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 271 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 271
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You work for a multinational organization that has systems deployed across multiple cloud providers, including Google Cloud. Your organization maintains an extensive on-premises security information and event management (SIEM) system. New security compliance regulations require that relevant Google Cloud logs be integrated seamlessly with the existing SIEM to provide a unified view of security events. You need to implement a solution that exports Google Cloud logs to your on-premises SIEM by using a push-based, near real-time approach. You must prioritize fault tolerance, security, and auto scaling capabilities. In particular, you must ensure that if a log delivery fails, logs are re-sent. What should you do?

A. Create a Pub/Sub topic for log aggregation. Write a custom Python script on a Cloud Function Leverage the Cloud Logging API to periodically pull logs from Google Cloud and forward the logs to the SIEM. Schedule the Cloud Function to run twice per day.

B. Collect all logs into an organization-level aggregated log sink and send the logs to a Pub/Sub topic. Implement a primary Dataflow pipeline that consumes logs from this Pub/Sub topic and delivers the logs to the SIEM. Implement a secondary Dataflow pipeline that replays failed messages.

C. Deploy a Cloud Logging sink with a filter that routes all logs directly to a syslog endpoint. The endpoint is based on a single Compute Engine hosted on Google Cloud that routes all logs to the on-premises SIEM. Implement a Cloud Function that triggers a retry action in case of failure.

D. Utilize custom firewall rules to allow your SIEM to directly query Google Cloud logs. Implement a Cloud Function that notifies the SIEM of a failed delivery and triggers a retry action.

Show Suggested Answer

by yakovan at Sept. 6, 2024, 1:30 a.m.

by yokoyan at Sept. 6, 2024, 1:39 a.m.

Comments

Type your comment...

Submit

Zek 7 months, 3 weeks ago

Selected Answer: B

B - https://cloud.google.com/architecture/stream-logs-from-google-cloud-to-splunk

upvoted 1 times

MoAk 8 months ago

Selected Answer: B

B 100%.

upvoted 1 times

KLei 8 months, 2 weeks ago

Selected Answer: B

use pub/sub. A is wrong as it says that "periodically pull logs" - Not near real-time and need programing works.

upvoted 1 times

BondleB 8 months, 3 weeks ago

Selected Answer: B

https://cloud.google.com/architecture/stream-logs-from-google-cloud-to-splunk

upvoted 1 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 1 times