

Google

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer



NEW QUESTION 1

Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google APIs or services. Which two settings must remain disabled to meet these requirements? (Choose two.)

- A. Public IP
- B. IP Forwarding
- C. Private Google Access
- D. Static routes
- E. IAM Network User Role

Answer: CD

NEW QUESTION 2

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet. What should your team grant to Engineering Group A to meet this requirement?

- A. Compute Network User Role at the host project level.
- B. Compute Network User Role at the subnet level.
- C. Compute Shared VPC Admin Role at the host project level.
- D. Compute Shared VPC Admin Role at the service project level.

Answer: C

NEW QUESTION 3

You will 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. What should you do?

- A. Create an Instance Template, and allow the Service Account Read Only access for the Compute Engine Access Scope.
- B. Create a custom role with the permission compute.instances.list and grant the Service Account this role.
- C. Give the Service Account the role of Compute Viewer, and use the new Service Account for all instances.
- D. Give the Service Account the role of Project Viewer, and use the new Service Account for all instances.

Answer: A

NEW QUESTION 4

Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

- A. Organization Administrator
- B. Super Admin
- C. GKE Cluster Admin
- D. Compute Admin
- E. Organization Role Viewer

Answer: AB

NEW QUESTION 5

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 6

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery. What should you do?

- A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.
- B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.
- C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.
- D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Answer: D

NEW QUESTION 7

An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier. Which Cloud Data Loss Prevention API technique should you use to accomplish this?

- A. Generalization

- B. Redaction
- C. CryptoHashConfig
- D. CryptoReplaceFfxFpeConfig

Answer: B

NEW QUESTION 8

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 9

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

- A. Send all logs to the SIEM system via an existing protocol such as syslog.
- B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.
- C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.
- D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Answer: C

NEW QUESTION 10

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk. What should you do?

- A. Migrate the application into an isolated project using a "Lift & Shift" approach
- B. Enable all internal TCP traffic using VPC Firewall rule
- C. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- D. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
- E. Refactor the application into a micro-services architecture in a GKE cluster
- F. Disable all traffic from outside the cluster using Firewall Rule
- G. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- H. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rule
- I. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Answer: C

NEW QUESTION 10

A customer's data science group wants to use Google Cloud Platform (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). The Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer and realized that their domain was already being used by G Suite. How should you best advise the Systems Engineer to proceed with the least disruption?

- A. Contact Google Support and initiate the Domain Contestation Process to use the domain name in your new Cloud Identity domain.
- B. Register a new domain name, and use that for the new Cloud Identity domain.
- C. Ask Google to provision the data science manager's account as a Super Administrator in the existing domain.
- D. Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

Answer: C

NEW QUESTION 12

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 15

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 application.
- D. Delete the old key from the Service Account.
- E. Create a new key, and use the new key in the application.
- F. Store the old key on the system as a backup key.

Answer: C

NEW QUESTION 20

A company is backing up application logs to a Cloud Storage bucket shared with both analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator. What should you do?

- A. Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket.
- B. If the scan detects PII, have the function move the file into a Cloud Storage bucket only accessible by the administrator.
- C. Upload the logs to both the shared bucket and the bucket only accessible by the administrator.
- D. Create a job trigger using the Cloud Data Loss Prevention API.
- E. Configure the trigger to delete any files from the shared bucket that contain PII.
- F. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.
- G. On the bucket shared with both the analysts and the administrator, configure a Cloud Storage Trigger that is only triggered when PII data is uploaded.
- H. Use Cloud Functions to capture the trigger and delete such files.

Answer: C

NEW QUESTION 23

A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing. How can you work with Infrastructure Operations Engineers to best ensure that Windows Compute Engine VMs are up to date with all the latest OS patches?

- A. Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.
- B. Federate a Domain Controller into Compute Engine, and roll out weekly patches via Group Policy Object.
- C. Use Deployment Manager to provision updated VMs into new serving Instance Groups (IGs).
- D. Reboot all VMs during the weekly maintenance window and allow the StartUp Script to download the latest patches from the internet.

Answer: D

NEW QUESTION 28

Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership. What should your team do to meet these requirements?

- A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Answer: B

NEW QUESTION 31

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior. What should you do to meet these requirements?

- A. Create a Folder per department under the Organization.
- B. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.
- C. Create a Folder per department under the Organization.
- D. For each department's Folder, assign the Project Browser role to the Google Group related to that department.
- E. Create a Project per department under the Organization.
- F. For each department's Project, assign the Project Viewer role to the Google Group related to that department.
- G. Create a Project per department under the Organization.
- H. For each department's Project, assign the Project Browser role to the Google Group related to that department.

Answer: C

NEW QUESTION 35

An application running on a Compute Engine instance needs to read data from a Cloud Storage bucket. Your team does not allow Cloud Storage buckets to be globally readable and wants to ensure the principle of least privilege. Which option meets the requirement of your team?

- A. Create a Cloud Storage ACL that allows read-only access from the Compute Engine instance's IP address and allows the application to read from the bucket without credentials.
- B. Use a service account with read-only access to the Cloud Storage bucket, and store the credentials to the service account in the config of the application on the Compute Engine instance.
- C. Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata.
- D. Encrypt the data in the Cloud Storage bucket using Cloud KMS, and allow the application to decrypt the data with the KMS key.

Answer: C

NEW QUESTION 40

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 44

.....

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](#)