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

Professional Cloud Security Engineer

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

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

QUESTION 1

A company is running their webshop on Google Kubernetes Engine and wants to analyze customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery What should you do?

A. Create a BigQuery view with regular expressions matching credit card numbers to query and delete affected rows.

B. Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.

C. Leverage Security Command Center to scan for the assets of type Credit Card Number in BigQuery.

D. Enable Cloud Identity-Aware Proxy to filter out credit card numbers before storing the logs in BigQuery.

Correct Answer: B

https://cloud.google.com/bigquery/docs/scan-with-dlp

Cloud Data Loss Prevention API allows to detect and redact or remove sensitive data before the comments or reviews are published. Cloud DLP will read information from BigQuery, Cloud Storage or Datastore and scan it for sensitive data.

QUESTION 2

You are working with a client that is concerned about control of their encryption keys for sensitive data. The client does not want to store encryption keys at rest in the same cloud service provider (CSP) as the data that the keys are encrypting.

Which Google Cloud encryption solutions should you recommend to this client? (Choose two.)

A. Customer-supplied encryption keys.

B. Google default encryption

C. Secret Manager

D. Cloud External Key Manager

E. Customer-managed encryption keys

Correct Answer: AD

QUESTION 3

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 4

You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

A. Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.

B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.

C. Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.

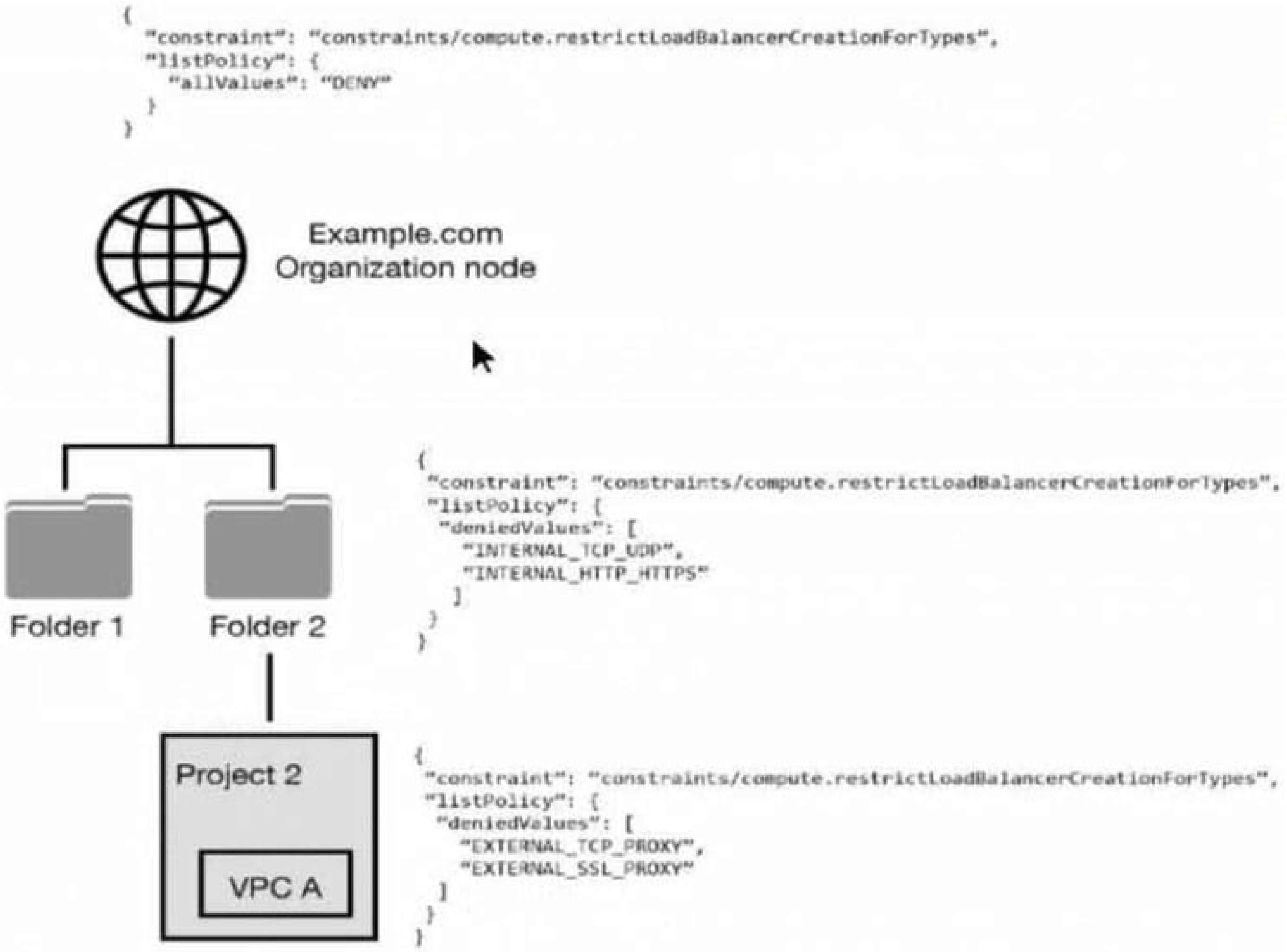
D. Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Correct Answer: B

https://cloud.google.com/storage/docs/public-access-prevention Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

QUESTION 5

You have the following resource hierarchy. There is an organization policy at each node in the hierarchy as shown. Which load balancer types are denied in VPC A?



```
{
  "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
  "listPolicy": {
    "allValues": "DENY"
  }
}
```

```
{
 "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
 "listPolicy": {
  "deniedValues": [
    "INTERNAL_TCP_UDP",
    "INTERNAL_HTTP_HTTPS"
  ]
  }
}
```

```
{
 "constraint": "constraints/compute.restrictLoadBalancerCreationForTypes",
 "listPolicy": {
  "deniedValues": [
    "EXTERNAL_TCP_PROXY",
    "EXTERNAL_SSL_PROXY"
  ]
  }
}
```

A. All load balancer types are denied in accordance with the global node\\'s policy.

B. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder\\'s policy.

C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project\\'s policy.

D. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project\\'s policies.

Correct Answer: A

QUESTION 6

You are a Security Administrator at your organization. You need to restrict service account creation capability within production environments. You want to accomplish this centrally across the organization. What should you do?

A. Use Identity and Access Management (IAM) to restrict access of all users and service accounts that have access to the production environment.

B. Use organization policy constraints/iam.disableServiceAccountKeyCreation boolean to disable the creation of new service accounts.

C. Use organization policy constraints/iam.disableServiceAccountKeyUpload boolean to disable the creation of new service accounts.

D. Use organization policy constraints/iam.disableServiceAccountCreation boolean to disable the creation of new service accounts.

Correct Answer: D

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#disable_service_account_creation You can use the iam.disableServiceAccountCreation boolean constraint to disable the creation of new service accounts. This allows you to centralize management of service accounts while not restricting the other permissions your developers have on projects.

QUESTION 7

You are working with a client who plans to migrate their data to Google Cloud. You are responsible for recommending an encryption service to manage their encrypted keys. You have the following requirements:

The master key must be rotated at least once every 45 days. The solution that stores the master key must be FIPS 140-2 Level 3 validated. The master key must be stored in multiple regions within the US for redundancy.

Which solution meets these requirements?

A. Customer-managed encryption keys with Cloud Key Management Service

B. Customer-managed encryption keys with Cloud HSM

C. Customer-supplied encryption keys

D. Google-managed encryption keys

Correct Answer: B

https://cloud.google.com/docs/security/key-management-deep-dive https://cloud.google.com/kms/docs/faq

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).

Correct Answer: C

This is a Customer-supplied encryption keys (CSEK). We generate our own encryption key and manage it on-premises. A KEK never leaves Cloud KMS.There is no KEK or KMS on-premises. Encryption at rest by default, with various key management options https://cloud.google.com/security/encryption-at-rest

Reference: https://cloud.google.com/security/encryption-at-rest/default-encryption/

QUESTION 9

Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of Google Cloud user accounts being compromised. What should you do?

A. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with security keys in the Google Admin console.

B. Create a Cloud Identity password policy with strong password settings, and configure 2-Step Verification with verification codes via text or phone call in the Google Admin console.

C. Create an Active Directory domain password policy with strong password settings, and configure post- SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.

D. Create an Active Directory domain password policy with strong password settings, and configure post- SSO (single sign-on) 2-Step Verification with verification codes via text or phone call in the Google Admin console.

Correct Answer: C

Reference: https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-introduction

"We recommend against using text messages. The National Institute of Standards and Technology (NIST) no longer recommends SMS-based 2SV due to the hijacking risk from state-sponsored entities."

QUESTION 10

You want to use the gcloud command-line tool to authenticate using a third-party single sign-on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)

A. SSO SAML as a third-party IdP

B. Identity Platform

C. OpenID Connect

D. Identity-Aware Proxy

E. Cloud Identity

Correct Answer: AC

To provide users with SSO-based access to selected cloud apps, Cloud Identity as your IdP supports the OpenID Connect (OIDC) and Security Assertion Markup Language 2.0 (SAML) protocols. https:// cloud.google.com/identity/solutions/ enable-sso

QUESTION 11

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.

Correct Answer: A

"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP. Once the identities have been replicated then it\\'s possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control."

QUESTION 12

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. Manage the IAM permissions at the Key level.

B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.

D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B

https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk

QUESTION 13

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.

Correct Answer: A

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

QUESTION 14

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

QUESTION 15

Your company recently published a security policy to minimize the usage of service account keys. On- premises Windows-based applications are interacting with Google Cloud APIs. You need to implement Workload Identity Federation (WIF) with your identity provider on-premises.

What should you do?

A. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS) Configure a rule to let principals in the pool impersonate the Google Cloud service account.

B. Set up a workload identity pool with your corporate Active Directory Federation Service (ADFS) Let all principals in the pool impersonate the Google Cloud service account.

C. Set up a workload identity pool with an OpenID Connect (OIDC) service on the name machine Configure a rule to let principals in the pool impersonate the Google Cloud service account.

D. Set up a workload identity pool with an OpenID Connect (OIDC) service on the same machine Let all principals in the pool impersonate the Google Cloud service account.

Correct Answer: A