[Nov-2023 Latest Google Professional-Cloud-Security-Engineer Certification Practice Test Questions [Q84-Q99

[Nov-2023] Latest Google Professional-Cloud-Security-Engineer Certification Practice Test Questions
Verified Professional-Cloud-Security-Engineer Dumps Q&As - 1 Year Free & Quickly Updates

QUESTION 84

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?
* Google Cloud Directory Sync (GCDS)
* Cloud Identity
* Security Assertion Markup Language (SAML)
* Pub/Sub

Reference:

https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction

QUESTION 85

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?
* VPC Flow Logs
* Cloud Armor
* DNS Security Extensions
* Cloud Identity-Aware Proxy

https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns

QUESTION 86

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?
* Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
* Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
* Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
* Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

QUESTION 87

Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?
* Use Security Health Analytics to determine user activity.
* Use the Cloud Monitoring console to filter audit logs by user.
* Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.
* Use the Logs Explorer to search for user activity.

We use audit logs by searching the Service Account and checking activities in the past 2 months. (the user identity will not be seen since he used the SA identity but we can make correlations based on ip address, working hour, etc.)

QUESTION 88

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?
* Cloud Armor
* Network Load Balancing
* SSL Proxy Load Balancing
* NAT Gateway

Explanation

https://cloud.google.com/armor/docs/security-policy-overview#edge-security

QUESTION 89

You want to make sure that your organization’s Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all Cloud Storage buckets. What should you do?
* Remove Owner roles from end users, and configure Cloud Data Loss Prevention.
* Remove Owner roles from end users, and enforce domain restricted sharing in an organization policy.
* Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.
* Remove *.setIamPolicy permissions from all roles, and enforce domain restricted sharing in an organization policy.
– Uniform bucket-level access: https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use

– Domain Restricted Sharing:
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public_data_sharing

QUESTION 90

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?
* Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.
* Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted projects as the exceptions in a deny operation.
* In Resource Manager, edit the project permissions for the trusted project. Add the organization as member with the role: Compute Image User.
* In Resource Manager, edit the organization permissions. Add the project ID as member with the role: Compute Image User.

QUESTION 91

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?
* Google Cloud Directory Sync (GCDS)
* Cloud Identity
* Security Assertion Markup Language (SAML)
* Pub/Sub
Explanation

Explanation/Reference: https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction

QUESTION 92

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?

* Use Cloud Storage as a federated Data Source.
* Use a Cloud Hardware Security Module (Cloud HSM).
* Customer-managed encryption keys (CMEK).
* Customer-supplied encryption keys (CSEK).

Explanation

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption keys (CMEK).
https://cloud.google.com/bigquery/docs/encryption-at-rest

QUESTION 93

A customer terminates an engineer and needs to make sure the engineer’s Google account is automatically deprovisioned.

What should the customer do?
* Use the Cloud SDK with their directory service to remove their IAM permissions in Cloud Identity.
* Use the Cloud SDK with their directory service to provision and deprovision users from Cloud Identity.
* Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity.
* Configure Cloud Directory Sync with their directory service to remove their IAM permissions in Cloud Identity.

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 94

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?
* Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
* Make sure that the ERP system can validate the identity headers in the HTTP requests.
* Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
* Make sure that the ERP system can validate the user’s unique identifier headers in the HTTP requests.

QUESTION 95

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?
* Enable Private Access on the VPC network in the production project.
* Remove the Editor role and grant the Compute Admin IAM role to the engineers.
* Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.
* Set up a VPC network with two subnets: one with public IPs and one without public IPs.

https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

QUESTION 96

A Cloud Development team needs to use service accounts extensively in their local development.

You need to provide the team with the keys for these service accounts. You want to follow Google-recommended practices. What should you do?
* Implement a daily key rotation process that generates a new key and commits it to the source code repository every day.
* Implement a daily key rotation process, and provide developers with a Cloud Storage bucket from which they can download the new key every day.
* Create a Google Group with all developers. Assign the group the IAM role of Service Account User, and have developers generate and download their own keys.
* Create a Google Group with all developers. Assign the group the IAM role of Service Account Admin, and have developers generate and download their own keys.
A is not correct because source code repository isn’t the place to store keys that expire/change.

B is correct because it allows for centralized admin managed key rotation process and doesn’t delegate key creation to developers which is easier and secure way to manage keys.

C is not correct because the IAM role specified doesn’t allow for creation of keys.

D is not correct because it veers away from best practices as the keys now reside in decentralized place and can be subjected to a leak.

https://cloud.google.com/blog/products/gcp/help-keep-your-google-cloud-service-account-keys-safe

https://cloud.google.com/iam/docs/understanding-service-accounts#best_practices

https://cloud.google.com/iam/docs/creating-managing-service-account-keys

QUESTION 97

Which international compliance standard provides guidelines for information security controls applicable to the provision and use of cloud services?
* ISO 27001
* ISO 27002
* ISO 27017
* ISO 27018
Explanation

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 98

You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud environment in the daily ETL process from an on-premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re-identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)
* Secret Manager
* Cloud Key Management Service
* Cloud Data Loss Prevention with cryptographic hashing

* Cloud Data Loss Prevention with automatic text redaction
* Cloud Data Loss Prevention with deterministic encryption using AES-SIV

Explanation

B: you need KMS to store the CryptoKey

https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#crypt E: for the de-identity you need to use CryptoReplaceFfxFpeConfig or CryptoDeterministicConfig

https://cloud.google.com/dlp/docs/reference/rest/v2/projects.deidentifyTemplates#cryptodeterministicconfig

https://cloud.google.com/dlp/docs/deidentify-sensitive-data

QUESTION 99

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?

* 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project.

2.Subscribe SIEM to the topic.

* 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project.

2.Process Cloud Storage objects in SIEM.

* 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.

2.Subscribe SIEM to the topic.

* 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.

2.Process Cloud Storage objects in SIEM.

Explanation

“Your team needs to obtain a unified log view of all development cloud projects in your SIEM” – This means we are ONLY interested in development projects. “The development projects are under the NONPROD organization folder with the test and pre-production projects” – We will need to filter out development from others i.e test and pre-prod. “The development projects share the ABC-BILLING billing account with the rest of the organization.” – This is unnecessary information.

Latest 2023 Realistic Verified Professional-Cloud-Security-Engineer Dumps - 100% Free Professional-Cloud-Security-Engineer Exam Dumps:
https://www.vceprep.com/Professional-Cloud-Security-Engineer-latest-vce-prep.html]