SPLK-1003$^{Q\&As}$

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

QUESTION 1

Within props. conf, which stanzas are valid for data modification? (select all that apply)

A. Host

B. Server

C. Source

D. Sourcetype

Correct Answer: ACD

https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Propsconf "* Reuse of the same field-extracting regular expression across multiple sources, source types, or hosts."https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec

QUESTION 2

What is the name of the object that stores events inside of an index?

A. Container

B. Bucket

C. Data layer

D. Indexer

Correct Answer: B

A bucket is the object that stores events inside of an index. According to the Splunk documentation, "An index is a collection of directories, also called buckets, that contain index files. Each bucket represents a specific time range." A bucket can be in one of several states, such as hot, warm, cold, frozen, or thawed. Buckets are managed by indexers or clusters of indexers.

QUESTION 3

What options are available when creating custom roles? (select all that apply)

A. Restrict search terms

B. Whitelist search terms

C. Limit the number of concurrent search jobs

D. Allow or restrict indexes that can be searched.

Correct Answer: ACD

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits "Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."

QUESTION 4

Which of the following applies only to Splunk index data integrity check?

A. Lookup table

B. Summary Index

C. Raw data in the index

D. Data model acceleration

Correct Answer: C

QUESTION 5

A Splunk administrator has been tasked with developing a retention strategy to have frequently accessed data sets on SSD storage and to have older, less frequently accessed data on slower NAS storage. They have set a mount point for the NAS. Which parameter do they need to modify to set the path for the older, less frequently accessed data in indexes.conf?

A. homepath

B. thawedPath

C. summaryHomePath

D. colddeath

Correct Answer: D

The coldPath parameter defines the path for the cold buckets, which are the oldest and least frequently accessed data in an index. By setting the coldPath to point to the NAS mount point, the Splunk administrator can achieve the retention strategy of having older data on slower NAS storage.