Free Questions for SPLK-4001 by certscare

Shared by Cote on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Alerts on team landing page.

B- Alerts on a dashboard.

C- Outbound notifications.

D- Links to a chart.

Answer:

C

Explanation:

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 sources1.

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 on2.You can also create a new notification channel by clicking the + icon2.

Enter the notification details for the selected channel.This may include your email address, Slack channel name, PagerDuty service key, webhook URL, and so on2.You can also customize the notification message with variables and markdown formatting2.

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

Question Type: **MultipleChoice**

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

Options:

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.

Answer:

D

Explanation:

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 to1

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 detector1

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 team2

To learn more about how to create and link detectors from charts on custom dashboards, you can refer to this documentation1.

1: https://docs.splunk.com/observability/alerts-detectors-notifications/link-detectors-to-charts.html 2: https://docs.splunk.com/observability/alerts-detectors-notifications/view-manage-alerts.html

Question 3

Question Type: **MultipleChoice**

When installing OpenTelemetry Collector, which error message is indicative that there is a misconfigured realm or access token?

Options:

A- 403 (NOT ALLOWED)

B- 404 (NOT FOUND)

C- 401 (UNAUTHORIZED)

D- 503 (SERVICE UNREACHABLE)

Answer:

C

Explanation:

The correct answer is C. 401 (UNAUTHORIZED).

According to the web search results, a 401 (UNAUTHORIZED) error message is indicative that there is a misconfigured realm or access token when installing OpenTelemetry Collector1. A 401 (UNAUTHORIZED) error message means that the request was not authorized by the server due to invalid credentials. A realm is a parameter that specifies the scope of protection for a resource, such as a Splunk Observability Cloud endpoint. An access token is a credential that grants access to a resource, such as a Splunk Observability Cloud API. If the realm or the access token is misconfigured, the request to install OpenTelemetry Collector will be rejected by the server with a 401 (UNAUTHORIZED) error message.

Option A is incorrect because a 403 (NOT ALLOWED) error message is not indicative that there is a misconfigured realm or access token when installing OpenTelemetry Collector. A 403 (NOT ALLOWED) error message means that the request was authorized by the server but not allowed due to insufficient permissions. Option B is incorrect because a 404 (NOT FOUND) error message is not indicative that there is a misconfigured realm or access token when installing OpenTelemetry Collector. A 404 (NOT FOUND) error message means that the request was not found by the server due to an invalid URL or resource. Option D is incorrect because a 503 (SERVICE UNREACHABLE) error message is not indicative that there is a misconfigured realm or access token when installing

OpenTelemetry Collector. A 503 (SERVICE UNREACHABLE) error message means that the server was unable to handle the request due to temporary overload or maintenance.

Question 4

Question Type: MultipleChoice

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

Options:

A- Single Value

B- Heatmap

C- Line

D- List

Answer:

A, D

Explanation:

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 chart1

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 documentation3.

1: https://docs.splunk.com/Observability/gdi/metrics/charts.html#Single-value 2: https://docs.splunk.com/Observability/gdi/metrics/charts.html#List 3: https://docs.splunk.com/Observability/gdi/metrics/charts.html

Question 5

Question Type: MultipleChoice

Which of the following statements about adding properties to MTS are true? (select all that apply)

Options:

A- Properties can be set via the API.

B- Properties are sent in with datapoints.

C- Properties are applied to dimension key:value pairs and propagated to all MTS with that dimension

D- Properties can be set in the UI under Metric Metadata.

Answer:

A, D

Explanation:

According to the web search results, properties are key-value pairs that you can assign to dimensions of existing metric time series (MTS) in Splunk Observability Cloud1. Properties provide additional context and information about the metrics, such as the environment, role, or owner of the dimension. For example, you can add the property use: QA to the host dimension of your metrics to indicate that the host that is sending the data is used for QA.

To add properties to MTS, you can use either the API or the UI.The API allows you to programmatically create, update, delete, and list properties for dimensions using HTTP requests2.The UI allows you to interactively create, edit, and delete properties for dimensions using the Metric Metadata page under Settings3. Therefore, option A and D are correct.

Question 6

Question Type: MultipleChoice

What is the limit on the number of properties that an MTS can have?

Options:

A- 64

B- 36

C- No limit

D- 50

Answer:

A

Explanation:

The correct answer is A. 64.

According to the web search results, the limit on the number of properties that an MTS can have is 64. A property is a key-value pair that you can assign to a dimension of an existing MTS to add more context to the metrics. For example, you can add the property use: QA to the host dimension of your metrics to indicate that the host is used for QA1

Properties are different from dimensions, which are key-value pairs that are sent along with the metrics at the time of ingest. Dimensions, along with the metric name, uniquely identify an MTS. The limit on the number of dimensions per MTS is 362

To learn more about how to use properties and dimensions in Splunk Observability Cloud, you can refer to this documentation2.

1: https://docs.splunk.com/Observability/metrics-and-metadata/metrics-dimensions-mts.html#Custom-properties 2: https://docs.splunk.com/Observability/metrics-and-metadata/metrics-dimensions-mts.html