

[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 312 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 312

Topic #: 1

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

A team at your organization collects logs in an on-premises security information and event management system (SIEM). You must provide a subset of Google Cloud logs for the SIEM, and minimize the risk of data exposure in your cloud environment. What should you do?

- A. Create a new BigQuery dataset. Stream all logs to this dataset. Provide the on-premises SIEM system access to the data in BigQuery by using workload identity federation and let the SIEM team filter for the relevant log data.
- B. Define a log view for the relevant logs. Provide access to the log view to a principal from your on-premises identity provider by using workforce identity federation.
- C. Create a log sink for the relevant logs. Send the logs to Pub/Sub. Retrieve the logs from Pub/Sub and push the logs to the SIEM by using Dataflow.
- D. Filter for the relevant logs. Store the logs in a Cloud Storage bucket. Grant the service account access to the bucket. Provide the service account key to the SIEM team.

[Show Suggested Answer](#)

by [abdelrahman89](#) at Oct. 25, 2024, 1:46 a.m.

## Comments

Type your comment...

  **Popa** 5 months ago

**Selected Answer: B**

Option C, does involve setting up multiple components (Pub/Sub, Dataflow, log sinks) and ensuring they are properly configured. This might add to the complexity of the setup.

That being said, option B is still a strong choice because it provides a more straightforward approach to controlling and accessing the logs using log views and identity federation

   upvoted 1 times

  **KLei** 7 months, 1 week ago

**Selected Answer: C**

B: Defining a log view provides access control but does not facilitate exporting logs to an external SIEM effectively.

   upvoted 1 times

  **BPzen** 8 months ago

**Selected Answer: C**

Why C is Correct:

Log Sink for Filtering:

A log sink allows you to filter and export only the relevant logs, ensuring unnecessary data is not sent, which reduces the risk of data exposure.

Pub/Sub for Delivery:

Exporting logs to Pub/Sub enables real-time streaming of filtered logs to external systems. This ensures the SIEM receives logs promptly and securely.

Dataflow for Transformation and Transfer:

Use Dataflow to process and transform logs as needed before pushing them to the on-premises SIEM.


   upvoted 2 times

  **MoAk** 8 months, 1 week ago

**Selected Answer: C**

Answer C.

   upvoted 1 times

  **kalbd2212** 8 months, 1 week ago

going with C..

   upvoted 2 times



  **irene062** 8 months, 2 weeks ago

**Selected Answer: B**

Log views let you grant a user access to only a subset of the logs stored in a log bucket.

<https://cloud.google.com/logging/docs/logs-views>

   upvoted 1 times

  **abdelrahman89** 9 months, 1 week ago

**Selected Answer: B**

Answer B

   upvoted 1 times



## Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

