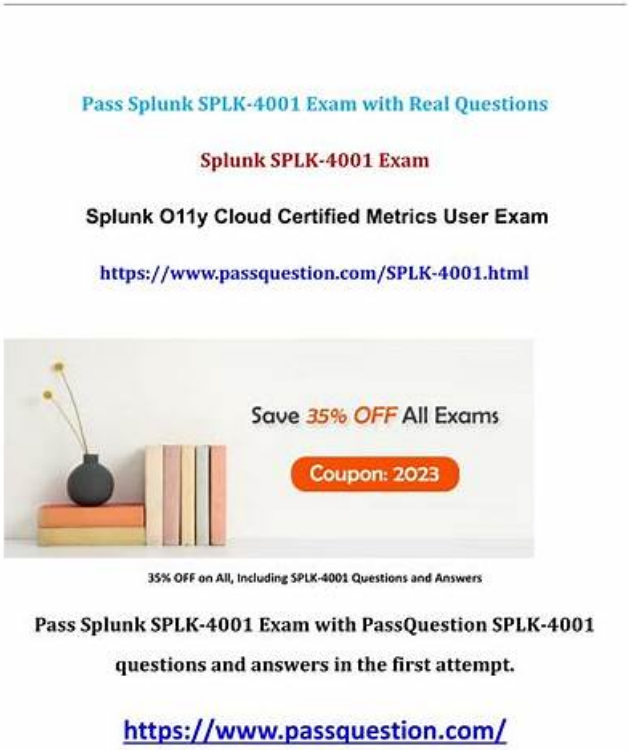
SPLK-4001 Lead2pass - New SPLK-4001 Test Questions



DOWNLOAD the newest TestsDumps SPLK-4001 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1A5ikPqGpIV1HxnDbSozX7I_AaKAw4Nzt

In order to save a lot of unnecessary trouble to users, we have completed our SPLK-4001 Learning Materials research and development of online learning platform, users do not need to download and install, only need your digital devices have a browser, can be done online operation of the SPLK-4001 study materials. This kind of learning method is very convenient for the user, especially in the time of our fast pace to get Splunk certification. In addition, our test data is completely free of user's computer memory, will only consume a small amount of running memory when the user is using our product.

Splunk SPLK-4001 certification exam is an online exam that can be taken from anywhere in the world. SPLK-4001 exam is designed to be completed in two hours and consists of 60 multiple-choice questions. SPLK-4001 exam is designed to test the candidate's knowledge and skills in using Splunk to monitor and measure the performance of cloud-based applications. SPLK-4001 Exam is proctored, which means that the candidate will be monitored throughout the exam to ensure that they are not cheating.

>> SPLK-4001 Lead2pass <<

Don't Miss Up to 365 Days of Free Updates - Buy Splunk SPLK-4001 Questions Now

While buying SPLK-4001 training materials online, you may pay more attention to money safety. If you choose SPLK-4001

learning materials of us, we can ensure you that your money and account safety can be guaranteed. Since we have professional technicians check the website every day, therefore the safety can be guaranteed. In addition, SPLK-4001 Training Materials of us are high quality, they contain both questions and answers, and it's convenient for you to check answers after practicing. We have online chat service stuff, if you have any questions about SPLK-4001 learning materials, you can have a conversion with us.

Splunk SPLK-4001 Certification Exam is a vendor-neutral certification that is recognized across the industry. It is an excellent way for individuals to demonstrate their skills and knowledge in using Splunk Cloud to monitor and analyze metrics data, which is becoming increasingly important as organizations move to the cloud. Splunk O11y Cloud Certified Metrics User certification exam is designed to be challenging, but with the right preparation, candidates can pass the exam and demonstrate their expertise in using Splunk Cloud to monitor and optimize system performance.

Splunk O11y Cloud Certified Metrics User Sample Questions (Q13-Q18):

NEW QUESTION # 13
A customer operates a caching web proxy. They want to calculate the cache hit rate for their service. What is the best way to achieve this?

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

Answer: D

Explanation:
According to the Splunk O11y Cloud Certified Metrics User Track document1, percentages and ratios are useful for calculating the proportion of one metric to another, such as cache hits to cache misses, or successful requests to failed requests. You can use the percentage() or ratio() functions in SignalFlow to compute these values and display them in charts. For example, to calculate the cache hit rate for a service, you can use the following SignalFlow code:
percentage(counters("cache.hits"), counters("cache.misses"))
This will return the percentage of cache hits out of the total number of cache attempts. You can also use the ratio() function to get the same result, but as a decimal value instead of a percentage.
ratio(counters("cache.hits"), counters("cache.misses"))

NEW QUESTION # 14
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. Add the link to the alert message body.
- B. Add a link to the Runbook URL.
- C. Add a link to the field.
- D. Build a global data link.

Answer: C,D

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 # 15
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. Duration
- B. Latency
- C. Max Delay
- D. Extrapolation Policy

Answer: C

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 # 16
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 be able to modify the alert parameters.
- D. To receive an email notification when a detector is triggered.

Answer: D

Explanation:
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 # 17
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. When creating the plot, add a discriminator.
- B. Add a filter to narrow the scope of the measurement.
- C. Add a restricted scope adjustment to the plot.
- D. Select the Sharded option when creating the plot.

Answer: B

Explanation:
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 # 18
.....