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

Which of the following are true about organization metrics? (select all that apply)

A. Organization metrics give insights into system usage, system limits, data ingested and token quotas.

B. Organization metrics count towards custom MTS limits.

C. Organization metrics are included for free.

D. A user can plot and alert on them like metrics they send to Splunk Observability Cloud.

Correct Answer: ACD

The correct answer is A, C, and D. Organization metrics give insights into system usage, system limits, data ingested and token quotas. Organization metrics are included for free. A user can plot and alert on them like metrics they send to

Splunk Observability Cloud.

Organization metrics are a set of metrics that Splunk Observability Cloud provides to help you measure your organization\\'s usage of the platform. They include metrics such as:

Ingest metrics: Measure the data you\\'re sending to Infrastructure Monitoring, such as the number of data points you\\'ve sent.

App usage metrics: Measure your use of application features, such as the number of dashboards in your organization.

Integration metrics: Measure your use of cloud services integrated with your organization, such as the number of calls to the AWS CloudWatch API. Resource metrics: Measure your use of resources that you can specify limits for, such as the

number of custom metric time series (MTS) you\\'ve created1 Organization metrics are not charged and do not count against any system limits. You can view them in built-in charts on the Organization Overview page or in custom charts using

the Metric Finder. You can also create alerts based on organization metrics to monitor your usage and performance

To learn more about how to use organization metrics in Splunk Observability Cloud, you can refer to this documentation.

https://docs.splunk.com/observability/admin/org-metrics.html

QUESTION 2

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

QUESTION 3

For a high-resolution metric, what is the highest possible native resolution of the metric?

A. 2 seconds

B. 15 seconds

C. 1 second

D. 5 seconds

Correct Answer: C

The correct answer is C. 1 second.

According to the Splunk Test Blueprint - O11y Cloud Metrics User document1, one of the metrics concepts that is covered in the exam is data resolution and rollups. Data resolution refers to the granularity of the metric data points, and rollups are the process of aggregating data points over time to reduce the amount of data stored. The Splunk O11y Cloud Certified Metrics User Track document2 states that one of the recommended courses for preparing for the exam is Introduction to Splunk Infrastructure Monitoring, which covers the basics of metrics monitoring and visualization. In the Introduction to Splunk Infrastructure Monitoring course, there is a section on Data Resolution and Rollups, which explains that Splunk Observability Cloud collects high- resolution metrics at 1-second intervals by default, and then applies rollups to reduce the data volume over time. The document also provides a table that shows the different rollup

intervals and retention periods for different resolutions. Therefore, based on these documents, we can conclude that for a high-resolution metric, the highest possible native resolution of the metric is 1 second.

QUESTION 4

Which of the following are ways to reduce flapping of a detector? (select all that apply)

A. Configure a duration or percent of duration for the alert.

B. Establish a reset threshold for the detector.

C. Enable the anti-flap setting in the detector options menu.

D. Apply a smoothing transformation (like a rolling mean) to the input data for the detector.

Correct Answer: AD

According to the Splunk Lantern article Resolving flapping detectors in Splunk Infrastructure Monitoring, flapping is a phenomenon where alerts fire and clear repeatedly in a short period of time, due to the signal fluctuating around the

threshold value. To reduce flapping, the article suggests the following ways:

Configure a duration or percent of duration for the alert: This means that you require the signal to stay above or below the threshold for a certain amount of time or percentage of time before triggering an alert. This can help filter out noise and

focus on more persistent issues.

Apply a smoothing transformation (like a rolling mean) to the input data for the detector: This means that you replace the original signal with the average of its last several values, where you can specify the window length. This can reduce the

impact of a single extreme observation and make the signal less fluctuating.

QUESTION 5

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

A. Jitter

B. Delay

C. Lag

D. Latency

Correct Answer: C

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.

Latest SPLK-4001 Dumps SPLK-4001 Practice Test SPLK-4001 Braindumps