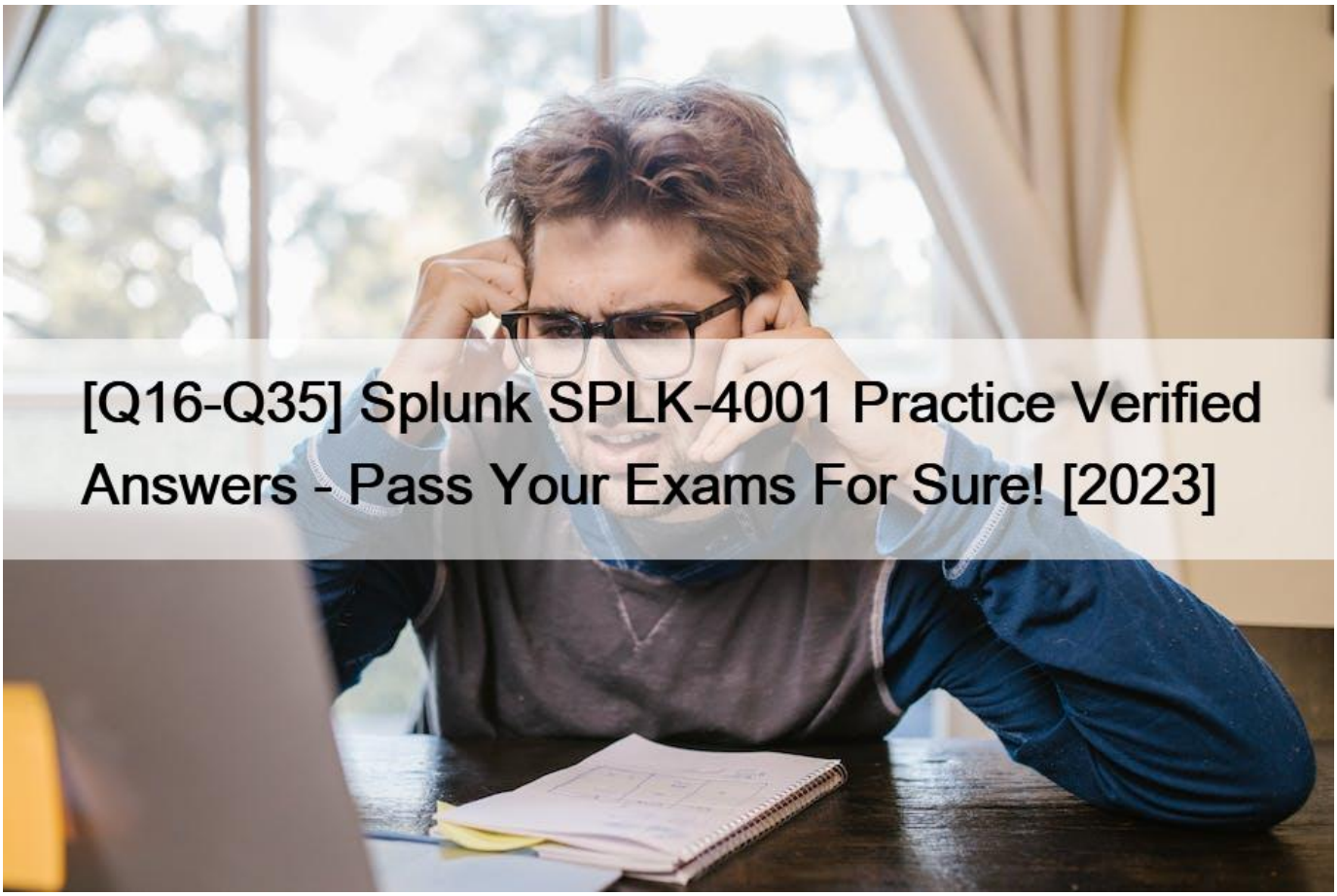
[Q16-Q35 Splunk SPLK-4001 Practice Verified Answers - Pass Your Exams For Sure! [2023



Splunk SPLK-4001 Practice Verified Answers - Pass Your Exams For Sure! [2023
Valid Way To Pass Splunk O11y Cloud Certified's SPLK-4001 Exam

The Splunk SPLK-4001 exam consists of 65 questions that are to be completed in 90 minutes. The questions are in a multiple-choice format with a passing score of 70% or higher. Splunk O11y Cloud Certified Metrics User certification is valid for two years and must be renewed after the expiration date. There is a registration fee to take the exam, and the exam can be taken at any Pearson VUE test center or online through remote proctoring. Splunk O11y Cloud Certified Metrics User certification exam requires thorough preparation, including self-study, practice tests, and attending Splunk training courses.

The Splunk SPLK-4001 exam covers a range of topics related to metrics monitoring, including data ingestion, visualization, analysis, and troubleshooting. It also includes questions on best practices for configuring and optimizing Splunk for cloud-based environments. To pass the exam, candidates must demonstrate a deep understanding of these topics and be able to apply their knowledge to real-world scenarios.

QUESTION 16

Which of the following statements are true about local data links? (select all that apply)
* Anyone with write permission for a dashboard can add local data links that appear on that dashboard.
* Local data links can only have a Splunk Observability Cloud internal destination.
* Only Splunk Observability Cloud administrators can create local links.
* Local data links are available on only one dashboard.

Explanation

The correct answers are A and D.

According to the Get started with Splunk Observability Cloud document1, one of the topics that is covered in the Getting Data into Splunk Observability Cloud course is global and local data links. Data links are shortcuts that provide convenient access to related resources, such as Splunk Observability Cloud dashboards, Splunk Cloud Platform and Splunk Enterprise, custom URLs, and Kibana logs.

The document explains that there are two types of data links: global and local. Global data links are available on all dashboards and charts, while local data links are available on only one dashboard. The document also provides the following information about local data links:

Anyone with write permission for a dashboard can add local data links that appear on that dashboard.

Local data links can have either a Splunk Observability Cloud internal destination or an external destination, such as a custom URL or a Kibana log.

Only Splunk Observability Cloud administrators can delete local data links.

Therefore, based on this document, we can conclude that A and D are true statements about local data links. B and C are false statements because:

B is false because local data links can have an external destination as well as an internal one.

C is false because anyone with write permission for a dashboard can create local data links, not just administrators.

QUESTION 17

A customer wants to share a collection of charts with their entire SRE organization. What feature of Splunk Observability Cloud makes this possible?
* Dashboard groups
* Shared charts
* Public dashboards
* Chart exporter

Explanation

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 18

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?
* Adjust the threshold.
* Adjust the Trigger sensitivity. Duration set to 1 minute.
* Adjust the notification sensitivity. Duration set to 1 minute.
* Choose another signal.

Explanation

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 19

Given that the metric demo. trans. count is being sent at a 10 second native resolution, which of the following is an accurate description of the data markers displayed in the chart below?

* Each data marker represents the average hourly rate of API calls.
* Each data marker represents the 10 second delta between counter values.
* Each data marker represents the average of the sum of datapoints over the last minute, averaged over the hour.
* Each data marker represents the sum of API calls in the hour leading up to the data marker.

Explanation

The correct answer is D. Each data marker represents the sum of API calls in the hour leading up to the data marker.

The metric demo.trans.count is a cumulative counter metric, which means that it represents the total number of API calls since the start of the measurement. A cumulative counter metric can be used to measure the rate of change or the sum of events over a time period1 The chart below shows the metric demo.trans.count with a one-hour rollup and a line chart type. A rollup is a way to aggregate data points over a specified time interval, such as one hour, to reduce the number of data points displayed on a chart. A line chart type connects the data points with a line to show the trend of the metric over time2 Each data marker on the chart represents the sum of API calls in the hour leading up to the data marker. This is because the rollup function for cumulative counter metrics is sum by default, which means that it adds up all the data points in each time interval. For example, the data marker at 10:00 AM shows the sum of API calls from 9:00 AM to 10:00 AM3 To learn more about how to use metrics and charts in Splunk Observability Cloud, you can refer to these documentations123.

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

https://docs.splunk.com/Observability/gdi/metrics/charts.html#Data-resolution-and-rollups-in-charts 3:

https://docs.splunk.com/Observability/gdi/metrics/charts.html#Rollup-functions-for-metric-types

QUESTION 20

A customer deals with a holiday rush of traffic during November each year, but does not want to be flooded with alerts when this happens. The increase in traffic is expected and consistent each year. Which detector condition should be used when creating a detector for this data?
* Outlier Detection
* Static Threshold
* Calendar Window
* Historical Anomaly

Explanation

historical anomaly is a detector condition that allows you to trigger an alert when a signal deviates from its historical pattern1. Historical anomaly uses machine learning to learn the normal behavior of a signal based on its past data, and then compares the current value of the signal with the expected value based on the learned pattern1. You can use historical anomaly to detect unusual changes in a signal that are not explained by seasonality, trends, or cycles1.

Historical anomaly is suitable for creating a detector for the customer’s data, because it can account for the expected and consistent increase in traffic during November each year. Historical anomaly can learn that the traffic pattern has a seasonal component that peaks in November, and then adjust the expected value of the traffic accordingly1. This way, historical anomaly can avoid triggering alerts when the traffic increases in November, as this is not an anomaly, but rather a normal variation. However, historical anomaly can still trigger alerts when the traffic deviates from the historical pattern in other ways, such as if it drops significantly or spikes unexpectedly1.

QUESTION 21

A Software Engineer is troubleshooting an issue with memory utilization in their application. They released a new canary version to production and now want to determine if the average memory usage is lower for requests with the ‘canary’ version dimension. They’ve already opened the graph of memory utilization for their service.

How does the engineer see if the new release lowered average memory utilization?

* On the chart for plot A, select Add Analytics, then select MeanrTransformation. In the window that appears, select ‘version’ from the Group By field.
* On the chart for plot A, scroll to the end and click Enter Function, then enter ‘A/B-l’.
* On the chart for plot A, select Add Analytics, then select Mean:Aggregation. In the window that appears, select ‘version’ from the Group By field.
* On the chart for plot A, click the Compare Means button. In the window that appears, type ‘version1.

Explanation

The correct answer is C. On the chart for plot A, select Add Analytics, then select Mean:Aggregation. In the window that appears, select ‘version’ from the Group By field.

This will create a new plot B that shows the average memory utilization for each version of the application.

The engineer can then compare the values of plot B for the ‘canary’ and ‘stable’ versions to see if there is a significant difference.

To learn more about how to use analytics functions in Splunk Observability Cloud, you can refer to this documentation1.

1: https://docs.splunk.com/Observability/gdi/metrics/analytics.html

QUESTION 22

When creating a standalone detector, individual rules in it are labeled according to severity. Which of the choices below represents the possible severity levels that can be selected?
* Info, Warning, Minor, Major, and Emergency.
* Debug, Warning, Minor, Major, and Critical.
* Info, Warning, Minor, Major, and Critical.
* Info, Warning, Minor, Severe, and Critical.

Explanation

The correct answer is C. Info, Warning, Minor, Major, and Critical.

When creating a standalone detector, you can define one or more rules that specify the alert conditions and the severity level for each rule. The severity level indicates how urgent or important the alert is, and it can also affect the notification settings and the escalation policy for the alert1 Splunk Observability Cloud provides five predefined severity levels that you can choose from when creating a rule: Info, Warning, Minor, Major, and Critical. Each severity level has a different color and icon to help you identify the alert status at a glance. You can also customize the severity levels by changing their names, colors, or icons2 To learn more about how to create standalone detectors and use severity levels in Splunk Observability Cloud, you can refer to these documentations12.

1:

https://docs.splunk.com/Observability/alerts-detectors-notifications/detectors.html#Create-a-standalone-detector

2: https://docs.splunk.com/Observability/alerts-detectors-notifications/detector-options.html#Severity-levels

QUESTION 23

When installing OpenTelemetry Collector, which error message is indicative that there is a misconfigured realm or access token?
* 403 (NOT ALLOWED)
* 404 (NOT FOUND)

* 401 (UNAUTHORIZED)
* 503 (SERVICE UNREACHABLE)

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 24

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

* Organization metrics give insights into system usage, system limits, data ingested and token quotas.
* Organization metrics count towards custom MTS limits.
* Organization metrics are included for free.
* A user can plot and alert on them like metrics they send to Splunk Observability Cloud.

Explanation

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 performance1 To learn more about how to use organization metrics in Splunk Observability Cloud, you can refer to this documentation1.

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

QUESTION 25

To refine a search for a metric a customer types host: test-*. What does this filter return?
* Only metrics with a dimension of host and a value beginning with test-.
* Error
* Every metric except those with a dimension of host and a value equal to test.
* Only metrics with a value of test- beginning with host.

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 26

Changes to which type of metadata result in a new metric time series?
* Dimensions
* Properties
* Sources
* Tags

Explanation

The correct answer is A. Dimensions.

Dimensions are metadata in the form of key-value pairs that are sent along with the metrics at the time of ingest. They provide additional information about the metric, such as the name of the host that sent the metric, or the location of the server. Along with the metric name, they uniquely identify a metric time series (MTS)1 Changes to dimensions result in a new MTS, because they create a different combination of metric name and dimensions. For example, if you change the hostname dimension from host1 to host2, you will create a new MTS for the same metric name1 Properties, sources, and tags are other types of metadata that can be applied to existing MTSes after ingest.

They do not contribute to uniquely identify an MTS, and they do not create a new MTS when changed2 To learn more about how to use metadata in Splunk Observability Cloud, you can refer to this documentation2.

1: https://docs.splunk.com/Observability/metrics-and-metadata/metrics.html#Dimensions 2:

https://docs.splunk.com/Observability/metrics-and-metadata/metrics-dimensions-mts.html

QUESTION 27

Which of the following are required in the configuration of a data point? (select all that apply)
* Metric Name
* Metric Type
* Timestamp
* Value
Explanation

The required components in the configuration of a data point are:

Metric Name: A metric name is a string that identifies the type of measurement that the data point represents, such as cpu.utilization, memory.usage, or response.time. A metric name is mandatory for every data point, and it must be unique within a Splunk Observability Cloud organization1 Timestamp: A timestamp is a numerical value that indicates the time at which the data point was collected or generated. A timestamp is mandatory for every data point, and it must be in epoch time format, which is the number of seconds since January 1, 1970 UTC1 Value: A value is a numerical value that indicates the magnitude or quantity of the measurement that the data point represents. A value is mandatory for every data point, and it must be compatible with the metric type of the data point1 Therefore, the correct answer is A, C, and D.

To learn more about how to configure data points in Splunk Observability Cloud, you can refer to this documentation1.

1: https://docs.splunk.com/Observability/gdi/metrics/metrics.html#Data-points

QUESTION 28

What is the limit on the number of properties that an MTS can have?
* 64
* 36
* No limit
* 50
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

QUESTION 29

One server in a customer’s data center is regularly restarting due to power supply issues. What type of dashboard could be

used to view charts and create detectors for this server?
* Single-instance dashboard
* Machine dashboard
* Multiple-service dashboard
* Server dashboard
Explanation

According to the Splunk O11y Cloud Certified Metrics User Track document1, a single-instance dashboard is a type of dashboard that displays charts and information for a single instance of a service or host. You can use a single-instance dashboard to monitor the performance and health of a specific server, such as the one that is restarting due to power supply issues. You can also create detectors for the metrics that are relevant to the server, such as CPU usage, memory usage, disk usage, and uptime. Therefore, option A is correct.

QUESTION 30

Which component of the OpenTelemetry Collector allows for the modification of metadata?
* Processors
* Pipelines
* Exporters
* Receivers
Explanation

The component of the OpenTelemetry Collector that allows for the modification of metadata is A. Processors.

Processors are components that can modify the telemetry data before sending it to exporters or other components. Processors can perform various transformations on metrics, traces, and logs, such as filtering, adding, deleting, or updating attributes, labels, or resources. Processors can also enrich the telemetry data with additional metadata from various sources, such as Kubernetes, environment variables, or system information1 For example, one of the processors that can modify metadata is the attributes processor. This processor can update, insert, delete, or replace existing attributes on metrics or traces. Attributes are key-value pairs that provide additional information about the telemetry data, such as the service name, the host name, or the span kind2 Another example is the resource processor. This processor can modify resource attributes on metrics or traces.

Resource attributes are key-value pairs that describe the entity that produced the telemetry data, such as the cloud provider, the region, or the instance type3 To learn more about how to use processors in the OpenTelemetry Collector, you can refer to this documentation1.

1: https://opentelemetry.io/docs/collector/configuration/#processors 2:

https://github.com/open-telemetry/opentelemetry-collector-contrib/tree/main/processor/attributesprocessor 3:

https://github.com/open-telemetry/opentelemetry-collector-contrib/tree/main/processor/resourceprocessor

QUESTION 31

For which types of charts can individual plot visualization be set?
* Line, Bar, Column
* Bar, Area, Column
* Line, Area, Column
* Histogram, Line, Column
Explanation

The correct answer is C. Line, Area, Column.

For line, area, and column charts, you can set the individual plot visualization to change the appearance of each plot in the chart. For example, you can change the color, shape, size, or style of the lines, areas, or columns. You can also change the rollup function, data resolution, or y-axis scale for each plot1 To set the individual plot visualization for line, area, and column charts, you need to select the chart from the Metric Finder, then click on Plot Chart Options and choose Individual Plot Visualization from the list of options. You can then customize each plot according to your preferences2 To learn more about how to use individual plot visualization in Splunk Observability Cloud, you can refer to this documentation2.

1: https://docs.splunk.com/Observability/gdi/metrics/charts.html#Individual-plot-visualization 2:

https://docs.splunk.com/Observability/gdi/metrics/charts.html#Set-individual-plot-visualization

QUESTION 32

Which of the following can be configured when subscribing to a built-in detector?
* Alerts on team landing page.
* Alerts on a dashboard.
* Outbound notifications.
* Links to a chart.

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 33

What are the best practices for creating detectors? (select all that apply)
* View data at highest resolution.

* Have a consistent value.
* View detector in a chart.
* Have a consistent type of measurement.

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 34

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?

* Create a temporary plot by dragging items A and B into the Analytics Explorer window.
* Create a plot C using the formula (A-B) and add a scale:percent function to express the rate of change as a percentage.
* 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.
* Create a temporary plot by clicking the Change% button in the upper-right corner of the plot showing lines A and B.

Explanation

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 latency1 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 documentations34.

1: https://www.mathsisfun.com/numbers/percentage-change.html 2:

https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Scale 3:

https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Formula 4:

https://docs.splunk.com/Observability/gdi/metrics/analytics.html#Scale

QUESTION 35

Which of the following are ways to reduce flapping of a detector? (select all that apply)
* Configure a duration or percent of duration for the alert.
* Establish a reset threshold for the detector.
* Enable the anti-flap setting in the detector options menu.
* Apply a smoothing transformation (like a rolling mean) to the input data for the detector.

Explanation

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.

Splunk SPLK-4001 Pre-Exam Practice Tests | Test4Engine:

https://www.test4engine.com/SPLK-4001_exam-latest-braindumps.html]