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 132 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 132

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google
Cloud resources. Your export must meet the following requirements:

✑ Export related logs for all projects in the Google Cloud organization.

✑ Export logs in near real-time to an external SIEM.

What should you do? (Choose two.)

A. Create a Log Sink at the organization level with a Pub/Sub destination.

B. Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.

C. Enable Data Access audit logs at the organization level to apply to all projects.

D. Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.

E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Show Suggested Answer

by ExamQnA at *May 20, 2022, 6:29 p.m.*

Comments

Type your comment...

Submit

cloudprincipal Highly Voted 3 years, 1 month ago

Selected Answer: BD

B
because for all projects

D
"Google Workspace Login Audit: Login Audit logs track user sign-ins to your domain. These logs only record the login event. They don't record which system was used to perform the login action."
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#services

upvoted 13 times

exambott 2 years, 6 months ago

Google cloud logs is different from Google Workspace logs. D is definitely incorrect.

upvoted 1 times

mikez2023 2 years, 5 months ago

There is no mentioning anything like "Google Workspace", why is D correct?

upvoted 2 times

ExamQnA Highly Voted 3 years, 2 months ago

Ans:B,C
https://cloud.google.com/logging/docs/export/aggregated_sinks: To use aggregated sinks, you create a sink in a Google Cloud organization or folder, and set the sink's includeChildren parameter to True. That sink can then route log entries from the organization or folder, plus (recursively) from any contained folders, billing accounts, or Cloud projects.
https://cloud.google.com/logging/docs/audit#data-access
Data Access audit logs-- except for BigQuery Data Access audit logs-- are disabled by default because audit logs can be quite large. If you want Data Access audit logs to be written for Google Cloud services other than BigQuery, you must explicitly enable them

upvoted 12 times

passex 2 years, 7 months ago

There is no mention about 'data access logs' in question

upvoted 2 times

Nik2592s 2 years, 2 months ago

API calls are tracked in Data access logs

upvoted 4 times

luca_scalzotto 1 year, 6 months ago

The question state: "API calls that modify configurations to Google
Cloud resources". From the documentation: "Admin Activity audit logs contain log entries for API calls or other actions that modify the configuration or metadata of resources. For example, these logs record when users create VM instances or change Identity and Access Management permissions." Therefore, cannot be C

upvoted 1 times

BPzen Most Recent 8 months ago

Selected Answer: BE

Why B. Create a Log Sink at the organization level with the includeChildren parameter and set the destination to a Pub/Sub topic is Correct: E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Why Not the Other Options:
C Enabling Data Access logs is not required for this use case. The question only asks for login activity and configuration changes, which are captured in Admin Activity logs
D. Enable Google Workspace audit logs
This is not directly relevant. Google Workspace audit logs are not required for capturing Google Cloud login activity and configuration changes.

upvoted 1 times

Mr_MIXER007 11 months ago

Selected Answer: BC

B
because for all projects
C

upvoted 1 times

60090d7 11 months, 2 weeks ago

Selected Answer: BD

turn on audit and sink, pub-sub (near realtime)

upvoted 1 times

piipo 1 year, 1 month ago

Selected Answer: BC

No Workspace

upvoted 1 times

pico 1 year, 2 months ago

Selected Answer: BC

why the other options are not as suitable:

A: While creating a log sink at the organization level is correct, it won't include logs from child projects unless the includeChildren parameter is set to true.
D: Google Workspace audit logs are separate from Google Cloud audit logs and won't provide the required information about Google Cloud console logins or API calls.
E: While processing the AuthenticationInfo field is essential for identifying actors, it is not a step in the setup of the log export itself.

upvoted 2 times

Bettoxicity 1 year, 4 months ago

Selected Answer: AE

AE
A: Setting up a Log Sink at the organization level with Pub/Sub as the destination guarantees you capture logs from all projects within your organization.
E: The AuthenticationInfo field within audit log entries provides valuable details about the user or service that made the configuration change or login attempt. Your SIEM needs to be able to process this field to extract identity information for security audit purposes.

B. IncludeChildren Parameter (Not Required)
C. Data Access Audit Logs (Not Specific)

upvoted 1 times

gurusen88 1 year, 5 months ago

B & E

B. Organization Level Log Sink with includeChildren parameter: Creating a log sink at the organization level with the includeChildren parameter ensures that you capture logs from all projects within the organization. Setting the destination to a Pub/Sub topic is suitable for real-time log export, meeting the requirement to export logs in near real-time to an external SIEM.

E. Processing the AuthenticationInfo field: The AuthenticationInfo field in the audit log entries contains identity information, which is crucial for auditing security logs for login activity. Ensuring that the SIEM processes this field allows for a detailed analysis of who is accessing what, fulfilling the requirement to audit login activity events and API calls that modify configurations.

upvoted 2 times

mjcts 1 year, 6 months ago

Selected Answer: BC

No mention of Google Workspace

upvoted 3 times

loonytunes 1 year, 9 months ago

ANS: B,D
Api calls that modify configuration of resources are in Admin Activity audit logs, which are on by default (along with System Events and Deny Policies). Thus not C. You can also enable Google Workspace logs to be forwarded to Google cloud at the Org Level
Same Link.
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#log-types

upvoted 1 times

aygitci 1 year, 9 months ago

Selected Answer: BC

Not mention og Google Workspace, definitely not D

upvoted 3 times

Xoxoo 1 year, 10 months ago

Selected Answer: BC

To export and audit security logs for login activity events in the Google Cloud Console and API calls that modify configurations to Google Cloud resources with the specified requirements, you should take the following steps:

B. Create a Log Sink at the organization level with the includeChildren parameter and set the destination to a Pub/Sub topic: This step will export related logs from all projects within the Google Cloud organization, including the logs you need. The use of Pub/Sub allows near real-time export of logs.

C. Enable Data Access audit logs at the organization level to apply to all projects: Enabling Data Access audit logs at the organization level ensures that logs related to API calls that modify configurations to Google Cloud resources are captured.

upvoted 5 times

Xoxoo 1 year, 10 months ago

The other options are not relevant or necessary for meeting the specified requirements:

D. "Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console" is not directly related to exporting logs for Google Cloud Console and API calls.

E. "Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information" is a consideration for how the SIEM system processes logs but is not a configuration step for exporting logs.

upvoted 2 times

desertlotus1211 1 year, 10 months ago

Can someone explain how or why 'D' can be correct? The logs are Google Cloud not Workspace...

upvoted 2 times

[Removed] 2 years ago

Selected Answer: BD

"B", "D"
B because you need an aggregate sink to recursively pull from children entities otherwise scope is limited to the specific level where it's created. So this also excludes A.
https://cloud.google.com/logging/docs/export/aggregated_sinks#create_an_aggregated_sink

C - Data Access Audit Logs - Even though they include API events, they don't explicitly say they also include log-in events.
https://cloud.google.com/logging/docs/audit#data-access

D - For Workspace Audit Logs, they explicitly say that API calls and log-in events are captured which makes it a more complete option than "C". Also, cloud identity, which is used to manage users of GCP, is a workspace service. It would make sense that workspace logging providing cloud identity related sign-in logs.
https://cloud.google.com/logging/docs/audit/gsuite-audit-logging
https://support.google.com/cloudidentity/answer/7319251

upvoted 1 times

gcpengineer 2 years, 2 months ago

Selected Answer: BE

change to BE

upvoted 2 times

gcpengineer 2 years, 2 months ago

Selected Answer: BC

BC looks lik ans

upvoted 3 times

Load full discussion...

- Examtopics PRO
- Training Courses