SPLK-4001$^{Q\&As}$

Splunk O11y Cloud Certified Metrics User

Pass Splunk SPLK-4001 Exam with 100% Guarantee

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

An SRE creates an event feed chart in a dashboard that shows a list of events that meet criteria they specify. Which of the following should they include? (select all that apply)

A. Custom events that have been sent in from an external source.

B. Events created when a detector clears an alert.

C. Random alerts from active detectors.

D. Events created when a detector triggers an alert.

Correct Answer: ABD

According to the web search results, an event feed chart is a type of chart that shows a list of events that meet criteria you specify. An event feed chart can display one or more event types depending on how you specify the criteria. The event

types that you can include in an event feed chart are:

Custom events that have been sent in from an external source: These are events that you have created or received from a third-party service or tool, such as AWS CloudWatch, GitHub, Jenkins, or PagerDuty. You can send custom events to

Splunk Observability Cloud using the API or the Event Ingest Service. Events created when a detector triggers or clears an alert: These are events that are automatically generated by Splunk Observability Cloud when a detector evaluates a

metric or dimension and finds that it meets the alert condition or returns to normal. You can create detectors to monitor and alert on various metrics and dimensions using the UI or the API.

Therefore, option A, B, and D are correct.

QUESTION 2

With exceptions for transformations or timeshifts, at what resolution do detectors operate?

A. 10 seconds

B. The resolution of the chart

C. The resolution of the dashboard

D. Native resolution

Correct Answer: D

According to the Splunk Observability Cloud documentation1, detectors operate at the native resolution of the metric or dimension that they monitor, with some exceptions for transformations or timeshifts. The native resolution is the frequency at which the data points are reported by the source. For example, if a metric is reported every 10 seconds, the detector will evaluate the metric every 10 seconds. The native resolution ensures that the detector uses the most granular and accurate data available for alerting.

QUESTION 3

For which types of charts can individual plot visualization be set?

A. Line, Bar, Column

B. Bar, Area, Column

C. Line, Area, Column

D. Histogram, Line, Column

Correct Answer: C

The correct answer is C. Line, Area, Column. For line, area, and column charts, you can set the individual plot visualization to change the appearance of each plot in the chart. For example, you can change the color, shape, size, or style of the lines, areas, or columns. You can also change the rollup function, data resolution, or y-axis scale for each plot To set the individual plot visualization for line, area, and column charts, you need to select the chart from the Metric Finder, then click on Plot Chart Options and choose Individual Plot Visualization from the list of options. You can then customize each plot according to your preferences To learn more about how to use individual plot visualization in Splunk Observability Cloud, you can refer to this documentation.
https://docs.splunk.com/Observability/gdi/metrics/charts.html#Individual-plot-visualization
https://docs.splunk.com/Observability/gdi/metrics/charts.html#Set-individual-plot- visualization

QUESTION 4

Which of the following rollups will display the time delta between a datapoint being sent and a datapoint being received?

A. Jitter

B. Delay

C. Lag

D. Latency

Correct Answer: C

According to the Splunk Observability Cloud documentation1, lag is a rollup function that returns the difference between the most recent and the previous data point values seen in the metric time series reporting interval. This can be used to measure the time delta between a data point being sent and a data point being received, as long as the data points have timestamps that reflect their send and receive times. For example, if a data point is sent at 10:00:00 and received at 10:00:05, the lag value for that data point is 5 seconds.

QUESTION 5

What are the best practices for creating detectors? (select all that apply)

A. View data at highest resolution.

B. Have a consistent value.

C. View detector in a chart.

D. Have a consistent type of measurement.

Correct Answer: ABCD

The best practices for creating detectors are: View data at highest resolution. This helps to avoid missing important signals or patterns in the data that could indicate anomalies or issues Have a consistent value. This means that the metric or dimension used for detection should have a clear and stable meaning across different sources, contexts, and time periods. For example, avoid using metrics that are affected by changes in configuration, sampling, or aggregation View detector in a chart. This helps to visualize the data and the detector logic, as well as to identify any false positives or negatives. It also allows to adjust the detector parameters and thresholds based on the data distribution and behavior Have a consistent type of measurement. This means that the metric or dimension used for detection should have the same unit and scale across different sources, contexts, and time periods. For example, avoid mixing bytes and bits, or seconds and milliseconds. https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best-practices-for-detectors https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best- practices-for-detectors https://docs.splunk.com/Observability/gdi/metrics/detectors.html#View-detector-in-a-chart : https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best-practices-for- detectors

Latest SPLK-4001 Dumps   SPLK-4001 Practice Test   SPLK-4001 Study Guide