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

Your organization recently activated the Security Command Center {SCO standard tier. There are a few Cloud Storage buckets that were accidentally made accessible to the public. You need to investigate the impact of the incident and remediate it.

What should you do?

A. 1 Remove the Identity and Access Management (IAM) granting access to allusers from the buckets 2 Apply the organization policy storage. unifromBucketLevelAccess to prevent regressions 3 Query the data access logs to report on unauthorized access

B. 1 Change bucket permissions to limit access 2 Query the data access audit logs for any unauthorized access to the buckets 3 After the misconfiguration is corrected mute the finding in the Security Command Center

C. 1 Change permissions to limit access for authorized users 2 Enforce a VPC Service Controls perimeter around all the production projects to immediately stop any unauthorized access 3 Review the administrator activity audit logs to report on any unauthorized access

D. 1 Change the bucket permissions to limit access 2 Query the buckets usage logs to report on unauthorized access to the data 3 Enforce the organization policy storage.publicAccessPrevention to avoid regressions

Correct Answer: D

QUESTION 2

You plan to synchronize identities to Cloud Identity from a third-party identity provider (IdP). You discovered that some employees used their corporate email address to set up consumer accounts to access Google services. You need to

ensure that the organization has control over the configuration, security, and lifecycle of these consumer accounts.

What should you do? (Choose two.)

A. Mandate that those corporate employees delete their unmanaged consumer accounts.

B. Reconcile accounts that exist in Cloud Identity but not in the third-party IdP.

C. Evict the unmanaged consumer accounts in the third-party IdP before you sync identities.

D. Use Google Cloud Directory Sync (GCDS) to migrate the unmanaged consumer accounts\\' emails as user aliases.

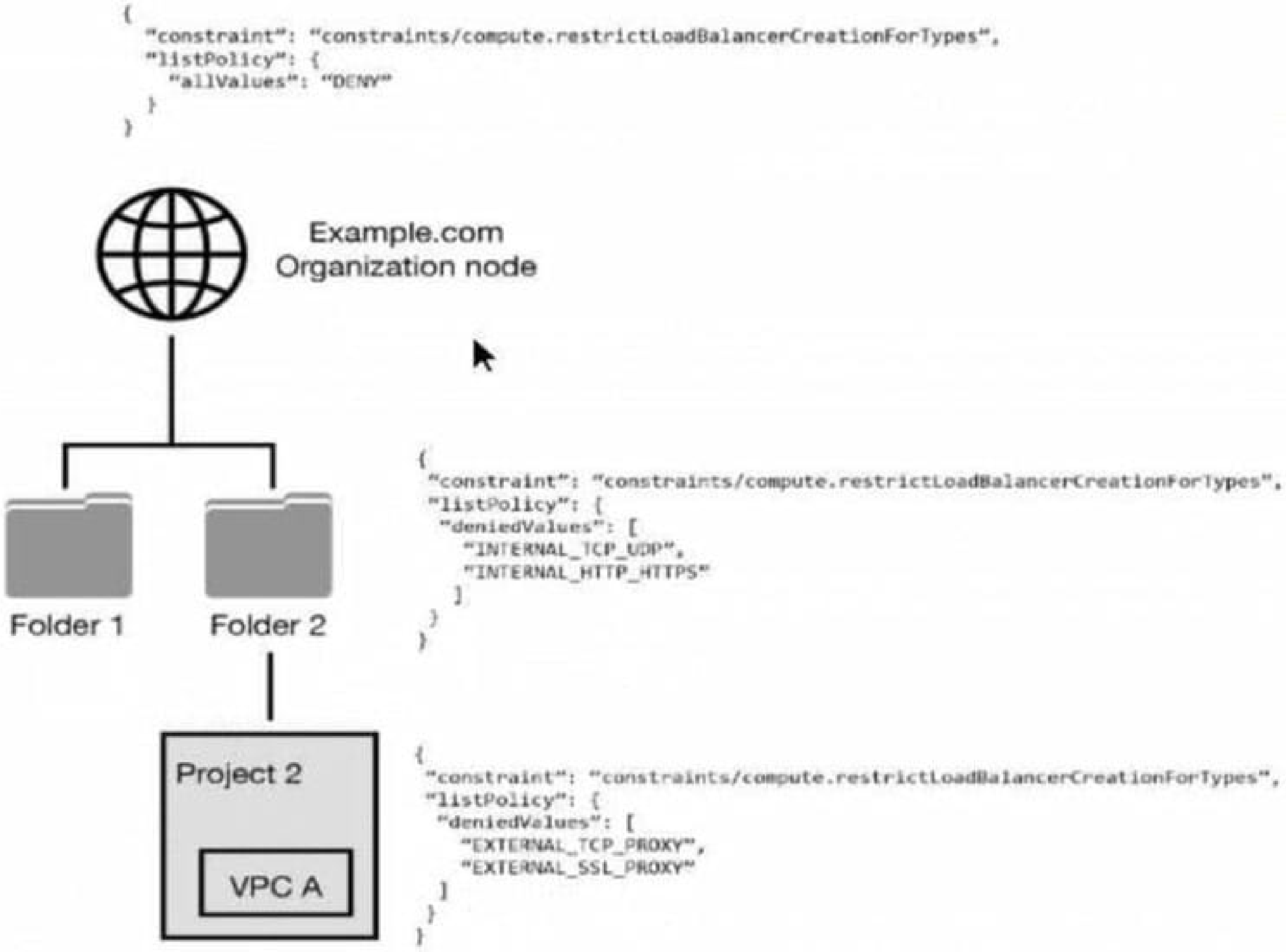
E. Use the transfer tool to invite those corporate employees to transfer their unmanaged consumer accounts to the corporate domain.

Correct Answer: BE

To ensure control over the configuration, security, and lifecycle of consumer accounts created with corporate email addresses, you should reconcile accounts that exist in Cloud Identity but not in the third- party IdP (B). This helps to align accounts and ensure consistent management. Additionally, you can use the transfer tool to invite employees to transfer their unmanaged consumer accounts to the corporate domain (E), which allows you to bring these accounts under the organization\\'s control in Cloud Identity.

QUESTION 3

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 4

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 5

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.

Correct Answer: B

https://cloud.google.com/compute/docs/access/iam

PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps

PROFESSIONAL-CLOUD-SECURITY-ENGINEER VCE Dumps

PROFESSIONAL-CLOUD-SECURITY-ENGINEER Practice Test