

Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer



NEW QUESTION 1

In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

- A. Hardware
- B. Network Security
- C. Storage Encryption
- D. Access Policies
- E. Boot

Answer: CD

NEW QUESTION 2

While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password. What should you do?

- A. Manually synchronize the data in Google domain with your existing Active Directory or LDAP server.
- B. Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server.
- C. Users sign in directly to the GCP Console using the credentials from your on-premises Kerberos-compliant identity provider.
- D. Users sign in using OpenID (OIDC) compatible IdP, receive an authentication token, then use that token to log in to the GCP Console.

Answer: B

NEW QUESTION 3

Which two implied firewall rules are defined on a VPC network? (Choose two.)

- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections

Answer: AB

NEW QUESTION 4

An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well-established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the "source of truth" directory for identities. Which solution meets the organization's requirements?

- A. Google Cloud Directory Sync (GCDS)
- B. Cloud Identity
- C. Security Assertion Markup Language (SAML)
- D. Pub/Sub

Answer: B

NEW QUESTION 5

You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account. What should you do?

- A. Query Data Access logs.
- B. Query Admin Activity logs.
- C. Query Access Transparency logs.
- D. Query Stackdriver Monitoring Workspace.

Answer: A

NEW QUESTION 6

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

- A. App Engine
- B. Cloud Functions
- C. Compute Engine
- D. Google Kubernetes Engine
- E. Cloud Storage

Answer: AC

NEW QUESTION 7

A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs. What should you do?

- A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired

threshol

- B. Enable notifications.
- C. Create an Alerting Policy in Stackdriver using the CPU usage metri
- D. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
- E. Log every execution of the script to Stackdriver Loggin
- F. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
- G. Log every execution of the script to Stackdriver Loggin
- H. Configure BigQuery as a log sink, and create aBigQuery scheduled query to count the number of executions in a specific timeframe.

Answer: C

NEW QUESTION 8

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

- A. Run each tier in its own Project, and segregate using Project labels.
- B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
- C. Run each tier in its own subnet, and use subnet-based firewall rules.
- D. Run each tier with its own VM tags, and use tag-based firewall rules.

Answer: C

NEW QUESTION 9

A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned.
What should the customer do?

- A. Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
- B. Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
- C. Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
- D. Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

Answer: C

NEW QUESTION 10

A customer needs an alternative to storing their plain text secrets in their source-code management (SCM) system.
How should the customer achieve this using Google Cloud Platform?

- A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
- B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
- C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.
- D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

NEW QUESTION 10

A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE).
How should the DevOps team accomplish this?

- A. Use Puppet or Chef to push out the patch to the running container.
- B. Verify that auto upgrade is enabled; if so, Google will upgrade the nodes in a GKE cluster.
- C. Update the application code or apply a patch, build a new image, and redeploy it.
- D. Configure containers to automatically upgrade when the base image is available in Container Registry.

Answer: B

NEW QUESTION 13

For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods reside on "in- scope" Nodes only. These Nodes can only contain the "in-scope" Pods.

How should the organization achieve this objective?

- A. Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.
- B. Create a node pool with the label inscope: true and a Pod Security Policy that only allows the Pods to run on Nodes with that label.
- C. Place a taint on the Nodes with the label inscope: true and effect NoSchedule and a toleration to match in the Pod configuration.
- D. Run all in-scope Pods in the namespace "in-scope-pci".

Answer: C

NEW QUESTION 16

An organization's security and risk management teams are concerned about where their responsibility lies for certain production workloads they are running in Google Cloud Platform (GCP), and where Google's responsibility lies. They are mostly running workloads using Google Cloud's Platform-as-a-Service (PaaS) offerings, including App Engine primarily.

Which one of these areas in the technology stack would they need to focus on as their primary responsibility when using App Engine?

- A. Configuring and monitoring VPC Flow Logs
- B. Defending against XSS and SQLi attacks
- C. Manage the latest updates and security patches for the Guest OS
- D. Encrypting all stored data

Answer: D

NEW QUESTION 17

Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.

What should you do?

- A. Store the data in a single Persistent Disk, and delete the disk at expiration time.
- B. Store the data in a single BigQuery table and set the appropriate table expiration time.
- C. Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.
- D. Store the data in a single BigTable table and set an expiration time on the column families.

Answer: B

NEW QUESTION 18

A customer is running an analytics workload on Google Cloud Platform (GCP) where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet.

Which two strategies should your team use to meet these requirements? (Choose two.)

- A. Configure Private Google Access on the Compute Engine subnet
- B. Avoid assigning public IP addresses to the Compute Engine cluster.
- C. Make sure that the Compute Engine cluster is running on a separate subnet.
- D. Turn off IP forwarding on the Compute Engine instances in the cluster.
- E. Configure a Cloud NAT gateway.

Answer: BE

NEW QUESTION 20

A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.

What should they do?

- A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
- B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
- C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
- D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

Answer: A

NEW QUESTION 21

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

- A. Central management of routes, firewalls, and VPNs for peered networks
- B. Non-transitive peered networks; where only directly peered networks can communicate
- C. Ability to peer networks that belong to different Google Cloud Platform organizations
- D. Firewall rules that can be created with a tag from one peered network to another peered network
- E. Ability to share specific subnets across peered networks

Answer: AD

NEW QUESTION 26

In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard

Which options should you recommend to meet the requirements?

- A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
- B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
- C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
- D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

Answer: D

NEW QUESTION 29

Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer.

What type of Load Balancing should you use?

- A. Network Load Balancing
- B. HTTP(S) Load Balancing
- C. TCP Proxy Load Balancing
- D. SSL Proxy Load Balancing

Answer: D

NEW QUESTION 32

Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization. Which logging export strategy should you use to meet the requirements?

- A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM projec
- B. 2. Subscribe SIEM to the topic.
- C. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM projec
- D. 2. Process Cloud Storage objects in SIEM.
- E. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM projec
- F. 2. Subscribe SIEM to the topic.
- G. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each projec
- H. 2. Process Cloud Storage objects in SIEM.

Answer: B

NEW QUESTION 36

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

Answer: C

NEW QUESTION 38

A company's application is deployed with a user-managed Service Account key. You want to use Google- recommended practices to rotate the key. What should you do?

- A. Open Cloud Shell and run `gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT`.
- B. Open Cloud Shell and run `gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT--key=NEW_KEY`.
- C. Create a new key, and use the new key in the applicatio
- D. Delete the old key from the Service Account.
- E. Create a new key, and use the new key in the applicatio
- F. Store the old key on the system as a backup key.

Answer: C

NEW QUESTION 42

An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented. Which GCP solution should the organization use?

- A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
- B. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect
- C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
- D. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN

Answer: B

NEW QUESTION 47

You are creating an internal App Engine application that needs to access a user's Google Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google recommended practices. What should you do?

- A. Create a new Service account, and give all application users the role of Service Account User.
- B. Create a new Service account, and add all application users to a Google Grou
- C. Give this group the role of Service Account User.
- D. Use a dedicated G Suite Admin account, and authenticate the application's operations with these G Suite credentials.
- E. Create a new service account, and grant it G Suite domain-wide delegatio
- F. Have the application use it to impersonate the user.

Answer: A

NEW QUESTION 49

Your team wants to make sure Compute Engine instances running in your production project do not have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this requirement. How should your team meet these requirements?

- A. Enable Private Access on the VPC network in the production project.
- B. Remove the Editor role and grant the Compute Admin IAM role to the engineers.
- C. Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
- D. Set up a VPC network with two subnets: one with public IPs and one without public IPs.

Answer: C

NEW QUESTION 52

Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?

- A. ISO 27001
- B. ISO 27002
- C. ISO 27017
- D. ISO 27018

Answer: C

Explanation:

Create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.

NEW QUESTION 55

Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions.

What should you do?

- A. Change the load balancer backend configuration to use network endpoint groups instead of instance groups.
- B. Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.
- C. Create a new load balancer in us-east-2 using the Standard Tier network, and assign a static external IP address.
- D. Create a Cloud VPN connection between the two regions, and enable Google Private Access.

Answer: A

NEW QUESTION 56

A company is deploying their application on Google Cloud Platform. Company policy requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places.

Which Storage solution are they allowed to use?

- A. Cloud Bigtable
- B. Cloud BigQuery
- C. Compute Engine SSD Disk
- D. Compute Engine Persistent Disk

Answer: B

NEW QUESTION 59

An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

- A. Ensure that firewall rules are in place to meet the required controls.
- B. Set up Cloud Armor to ensure that network security controls can be managed for G Suite.
- C. Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite.
- D. Set up an array of Virtual Private Cloud (VPC) networks to control network security as mandated by the relevant regulation.

Answer: B

NEW QUESTION 64

An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable their developer teams to deploy new applications without the overhead of this full review.

How should you advise this organization?

- A. Use Forseti with Firewall filters to catch any unwanted configurations in production.
- B. Mandate use of infrastructure as code and provide static analysis in the CI/CD pipelines to enforce policies.
- C. Route all VPC traffic through customer-managed routers to detect malicious patterns in production.
- D. All production applications will run on-premise
- E. Allow developers free rein in GCP as their dev and QA platforms.

Answer: B

NEW QUESTION 65

A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries.

Where should you export the logs?

- A. BigQuery datasets
- B. Cloud Storage buckets
- C. StackDriver logging
- D. Cloud Pub/Sub topics

Answer: C

NEW QUESTION 66

A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time. What should you do?

- A. Use Resource Manager on the organization level.
- B. Use Forseti Security to automate inventory snapshots.
- C. Use Stackdriver to create a dashboard across all projects.
- D. Use Security Command Center to view all assets across the organization.

Answer: C

NEW QUESTION 69

A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published.

Which Google Cloud Service should be used to achieve this?

- A. Cloud Key Management Service
- B. Cloud Data Loss Prevention API
- C. BigQuery
- D. Cloud Security Scanner

Answer: D

NEW QUESTION 74

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

Professional-Cloud-Security-Engineer Practice Exam Features:

- * Professional-Cloud-Security-Engineer Questions and Answers Updated Frequently
- * Professional-Cloud-Security-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * Professional-Cloud-Security-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Professional-Cloud-Security-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The Professional-Cloud-Security-Engineer Practice Test Here](#)