# PROFESSIONAL-CLOUD-SECURITY-ENGINEER<sup>Q&As</sup>

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.leads4pass.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

2 / 6

## QUESTION 1

Your company\\'s users access data in a BigQuery table. You want to ensure they can only access the data during working hours.

What should you do?

A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

B. Run a gsutil script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.

C. Assign a BigQuery Data Viewer role to a service account that adds and removes the users daily during the specified working hours.

D. Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraint for BigQuery during the specified working hours.
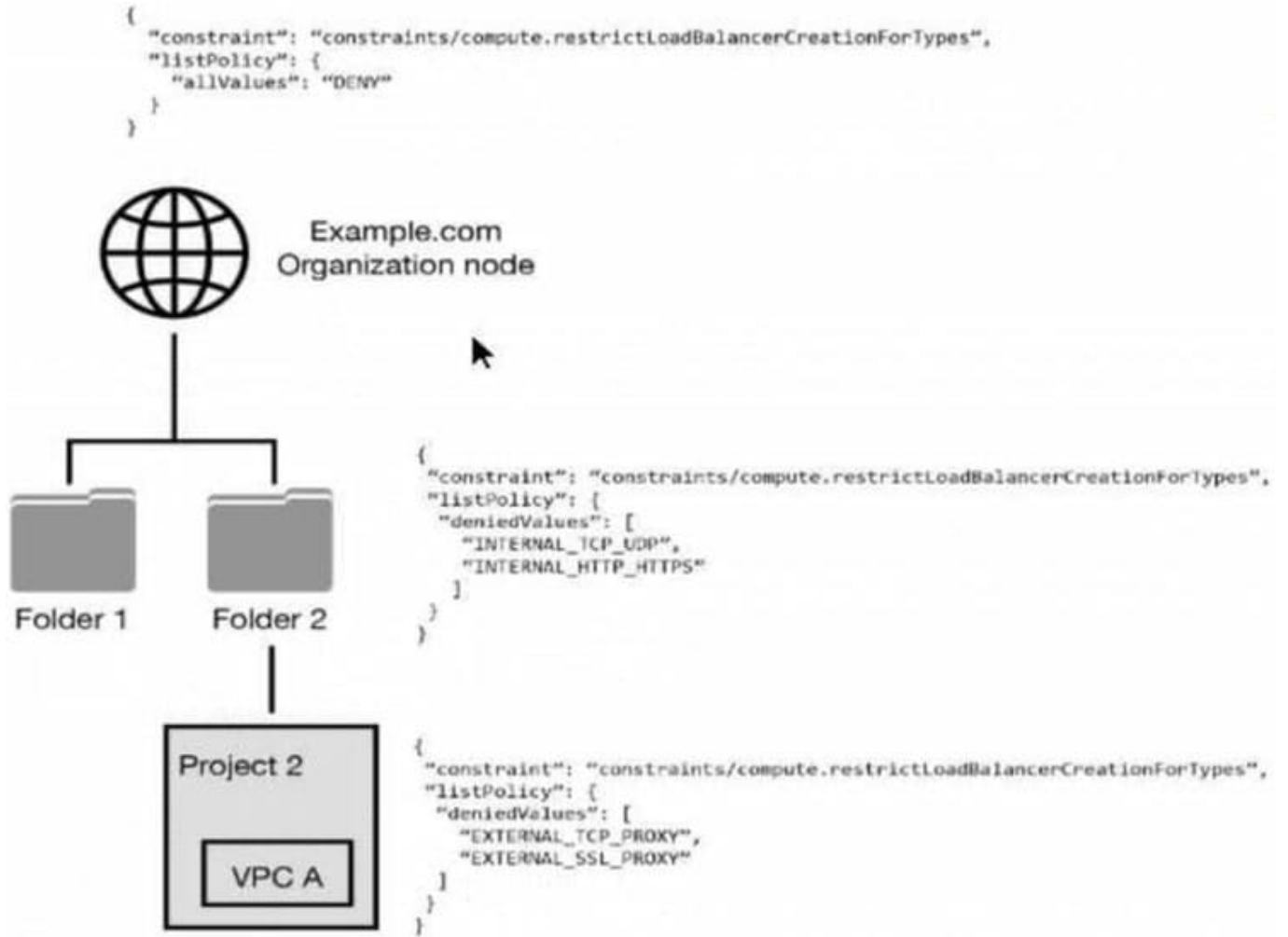
Correct Answer: A

The correct answer is A. Assign a BigQuery Data Viewer role along with an IAM condition that limits the access to specified working hours.

IAM conditions in Google Cloud can be used to fine-tune access control according to attributes like time, date, and IP address. In this case, you can create an IAM condition that allows access only during working hours. This condition can be attached to the BigQuery Data Viewer role, ensuring that users can only access the data in the BigQuery table during the specified times.

## QUESTION 2

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"
    }
}
```

Example.com
Organization node

Folder 1      Folder 2

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

Project 2

VPC A

```
{
    "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 3**

Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that

meets the following requirements:

Only allows communication between the Web and App tiers.

Enforces consistent network security when autoscaling the Web and App tiers.

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

4 / 6

Prevents Compute Engine Instance Admins from altering network traffic.

What should you do?

A. 1. Configure all running Web and App servers with respective network tags.

2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.

B. 1. Configure all running Web and App servers with respective service accounts.

2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

C. 1. Re-deploy the Web and App servers with instance templates configured with respective network tags.

2. Create an allow VPC firewall rule that specifies the target/source with respective network tags.

D. 1. Re-deploy the Web and App servers with instance templates configured with respective service accounts.

2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

Correct Answer: D

https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags

https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags A service account represents an identity associated with an instance. Only one service account can be associated with an instance. You control access to the service account by controlling the grant of the Service Account User role for other IAM principals. For an IAM principal to start an instance by using a service account, that principal must have the Service Account User role to at least use that service account and appropriate permissions to create instances (for example, having the Compute Engine Instance Admin role to the project).

---

**QUESTION 4**

When working with agents in a support center via online chat, an organization\\'s customers often share pictures of their documents with personally identifiable information (PII). The organization that owns the support center is concerned that the PII is being stored in their databases as part of the regular chat logs they retain for review by internal or external analysts for customer service trend analysis.

Which Google Cloud solution should the organization use to help resolve this concern for the customer while still maintaining data utility?

A. Use Cloud Key Management Service (KMS) to encrypt the PII data shared by customers before storing it for analysis.

B. Use Object Lifecycle Management to make sure that all chat records with PII in them are discarded and not saved for analysis.

C. Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.

D. Use the generalization and bucketing actions of the DLP API solution to redact PII from the texts before storing them for analysis.

Correct Answer: C

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

5 / 6

https://cloud.google.com/dlp/docs/concepts-image-redaction

**QUESTION 5**

A company allows every employee to use Google Cloud Platform. Each department has a Google Group, with all department members as group members. If a department member creates a new project, all members of that department should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. You need to configure this behavior.

What should you do to meet these requirements?

A. Create a Folder per department under the Organization. For each department\\\'s Folder, assign the Project Viewer role to the Google Group related to that department.

B. Create a Folder per department under the Organization. For each department\\\'s Folder, assign the Project Browser role to the Google Group related to that department.

C. Create a Project per department under the Organization. For each department\\\'s Project, assign the Project Viewer role to the Google Group related to that department.

D. Create a Project per department under the Organization. For each department\\\'s Project, assign the Project Browser role to the Google Group related to that department.

Correct Answer: A

https://cloud.google.com/iam/docs/understanding-roles#project-roles