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.geekcert.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

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 2

For a high-resolution metric, what is the highest possible native resolution of the metric?

A. 2 seconds

B. 15 seconds

C. 1 second

D. 5 seconds

Correct Answer: C

The correct answer is C. 1 second.

According to the Splunk Test Blueprint - O11y Cloud Metrics User document1, one of the metrics concepts that is covered in the exam is data resolution and rollups. Data resolution refers to the granularity of the metric data points, and rollups are the process of aggregating data points over time to reduce the amount of data stored. The Splunk O11y Cloud Certified Metrics User Track document2 states that one of the recommended courses for preparing for the exam is Introduction to Splunk Infrastructure Monitoring, which covers the basics of metrics monitoring and visualization. In the Introduction to Splunk Infrastructure Monitoring course, there is a section on Data Resolution and Rollups, which explains that Splunk Observability Cloud collects high- resolution metrics at 1-second intervals by default, and then applies rollups to reduce the data volume over time. The document also provides a table that shows the different rollup intervals and retention periods for different resolutions. Therefore, based on these documents, we can conclude that for a high-resolution metric, the highest possible native resolution of the metric is 1 second.

QUESTION 3

Which of the following are supported rollup functions in Splunk Observability Cloud?

A. average, latest, lag, min, max, sum, rate

B. std_dev, mean, median, mode, min, max

C. sigma, epsilon, pi, omega, beta, tau

D. 1min, 5min, 10min, 15min, 30min

Correct Answer: A

According to the Splunk O11y Cloud Certified Metrics User Track document1, Observability Cloud has the following rollup functions: Sum: (default for counter metrics): Returns the sum of all data points in the MTS reporting interval. Average

(default for gauge metrics):

Returns the average value of all data points in the MTS reporting interval. Min: Returns the minimum data point value seen in the MTS reporting interval. Max: Returns the maximum data point value seen in the MTS reporting interval. Latest:

Returns the most recent data point value seen in the MTS reporting interval. Lag: Returns the difference between the most recent and the previous data point values seen in the MTS reporting interval. Rate:

Returns the rate of change of data points in the MTS reporting interval. Therefore, option A is correct.

QUESTION 4

A Software Engineer is troubleshooting an issue with memory utilization in their application. They released a new canary version to production and now want to determine if the average memory usage is lower for requests with the \\'canary\\' version dimension. They\\'ve already opened the graph of memory utilization for their service.

How does the engineer see if the new release lowered average memory utilization?

A. On the chart for plot A, select Add Analytics, then select MeanrTransformation. In the window that appears, select \\'version\\' from the Group By field.

B. On the chart for plot A, scroll to the end and click Enter Function, then enter \\'A/B-l\\'.

C. On the chart for plot A, select Add Analytics, then select Mean:Aggregation. In the window that appears, select \\'version\\' from the Group By field.

D. On the chart for plot A, click the Compare Means button. In the window that appears, type \\'version1.

Correct Answer: C

The correct answer is C. On the chart for plot A, select Add Analytics, then select Mean:Aggregation. In the window that appears, select `version\\' from the Group By field.

This will create a new plot B that shows the average memory utilization for each version of the application. The engineer can then compare the values of plot B for the `canary\\' and `stable\\' versions to see if there is a significant difference. To

learn more about how to use analytics functions in Splunk Observability Cloud, you can refer to this documentation1.

1: https://docs.splunk.com/Observability/gdi/metrics/analytics.html

QUESTION 5

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