Exam Questions SPLK-4001

Splunk O11y Cloud Certified Metrics User

https://www.2passeasy.com/dumps/SPLK-4001/

NEW QUESTION 1
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)

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

NEW QUESTION 2
A user wants to add a link to an existing dashboard from an alert. When they click the dimension value in the alert message, they are taken to the dashboard keeping the context. How can this be accomplished? (select all that apply)

A. Build a global data link.
B. Add a link to the Runbook URL.
C. Add a link to the field.
D. Add the link to the alert message body.

Answer: AC

Explanation:
The possible ways to add a link to an existing dashboard from an alert are:
? Build a global data link. A global data link is a feature that allows you to create a link from any dimension value in any chart or table to a dashboard of your choice. You can specify the source and target dashboards, the dimension name and value, and the query parameters to pass along. When you click on the dimension value in the alert message, you will be taken to the dashboard with the context preserved1
? Add a link to the field. A field link is a feature that allows you to create a link from any field value in any search result or alert message to a dashboard of your choice. You can specify the field name and value, the dashboard name and ID, and the query parameters to pass along. When you click on the field value in the alert message, you will be taken to the dashboard with the context preserved2
Therefore, the correct answer is A and C.
To learn more about how to use global data links and field links in Splunk Observability Cloud, you can refer to these documentations12.
1: https://docs.splunk.com/Observability/gdi/metrics/charts.html#Global-data-links 2: https://docs.splunk.com/Observability/gdi/metrics/search.html#Field-links

NEW QUESTION 3
What constitutes a single metrics time series (MTS)?

A. A series of timestamps that all reflect the same metric.
B. A set of data points that all have the same metric name and list of dimensions.
C. A set of data points that use different dimensions but the same metric name.
D. A set of metrics that are ordered in series based on timestamp.

Answer: B

Explanation:
The correct answer is B. A set of data points that all have the same metric name and list of dimensions.
A metric time series (MTS) is a collection of data points that have the same metric and the same set of dimensions. For example, the following sets of data points are in three separate MTS:
MTS1: Gauge metric cpu.utilization, dimension “hostname”: “host1” MTS2: Gauge metric cpu.utilization, dimension “hostname”: “host2” MTS3: Gauge metric memory.usage, dimension “hostname”: “host1”
A metric is a numerical measurement that varies over time, such as CPU utilization or memory usage. A dimension is a key-value pair that provides additional information about the metric, such as the hostname or the location. A data point is a combination of a metric, a dimension, a value, and a timestamp1

NEW QUESTION 4
What happens when the limit of allowed dimensions is exceeded for an MTS?

A. The additional dimensions are dropped.
B. The datapoint is averaged.
C. The datapoint is updated.
D. The datapoint is dropped.

Answer: A

Explanation:
According to the web search results, dimensions are metadata in the form of key-value pairs that monitoring software sends in along with the metrics. The set of metric time series (MTS) dimensions sent during ingest is used, along with the metric name, to uniquely identify an MTS1. Splunk Observability Cloud has a limit of 36 unique dimensions per MTS2. If the limit of allowed dimensions is exceeded for an MTS, the additional dimensions are dropped and not stored or indexed by Observability Cloud2. This means that the data point is still ingested, but without the extra dimensions. Therefore, option A is correct.

NEW QUESTION 5
Which of the following chart visualization types are unaffected by changing the time picker on a dashboard? (select all that apply)

A. Single Value
B. Heatmap
C. Line
D. List

Answer: AD

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

NEW QUESTION 6
Which of the following is optional, but highly recommended to include in a datapoint?

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

NEW QUESTION 7
What Pod conditions does the Analyzer panel in Kubernetes Navigator monitor? (select all that apply)

A. Not Scheduled
B. Unknown
C. Failed
D. Pending

Answer: ABCD

Explanation:
The Pod conditions that the Analyzer panel in Kubernetes Navigator monitors are:
? Not Scheduled: This condition indicates that the Pod has not been assigned to a Node yet. This could be due to insufficient resources, node affinity, or other scheduling constraints1
? Unknown: This condition indicates that the Pod status could not be obtained or is not known by the system. This could be due to communication errors, node failures, or other unexpected situations1
? Failed: This condition indicates that the Pod has terminated in a failure state. This could be due to errors in the application code, container configuration, or external factors1
? Pending: This condition indicates that the Pod has been accepted by the system, but one or more of its containers has not been created or started yet. This could be due to image pulling, volume mounting, or network issues1
Therefore, the correct answer is A, B, C, and D.
To learn more about how to use the Analyzer panel in Kubernetes Navigator, you can refer to this documentation2.
1: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#pod-phase 2: https://docs.splunk.com/observability/infrastructure/monitor/k8s-nav.html#Analyzer-panel

NEW QUESTION 8
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?

A. Adjust the threshold.
B. Adjust the Trigger sensitivit
C. Duration set to 1 minute.
D. Adjust the notification sensitivit
E. Duration set to 1 minute.
F. Choose another signal.

Answer: B

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.

NEW QUESTION 9
Which of the following can be configured when subscribing to a built-in detector?

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.

NEW QUESTION 10
With exceptions for transformations or timeshifts, at what resolution do detectors operate?

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.

NEW QUESTION 10
What is the limit on the number of properties that an MTS can have?

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

NEW QUESTION 13
When writing a detector with a large number of MTS, such as memory. free in a deployment with 30,000 hosts, it is possible to exceed the cap of MTS that can be contained in a single plot. Which of the choices below would most likely reduce the number of MTS below the plot cap?

A. Select the Sharded option when creating the plot.
B. Add a filter to narrow the scope of the measurement.
C. Add a restricted scope adjustment to the plot.
D. When creating the plot, add a discriminator.

Answer: B

Explanation:
The correct answer is B. Add a filter to narrow the scope of the measurement.
A filter is a way to reduce the number of metric time series (MTS) that are displayed on a chart or used in a detector. A filter specifies one or more dimensions and

values that the MTS must have in order to be included. For example, if you want to monitor the memory.free metric only for hosts that belong to a certain cluster, you can add a filter like cluster:my-cluster to the plot or detector. This will exclude any MTS that do not have the cluster dimension or have a different value for it1 Adding a filter can help you avoid exceeding the plot cap, which is the maximum number of MTS that can be contained in a single plot. The plot cap is 100,000 by default, but it can be changed by contacting Splunk Support2
To learn more about how to use filters in Splunk Observability Cloud, you can refer to this documentation3.
1: https://docs.splunk.com/Observability/gdi/metrics/search.html#Filter-metrics 2: https://docs.splunk.com/Observability/gdi/metrics/detectors.html#Plot-cap 3: https://docs.splunk.com/Observability/gdi/metrics/search.html

NEW QUESTION 16
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.

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

NEW QUESTION 17
A customer is sending data from a machine that is over-utilized. Because of a lack of system resources, datapoints from this machine are often delayed by up to 10 minutes. Which setting can be modified in a detector to prevent alerts from firing before the datapoints arrive?

A. Max Delay
B. Duration
C. Latency
D. Extrapolation Policy

Answer: A

Explanation:
The correct answer is A. Max Delay.
Max Delay is a parameter that specifies the maximum amount of time that the analytics engine can wait for data to arrive for a specific detector. For example, if Max Delay is set to 10 minutes, the detector will wait for only a maximum of 10 minutes even if some data points have not arrived. By default, Max Delay is set to Auto, allowing the analytics engine to determine the appropriate amount of time to wait for data points1
In this case, since the customer knows that the data from the over-utilized machine can be delayed by up to 10 minutes, they can modify the Max Delay setting for the detector to 10 minutes. This will prevent the detector from firing alerts before the data points arrive, and avoid false positives or missing data1
To learn more about how to use Max Delay in Splunk Observability Cloud, you can refer to this documentation1.
1: https://docs.splunk.com/observability/alerts-detectors-notifications/detector- options.html#Max-Delay

NEW QUESTION 19
The built-in Kubernetes Navigator includes which of the following?

A. Map, Nodes, Workloads, Node Detail, Workload Detail, Group Detail, Container Detail
B. Map, Nodes, Processors, Node Detail, Workload Detail, Pod Detail, Container Detail
C. Map, Clusters, Workloads, Node Detail, Workload Detail, Pod Detail, Container Detail
D. Map, Nodes, Workloads, Node Detail, Workload Detail, Pod Detail, Container Detail

Answer: D

Explanation:
The correct answer is D. Map, Nodes, Workloads, Node Detail, Workload Detail, Pod Detail, Container Detail.
The built-in Kubernetes Navigator is a feature of Splunk Observability Cloud that provides a
comprehensive and intuitive way to monitor the performance and health of Kubernetes environments. It includes the following views:
? Map: A graphical representation of the Kubernetes cluster topology, showing the
relationships and dependencies among nodes, pods, containers, and services. You can use the map to quickly identify and troubleshoot issues in your cluster1
? Nodes: A tabular view of all the nodes in your cluster, showing key metrics such as
CPU utilization, memory usage, disk usage, and network traffic. You can use the nodes view to compare and analyze the performance of different nodes1
? Workloads: A tabular view of all the workloads in your cluster, showing key metrics
such as CPU utilization, memory usage, network traffic, and error rate. You can use the workloads view to compare and analyze the performance of different workloads, such as deployments, stateful sets, daemon sets, or jobs1
? Node Detail: A detailed view of a specific node in your cluster, showing key metrics
and charts for CPU utilization, memory usage, disk usage, network traffic, and pod count. You can also see the list of pods running on the node and their status. You can use the node detail view to drill down into the performance of a single node2
? Workload Detail: A detailed view of a specific workload in your cluster, showing
key metrics and charts for CPU utilization, memory usage, network traffic, error rate, and pod count. You can also see the list of pods belonging to the workload and their status. You can use the workload detail view to drill down into the performance of a single workload2
? Pod Detail: A detailed view of a specific pod in your cluster, showing key metrics
and charts for CPU utilization, memory usage, network traffic, error rate, and container count. You can also see the list of containers within the pod and their status. You can use the pod detail view to drill down into the performance of a single pod2
? Container Detail: A detailed view of a specific container in your cluster, showing
key metrics and charts for CPU utilization, memory usage, network traffic, error rate, and log events. You can use the container detail view to drill down into the performance of a single container2
To learn more about how to use Kubernetes Navigator in Splunk Observability Cloud, you can refer to this documentation3.

1: https://docs.splunk.com/observability/infrastructure/monitor/k8s-nav.html#Kubernetes-Navigator 2: https://docs.splunk.com/observability/infrastructure/monitor/k8s-nav.html#Detail-pages 3: https://docs.splunk.com/observability/infrastructure/monitor/k8s- nav.html

NEW QUESTION 21
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?

A. Single-instance dashboard
B. Machine dashboard
C. Multiple-service dashboard
D. Server dashboard

Answer: A

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.

NEW QUESTION 24
The Sum Aggregation option for analytic functions does which of the following?

A. Calculates the number of MTS present in the plot.
B. Calculates 1/2 of the values present in the input time series.
C. Calculates the sum of values present in the input time series across the entire environment or per group.
D. Calculates the sum of values per time series across a period of time.

Answer: C

Explanation:
According to the Splunk Test Blueprint - O11y Cloud Metrics User document1, one of the metrics concepts that is covered in the exam is analytic functions. Analytic functions are mathematical operations that can be applied to metrics to transform, aggregate, or analyze them.
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 Analytic Functions, which explains that analytic functions can be used to perform calculations on metrics, such as sum, average, min, max, count, etc. The document also provides examples of how to use analytic functions in charts and dashboards.
One of the analytic functions that can be used is Sum Aggregation, which calculates the
sum of values present in the input time series across the entire environment or per group. The document gives an example of how to use Sum Aggregation to calculate the total CPU usage across all hosts in a group by using the following syntax:
sum(cpu.utilization) by hostgroup

NEW QUESTION 28
Which of the following statements are true about local data links? (select all that apply)

A. Anyone with write permission for a dashboard can add local data links that appear on that dashboard.
B. Local data links can only have a Splunk Observability Cloud internal destination.
C. Only Splunk Observability Cloud administrators can create local links.
D. Local data links are available on only one dashboard.

Answer: AD

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.

NEW QUESTION 30
Changes to which type of metadata result in a new metric time series?

A. Dimensions
B. Properties
C. Sources
D. Tags

Answer: A

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

NEW QUESTION 31
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.

Answer: ABCD

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

NEW QUESTION 36
Which of the following are supported rollup functions in Splunk Observability Cloud?

A. average, latest, lag, min, max, sum, rate
B. std_dev, mean, median, mode, min, max
C. sigma, epsilon, pi, omega, beta, tau
D. 1min, 5min, 10min, 15min, 30min

Answer: A

Explanation:
According to the Splunk O11y Cloud Certified Metrics User Track document1, Observability Cloud has the following rollup functions: Sum: (default for counter metrics): Returns the sum of all data points in the MTS reporting interval. Average (default for gauge metrics): Returns the average value of all data points in the MTS reporting interval. Min: Returns the minimum data point value seen in the MTS reporting interval. Max: Returns the maximum data point value seen in the MTS reporting interval. Latest: Returns the most recent data point value seen in the MTS reporting interval. Lag: Returns the difference between the most recent and the previous data point values seen in the MTS reporting interval. Rate: Returns the rate of change of data points in the MTS reporting interval. Therefore, option A is correct.

NEW QUESTION 38
Which of the following are required in the configuration of a data point? (select all that apply)

A. Metric Name
B. Metric Type
C. Timestamp
D. Value

Answer: ACD

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

NEW QUESTION 40
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

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.

NEW QUESTION 45
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?

A. Info, Warning, Minor, Major, and Emergency.
B. Debug, Warning, Minor, Major, and Critical.
C. Info, Warning, Minor, Major, and Critical.
D. Info, Warning, Minor, Severe, and Critical.

Answer: C

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

NEW QUESTION 46
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-4001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-4001 Product From:

https://www.2passeasy.com/dumps/SPLK-4001/

Money Back Guarantee

SPLK-4001 Practice Exam Features:

* SPLK-4001 Questions and Answers Updated Frequently

* SPLK-4001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-4001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-4001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year