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 20 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 20

Topic #: 1

[All Professional Cloud Security Engineer Questions]

How should a customer reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Send all logs to the SIEM system via an existing protocol such as syslog.

B. Configure every project to export all their logs to a common BigQuery DataSet, which will be queried by the SIEM system.

C. Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.

D. Build a connector for the SIEM to query for all logs in real time from the GCP RESTful JSON APIs.

Show Suggested Answer

by xhova at *April 4, 2020, 2:34 a.m.*

### Comments

Type your comment...

Submit

⊟ ESP_SAP Highly Voted 3 years, 8 months ago

Correct answer is (C):

Scenarios for exporting Cloud Logging data: Splunk

This scenario shows how to export selected logs from Cloud Logging to Pub/Sub for ingestion into Splunk. Splunk is a security information and event management (SIEM) solution that supports several ways of ingesting data, such as receiving streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs streaming data out of Google Cloud through Splunk HTTP Event Collector (HEC) or by fetching data from Google Cloud APIs through Splunk Add-on for Google Cloud.

Using the Pub/Sub to Splunk Dataflow template, you can natively forward logs and events from a Pub/Sub topic into Splunk HEC. If Splunk HEC is not available in your Splunk deployment, you can use the Add-on to collect the logs and events from the Pub/Sub topic.
https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk

upvoted 18 times

**AzureDP900** 1 year, 8 months ago

I will go with C

upvoted 1 times

**bkovari** Most Recent 11 months, 3 weeks ago

C is the only way to go

upvoted 2 times

**GCP72** 1 year, 11 months ago

Selected Answer: C

I will go with C

upvoted 4 times

**DebasishLowes** 3 years, 4 months ago

Ans : C

upvoted 2 times

**BlahBaller** 3 years, 6 months ago

As I was the Logging Service Manager when we set this up with GCP. I can verify that C is how we have it setup, based on the Google's recommendations.

upvoted 2 times

**Moss2011** 3 years, 8 months ago

I think the correct one its D because C mention "Dataflow" and it cannot be connected to any sink out of GCP.

upvoted 1 times

**deevisrk** 3 years, 9 months ago

C looks correct..
https://cloud.google.com/solutions/exporting-stackdriver-logging-for-splunk
Splunk is on premises SIEM solution in above example.

upvoted 2 times

**saurabh1805** 3 years, 9 months ago

I will go with Option B.

Read this email for more reason. C is not workable solution so that is first one not to consider.

upvoted 1 times

**CHECK666** 3 years, 10 months ago

C is the answer.

upvoted 1 times

**ArizonaClassics** 3 years, 12 months ago

I will go with C

upvoted 3 times

**xhova** 4 years, 3 months ago

C is correct

upvoted 4 times

- Home
- All Exams
- Examtopics PRO
- Training Courses