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

Which of the following can be configured when subscribing to a built-in detector?

A. Alerts on team landing page.

B. Alerts on a dashboard.

C. Outbound notifications.

D. Links to a chart.

Correct Answer: C

According to the web search results1, subscribing to a built-in detector is a way to receive alerts and notifications from Splunk Observability Cloud when certain criteria are met. A built-in detector is a detector that is automatically created and

configured by Splunk Observability Cloud based on the data from your integrations, such as AWS, Kubernetes, or OpenTelemetry1. To subscribe to a built-in detector, you need to do the following steps:

Find the built-in detector that you want to subscribe to. You can use the metric finder or the dashboard groups to locate the built-in detectors that are relevant to your data sources.

Hover over the built-in detector and click the Subscribe button. This will open a dialog box where you can configure your subscription settings1. Choose an outbound notification channel from the drop-down menu. This is where you can

specify how you want to receive the alert notifications from the built-in detector. You can choose from various channels, such as email, Slack, PagerDuty, webhook, and so on. You can also create a new notification channel by clicking the +

icon.

Enter the notification details for the selected channel. This may include your email address, Slack channel name, PagerDuty service key, webhook URL, and so on. You can also customize the notification message with variables and

markdown formatting.

Click Save. This will subscribe you to the built-in detector and send you alert notifications through the chosen channel when the detector triggers or clears an alert.

Therefore, option C is correct.

QUESTION 2

An SRE creates a new detector to receive an alert when server latency is higher than 260 milliseconds. Latency below 260 milliseconds is healthy for their service. The SRE creates a New Detector with a Custom Metrics Alert Rule for latency and sets a Static Threshold alert condition at 260ms.

How can the number of alerts be reduced?

A. Adjust the threshold.

B. Adjust the Trigger sensitivity. Duration set to 1 minute.

C. Adjust the notification sensitivity. Duration set to 1 minute.

D. Choose another signal.

Correct Answer: B

According to the Splunk O11y Cloud Certified Metrics User Track document1, trigger sensitivity is a setting that determines how long a signal must remain above or below a threshold before an alert is triggered. By default, trigger sensitivity is set to Immediate, which means that an alert is triggered as soon as the signal crosses the threshold. This can result in a lot of alerts, especially if the signal fluctuates frequently around the threshold value. To reduce the number of alerts, you can adjust the trigger sensitivity to a longer duration, such as 1 minute, 5 minutes, or 15 minutes. This means that an alert is only triggered if the signal stays above or below the threshold for the specified duration. This can help filter out noise and focus on more persistent issues.

QUESTION 3

An SRE creates an event feed chart in a dashboard that shows a list of events that meet criteria they specify. Which of the following should they include? (select all that apply)

A. Custom events that have been sent in from an external source.

B. Events created when a detector clears an alert.

C. Random alerts from active detectors.

D. Events created when a detector triggers an alert.

Correct Answer: ABD

According to the web search results, an event feed chart is a type of chart that shows a list of events that meet criteria you specify. An event feed chart can display one or more event types depending on how you specify the criteria. The event

types that you can include in an event feed chart are:

Custom events that have been sent in from an external source: These are events that you have created or received from a third-party service or tool, such as AWS CloudWatch, GitHub, Jenkins, or PagerDuty. You can send custom events to

Splunk Observability Cloud using the API or the Event Ingest Service. Events created when a detector triggers or clears an alert: These are events that are automatically generated by Splunk Observability Cloud when a detector evaluates a

metric or dimension and finds that it meets the alert condition or returns to normal. You can create detectors to monitor and alert on various metrics and dimensions using the UI or the API.

Therefore, option A, B, and D are correct.

QUESTION 4

A customer wants to share a collection of charts with their entire SRE organization. What feature of Splunk Observability Cloud makes this possible?

A. Dashboard groups

B. Shared charts

C. Public dashboards

D. Chart exporter

Correct Answer: A

According to the web search results, dashboard groups are a feature of Splunk Observability Cloud that allows you to organize and share dashboards with other users in your organization1. You can create dashboard groups based on different criteria, such as service, team, role, or topic. You can also set permissions for each dashboard group, such as who can view, edit, or manage the dashboards in the group. Dashboard groups make it possible to share a collection of charts with your entire SRE organization, or any other group of users that you want to collaborate with.

QUESTION 5

A DevOps engineer wants to determine if the latency their application experiences is growing fester after a new software release a week ago. They have already created two plot lines, A and B, that represent the current latency and the latency a week ago, respectively. How can the engineer use these two plot lines to determine the rate of change in latency?

A. Create a temporary plot by dragging items A and B into the Analytics Explorer window.

B. Create a plot C using the formula (A-B) and add a scale:percent function to express the rate of change as a percentage.

C. Create a plot C using the formula (A/B-l) and add a scale: 100 function to express the rate of change as a percentage.

D. Create a temporary plot by clicking the Change% button in the upper-right corner of the plot showing lines A and B.

Correct Answer: C

The correct answer is C. Create a plot C using the formula (A/B-l) and add a scale: 100 function to express the rate of change as a percentage. To calculate the rate of change in latency, you need to compare the current latency (plot A) with the latency a week ago (plot B). One way to do this is to use the formula (A/B-l), which gives you the ratio of the current latency to the previous latency minus one. This ratio represents how much the current latency has increased or decreased relative to the previous latency. For example, if the current latency is 200 ms and the previous latency is 100 ms, then the ratio is (200/100-l) = 1, which means the current latency is 100% higher than the previous latency To express the rate of change as a percentage, you need to multiply the ratio by 100. You can do this by adding a scale: 100 function to the formula. This function scales the values of the plot by a factor of 100. For example, if the ratio is 1, then the scaled value is 100%2 To create a plot C using the formula (A/B-l) and add a scale: 100 function, you need to follow these steps: Select plot A and plot B from the Metric Finder. Click on Add Analytics and choose Formula from the list of functions. In the Formula window, enter (A/B-l) as the formula and click Apply. Click on Add Analytics again and choose Scale from the list of functions. In the Scale window, enter 100 as the factor and click Apply. You should see a new plot C that shows the rate of change in latency as a percentage. To learn more about how to use formulas and scale functions in Splunk Observability Cloud, you can refer to these documentations.
https://www.mathsisfun.com/numbers/percentage-change.html
https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Scale
https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Formula
https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Scale