SPLK-4001 Q&As

Splunk O11y Cloud Certified Metrics User

Pass Splunk SPLK-4001 Exam with 100% Guarantee

QUESTION 1

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 2

Which of the following chart visualization types are unaffected by changing the time picker on a dashboard? (select all that apply)

A. Single Value

B. Heatmap

C. Line

D. List

Correct Answer: AD

The chart visualization types that are unaffected by changing the time picker on a dashboard are: Single Value: A single value chart shows the current value of a metric or an expression. It does not depend on the time range of the dashboard, but only on the data resolution and rollup function of the chart List: A list chart shows the values of a metric or an expression for each dimension value in a table format. It does not depend on the time range of the dashboard, but only on the data resolution and rollup function of the chart2 Therefore, the correct answer is A and D. To learn more about how to use different chart visualization types in Splunk Observability Cloud, you can refer to this documentation
https://docs.splunk.com/Observability/gdi/metrics/charts.html#Single-value
https://docs.splunk.com/Observability/gdi/metrics/charts.html#List
https://docs.splunk.com/Observability/gdi/metrics/charts.html

QUESTION 3

Which of the following statements is true of detectors created from a chart on a custom dashboard?

A. Changes made to the chart affect the detector.

B. Changes made to the detector affect the chart.

C. The alerts will show up in the team landing page.

D. The detector is automatically linked to the chart.

Correct Answer: D

The correct answer is D. The detector is automatically linked to the chart. When you create a detector from a chart on a custom dashboard, the detector is automatically linked to the chart. This means that you can see the detector status and alerts on the chart, and you can access the detector settings from the chart menu. You can also unlink the detector from the chart if you want to Changes made to the chart do not affect the detector, and changes made to the detector do not affect the chart. The detector and the chart are independent entities that have their own settings and parameters. However, if you change the metric or dimension of the chart, you might lose the link to the detector The alerts generated by the detector will show up in the Alerts page, where you can view, manage, and acknowledge them. You can also see them on the team landing page if you assign the detector to a team To learn more about how to create and link detectors from charts on custom dashboards, you can refer to this documentation.
https://docs.splunk.com/observability/alerts-detectors-notifications/link-detectors-to- charts.html
https://docs.splunk.com/observability/alerts-detectors-notifications/view- manage-alerts.html

QUESTION 4

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 5

The Sum Aggregation option for analytic functions does which of the following?

A. Calculates the number of MTS present in the plot.

B. Calculates 1/2 of the values present in the input time series.

C. Calculates the sum of values present in the input time series across the entire environment or per group.

D. Calculates the sum of values per time series across a period of time.

Correct Answer: C

According to the Splunk Test Blueprint - O11y Cloud Metrics User document1, one of the metrics concepts that is covered in the exam is analytic functions. Analytic functions are mathematical operations that can be applied to metrics to transform, aggregate, or analyze them. 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 Analytic Functions, which explains that analytic functions can be used to perform calculations on metrics, such as sum, average, min, max, count, etc. The document also provides examples of how to use analytic functions in charts and dashboards. One of the analytic functions that can be used is Sum Aggregation, which calculates the sum of values present in the input time series across the entire environment or per group. The document gives an example of how to use Sum Aggregation to calculate the total CPU usage across all hosts in a group by using the following syntax: sum(cpu.utilization) by hostgroup

QUESTION 6

A customer has a very dynamic infrastructure. During every deployment, all existing instances are destroyed, and new ones are created Given this deployment model, how should a detector be created that will not send false notifications of instances being down?

A. Create the detector. Select Alert settings, then select Auto-Clear Alerts and enter an appropriate time period.

B. Create the detector. Select Alert settings, then select Ephemeral Infrastructure and enter the expected lifetime of an instance.

C. Check the Dynamic checkbox when creating the detector.

D. Check the Ephemeral checkbox when creating the detector.

Correct Answer: B

According to the web search results, ephemeral infrastructure is a term that describes instances that are auto-scaled up or down, or are brought up with new code versions and discarded or recycled when the next code version is deployed1.

Splunk Observability Cloud has a feature that allows you to create detectors for ephemeral infrastructure without sending false notifications of instances being down. To use this feature, you need to do the following steps:

Create the detector as usual, by selecting the metric or dimension that you want to monitor and alert on, and choosing the alert condition and severity level. Select Alert settings, then select Ephemeral Infrastructure. This will enable a special

mode for the detector that will automatically clear alerts for instances that are expected to be terminated.

Enter the expected lifetime of an instance in minutes. This is the maximum amount of time that an instance is expected to live before being replaced by a new one. For example, if your instances are replaced every hour, you can enter 60

minutes as the expected lifetime.

Save the detector and activate it.

With this feature, the detector will only trigger alerts when an instance stops reporting a metric unexpectedly, based on its expected lifetime. If an instance stops reporting a metric within its expected lifetime, the detector will assume that it was

terminated on purpose and will not trigger an alert. Therefore, option B is correct.

QUESTION 7

Clicking a metric name from the results in metric finder displays the metric in Chart Builder. What action needs to be taken in order to save the chart created in the UI?

A. Create a new dashboard and save the chart.

B. Save the chart to multiple dashboards.

C. Make sure that data is coming in for the metric then save the chart.

D. Save the chart to a dashboard.

Correct Answer: D

According to the web search results, clicking a metric name from the results in metric finder displays the metric in Chart Builder1. Chart Builder is a tool that allows you to create and customize charts using metrics, dimensions, and analytics

functions2. To save the chart created in the UI, you need to do the following steps:

Click the Save button on the top right corner of the Chart Builder. This will open a dialog box where you can enter the chart name and description, and choose the dashboard where you want to save the chart.

Enter a name and a description for your chart. The name should be descriptive and unique, and the description should explain the purpose and meaning of the chart.

Choose an existing dashboard from the drop-down menu, or create a new dashboard by clicking the + icon. A dashboard is a collection of charts that display metrics and events for your services or hosts. You can organize and share

dashboards with other users in your organization using dashboard groups. Click Save. This will save your chart to the selected dashboard and redirect you to the dashboard view. You can also access your saved chart from the Dashboards

menu on the left navigation bar.

QUESTION 8

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

A. Line, Bar, Column

B. Bar, Area, Column

C. Line, Area, Column

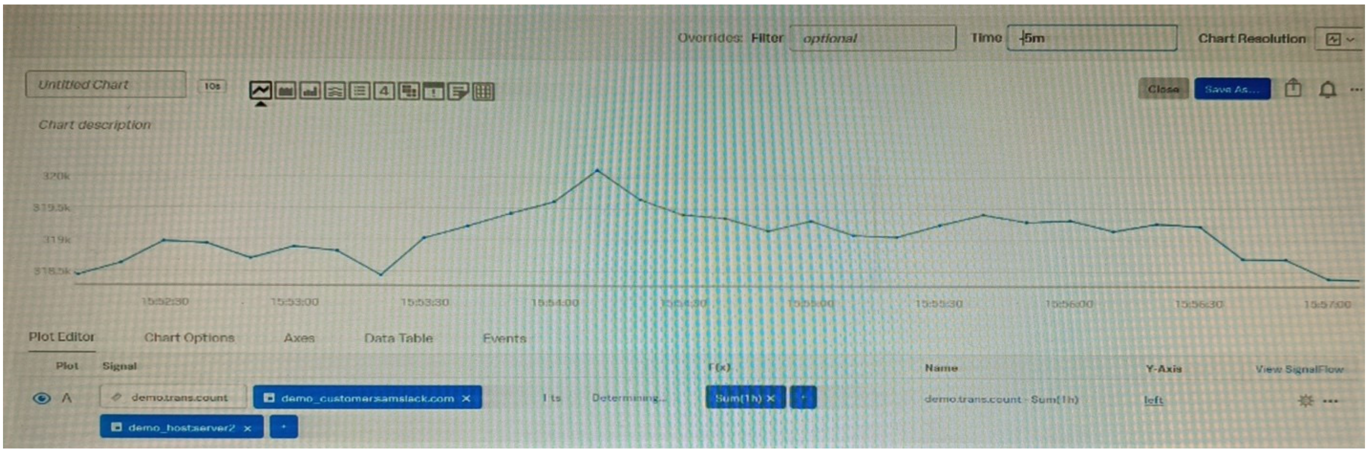
D. Histogram, Line, Column

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 9

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?



Overrides: Filter optional

Time -5m

Chart Resolution

Untitled Chart 10s

Chart description

Plot	Signal			F(x)	Name	Y-Axis
A	demo.trans.count demo_customersamslack.com × demo_hostserver2 ×	1 ts	Determining...	Sum(1h) ×	demo.trans.count - Sum(1h)	left

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 10

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