SPLK-1001$^{\text{Q\&As}}$

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

What is the proper SPL terminology for specifying a particular index in a search?

A. indexer--index_name

B. indexer name--index_name

C. index=index_name

D. index name=index_name

Correct Answer: C

This means that you can use the index field to filter your search results by the name of the index that contains the events you want to see. For example, if you want to search for events in the index named "gcp_logs", you can use the following SPL: index=gcp_logs You can also specify multiple indexes by using the OR operator, such as: index=gcp_logs OR index=oswin

QUESTION 2

Zoom Out and Zoom to Selection re-executes the search.

A. No

B. Yes

Correct Answer: B

QUESTION 3

Which search matches the events containing the terms "error" and "fail"?

A. index=security Error Fail

B. index=security error OR fail

C. index=security "error failure"

D. index=security NOT error NOT fail

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

QUESTION 4

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

Correct Answer: B

QUESTION 5

Which Field/Value pair will return only events found in the index named security?

A. index!=Security

B. Index-security

C. Index=Security

D. index=Security

Correct Answer: D

The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. To query for events that are found in the index named security, you would use the following KQL query:

index=Security

This query will return all events that are found in the security index. It is important to note that the "=" operator must be used in order to match the exact index name.