EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 264 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 264
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Customers complain about error messages when they access your organization's website. You suspect that the web application firewall rules configured in Cloud Armor are too strict. You want to collect request logs to investigate what triggered the rules and blocked the traffic. What should you do?

A. Modify the Application Load Balancer backend and increase the tog sample rate to a higher number.

B. Enable logging in the Application Load Balancer backend and set the log level to VERBOSE in the Cloud Armor policy.

C. Change the configuration of suspicious web application firewall rules in the Cloud Armor policy to preview mode.

D. Create a log sink with a filter for togs containing redirected_by_security_policy and set a BigQuery dataset as destination.

Show Suggested Answer

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

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: B

https://cloud.google.com/armor/docs/verbose-logging

You can adjust the level of detail recorded in your logs. We recommend that you enable verbose logging only when you first create a policy, make changes to a policy, or troubleshoot a policy. If you enable verbose logging, it is in effect for rules in preview mode as well as active (non-previewed) rules during standard operations.

upvoted 1 times

cachopo 7 months, 3 weeks ago

Selected Answer: B

Enabling verbose logging for your Cloud Armor policy provides the most detailed logs, including information about why specific requests triggered a WAF rule. This level of detail is critical for troubleshooting and refining security policies.

- Verbose logging captures detailed request attributes that caused WAF rules to trigger, which are not available in default (normal) logs.
- By setting the log level to VERBOSE using the gcloud compute security-policies update command, you can collect the detailed logs needed for investigation.

upvoted 1 times

BPzen 8 months ago

Selected Answer: C

Other Rules Still Enforced:

Only the specific rules switched to preview mode are not enforced. All other active rules in the Cloud Armor policy continue to block or redirect traffic as configured.
This minimizes the exposure since you're not disabling the entire firewall.

B. Enable logging in the Application Load Balancer backend and set the log level to VERBOSE in the Cloud Armor policy.

Cloud Armor policies do not have a "VERBOSE" log level. While enabling logging at the backend captures some information, it does not specifically provide insights into which WAF rules were triggered.

upvoted 1 times

cachopo 7 months, 3 weeks ago

Actually, Cloud Armor does have "Verbose" log-level:
https://cloud.google.com/armor/docs/verbose-logging

It's okay to look for answers on Chatgpt. But try to compare the answers too because it's not foolproof.

upvoted 1 times

nah99 8 months ago

Selected Answer: B

B collects the logs you want. C has the side-effect of allowing the traffic which may not be appropriate during investigation

upvoted 1 times

kalbd2212 8 months, 1 week ago

C .. This helps you pinpoint the exact rules that are causing problems and understand why they are being triggered.

upvoted 1 times

d0fa7d5 10 months, 3 weeks ago

Selected Answer: B

I thought B is the correct answer. C is useful for testing the rule, but it doesn't provide detailed logs. With B, detailed information about which rule caused the block is recorded, which helps in investigating the cause.

upvoted 4 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 1 times