Audit log Alerts

Last updated by | Sergio Fonseca | Aug 10, 2020 at 6:00 AM PDT

Contents

Issue

There are some scenarios where customer would like to set up an **alert rule based on audit logs** when this is not a buildin function

Mitigation

Audit to LOG Analytics

Cx can create alerts based on **Audit to LOG Analytics** follow up **AZURE SQL DB AND LOG ANALYTICS BETTER TOGETHER - Post** for details

- PART #2 – ALERTS

TRIGGER (T-SQL)

You can use to execute a sproc when specific events occur on the server/database, however this is not purely an alert. Additional info on triggers can be found here:

- https://docs.microsoft.com/en-us/sql/t-sql/statements/create-trigger-transact-sql
- https://docs.microsoft.com/en-us/sql/relational-databases/triggers/ddl-triggers

Blob Auditing + OMS

Enable **Blob Auditing** on the database with a granular auditing policy, which only audits only the specific events that you’re looking to monitor (e.g. create user).

- Use the following OMS sync application that we created for pushing the audit events into OMS:
  - https://github.com/Microsoft/Azure-SQL-DB-auditing-OMS-integration
- Create an alert in OMS based on the event that you’re monitoring:
  - https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-alerts-actions

However, note that there are variables that can go wrong here (it’s not bullet proof, as it relies on an application), and it’s also not in real time – it can take 5 minutes for the audit logs to be pushed into OMS and then another few minutes for the OMS alert to trigger.ca

Internal Reference

- Auditing

Root Cause Classification

Root cause Tree - Security/User issue/error/Auditing

How good have you found this content?

🙂 🙁