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

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 2

Which of the following statements are true about local data links? (select all that apply)

A. Anyone with write permission for a dashboard can add local data links that appear on that dashboard.

B. Local data links can only have a Splunk Observability Cloud internal destination.

C. Only Splunk Observability Cloud administrators can create local links.

D. Local data links are available on only one dashboard.

Correct Answer: AD

The correct answers are A and D.

According to the Get started with Splunk Observability Cloud document1, one of the topics that is covered in the Getting Data into Splunk Observability Cloud course is global and local data links. Data links are shortcuts that provide

convenient access to related resources, such as Splunk Observability Cloud dashboards, Splunk Cloud Platform and Splunk Enterprise, custom URLs, and Kibana logs. The document explains that there are two types of data links: global and

local. Global data links are available on all dashboards and charts, while local data links are available on only one dashboard. The document also provides the following information about local data links:

Anyone with write permission for a dashboard can add local data links that appear on that dashboard.

Local data links can have either a Splunk Observability Cloud internal destination or an external destination, such as a custom URL or a Kibana log. Only Splunk Observability Cloud administrators can delete local data links. Therefore, based

on this document, we can conclude that A and D are true statements about local data links. B and C are false statements because:

B is false because local data links can have an external destination as well as an internal one.

C is false because anyone with write permission for a dashboard can create local data links, not just administrators.

QUESTION 3

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 4

What information is needed to create a detector?

A. Alert Status, Alert Criteria, Alert Settings, Alert Message, Alert Recipients

B. Alert Signal, Alert Criteria, Alert Settings, Alert Message, Alert Recipients

C. Alert Signal, Alert Condition, Alert Settings, Alert Message, Alert Recipients

D. Alert Status, Alert Condition, Alert Settings, Alert Meaning, Alert Recipients

Correct Answer: C

According to the Splunk Observability Cloud documentation1, to create a detector, you need the following information:

Alert Signal: This is the metric or dimension that you want to monitor and alert on. You can select a signal from a chart or a dashboard, or enter a SignalFlow query to define the signal.

Alert Condition: This is the criteria that determines when an alert is triggered or cleared. You can choose from various built-in alert conditions, such as static threshold, dynamic threshold, outlier, missing data, and so on. You can also specify

the severity level and the trigger sensitivity for each alert condition. Alert Settings: This is the configuration that determines how the detector behaves and interacts with other detectors. You can set the detector name, description, resolution,

run lag, max delay, and detector rules. You can also enable or disable the detector, and mute or unmute the alerts.

Alert Message: This is the text that appears in the alert notification and event feed. You can customize the alert message with variables, such as signal name, value, condition, severity, and so on. You can also use markdown formatting to

enhance the message appearance.

Alert Recipients: This is the list of destinations where you want to send the alert notifications. You can choose from various channels, such as email, Slack, PagerDuty, webhook, and so on. You can also specify the notification frequency and

suppression settings.

QUESTION 5

A customer deals with a holiday rush of traffic during November each year, but does not want to be flooded with alerts when this happens. The increase in traffic is expected and consistent each year. Which detector condition should be used when creating a detector for this data?

A. Outlier Detection

B. Static Threshold

C. Calendar Window

D. Historical Anomaly

Correct Answer: D

historical anomaly is a detector condition that allows you to trigger an alert when a signal deviates from its historical pattern. Historical anomaly uses machine learning to learn the normal behavior of a signal based on its past data, and then compares the current value of the signal with the expected value based on the learned pattern. You can use historical anomaly to detect unusual changes in a signal that are not explained by seasonality, trends, or cycles. Historical anomaly is suitable for creating a detector for the customer\\'s data, because it can account for the expected and consistent increase in traffic during November each year. Historical anomaly can learn that the traffic pattern has a seasonal component that peaks in November, and then adjust the expected value of the traffic accordingly. This way, historical anomaly can avoid triggering alerts when the traffic increases in November, as this is not an anomaly, but rather a normal variation. However, historical anomaly can still trigger alerts when the traffic deviates from the historical pattern in other ways, such as if it drops significantly or spikes unexpectedly.