

Connector Health Q&A

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

How to enable the health feature

<https://docs.microsoft.com/en-us/azure/sentinel/monitor-data-connector-health#turn-on-microsoft-sentinel-health-for-your-workspace> 

Once the feature is enabled and only if the customer connected at least one of the supported connectors, a SentinelHealth table will appear in LogA.

Is it billable?

At the moment, it's billed like any other LogA table; however, the cost should be negligible.

In a few weeks (or maybe months) it will become free. We've already got an approval in principle, but the change has not been performed AFAIK.

When are health logs seen in LogA?

Up to 1 hour after activating the feature, and only if the customer has one of the supported connectors.

Which connectors are supported?

<https://docs.microsoft.com/en-us/azure/sentinel/monitor-data-connector-health#supported-data-connectors> 

Additionally, API Polling (CCP) and AWS S3 are also supported - they are not mentioned in the documentation since they are currently in private-preview.

What is covered by the logs in SentinelHealth table?

At the moment, not all data-collection issues are covered.

Only the polling step of data-collection is covered (polling performed by Scuba & TI and only for supported connectors).

While this is the most fragile and error-prone step of data-collection, this is not the only step that can break down.

Thus, a user can see 'Success' in his 'Data fetch status change' record in SentinelHealth - but that only means the 'fetch' part is ok, not that the later ingestion parts are ok.

Data can still not be flowing for the connector, due to a later ingestion problem (for example, in ODS, GT, Log-Analytics itself, etc.).

If the customer sees 'Success' in SentinelHealth, does it mean everything is ok with his connector?

No, as explained in the previous item. It just means that the polling step was successful.