Troubleshooting Windows metrics observability

You have installed and configured the Windows Open Telemetry Connector in your Splunk Observability Cloud, but you are still experiencing some problems with your data.

Check the logs

- **Start > Administrative Tools > Event Viewer**, select **Windows Logs** then **Application Logs**.
- The default logging level is info. Set it to debug as needed in the config file, which you can access at `\ProgramData\Splunk\OpenTelemetry Collector\agent_config.yaml`.
- You must stop and start the agent after making a configuration change. This is done from PowerShell: `Stop-Service splunk-otel-collector` then `Start-Service splunk-otel-collector`.
- Check for HTTP error codes.
  - 401 (UNAUTHORIZED): Configured access token or realm is incorrect.
  - 404 (NOT FOUND): Likely configuration parameter is wrong like endpoint or path (e.g. /v1/log); possible network/firewall/port issue.
  - 429 (TOO MANY REQUESTS): Org is not provisioned for the amount of traffic being sent; reduce traffic or request increase in capacity.
  - 503 (SERVICE UNAVAILABLE): If using the Log Observer, this is the same as 429 (because that is how HECv1 responds).

Check for metric time series creation throttling

Splunk limits the number of metric time series you can create, which is 6,000 per minute or more, based on your subscription. This throttle is a funnel. New metric time series will eventually be created. You can do any of the following to understand your limits:

- Plot the sf.org.limit.metricTimeSeriesCreatedPerMinute metric to see your limit.
- Plot the sf.org.numMetricTimeSeriesCreated metric to see the number of MTS created.
- Plot the sf.org.numThrottledMetricTimeSeriesCreateCallsByToken metric to see number of creations throttled.

Check your active metric time series limits

Splunk limits the number of active metric time series you can have, based on your subscription. New metric time series will not be created until you are under your limit. You can do any of the following to understand your limits:

- Plot the sf.org.limit.activeTimeSeries metric to see your limit.
- Plot the sf.org.numActiveTimeSeries metric to see your number of active MTS.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
• Plot the sf.org.numLimitedMetricTimeSeriesCreateCalls metric to see whether new MTS creations are limited.

Next steps

These additional Splunk resources might help you understand and implement these recommendations:

• Splunk Docs: Collect Windows Data
• Github: Splunk Otel Collector, Windows Manual