ExamsIndex
Practice Materials & Tests

DEMO VERSION

Splunk

SPLK-4001 Exam

Splunk O11y Cloud Certified Metrics User

Exam Latest Version: 6.2

Question 1. (Multi Select)

What are the best practices for creating detectors? (select all that apply)

A: View data at highest resolution.
B: Have a consistent value.
C: View detector in a chart.
D: Have a consistent type of measurement.

Correct Answer: A, B, C, D

Explanation:

The best practices for creating detectors are:

View data at highest resolution. This helps to avoid missing important signals or patterns in the data that could indicate anomalies or issues1

Have a consistent value. This means that the metric or dimension used for detection should have a clear and stable meaning across different sources, contexts, and time periods. For example, avoid using metrics that are affected by changes in configuration, sampling, or aggregation2

View detector in a chart. This helps to visualize the data and the detector logic, as well as to identify any false positives or negatives. It also allows to adjust the detector parameters and thresholds based on the data distribution and behavior3

Have a consistent type of measurement. This means that the metric or dimension used for detection should have the same unit and scale across different sources, contexts, and time periods. For example, avoid mixing bytes and bits, or seconds and milliseconds.

1: https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best-practices-for-detectors
2: https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best-practices-for-detectors
3: https://docs.splunk.com/Observability/gdi/metrics/detectors.html#View-detector-in-a-chart : https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Best-practices-for-detectors

Question 2. (Single Select)

An SRE came across an existing detector that is a good starting point for a detector they want to create. They clone the detector, update the metric, and add multiple new signals. As a result of the cloned detector, which of the following is true?

A: The new signals will be reflected in the original detector.
B: The new signals will be reflected in the original chart.
C: You can only monitor one of the new signals.
D: The new signals will not be added to the original detector.

Correct Answer: D

Explanation:

According to the Splunk O11y Cloud Certified Metrics User Track document1, cloning a detector creates a copy of the detector that you can modify without affecting the original detector. You can change the metric, filter, and signal settings of the cloned detector. However, the new signals that you add to the cloned detector will not be reflected in the original detector, nor in the original chart that the detector was based on. Therefore, option D is correct.

Option A is incorrect because the new signals will not be reflected in the original detector. Option B is incorrect because the new signals will not be reflected in the original chart. Option C is incorrect because you can monitor all of the new signals that you add to the cloned detector.

Question 3. (Single Select)

To refine a search for a metric a customer types host: test-*. What does this filter return?

A: Only metrics with a dimension of host and a value beginning with test-.
B: Error
C: Every metric except those with a dimension of host and a value equal to test.
D: Only metrics with a value of test- beginning with host.

Correct Answer: A

Explanation:

The correct answer is A. Only metrics with a dimension of host and a value beginning with test-.

This filter returns the metrics that have a host dimension that matches the pattern test-. For example, test-01, test-abc, test-xyz, etc. The asterisk () is a wildcard character that can match any string of characters1

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

1: https://docs.splunk.com/Observability/gdi/metrics/search.html#Filter-metrics 2: https://docs.splunk.com/Observability/gdi/metrics/search.html

---

Question 4. (Single Select)

A customer operates a caching web proxy. They want to calculate the cache hit rate for their service. What is the best way to achieve this?

A: Percentages and ratios
B: Timeshift and Bottom N
C: Timeshift and Top N
D: Chart Options and metadata

Correct Answer: A

Explanation:

According to the Splunk O11y Cloud Certified Metrics User Track document1, percentages and ratios are useful for calculating the proportion of one metric to another, such as cache hits to cache misses, or successful requests to failed requests. You can use the percentage() or ratio() functions in SignalFlow to compute these values and display them in charts. For example, to calculate the cache hit rate for a service, you can use the following SignalFlow code:

percentage(counters(“cache.hits”), counters(“cache.misses”))

This will return the percentage of cache hits out of the total number of cache attempts. You can

also use the ratio() function to get the same result, but as a decimal value instead of a percentage.

ratio(counters(“cache.hits”), counters(“cache.misses”))

Question 5. (Single Select)

Which of the following are correct ports for the specified components in the OpenTelemetry Collector?

A: gRPC (4000), SignalFx (9943), Fluentd (6060)
B: gRPC (6831), SignalFx (4317), Fluentd (9080)
C: gRPC (4459), SignalFx (9166), Fluentd (8956)
D: gRPC (4317), SignalFx (9080), Fluentd (8006)

Correct Answer: D

Explanation:

The correct answer is D. gRPC (4317), SignalFx (9080), Fluentd (8006).

According to the web search results, these are the default ports for the corresponding components in the OpenTelemetry Collector. You can verify this by looking at the table of exposed ports and endpoints in the first result1. You can also see the agent and gateway configuration files in the same result for more details.

1: https://docs.splunk.com/observability/gdi/opentelemetry/exposed-endpoints.html

ExamsIndex

Demo PDF Complete

Your SPLK-4001 Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 30% off, use Coupon Code: NEWYEAR30

https://examsindex.com/exam/splk-4001