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 is experiencing an issue where their detector is not sending email notifications but is generating alerts within the Splunk Observability UI. Which of the below is the root cause?

A. The detector has an incorrect alert rule.

B. The detector has an incorrect signal,

C. The detector is disabled.

D. The detector has a muting rule.

Correct Answer: D

The most likely root cause of the issue is D. The detector has a muting rule. A muting rule is a way to temporarily stop a detector from sending notifications for certain alerts, without disabling the detector or changing its alert conditions. A muting rule can be useful when you want to avoid alert noise during planned maintenance, testing, or other situations where you expect the metrics to deviate from normal When a detector has a muting rule, it will still generate alerts within the Splunk Observability UI, but it will not send email notifications or any other types of notifications that you have configured for the detector. You can see if a detector has a muting rule by looking at the Muting Rules tab on the detector page. You can also create, edit, or delete muting rules from there To learn more about how to use muting rules in Splunk Observability Cloud, you can refer to this documentation.

QUESTION 2

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 3

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 4

Where does the Splunk distribution of the OpenTelemetry Collector store the configuration files on Linux machines by default?

A. /opt/splunk/

B. /etc/otel/collector/

C. /etc/opentelemetry/

D. /etc/system/default/

Correct Answer: B

The correct answer is B. /etc/otel/collector/ According to the web search results, the Splunk distribution of the OpenTelemetry Collector stores the configuration files on Linux machines in the /etc/otel/collector/ directory by default. You can verify this by looking at the first result, which explains how to install the Collector for Linux manually. It also provides the locations of the default configuration file, the agent configuration file, and the gateway configuration file. To learn more about how to install and configure the Splunk distribution of the OpenTelemetry Collector, you can refer to this documentation. https://docs.splunk.com/Observability/gdi/opentelemetry/install-linux-manual.html https://docs.splunk.com/Observability/gdi/opentelemetry.html

QUESTION 5

To smooth a very spiky cpu.utilization metric, what is the correct analytic function to better see if the cpu. utilization for servers is trending up over time?

A. Rate/Sec

B. Median

C. Mean (by host)

D. Mean (Transformation)

Correct Answer: D

The correct answer is D. Mean (Transformation).

According to the web search results, a mean transformation is an analytic function that returns the average value of a metric or a dimension over a specified time interval. A mean transformation can be used to smooth a very spiky metric, such as cpu.utilization, by reducing the impact of outliers and noise. A mean transformation can also help to see if the metric is trending up or down over time, by showing the general direction of the average value. For example, to smooth the cpu.utilization metric and see if it is trending up over time, you can use the following SignalFlow code: mean(1h, counters("cpu.utilization")) This will return the average value of the cpu.utilization counter metric for each metric time series (MTS) over the last hour. You can then use a chart to visualize the results and compare the mean values across different MTS. Option A is incorrect because rate/sec is not an analytic function, but rather a rollup function that returns the rate of change of data points in the MTS reporting interval1. Rate/sec can be used to convert cumulative counter metrics into counter metrics, but it does not smooth or trend a metric. Option B is incorrect because median is not an analytic function, but rather an aggregation function that returns the middle value of a metric or a dimension over the entire time range1. Median can be used to find the typical value of a metric, but it does not smooth or trend a metric. Option C is incorrect because mean (by host) is not an analytic function, but rather an aggregation function that returns the average value of a metric or a dimension across all MTS with the same host dimension1. Mean (by host) can be used to compare the performance of different hosts, but it does not smooth or trend a metric. Mean (Transformation) is an analytic function that allows you to smooth a very spiky metric by applying a moving average over a specified time window. This can help you see the general trend of the metric over time, without being distracted by the short-term fluctuations To use Mean (Transformation) on a cpu.utilization metric, you need to select the metric from the Metric Finder, then click on Add Analytics and choose Mean (Transformation) from the list of functions. You can then specify the time window for the moving average, such as 5 minutes, 15 minutes, or 1 hour. You can also group the metric by host or any other dimension to compare the smoothed values across different servers2 To learn more about how to use Mean (Transformation) and other analytic functions in Splunk Observability Cloud, you can refer to this documentation. https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Mean-Transformation https://docs.splunk.com/Observability/gdi/metrics/analytics.html