Splunk

Exam Questions SPLK-4001

Splunk O11y Cloud Certified Metrics User

NEW QUESTION 1

A customer has a very dynamic infrastructure. During every deployment, all existing instances are destroyed, and new ones are created Given this deployment model, how should a detector be created that will not send false notifications of instances being down?

A. Create the detecto
B. Select Alert settings, then select Auto-Clear Alerts and enter an appropriate time period.
C. Create the detecto
D. Select Alert settings, then select Ephemeral Infrastructure and enter the expected lifetime of an instance.
E. Check the Dynamic checkbox when creating the detector.
F. Check the Ephemeral checkbox when creating the detector.

Answer: B

Explanation:

According to the web search results, ephemeral infrastructure is a term that describes instances that are auto-scaled up or down, or are brought up with new code versions and discarded or recycled when the next code version is deployed1. Splunk Observability Cloud has a feature that allows you to create detectors for ephemeral infrastructure without sending false notifications of instances being down2. To use this feature, you need to do the following steps:

? Create the detector as usual, by selecting the metric or dimension that you want to monitor and alert on, and choosing the alert condition and severity level.

? Select Alert settings, then select Ephemeral Infrastructure. This will enable a special mode for the detector that will automatically clear alerts for instances that are expected to be terminated.

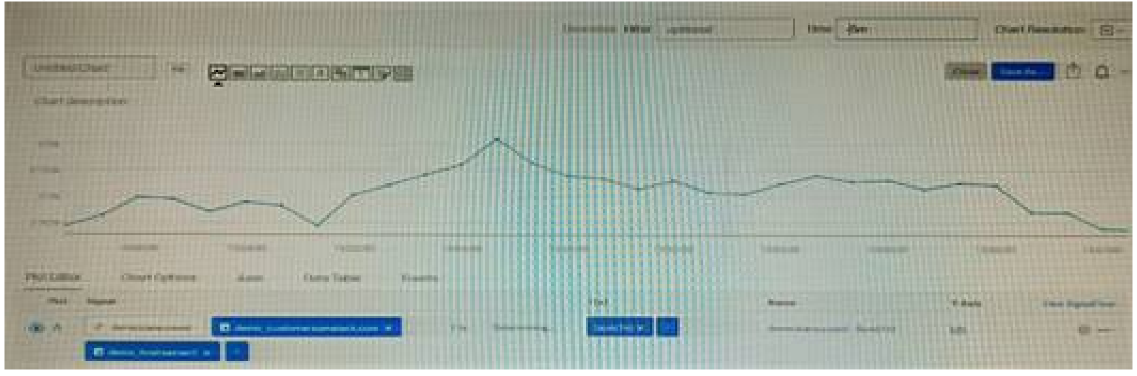
? Enter the expected lifetime of an instance in minutes. This is the maximum amount of time that an instance is expected to live before being replaced by a new one. For example, if your instances are replaced every hour, you can enter 60 minutes as the expected lifetime.

? Save the detector and activate it.

With this feature, the detector will only trigger alerts when an instance stops reporting a metric unexpectedly, based on its expected lifetime. If an instance stops reporting a metric within its expected lifetime, the detector will assume that it was terminated on purpose and will not trigger an alert. Therefore, option B is correct.

NEW QUESTION 2

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?



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

Answer: D

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

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
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 5
A customer is experiencing an issue where their detector is not sending email notifications but is generating alerts within the Splunk Observability UI. Which of the below is the root cause?

A. The detector has an incorrect alert rule.
B. The detector has an incorrect signal,
C. The detector is disabled.
D. The detector has a muting rule.

Answer: D

Explanation:
The most likely root cause of the issue is D. The detector has a muting rule. A muting rule is a way to temporarily stop a detector from sending notifications for certain alerts, without disabling the detector or changing its alert conditions. A muting rule can be useful when you want to avoid alert noise during planned maintenance, testing, or other situations where you expect the metrics to deviate from normal1
When a detector has a muting rule, it will still generate alerts within the Splunk Observability UI, but it will not send email notifications or any other types of notifications that you have configured for the detector. You can see if a detector has a muting rule by looking at the Muting Rules tab on the detector page. You can also create, edit, or delete muting rules from there1
To learn more about how to use muting rules in Splunk Observability Cloud, you can refer to this documentation1.

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
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 8
How is it possible to create a dashboard group that no one else can edit?

A. Ask the admin to lock the dashboard group.
B. Restrict the write access on the dashboard group.
C. Link the dashboard group to the team.
D. Hide the edit menu on the dashboard group.

Answer: B

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 set permissions for each dashboard group, such as who can view, edit, or manage the dashboards in the group1. To create a dashboard group that no one else can edit, you need to do the following steps:
? Create a dashboard group as usual, by selecting Dashboard Group from the
Create menu on the navigation bar, entering a name and description, and adding dashboards to the group1.
? Select Alert settings from the Dashboard actions menu () on the top right corner of the dashboard group. This will open a dialog box where you can configure the permissions for the dashboard group1.
? Under Write access, select Only me. This will restrict the write access to the
dashboard group to yourself only. No one else will be able to edit or delete the dashboards in the group1.
? Click Save. This will create a dashboard group that no one else can edit.

NEW QUESTION 9
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)

A. Invoke a webhook URL.
B. Export to CSV.
C. Send an SMS message.
D. Send to email addresses.

Answer: ACD

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

NEW QUESTION 10
What is one reason a user of Splunk Observability Cloud would want to subscribe to an alert?

A. To determine the root cause of the Issue triggering the detector.
B. To perform transformations on the data used by the detector.
C. To receive an email notification when a detector is triggered.
D. To be able to modify the alert parameters.

Answer: C

Explanation:
One reason a user of Splunk Observability Cloud would want to subscribe to an alert is C. To receive an email notification when a detector is triggered.
A detector is a component of Splunk Observability Cloud that monitors metrics or events and triggers alerts when certain conditions are met. A user can create and configure detectors to suit their monitoring needs and goals1
A subscription is a way for a user to receive notifications when a detector triggers an alert. A user can subscribe to a detector by entering their email address in the Subscription tab of
the detector page. A user can also unsubscribe from a detector at any time2
When a user subscribes to an alert, they will receive an email notification that contains information about the alert, such as the detector name, the alert status, the alert severity, the alert time, and the alert message. The email notification also includes links to view the detector, acknowledge the alert, or unsubscribe from the detector2
To learn more about how to use detectors and subscriptions in Splunk Observability Cloud, you can refer to these documentations12.
1: https://docs.splunk.com/Observability/alerts-detectors-notifications/detectors.html 2: https://docs.splunk.com/Observability/alerts-detectors-notifications/subscribe-to- detectors.html

NEW QUESTION 10

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 13
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 16
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 20

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 22

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.

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.

NEW QUESTION 24

......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-4001 Practice Test Here