SPLK-4001 Q&As

Splunk O11y Cloud Certified Metrics User

Pass Splunk SPLK-4001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-4001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A customer operates a caching web proxy. They want to calculate the cache hit rate for their service. What is the best way to achieve this?

A. Percentages and ratios

B. Timeshift and Bottom N

C. Timeshift and Top N

D. Chart Options and metadata

Correct Answer: A

According to the Splunk O11y Cloud Certified Metrics User Track document, percentages and ratios are useful for calculating the proportion of one metric to another, such as cache hits to cache misses, or successful requests to failed

requests. You can use the percentage() or ratio() functions in SignalFlow to compute these values and display them in charts. For example, to calculate the cache hit rate for a service, you can use the following SignalFlow code:

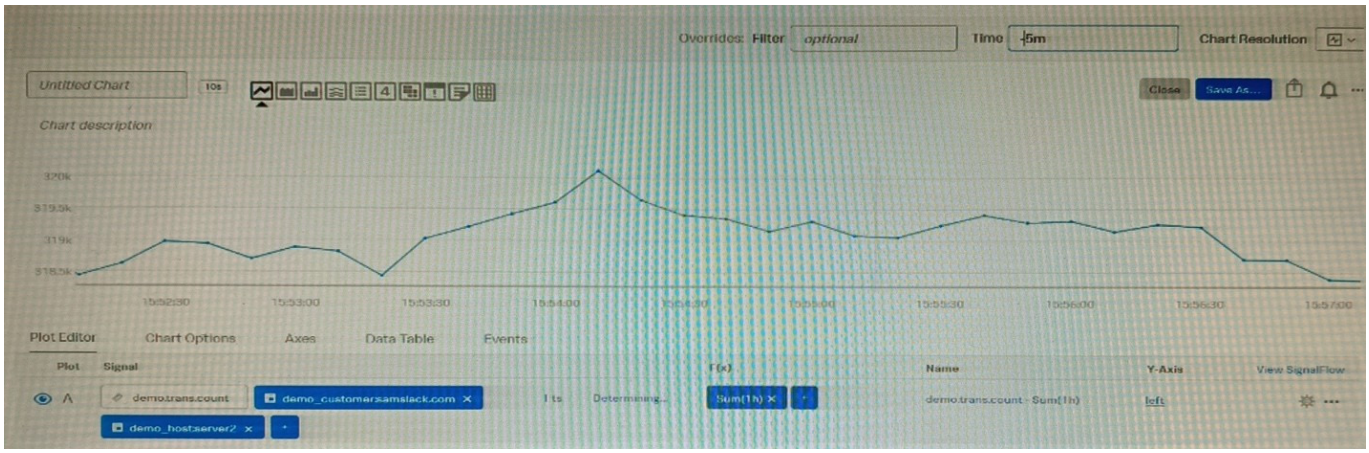
percentage(counters("cache.hits"), counters("cache.misses")) This will return the percentage of cache hits out of the total number of cache attempts. You can also use the ratio() function to get the same result, but as a decimal value instead

of a percentage.

ratio(counters("cache.hits"), counters("cache.misses"))

QUESTION 2

Given that the metric demo. trans. count is being sent at a 10 second native resolution, which of the following is an accurate description of the data markers displayed in the chart below?



A. Each data marker represents the average hourly rate of API calls.

B. Each data marker represents the 10 second delta between counter values.

C. Each data marker represents the average of the sum of datapoints over the last minute, averaged over the hour.

D. Each data marker represents the sum of API calls in the hour leading up to the data marker.

Correct Answer: D

The correct answer is D. Each data marker represents the sum of API calls in the hour leading up to the data marker. The metric demo.trans.count is a cumulative counter metric, which means that it represents the total number of API calls since the start of the measurement. A cumulative counter metric can be used to measure the rate of change or the sum of events over a time period1 The chart below shows the metric demo.trans.count with a one-hour rollup and a line chart type. A rollup is a way to aggregate data points over a specified time interval, such as one hour, to reduce the number of data points displayed on a chart. A line chart type connects the data points with a line to show the trend of the metric over time Each data marker on the chart represents the sum of API calls in the hour leading up to the data marker. This is because the rollup function for cumulative counter metrics is sum by default, which means that it adds up all the data points in each time interval. For example, the data marker at 10:00 AM shows the sum of API calls from 9:00 AM to 10:00 AM To learn more about how to use metrics and charts in Splunk Observability Cloud, you can refer to these documentations. https://docs.splunk.com/Observability/gdi/metrics/metrics.html#Metric-types https://docs.splunk.com/Observability/gdi/metrics/charts.html#Data-resolution-and-rollups- in-charts https://docs.splunk.com/Observability/gdi/metrics/charts.html#Rollup-functions- for-metric-types

QUESTION 3

Which of the following is optional, but highly recommended to include in a datapoint?

A. Metric name

B. Timestamp

C. Value

D. Metric type

Correct Answer: D

The correct answer is D. Metric type. A metric type is an optional, but highly recommended field that specifies the kind of measurement that a datapoint represents. For example, a metric type can be gauge, counter, cumulative counter, or histogram. A metric type helps Splunk Observability Cloud to interpret and display the data correctly To learn more about how to send metrics to Splunk Observability Cloud, you can refer to this documentation. https://docs.splunk.com/Observability/gdi/metrics/metrics.html#Metric-types https://docs.splunk.com/Observability/gdi/metrics/metrics.html

QUESTION 4

A user wants to add a link to an existing dashboard from an alert. When they click the dimension value in the alert message, they are taken to the dashboard keeping the context. How can this be accomplished? (select all that apply)

A. Build a global data link.

B. Add a link to the Runbook URL.

C. Add a link to the field.

D. Add the link to the alert message body.

Correct Answer: AC

The possible ways to add a link to an existing dashboard from an alert are: Build a global data link. A global data link is a feature that allows you to create a link from any dimension value in any chart or table to a dashboard of your choice. You can specify the source and target dashboards, the dimension name and value, and the query parameters to pass along. When you click on the dimension value in the alert message, you will be taken to the dashboard with the context preserved Add a link to the field. A field link is a feature that allows you to create a link from any field value in any search result or alert message to a dashboard of your choice. You can specify the field name and value, the dashboard name and ID, and the query parameters to pass along. When you click on the field value in the alert message, you will be taken to the dashboard with the context preserved Therefore, the correct answer is A and C. To learn more about how to use global data links and field links in Splunk Observability Cloud, you can refer to these documentations.
https://docs.splunk.com/Observability/gdi/metrics/charts.html#Global-data-links
https://docs.splunk.com/Observability/gdi/metrics/search.html#Field-links

QUESTION 5

To refine a search for a metric a customer types host: test-*. What does this filter return?

A. Only metrics with a dimension of host and a value beginning with test-.

B. Error

C. Every metric except those with a dimension of host and a value equal to test.

D. Only metrics with a value of test- beginning with host.

Correct Answer: A

The correct answer is A. Only metrics with a dimension of host and a value beginning with test-. This filter returns the metrics that have a host dimension that matches the pattern test-. For example, test-01, test-abc, test-xyz, etc. The asterisk () is a wildcard character that can match any string of characters To learn more about how to filter metrics in Splunk Observability Cloud, you can refer to this documentation.
https://docs.splunk.com/Observability/gdi/metrics/search.html#Filter-metrics
https://docs.splunk.com/Observability/gdi/metrics/search.html