Updated Jul-2024 Pass SPLK-1001 Exam - Real Practice Test Questions [Q55-Q69

Updated Jul-2024 Pass SPLK-1001 Exam - Real Practice Test Questions
Download Free Splunk SPLK-1001 Real Exam Questions

The SPLK-1001 certification is ideal for individuals who are new to Splunk or have limited experience in using it. It is also suitable for professionals who work with Splunk data but do not have a technical background. Splunk Core Certified User certification demonstrates that the candidate has a fundamental understanding of Splunk and can use it to extract meaningful insights from data.

Q55. _______________ transforms raw data into events and distributes the results into an index.
* Index
* Search Head
* Indexer
* Forwarder

Q56. When is the pipe character, I, used in search strings?

* Before clauses. For example: stats sum(bytes) | by host
* Before commands. For example: | stats sum(bytes) by host
* Before arguments. For example: stats sum| (bytes) by host
* Before functions. For example: stats |sum(bytes) by host
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes_and_escaping_characters

Q57. The new data uploaded in Splunk are shown in ________________.
* Real-time
* 10 Minutes
* Overnight Download
* 30 Minutes

Q58. Splunk indexes the data on the basis of timestamps.
* True
* False

Q59. Creating Data Models:

Object ATTRIBUTES do not define ___________.
* a base search for the object
* fields for the object

Q60. What are the two most efficient search filters?
* _time and host
* _time and index
* host and sourcetype
* index and sourcetype
This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1. The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2. The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.

Q61. Which search string only returns events from hostWWW3?
* host=*
* host=WWW3
* host=WWW*
* Host=WWW3

Q62. What options do you get after selecting timeline? (Choose four.)
* Zoom to selection
* Format Timeline
* Deselect
* Delete
* Zoom Out

Q63. After running a search, what effect does clicking and dragging across the timeline have?
* Executes a new search.
* Filters current search results.
* Moves to past or future events.

* Expands the time range of the search.

Q64. When viewing results of a search job from the Activity menu, which of the following is displayed?
* New events based on the current time range picker
* The same events based on the current time range picker
* The same events from when the original search was executed
* New events in addition to the same events from the original search

Q65. Which of the following is a metadata field assigned to every event in Splunk?
* host
* owner
* bytes
* action

Q66. Interesting fields are the fields that have at least 20% of resulting fields.
* True
* False

Q67. Query &#8211; status != 100:
* Will return event where status field exist but value of that field is not 100.
* Will return event where status field exist but value of that field is not 100 and all events where status field doesn&#8217;t exist.
* Will get different results depending on data.
Explanation/Reference:

Q68. Which of the following is true about user account settings and preferences?
* Search & Reporting is the only app that can be set as the default application.
* Full names can only be changed by accounts with a Power User or Admin role.
* Time zones are automatically updated based on the setting of the computer accessing Splunk.
* Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.
Explanation/Reference:

Q69. What is the primary use for the rarecommand?
* To sort field values in descending order.
* To return only fields containing five of fewer values.
* To find the least common values of a field in a dataset.
* To find the fields with the fewest number of values across a dataset.
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Rare

Splunk SPLK-1001 (Splunk Core Certified User) Certification Exam is a globally recognized certification exam that measures an individual's knowledge and skills in using Splunk software for data analysis and visualization. SPLK-1001 exam is designed for individuals who want to demonstrate their proficiency in using Splunk to analyze machine-generated data and derive insights from it.

SPLK-1001 Dumps 100 Pass Guarantee With Latest Demo:
https://www.topexamcollection.com/SPLK-1001-vce-collection.html]