Google Discussions

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 113 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 113
Topic #: 1
[All Associate Cloud Engineer Questions]

You need to assign a Cloud Identity and Access Management (Cloud IAM) role to an external auditor. The auditor needs to have permissions to review your
Google Cloud Platform (GCP) Audit Logs and also to review your Data Access logs. What should you do?

A. Assign the auditor the IAM role roles/logging.privateLogViewer. Perform the export of logs to Cloud Storage.

B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

C. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Perform the export of logs to Cloud Storage.

D. Assign the auditor's IAM user to a custom role that has logging.privateLogEntries.list permission. Direct the auditor to also review the logs for changes to Cloud IAM policy.

Show Suggested Answer

by DarioFama23 at *July 7, 2020, 7:19 a.m.*

Comments

Type your comment...

Submit

ESP_SAP Highly Voted 4 years, 1 month ago

Correct Answer is (B):

Background
Google Cloud provides Cloud Audit Logs, which is an integral part of Cloud Logging. It consists of two log streams for each project: Admin Activity and Data Access.
Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. Admin Activity logs are always enabled. There is no charge for your Admin Activity audit logs.
Data Access logs record API calls that create, modify, or read user-provided data. Data Access audit logs are disabled by default because they can be large.

logging.viewer: The logging.viewer role gives the security admin team the ability to view the Admin Activity logs.
logging.privateLogViewer : The logging.privateLogViewer role gives the ability to view the Data Access logs.

upvoted 65 times

ESP_SAP 4 years, 1 month ago

Correct Answer is (B): (Continuation).
Scenario: External auditors
In this scenario, audit logs for an organization are aggregated and exported to a central sink location. A third-party auditor is granted access several
times a year to review the organization's audit logs. The auditor is not authorized to view PII data in the Admin Activity logs.

During normal access, the auditors' Google group is only granted access to view the historic logs stored in BigQuery. If any anomalies are discovered,
the group is granted permission to view the actual Cloud Logging Admin Activity logs via the dashboard's elevated access mode. At the end of each audit period,
the group's access is then revoked.

Data is redacted using Cloud DLP before being made accessible for viewing via the dashboard application.

upvoted 24 times

ESP_SAP 4 years, 1 month ago

Correct Answer is (B): (Continuation).
The table below explains IAM logging roles that an Organization Administrator can grant to the service account used by the dashboard,
as well as the resource level at which the role is granted:

logging.viewer Organization Dashboard service account The logging.viewer role permits the service account to read the Admin Activity logs in Cloud Logging.
bigquery.dataViewer BigQuery dataset Dashboard service account The bigquery.dataViewer role permits the service account used by the dashboard application
to read the exported Admin Activity logs.

upvoted 21 times

DarioFama23 Highly Voted 4 years, 3 months ago

for me B is the correct answer..

upvoted 17 times

Eshkrkrkr 3 years, 11 months ago

Yes, B is correct because:
1) Question doesn't ask us to export and store logs for any long period of time.
2) Custom role with only logging.privateLogEntries.list permission won't let the auditor to access Log Exporer at all (https://cloud.google.com/logging/docs/access-control#console_permissions - Minimal read-only access: logging.logEntries.list)

upvoted 8 times

Cynthia2023 Most Recent 9 months, 3 weeks ago

Selected Answer: B

There is no need to export logs to Cloud Storage for the auditor to review them unless there's a specific requirement or preference for reviewing them outside the GCP environment. The Logging service provides the necessary tools for log viewing and querying within the console.

Directing the auditor to review logs for changes to Cloud IAM policy is part of their duties to ensure that the IAM policies have been correctly managed and modified. This does not require a separate permission as the privateLogViewer role already provides the necessary access.

upvoted 2 times

upvoted 2 times

BAofBK 11 months, 2 weeks ago

The correct answer is B

upvoted 2 times

ziomek666 1 year ago

No logs in cloud storage since reviewer won't have access to it

upvoted 1 times

scanner2 1 year, 1 month ago

Selected Answer: B

- The Logs Viewer role (roles/logging.viewer) gives you read-only access to Admin Activity, Policy Denied, and System Event audit logs. If you have just this role, you cannot view Data Access audit logs that are in the _Default bucket.
- The Private Logs Viewer role(roles/logging.privateLogViewer) includes the permissions contained in roles/logging.viewer, plus the ability to read Data Access audit logs in the _Default bucket.
Therefore, no need to export logs to Cloud storage explicitly, the _Default bucket sink access is already provided from the above role.
https://cloud.google.com/iam/docs/audit-logging#audit_log_permissions

upvoted 1 times

Captain1212 1 year, 1 month ago

Selected Answer: B

b is the correect answer

upvoted 1 times

Neha_Pallavi 1 year, 1 month ago

B. Assign the auditor the IAM role roles/logging.privateLogViewer. Direct the auditor to also review the logs for changes to Cloud IAM policy.

upvoted 1 times

MilanRajGupta 1 year, 2 months ago

This answer is similar to answer choice B, but it suggests creating a custom role for the auditor that includes the "logging.privateLogEntries.list" permission. While this would provide the auditor with access to the necessary logs, directing them to also review Cloud IAM policy logs is not relevant to their request. Therefore, this answer is also not correct.

upvoted 1 times

MilanRajGupta 1 year, 2 months ago

Correct Ans: B

upvoted 1 times

anjanc 1 year, 10 months ago

I also think B

upvoted 1 times

AzureDP900 2 years, 4 months ago

B is right. Similar practice question in tutorials dojo

upvoted 1 times

Rutu_98 2 years, 5 months ago

Selected Answer: B

B is correct ans

upvoted 1 times

luciorifa 2 years, 8 months ago

Selected Answer: B

B is the correct answer

upvoted 3 times

lazyabhi606 2 years, 10 months ago

Selected Answer: B

Correct Answer is (B)

upvoted 1 times

maggieli 2 years, 11 months ago

Correct Answer is B.

upvoted 1 times

ankatsu2010 3 years ago

A is the correct answer. Exporting logging data to Cloud Storage is ideal, and 'Cloud IAM Policy' is not mentioned in this question.

upvoted 3 times

Load full discussion...