

[Google Discussions](#)

## Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

### EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 208 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 208

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

Your organization recently activated the Security Command Center (SCC) 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 all Users from the buckets.  
2. Apply the organization policy storage.uniformBucketLevelAccess to prevent regressions.  
3. Query the data access logs to report on unauthorized access.
- B. 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.
- C. 1. Change the bucket permissions to limit access.  
2. Query the bucket's usage logs to report on unauthorized access to the data.  
3. Enforce the organization policy storage.publicAccessPrevention to avoid regressions.
- D. 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.

[Show Suggested Answer](#)

## Comments

Type your comment...

Submit

  **Xoxoo** 10 months, 1 week ago

**Selected Answer: C**

Here's why option C is the most appropriate choice:

Change Bucket Permissions to Limit Access: The first step is to immediately change the bucket permissions to limit access and revoke public access. This is crucial for preventing further unauthorized access to the data stored in the Cloud Storage buckets.

Query Bucket's Usage Logs: Querying the bucket's usage logs allows you to investigate the impact of the incident by identifying any unauthorized access or suspicious activity. You can use these logs to assess the extent of the breach and gather information about which objects or data were accessed.

Enforce storage.publicAccessPrevention: To prevent similar incidents from happening in the future, you should enforce the organization policy storage.publicAccessPrevention. This policy helps ensure that public access is prevented at the organizational level, reducing the risk of accidental misconfigurations.

   upvoted 4 times

  **Xoxoo** 10 months, 1 week ago

Option A is not as comprehensive because it doesn't include enforcing the organization policy to prevent regressions (storage.publicAccessPrevention).

Option B suggests enforcing VPC Service Controls, which is a good practice for network-level security, but it may not be directly related to securing Cloud Storage buckets and investigating unauthorized access. Additionally, reviewing administrator activity audit logs is not as effective for investigating the impact on unauthorized data access as querying the bucket's usage logs.

Option D is similar to Option C but does not include the proactive enforcement of storage.publicAccessPrevention to prevent future regressions. Enforcing this policy is essential to maintain security.

   upvoted 2 times

  **anshad666** 11 months ago

**Selected Answer: C**

c -looks good

   upvoted 1 times

  **akg001** 11 months, 2 weeks ago

**Selected Answer: C**

C - is correct

   upvoted 2 times

  **pfilourenco** 11 months, 4 weeks ago

**Selected Answer: C**

C - usage logs to track access that occurs because a resource has allUsers or allAuthenticatedUsers - <https://cloud.google.com/storage/docs/access-logs#should-you-use> and the constraint - <https://cloud.google.com/storage/docs/org-policy-constraints#public-access-prevention>

   upvoted 4 times

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics