PROFESSIONAL-CLOUD-SECURITY-ENGINEER^{Q&As}

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google
Official Exam Center

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps

1 / 5

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps

2 / 5

QUESTION 1

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google Cloud resources. Your export must meet the following requirements:

Export related logs for all projects in the Google Cloud organization.

Export logs in near real-time to an external SIEM.

What should you do? (Choose two.)

A. Create a Log Sink at the organization level with a Pub/Sub destination.

B. Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.

C. Enable Data Access audit logs at the organization level to apply to all projects.

D. Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.

E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Correct Answer: BD

Reference:

https://www.datadoghq.com/blog/monitoring-gcp-audit-logs/ https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#services "Google Workspace Login Audit: Login Audit logs track user sign-ins to your domain. These logs only

record the login event. They don\\'t record which system was used to perform the login action."

QUESTION 2

You need to implement an encryption at-rest strategy that reduces key management complexity for non- sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types.

What should you do?

A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.

B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service

C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.

D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Correct Answer: D

Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provideflexibility of

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps

3 / 5

controlling the key residency and rotation schedule, use google provided key for non- sensitive and encrypt sensitive data with Cloud Key Management Service

---

QUESTION 3

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.

Correct Answer: A

https://cloud.google.com/load-balancing/docs/tcp https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing

TCP Proxy Load Balancing is implemented on GFEs that are distributed globally. If you choose the Premium Tier of Network Service Tiers, a TCP proxy load balancer is global. In Premium Tier, you can deploy backends in multiple regions, and the load balancer automatically directs user traffic to the closest region that has capacity. If you choose the Standard Tier, a TCP proxy load balancer can only direct traffic among backends in a single region.

QUESTION 4

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments.

How should you design the network to inspect the traffic?

A. 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.

B. 1. Set up one VPC with two subnets: one trusted and the other untrusted.

2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.

C. 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together.

2. Configure a custom route on each network pointed to the virtual appliance.

D. 1. Set up two VPC networks: one trusted and the other untrusted.

2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

Correct Answer: D

Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps |
PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps

4 / 5

Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.

https://cloud.google.com/architecture/best-practices-vpc-design#l7

This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

QUESTION 5

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. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.

B. Upload the logs to both the shared bucket and the bucket only accessible by the administrator. Create a job trigger using the Cloud Data Loss Prevention API. Configure the trigger to delete any files from the shared bucket that contain PII.

C. On the bucket shared with both the analysts and the administrator, configure Object Lifecycle Management to delete objects that contain any PII.

D. 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. Use Cloud Functions to capture the trigger and delete such files.

Correct Answer: A

https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0
https://www.youtube.com/watch?v=0TmO1f-Ox40