

[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 115 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 115

Topic #: 1

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

The security operations team needs access to the security-related logs for all projects in their organization. They have the following requirements:

- ⇒ Follow the least privilege model by having only view access to logs.
- ⇒ Have access to Admin Activity logs.
- ⇒ Have access to Data Access logs.
- ⇒ Have access to Access Transparency logs.

Which Identity and Access Management (IAM) role should the security operations team be granted?

- A. roles/logging.privateLogViewer
- B. roles/logging.admin
- C. roles/viewer
- D. roles/logging.viewer




[Show Suggested Answer](#)

by [Nicky1402](#) at May 9, 2022, 10:22 a.m.

Comments

Type your comment...

[Submit](#)

  **mouchu** Highly Voted  2 years, 8 months ago

Answer = A




roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default bucket.

   upvoted 18 times

  **mT3** 2 years, 8 months ago

Ref: <https://cloud.google.com/logging/docs/access-control>

   upvoted 5 times

  **Littleivy** Highly Voted  2 years, 2 months ago

Selected Answer: A

You need roles/logging.privateLogViewer to view data access log and Access Transparency logs

<https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs#viewing-logs>

https://developers.google.com/cloud-search/docs/guides/audit-logging-manual#audit_log_permissions


   upvoted 5 times

  **KLei** Most Recent  7 months, 1 week ago

Selected Answer: A

For access to all logs in the _Required bucket, and access to the _Default view on the _Default bucket, grant the Logs Viewer (roles/logging.viewer) role.

For access to all logs in the _Required and _Default buckets, including data access logs, grant the Private Logs Viewer (roles/logging.privateLogViewer) role.

   upvoted 2 times



  **ale183** 1 year, 4 months ago

Answer= A

To view all logs in the _Required bucket, and to view logs in the _Default view on the _Default bucket, you must have the Logs Viewer (roles/logging.viewer) role.

To view all logs in the _Required and _Default buckets, including data access logs, you must have the Private Logs Viewer (roles/logging.privateLogViewer) role.

   upvoted 2 times

  **blacortik** 1 year, 5 months ago

Selected Answer: D

D. roles/logging.viewer

The security operations team should be granted the roles/logging.viewer IAM role. This role provides the necessary permissions to view logs within the organization's projects, and it aligns with the least privilege principle as it grants only view access to logs.

   upvoted 2 times

  **gcpengineer** 1 year, 8 months ago

Selected Answer: A

A is the ans

   upvoted 1 times

  **bruh_1** 1 year, 10 months ago

D is the answer: The security operations team needs to have access to specific logs across all projects in their organization while following the least privilege model. The appropriate IAM role to grant them would be roles/logging.viewer. This role provides read-only access to all logs in the project, including Admin Activity logs, Data Access logs, and Access Transparency logs. It does not provide access to any other resources in the project, such as compute instances or storage buckets. This ensures that the security operations team can only view the logs and cannot make any modifications to the resources.

   upvoted 1 times

  **AzureDP900** 2 years, 2 months ago

A is the answer.

   upvoted 1 times

  **AwesomeGCP** 2 years, 3 months ago

Selected Answer: A

A. roles/logging.privateLogViewer

   upvoted 1 times

👤 **zellick** 2 years, 4 months ago

A is the answer.

<https://cloud.google.com/logging/docs/access-control#considerations>
roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default bucket.

👍 🔄 🚩 upvoted 2 times

👤 **cloudprincipal** 2 years, 7 months ago

Selected Answer: A

roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default bucket.

<https://cloud.google.com/logging/docs/access-control>

👍 🔄 🚩 upvoted 3 times

👤 **Nicky1402** 2 years, 8 months ago

I think the correct answer is A.

logging.admin is too broad a permission.

We need to give "only view access to logs". And we need to:

⇒ Have access to Admin Activity logs.

⇒ Have access to Data Access logs.

⇒ Have access to Access Transparency logs.

Only the roles/logging.privateLogViewer role has all these permissions.

Private Logs Viewer

(roles/logging.privateLogViewer)

Provides permissions of the Logs Viewer role and in addition, provides read-only access to log entries in private logs.

Lowest-level resources where you can grant this role:

Project

After you've configured Access Transparency for your Google Cloud organization, you can set controls for who can access the Access Transparency logs by assigning a user or group the Private Logs Viewer role.

Links for reference:

<https://cloud.google.com/logging/docs/access-control>

<https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs?hl=en>

👍 🔄 🚩 upvoted 4 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

