the developer deploy the newly built container image on the development cluster.
B. 1. 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.
2. After a successful commit, have the developer deploy the newly built container image on the development cluster.
C. 1. Create a Cloud Build trigger based on the development branch that tests the code, builds the container, and stores it in Artifact Registry.
2. Create a deployment pipeline that watches for new images and deploys the new image on the development cluster.
3. Ensure only the deployment tool has access to deploy new versions.
D. 1. Create a Cloud Build trigger based on the development branch to build a new container image and store it in Artifact Registry.
2. Rely on Vulnerability Scanning to ensure the code tests succeed.
3. As the final step of the Cloud Build process, deploy the new container image on the development cluster.
4. Ensure only Cloud Build has access to deploy new versions.


Certified - Professional Cloud Architect (Engl
Time Remaining: 00:13:28 Hide
7 of 60. You are designing the observability strategy for a new microservices application running on Google Kubernetes Engine (GKE). The application consists of multiple services (e.g., frontend, orders, payments). During load testing, you observe an error in the frontend service's logs, but you cannot find the corresponding logs in the downstream services to investigate the root cause because the logs are not correlated. You need to implement a solution that allows you to follow a single user request across all microservices involved in the transaction. The solution must not require developers to manually add correlation logic to their application code. What should you do?
D822D0DB7DACE4466ABD3C34EFC499FB
A. Require developers to generate a unique correlation-id at the frontend, and manually add it as a field to every log message in all services.
B. Implement Cloud Trace by ensuring the traceparent header is propagated between microservice calls to link logs to a single trace.
C. Create custom metrics in Cloud Monitoring for error counts in each service and correlate incident spikes using a shared dashboard.
D. Configure all containers to write logs to STDOUT/STDERR, and then filter logs by pod name and timestamp in the Logs Explorer.
Mark this item for later review.


Time Remaining: 00:06:04 Hide
1 of 60. For this question, refer to the EHR Healthcare case study. Due to the growing partnerships with new insurance providers, EHR Healthcare needs a solution to streamline the creation of secure Google Cloud environments for each provider. You need to automate the provisioning and management of these secure environments, ensure that each provider's environment is consistently configured and managed, and provide a consistent user experience across all providers. What should you do?
A. Develop custom Cloud Run functions to automate the provisioning of new Google Cloud environments. Incorporate security measures and pre-defined configurations within the functions to ensure consistency and protection.
B. Leverage Google Kubernetes Engine (GKE) for workload deployments. Use cluster autoscaling and node auto-provisioning features to scale the cluster based on resource usage.
C. Provision and configure each new environment and resources through the Google Cloud console.
D. Utilize Infrastructure as Code (IaC) tools, such as Terraform, to define and manage infrastructure configurations.
Mark this item for later review.
Next >
Review All
Submit Exam


Google Cloud Certified - Professional Cloud Architect (English)
Time Remaining: 00:07:08 Hide
2 of 60. For this question, refer to the EHR Healthcare case study. EHR Healthcare recently experienced unauthorized access of their Kubernetes-based applications due to compromised credentials, resulting in a security breach. You need to secure access between their on-premises systems and the Google Kubernetes Engine (GKE) environment, while maintaining regulatory compliance and integrating with EHR's existing identity provider. What should you do?
A. Establish a secure VPN tunnel between the on-premises network and the GKE VPC, and implement strict firewall rules to restrict access based on source IP addresses and ports.
B. Deploy an OpenID Connect (OIDC) identity provider in GKE, and integrate it with Active Directory for centralized authentication and fine-grained authorization controls.
C. Create a service account with minimal permissions for each application running in GKE, and distribute the credentials securely to the on-premises systems.
D. Configure Workload Identity Federation with Active Directory to enable authentication and authorization for applications across both Kubernetes environments.
Mark this item for later review.


Time Remaining: 00:02:10 Hide
21 of 60. Your company is expanding its AI-powered operations nationwide and has chosen accelerator-based compute for the AI workloads. The batch image processing workloads are not time-sensitive and can tolerate interruptions. You need to rapidly deploy cost-effective accelerator nodes for these batch tasks, ensuring rapid deployment and data persistence when necessary. What should you do?
A. Deploy spot VMs with local SSD to reduce time for bursty workloads.
B. Deploy standard VMs with configured accelerators and attached persistent disks.
C. Deploy Cloud Run functions with ephemeral local SSD.
D. Deploy spot VMs with attached persistent disks and implement checkpoint mechanisms.
Mark this item for later review.
< Back
Next >
Review All
Submit Exam