Free Questions for SPLK-4001 by braindumpscollection

Shared by Joyner on 15-04-2024

Question 1

Question Type: **MultipleChoice**

With exceptions for transformations or timeshifts, at what resolution do detectors operate?

Options:

A- 10 seconds

B- The resolution of the chart

C- The resolution of the dashboard

D- Native resolution

Answer:

D

Explanation:

According to the Splunk Observability Cloud documentation1, detectors operate at the native resolution of the metric or dimension that they monitor, with some exceptions for transformations or timeshifts. The native resolution is the frequency at which the data points are reported by the source. For example, if a metric is reported every 10 seconds, the detector will evaluate the metric every 10 seconds.

The native resolution ensures that the detector uses the most granular and accurate data available for alerting.

Question 2

Question Type: MultipleChoice

The alert recipients tab specifies where notification messages should be sent when alerts are triggered or cleared. Which of the below options can be used? (select all that apply)

Options:

A- Invoke a webhook URL.

B- Export to CSV.

C- Send an SMS message.

D- Send to email addresses.

Answer:

A, C, D

Explanation:

The alert recipients tab specifies where notification messages should be sent when alerts are triggered or cleared. The options that can be used are:

Invoke a webhook URL. This option allows you to send a HTTP POST request to a custom URL that can perform various actions based on the alert information. For example, you can use a webhook to create a ticket in a service desk system, post a message to a chat channel, or trigger another workflow1

Send an SMS message. This option allows you to send a text message to one or more phone numbers when an alert is triggered or cleared. You can customize the message content and format using variables and templates2

Send to email addresses. This option allows you to send an email notification to one or more recipients when an alert is triggered or cleared. You can customize the email subject, body, and attachments using variables and templates. You can also include information from search results, the search job, and alert triggering in the email3

Therefore, the correct answer is A, C, and D.

1: https://docs.splunk.com/Documentation/Splunk/latest/Alert/Webhooks 2: https://docs.splunk.com/Documentation/Splunk/latest/Alert/SMSnotification 3: https://docs.splunk.com/Documentation/Splunk/latest/Alert/Emailnotification

Question 3

Question Type: MultipleChoice

A customer has a large population of servers. They want to identify the servers where utilization has increased the most since last week. Which analytics function is needed to achieve this?

Options:

A- Rate

B- Sum transformation

C- Tlmeshift

D- Standard deviation

Answer:

C

Explanation:

The correct answer is C. Timeshift.

According to the Splunk Observability Cloud documentation1, timeshift is an analytic function that allows you to compare the current value of a metric with its value at a previous time interval, such as an hour ago or a week ago. You can use the timeshift function to measure the change in a metric over time and identify trends, anomalies, or patterns. For example, to identify the servers where utilization has increased the most since last week, you can use the following SignalFlow code:

```
timeshift(1w, counters("server.utilization"))
```

This will return the value of the server.utilization counter metric for each server one week ago. You can then subtract this value from the current value of the same metric to get the difference in utilization. You can also use a chart to visualize the results and sort them by the highest difference in utilization.

Question 4

Question Type: MultipleChoice

What information is needed to create a detector?

Options:

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

Answer:

C

Explanation:

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

Question Type: MultipleChoice

A customer is experiencing issues getting metrics from a new receiver they have configured in the OpenTelemetry Collector. How would the customer go about troubleshooting further with the logging exporter?

Options:

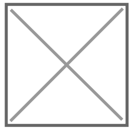
A- Adding debug into the metrics receiver pipeline:

Image not found or type unknown

B- Adding logging into the metrics receiver pipeline:

C- Adding logging into the metrics exporter pipeline:

D- Adding debug into the metrics exporter pipeline:



Answer:

B

Explanation:

The correct answer is B. Adding logging into the metrics receiver pipeline.

The logging exporter is a component that allows the OpenTelemetry Collector to send traces, metrics, and logs directly to the console. It can be used to diagnose and troubleshoot issues with telemetry received and processed by the Collector, or to obtain samples for other purposes1

To activate the logging exporter, you need to add it to the pipeline that you want to diagnose. In this case, since you are experiencing issues with a new receiver for metrics, you need to add the logging exporter to the metrics receiver pipeline. This will create a new plot that shows the metrics received by the Collector and any errors or warnings that might occur1

The image that you have sent with your question shows how to add the logging exporter to the metrics receiver pipeline. You can see that the exporters section of the metrics pipeline includes logging as one of the options. This means that the metrics received by any of the receivers listed in the receivers section will be sent to the logging exporter as well as to any other exporters listed2

To learn more about how to use the logging exporter in Splunk Observability Cloud, you can refer to this documentation1.

1: https://docs.splunk.com/Observability/gdi/opentelemetry/components/logging-exporter.html 2: https://docs.splunk.com/Observability/gdi/opentelemetry/exposed-endpoints.html

Question 6

Question Type: MultipleChoice

Which analytic function can be used to discover peak page visits for a site over the last day?

Options:

A- Maximum: Transformation (24h)

B- Maximum: Aggregation (Id)

C- Lag: (24h)

D- Count: (Id)

Answer:

A

Explanation:

According to the Splunk Observability Cloud documentation1, the maximum function is an analytic function that returns the highest value of a metric or a dimension over a specified time interval. The maximum function can be used as a transformation or an aggregation. A transformation applies the function to each metric time series (MTS) individually, while an aggregation applies the function to all MTS and returns a single value. For example, to discover the peak page visits for a site over the last day, you can use the following SignalFlow code:

```
maximum(24h, counters("page.visits"))
```

This will return the highest value of the page.visits counter metric for each MTS over the last 24 hours. You can then use a chart to visualize the results and identify the peak page visits for each MTS.

Question 7

Question Type: MultipleChoice

Which of the following is optional, but highly recommended to include in a datapoint?

Options:

A- Metric name

B- Timestamp

C- Value

D- Metric type

Answer:

D

Explanation:

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 correctly1

To learn more about how to send metrics to Splunk Observability Cloud, you can refer to this documentation2.

1: https://docs.splunk.com/Observability/gdi/metrics/metrics.html#Metric-types 2: https://docs.splunk.com/Observability/gdi/metrics/metrics.html

Question 8

Question Type: **MultipleChoice**

Which of the following rollups will display the time delta between a datapoint being sent and a datapoint being received?

Options:

A- Jitter

B- Delay

C- Lag

D- Latency

Answer:

C

Explanation:

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.

20%
DISCOUNT