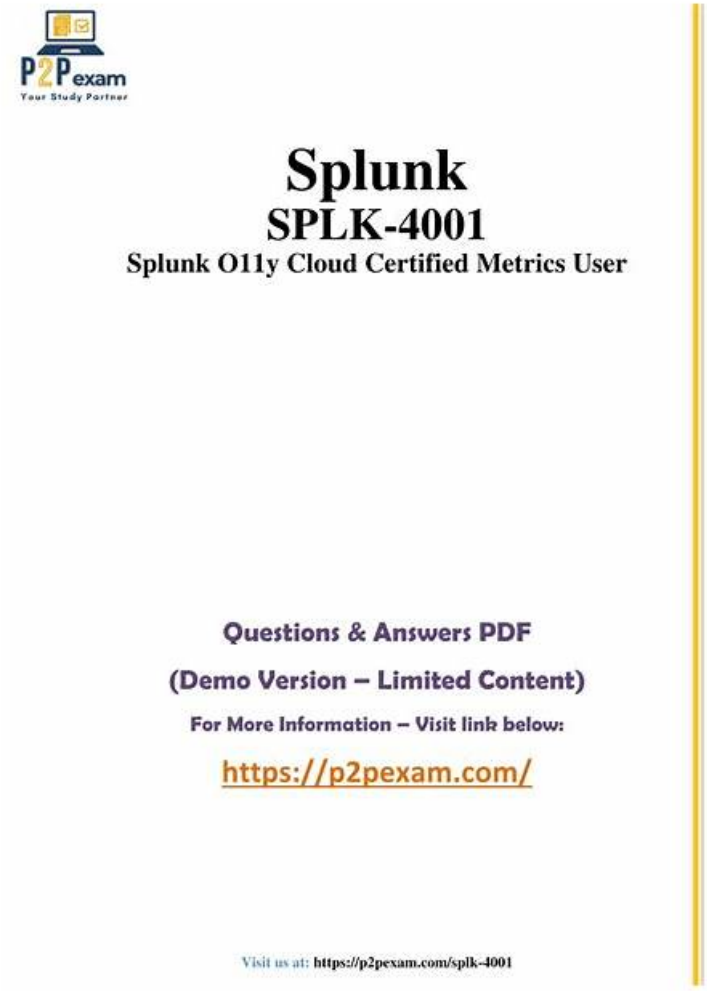
Reliable Splunk SPLK-4001 Exam Answers - SPLK-4001 Latest Exam



P.S. Free & New SPLK-4001 dumps are available on Google Drive shared by VCETorrent: https://drive.google.com/open?id=18iIzEkme7k7zAcuhF9R_gUxDR8Fd-WOe

The 24/7 support team is just an e-mail away for our customers so that they can contact us anytime. Our team will solve all of their issues as quickly as possible. Free demos and up to 1 year of free updates of our Sitecore Exams are also available at VCETorrent. Buy updated and Real SPLK-4001 Exam Questions now and earn your dream SPLK-4001 certification with VCETorrent!

Splunk SPLK-4001 Exam is an essential credential for professionals who want to demonstrate their expertise in cloud-based metrics monitoring and observability. It is a valuable certification that can help individuals advance their careers and increase their earning potential, as well as provide organizations with the assurance that their IT infrastructure is being monitored and optimized by certified experts.

>> Reliable Splunk SPLK-4001 Exam Answers <<

SPLK-4001 Latest Exam | Answers SPLK-4001 Real Questions

Get the latest SPLK-4001 actual exam questions for SPLK-4001 Exam. You can practice the questions on practice software in simulated real SPLK-4001 exam scenario or you can use simple PDF format to go through all the real SPLK-4001 exam questions. Our products are better than all the cheap SPLK-4001 Exam braindumps you can find elsewhere, try free demo. You can pass your actual SPLK-4001 Exam in first attempt. Our SPLK-4001 exam material is good to pass the exam within a week. VCETorrent is considered as the top preparation material seller for SPLK-4001 exam dumps, and inevitable to carry you the finest knowledge on SPLK-4001 exam certification syllabus contents.

The Splunk SPLK-4001 Exam covers a wide range of topics including the use of Splunk metrics, the configuration of metrics, the use of dashboards, and the creation of alerts. It also covers the use of the Splunk Cloud platform and the integration of metrics with other cloud-based platforms.

The Splunk O11y Cloud Certified Metrics User certification exam will test the candidate's knowledge and skills in various aspects of the Splunk Metrics platform, including data ingestion, troubleshooting, and analysis. Through this certification program, candidates will also learn about the various tools and technologies used to collect and analyze metrics, such as dashboards, reports, and alerts. In addition, the exam will cover various topics related to cloud monitoring and analytics, such as monitoring cloud-based applications and infrastructure, detecting and troubleshooting issues, and optimizing performance.

Splunk O11y Cloud Certified Metrics User Sample Questions (Q37-Q42):

NEW QUESTION # 37
Clicking a metric name from the results in metric finder displays the metric in Chart Builder. What action needs to be taken in order to save the chart created in the UI?

- A. Create a new dashboard and save the chart.
- B. Save the chart to a dashboard.
- C. Save the chart to multiple dashboards.
- D. Make sure that data is coming in for the metric then save the chart.

Answer: B

Explanation:
Explanation
According to the web search results, clicking a metric name from the results in metric finder displays the metric in Chart Builder1. Chart Builder is a tool that allows you to create and customize charts using metrics, dimensions, and analytics functions2. To save the chart created in the UI, you need to do the following steps:
Click the Save button on the top right corner of the Chart Builder. This will open a dialog box where you can enter the chart name and description, and choose the dashboard where you want to save the chart.
Enter a name and a description for your chart. The name should be descriptive and unique, and the description should explain the purpose and meaning of the chart.
Choose an existing dashboard from the drop-down menu, or create a new dashboard by clicking the + icon. A dashboard is a collection of charts that display metrics and events for your services or hosts3. You can organize and share dashboards with other users in your organization using dashboard groups3.
Click Save. This will save your chart to the selected dashboard and redirect you to the dashboard view.
You can also access your saved chart from the Dashboards menu on the left navigation bar.

NEW QUESTION # 38
Which of the following aggregate analytic functions will allow a user to see the highest or lowest n values of a metric?

- A. Exclude / Include
- B. Best/Worst
- C. Top / Bottom
- D. Maximum / Minimum

Answer: C

Explanation:
Explanation
The correct answer is D. Top / Bottom.
Top and bottom are aggregate analytic functions that allow a user to see the highest or lowest n values of a metric. They can be used to select a subset of the time series in the plot by count or by percent. For example, top (5) will show the five time series with the highest values in each time period, while bottom (10%) will show the 10% of time series with the lowest values in each time period1
To learn more about how to use top and bottom functions in Splunk Observability Cloud, you can refer to this documentation1.

NEW QUESTION # 39
Which of the following can be configured when subscribing to a built-in detector?

- A. Alerts on a dashboard.
- B. Outbound notifications.
- C. Alerts on team landing page.
- D. Links to a chart.

Answer: B

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 # 40
An SRE creates an event feed chart in a dashboard that shows a list of events that meet criteria they specify. Which of the following should they include? (select all that apply)

- A. Events created when a detector clears an alert.
- B. Random alerts from active detectors.
- C. Custom events that have been sent in from an external source.
- D. Events created when a detector triggers an alert.

Answer: A,C,D

Explanation:
According to the web search results1, an event feed chart is a type of chart that shows a list of events that meet criteria you specify. An event feed chart can display one or more event types depending on how you specify the criteria. The event types that you can include in an event feed chart are:
Custom events that have been sent in from an external source: These are events that you have created or received from a third-party service or tool, such as AWS CloudWatch, GitHub, Jenkins, or PagerDuty. You can send custom events to Splunk Observability Cloud using the API or the Event Ingest Service.
Events created when a detector triggers or clears an alert: These are events that are automatically generated by Splunk Observability Cloud when a detector evaluates a metric or dimension and finds that it meets the alert condition or returns to normal. You can create detectors to monitor and alert on various metrics and dimensions using the UI or the API.
Therefore, option A, B, and D are correct.

NEW QUESTION # 41
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. When creating the plot, add a discriminator.
- C. Add a restricted scope adjustment to the plot.
- D. Add a filter to narrow the scope of the measurement.

Answer: D

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 # 42
.....