

Exam Questions Professional-Cloud-Security-Engineer

Google Cloud Certified - Professional Cloud Security Engineer

<https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/>



NEW QUESTION 1

A customer's company has multiple business units. Each business unit operates independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions.

Which strategy should you use to meet these needs?

- A. Create an organization node, and assign folders for each business unit.
- B. Establish standalone projects for each business unit, using gmail.com accounts.
- C. Assign GCP resources in a project, with a label identifying which business unit owns the resource.
- D. Assign GCP resources in a VPC for each business unit to separate network access.

Answer: A

NEW QUESTION 2

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 3

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised. What should you do?

- A. Enforce 2-factor authentication in GSuite for all users.
- B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
- C. Provision user passwords using GSuite Password Sync.
- D. Configure Cloud VPN between your private network and GCP.

Answer: D

NEW QUESTION 4

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 5

A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

- A. Configure the project with Cloud VPN.
- B. Configure the project with Shared VPC.
- C. Configure the project with Cloud Interconnect.
- D. Configure the project with VPC peering.
- E. Configure all Compute Engine instances with Private Access.

Answer: DE

NEW QUESTION 6

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 7

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 8

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 9

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 10

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 10

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 15

Applications often require access to "secrets" - small pieces of sensitive data at build or run time. The administrator managing these secrets on GCP wants to keep a track of "who did what, where, and when?" within their GCP projects.

Which two log streams would provide the information that the administrator is looking for? (Choose two.)

- A. Admin Activity logs
- B. System Event logs
- C. Data Access logs
- D. VPC Flow logs
- E. Agent logs

Answer: AC

NEW QUESTION 20

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 21

As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name. Which cost reduction options should you recommend?

- A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.
- B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.
- C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.
- D. Use FindingLimits and TimespanConfig to sample data and minimize transformation units.

Answer: C

NEW QUESTION 26

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 28

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 31

You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project. What should you do?

- A. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level
- B. List the trusted project as the whitelist in an allow operation.
- C. Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level
- D. List the trusted projects as the exceptions in a deny operation.
- E. In Resource Manager, edit the project permissions for the trusted project
- F. Add the organization as member with the role: Compute Image User.
- G. In Resource Manager, edit the organization permission
- H. Add the project ID as member with the role: Compute Image User.

Answer: B

NEW QUESTION 35

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 39

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 43

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 48

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 51

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Security-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Security-Engineer Product From:

<https://www.2passeasy.com/dumps/Professional-Cloud-Security-Engineer/>

Money Back Guarantee

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