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.pass2lead.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

QUESTION 1

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.

Correct Answer: C

https://cloud.google.com/identity/solutions/automate-user- provisioning#cloud_identity_automated_provisioning

"Cloud Identity has a catalog of automated provisioning connectors, which act as a bridge between Cloud Identity and third-party cloud apps."

QUESTION 2

You define central security controls in your Google Cloud environment for one of the folders in your organization you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later you receive an alert about a new VM with an external IP address under that folder.

What could have caused this alert?

A. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.

B. The organizational policy constraint wasn\\'t properly enforced and is running in "dry run mode.

C. At project level, the organizational policy control has been overwritten with an \\'allow\\' value.

D. The policy constraint on the folder level does not have any effect because of an allow" value for that constraint on the organizational level.

Correct Answer: C

QUESTION 3

Which type of load balancer should you use to maintain client IP by default while using the standard network tier?

A. SSL Proxy

B. TCP Proxy

C. Internal TCP/UDP

D. TCP/UDP Network

Correct Answer: D

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

QUESTION 4

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

Correct Answer: C

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. https://cloud.google.com/security/compliance/iso-27017

QUESTION 5

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

Correct Answer: AB

Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules

QUESTION 6

Your company conducts clinical trials and needs to analyze the results of a recent study that are stored in BigQuery. The interval when the medicine was taken contains start and stop dates. The interval data is critical to the analysis, but specific dates may identify a particular batch and introduce bias. You need to obfuscate the start and end dates for each

row and preserve the interval data.

What should you do?

A. Use date shifting with the context set to the unique ID of the test subject.

B. Extract the date using TimePartConfig from each date field and append a random month and year.

C. Use bucketing to shift values to a predetermined date based on the initial value.

D. Use the FFX mode of format preserving encryption (FPE) and maintain data consistency.

Correct Answer: A

Option A and D works, but the focus here is to preserve the interval data.

So option A is more suited in this case.

"Date shifting techniques randomly shift a set of dates but preserve the sequence and duration of a period of time. Shifting dates is usually done in context to an individual or an entity. That is, each individual\\'s dates are shifted by an amount

of time that is unique to that individual."

QUESTION 7

A database administrator notices malicious activities within their Cloud SQL instance. The database administrator wants to monitor the API calls that read the configuration or metadata of resources. Which logs should the database administrator review?

A. Admin Activity

B. System Event

C. Access Transparency

D. Data Access

Correct Answer: D

https://cloud.google.com/logging/docs/audit/#data-access "Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data."

QUESTION 8

Your company\\'s chief information security officer (CISO) is requiring business data to be stored in specific locations due to regulatory requirements that affect the company\\'s global expansion plans. After working on a plan to implement this requirement, you determine the following:

1.

The services in scope are included in the Google Cloud data residency requirements.

2.

The business data remains within specific locations under the same organization. The folder structure can contain multiple data residency locations.

3.

The projects are aligned to specific locations.

You plan to use the Resource Location Restriction organization policy constraint with very granular control. At which level in the hierarchy should you set the constraint?

A. Organization

B. Resource

C. Project

D. Folder

Correct Answer: C

QUESTION 9

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

Correct Answer: CD

App Engine ingress firewall rules are available, but egress rules are not currently available. Per requirements 1.2.1 and 1.3.4, you must ensure that all outbound traffic is authorized. SAQ A-EP and SAQ D-Type merchants must provide compensating controls or use a different Google Cloud product. Compute Engine and GKE are the preferred alternatives. https://cloud.google.com/solutions/pci-dss-compliance-in- gcp

QUESTION 10

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 11

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.

Correct Answer: B

"Isolate VMs using service accounts when possible" "even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped." https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts

---

QUESTION 12

A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to manage and rotate the encryption keys.

Which boot disk encryption solution should you use on the cluster to meet this customer\\'s requirements?

A. Customer-supplied encryption keys (CSEK)

B. Customer-managed encryption keys (CMEK) using Cloud Key Management Service (KMS)

C. Encryption by default

D. Pre-encrypting files before transferring to Google Cloud Platform (GCP) for analysis

Correct Answer: B

Reference https://cloud.google.com/kubernetes-engine/docs/how-to/dynamic-provisioning-cmek

QUESTION 13

Your application is deployed as a highly available cross-region solution behind a global external HTTP(S) load balancer. You notice significant spikes in traffic from multiple IP addresses but it is unknown whether the IPs are malicious. You are concerned about your application\\'s availability. You want to limit traffic from these clients over a specified time interval.

What should you do?

A. Configure a rate_based_ban action by using Google Cloud Armor and set the ban_duration_sec parameter to the specified time interval.

B. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.

C. Configure a throttle action by using Google Cloud Armor to limit the number of requests per client over a specified time interval.

D. Configure a firewall rule in your VPC to throttle traffic from the identified IP addresses.

Correct Answer: C

QUESTION 14

Your company\\'s new CEO recently sold two of the company\\'s divisions. Your Director asks you to help migrate the Google Cloud projects associated with those divisions to a new organization node. Which preparation steps are necessary before this migration occurs? (Choose two.)

A. Remove all project-level custom Identity and Access Management (1AM) roles.

B. Disallow inheritance of organization policies.

C. Identify inherited Identity and Access Management (1AM) roles on projects to be migrated.

D. Create a new folder for all projects to be migrated.

E. Remove the specific migration projects from any VPC Service Controls perimeters and bridges.

Correct Answer: CE

QUESTION 15

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.

Correct Answer: C

https://cloud.google.com/containers/security Containers are meant to be immutable, so you deploy a new image in order to make changes. You can simplify patch management by rebuilding your images regularly, so the patch is picked up the next time a container is deployed. Get the full picture of your environment with regular image security reviews.