


Azure Activity Log

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

Logs on Portal

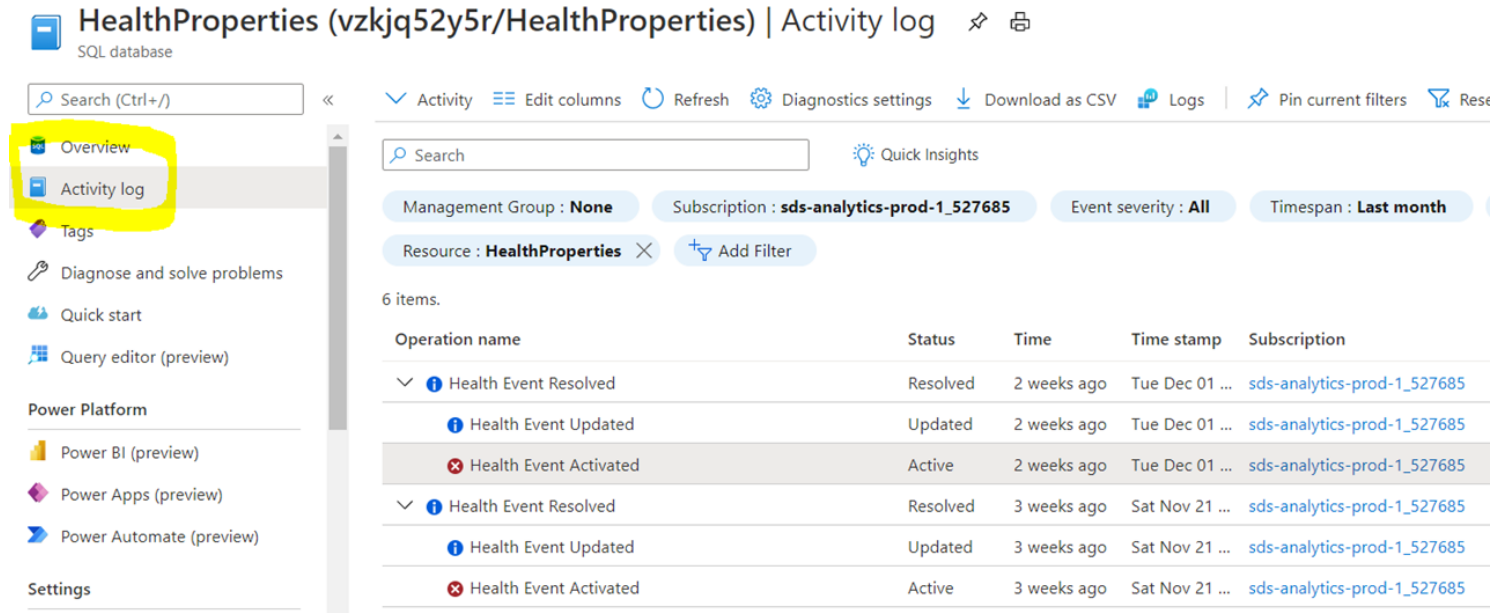
Activity Log, SQL Auditing Log and Diagnostic Setting are three different types of customer facing logs.

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).



HealthProperties (vzkjq52y5r/HealthProperties) | Activity log

SQL database

Search (Ctrl+/) << Activity Edit columns Refresh Diagnostics settings Download as CSV Logs Pin current filters Rese

Overview Activity log Tags Diagnose and solve problems Quick start Query editor (preview) Power Platform Power BI (preview) Power Apps (preview) Power Automate (preview) Settings

Search Quick Insights

Management Group : None Subscription : sds-analytics-prod-1_527685 Event severity : All Timespan : Last month

Resource : HealthProperties Add Filter

6 items.

Operation name	Status	Time	Time stamp	Subscription
Health Event Resolved	Resolved	2 weeks ago	Tue Dec 01 ...	sds-analytics-prod-1_527685
Health Event Updated	Updated	2 weeks ago	Tue Dec 01 ...	sds-analytics-prod-1_527685
Health Event Activated	Active	2 weeks ago	Tue Dec 01 ...	sds-analytics-prod-1_527685
Health Event Resolved	Resolved	3 weeks ago	Sat Nov 21 ...	sds-analytics-prod-1_527685
Health Event Updated	Updated	3 weeks ago	Sat Nov 21 ...	sds-analytics-prod-1_527685
Health Event Activated	Active	3 weeks ago	Sat Nov 21 ...	sds-analytics-prod-1_527685

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 Auditing logs any data plane read/write query.

HealthProperties (vzkjq52y5r/HealthProperties) | Auditing

SQL database

Search (Ctrl+ /)

Stream analytics (preview)

Security

- Auditing**
- Data Discovery & Classification
- Dynamic Data Masking
- Security Center
- Transparent data encryption

Intelligent Performance

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

Monitoring

- Alerts
- Metrics

Save Discard View audit logs Feedback

If Blob Auditing is enabled on the server, it will always apply to the database, regardless of database settings.

Potential cross-region reads/writes detected

View server settings

Server-level Auditing: **Disabled**

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing ☒ ON OFF

Audit log destination (choose at least one):

☒ Storage

Storage details

hpauditing

☐ Log Analytics (Preview)

☐ Event Hub (Preview)

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 categories that customers can opt in and route log to their own storage account or Log Analytics workspace.

HealthProperties (vzkjq52y5r/HealthProperties) | Diagnostic settings

SQL database

Search (Ctrl+/) << Refresh Provide feedback

transparent data encryption

Intelligent Performance

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

Monitoring

- Alerts
- Metrics
- Diagnostic settings**
- Logs

Automation

- Tasks (preview)

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

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?

