



## Google

### Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls. Which document should you review to find the information?

- A. Google Cloud Platform: Customer Responsibility Matrix
- B. PCI DSS Requirements and Security Assessment Procedures
- C. PCI SSC Cloud Computing Guidelines
- D. Product documentation for Compute Engine

**Answer: C**

#### NEW QUESTION 2

You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM.

- A. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate one-way sync.
- B. Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have "user email address" as the attribute to facilitate bidirectional sync.
- C. Use a management tool to sync the subset based on the email address attribut
- D. Create a group in the Google domain
- E. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.
- F. Use a management tool to sync the subset based on group object class attribut
- G. Create a group in the Google domain
- H. A group created in a Google domain will automatically have an explicit Google Cloud Identity and Access Management (IAM) role.

**Answer: C**

#### NEW QUESTION 3

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 4

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 5

A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.

The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

- A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.
- B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
- C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.
- D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

**Answer: C**

#### NEW QUESTION 6

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 7

Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules,

subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection. The networking resources will need to be controlled by the network security team. Which type of networking design should your team use to meet these requirements?

- A. Shared VPC Network with a host project and service projects
- B. Grant Compute Admin role to the networking team for each engineering project
- C. VPC peering between all engineering projects using a hub and spoke model
- D. Cloud VPN Gateway between all engineering projects using a hub and spoke model

**Answer: A**

#### NEW QUESTION 8

Your company is storing sensitive data in Cloud Storage. You want a key generated on-premises to be used in the encryption process. What should you do?

- A. Use the Cloud Key Management Service to manage a data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage a key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

**Answer: A**

#### NEW QUESTION 9

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 10

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 10

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 11

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 16

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 18

A customer has 300 engineers. The company wants to grant different levels of access and efficiently manage IAM permissions between users in the development and production environment projects.

Which two steps should the company take to meet these requirements? (Choose two.)

- A. Create a project with multiple VPC networks for each environment.
- B. Create a folder for each development and production environment.
- C. Create a Google Group for the Engineering team, and assign permissions at the folder level.
- D. Create an Organizational Policy constraint for each folder environment.
- E. Create projects for each environment, and grant IAM rights to each engineering user.

**Answer:** BD

#### NEW QUESTION 20

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 23

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 25

You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards. What should you do?

- A. Use multi-factor authentication for admin access to the web application.
- B. Use only applications certified compliant with PA-DSS.
- C. Move the cardholder data environment into a separate GCP project.
- D. Use VPN for all connections between your office and cloud environments.

**Answer:** D

#### NEW QUESTION 28

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 29

You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.

How should you prevent and fix this vulnerability?

- A. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- B. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- C. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

**Answer:** D

#### NEW QUESTION 30

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 33

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 38

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 41

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 42

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 46

A customer wants to run a batch processing system on VMs and store the output files in a Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet. How should this be accomplished?

- A. Create a firewall rule to block internet traffic from the VM.
- B. Provision a NAT Gateway to access the Cloud Storage API endpoint.
- C. Enable Private Google Access on the VPC.
- D. Mount a Cloud Storage bucket as a local filesystem on every VM.

**Answer:** B

#### NEW QUESTION 47

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 project
- 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 project
- 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 project
- F. 2. Subscribe SIEM to the topic.
- G. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project
- H. 2. Process Cloud Storage objects in SIEM.

**Answer: B**

#### NEW QUESTION 50

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 53

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

- A. VPC Flow Logs
- B. Cloud Armor
- C. DNS Security Extensions
- D. Cloud Identity-Aware Proxy

**Answer: C**

#### NEW QUESTION 56

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 Group
- 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 delegation
- F. Have the application use it to impersonate the user.

**Answer: A**

#### NEW QUESTION 61

Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written to BigQuery was done using the App Engine Default Service Account.

What should you do?

- A. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Hide Matching Entry
- B. \* 4. Make sure the resulting list is empty.
- C. \* 1. Use StackDriver Logging and filter on BigQuery Insert Jobs.\* 2. Click on the email address in line with the App Engine Default Service Account in the authentication field.\* 3. Click Show Matching Entry
- D. \* 4. Make sure the resulting list is empty.
- E. \* 1. In BigQuery, select the related dataset.\* 2. Make sure the App Engine Default Service Account is the only account that can write to the dataset.
- F. \* 1. Go to the IAM section on the project.\* 2. Validate that the App Engine Default Service Account is the only account that has a role that can write to BigQuery.

**Answer: C**

#### NEW QUESTION 64

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 69

A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location. How should the company accomplish this?

- A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.
- B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.
- C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.
- D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

Answer: D

#### NEW QUESTION 71

You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects.

What should you do?

- A. Use a Shared VPC to enable communication between all projects, and use firewall rules to prevent data exfiltration.
- B. Create access levels in Access Context Manager to prevent data exfiltration, and use a shared VPC for communication between projects.
- C. Use an infrastructure-as-code software tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
- D. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.
- E. Use an infrastructure-as-code software tool to set up three different service perimeters for dev, staging, and prod and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Su
- F. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the respective perimeter.

Answer: B

#### NEW QUESTION 75

Your team uses a service account to authenticate data transfers from a given Compute Engine virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security.

What should you do?

- A. Temporarily disable authentication on the Cloud Storage bucket.
- B. Use the undelete command to recover the deleted service account.
- C. Create a new service account with the same name as the deleted service account.
- D. Update the permissions of another existing service account and supply those credentials to the applications.

Answer: B

#### NEW QUESTION 76

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.

Which product should be used to meet these requirements?

- A. Cloud Armor
- B. VPC Firewall Rules
- C. Cloud Identity and Access Management
- D. Cloud CDN

Answer: A

#### NEW QUESTION 80

An organization receives an increasing number of phishing emails.

Which method should be used to protect employee credentials in this situation?

- A. Multifactor Authentication
- B. A strict password policy
- C. Captcha on login pages
- D. Encrypted emails

Answer: D

#### NEW QUESTION 85

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 89

A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on Compute Engine. Their security team wants to add a security layer so that the ERP systems only accept traffic from Cloud Identity-Aware Proxy.  
What should the customer do to meet these requirements?

- A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
- B. Make sure that the ERP system can validate the identity headers in the HTTP requests.
- C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
- D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

**Answer: A**

#### NEW QUESTION 92

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 95

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.

Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses  
Which solution should your team implement to meet these requirements?

- A. Cloud Armor
- B. Network Load Balancing
- C. SSL Proxy Load Balancing
- D. NAT Gateway

**Answer: A**

#### NEW QUESTION 98

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.

What should you do?

- A. Use the Cloud Key Management Service to manage the data encryption key (DEK).
- B. Use the Cloud Key Management Service to manage the key encryption key (KEK).
- C. Use customer-supplied encryption keys to manage the data encryption key (DEK).
- D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

**Answer: A**

#### NEW QUESTION 101

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 102

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 103**

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys. What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing
- B. Manage the IAM permissions at the Key level.
- C. Create a single KeyRing for all persistent disks and all Keys in this KeyRing
- D. Manage the IAM permissions at the KeyRing level.
- E. Create a KeyRing per persistent disk, with each KeyRing containing a single Key
- F. Manage the IAM permissions at the Key level.
- G. Create a KeyRing per persistent disk, with each KeyRing containing a single Key
- H. Manage the IAM permissions at the KeyRing level.

**Answer: C**

**NEW QUESTION 108**

.....

## Relate Links

**100% Pass Your Professional-Cloud-Security-Engineer Exam with Examible Prep Materials**

<https://www.exambible.com/Professional-Cloud-Security-Engineer-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>