SPLK-1001 Q&As

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

A field exists in search results, but isn\\'t being displayed in the fields sidebar. How can it be added to the fields sidebar?

A. Click All Fields and select the field to add it to Selected Fields.

B. Click Interesting Fields and select the field to add it to Selected Fields.

C. Click Selected Fields and select the field to add it to Interesting Fields.

D. This scenario isn\\'t possible because all fields returned from a search always appear in the fields sidebar.

Correct Answer: A

QUESTION 2

Which of the following searches would return only events that match the following criteria?

1.

Events are inside the main index

2.

The field status exists in the event

3.

The value in the status field does not equal 200

A. index==main status!==200

B. index=main NOT status=200

C. index==main NOT status==200

D. index-main status!=200

Correct Answer: C

The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. It\\'s a powerful language that allows you to perform advanced queries and extract meaningful insights from your data. To query for events that match the criteria you specified, you would use the following KQL query:

index==main NOT status==200 This query will return all events that are inside the main index and have a status field, but the value of the status field does not equal 200. It is important to note that the "NOT" operator must be used in order to exclude events with a status value of 200. By using the "NOT" operator, the query will return only events that do not match the specified criteria. This is useful for narrowing down search results to only those events that are relevant to the query.

QUESTION 3

What is the default lifetime of every Splunk search job?

A. All search jobs are saved for 10 days

B. All search jobs are saved for 10 hours

C. All search jobs are saved for 10 weeks

D. All search jobs are saved for 10 minutes

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Extendjoblifetimes

QUESTION 4

Which statement is true about the top command?

A. It returns the top 10 results

B. It displays the output in table format

C. It returns the count and percent columns per row

D. All of the above

Correct Answer: D

QUESTION 5

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True

B. False

Correct Answer: A