Azure Activity Log

Last updated by | Charlene Wang | Feb 18, 2021 at 11:38 PM PST
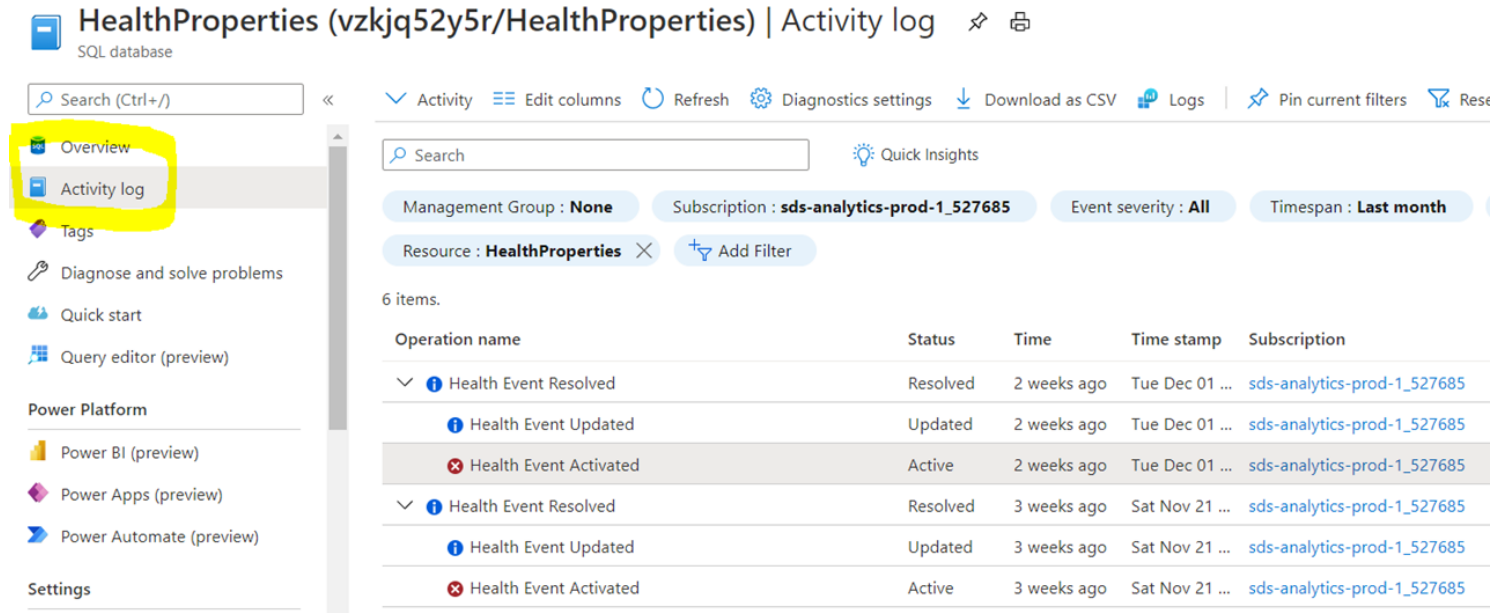
Logs on Portal

Activity Log, SQL Auditing Log and Diagnostic Setting are three different types of customer facing logs.

Activity Log

The Activity log is a platform log in Azure that provides insight into subscription-level events. Azure Activity Log 🗗

The activity log contains all write operations (PUT, POST, DELETE) for your resources. It doesn't include read operations (GET). Activity logs are kept for 90 days. View activity logs to monitor actions on resources 🗗

Activity Log shows Resource Health events, many control plane CRUD events (create/drop database, update database - firewall rule change, add user, etc).

Activity Log is free and always on.

To troubleshoot missing control plane CRUD events, ask customer to "Download as CSV" and share the file. Remind them that they need to expand the line item to see details like user who created/dropped the database. CRUD activities done through TSQL has fewer details than activities done on portal. That is a known issue.

MonManagement table in Kusto has CRUD details for each resource. Use it to confirm missing event.

To escalate missing control plane CRUD events in Activity Log, open ICM in Azure SQL DB / Provisioning and Elastic Jobs.

SQL Auditing

SQL Auditing is off by default and opt in. It is free, but customers need to pay for storage to store the log. SQL Audting logs any data plane read/write query.

To escalate SQL Auditing issue, open ICM in Azure SQL DB/Auditing.

Diagnostic Setting

Customers can opt in to get subset of logs for their subscription. This is off by default. SQLDB allows 13 log categorties that customers can op in and route log to their own storage account or Log Analytics workspace.

HealthProperties (vzkjq52y5r/HealthProperties) | Diagnostic settings
SQL database

⟳ Refresh   ☺ Provide feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics f
logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account
No diagnostic settings defined	

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- SQLInsights
- AutomaticTuning
- QueryStoreRuntimeStatistics
- QueryStoreWaitStatistics
- Errors
- DatabaseWaitStatistics
- Timeouts
- Blocks
- Deadlocks
- Basic
- InstanceAndAppAdvanced
- WorkloadManagement

Navigation menu (left):

Transparent data encryption

Intelligent Performance
- Performance overview
- Performance recommendations
- Query Performance Insight
- Automatic tuning

Monitoring
- Alerts
- Metrics
- Diagnostic settings
- Logs

Automation
- Tasks (preview)

Below is ownership of these log categories. Please note that SQLInsights log is used to generate workload insights in SQL Analytics. SQL Analytics has at-scale monitoring experience and workload insights. SQL Analytics will be announced for feature deprecation in Feb/March 2021. The insights for SQL Analytics are already disabled in North/West Europe, West/East US.

Most log categories require utilization to generate data. If customer reported that log is missing for one or more categories, make sure that they have workload to generate such log. Errors are filtered to only flow error severity level >= 16 to customers.

[Serbia / Telemetry] SQLInsights
[Serbia Auto Tuning] AutomaticTuning
[Perf] QueryStoreRuntimeStatistics
[Perf] QueryStoreWaitStatistics
[Perf] Errors
[Perf] DatabaseWaitStatistics
[Perf] Timeouts
[Perf] Blocks
[Perf] Deadlocks
[Perf metrics] Basic
[Perf metrics] InstanceAndAppAdvanced
[Perf] WorkloadManagement

For Diagnostic Log portal issue (cannot enable/disable log), open ICM in Azure Monitor Essentials / Sev 3 and 4 CRI - Diagnostic Logs.

Related links

[Azure SQL Auditing impact](#)

How good have you found this content?