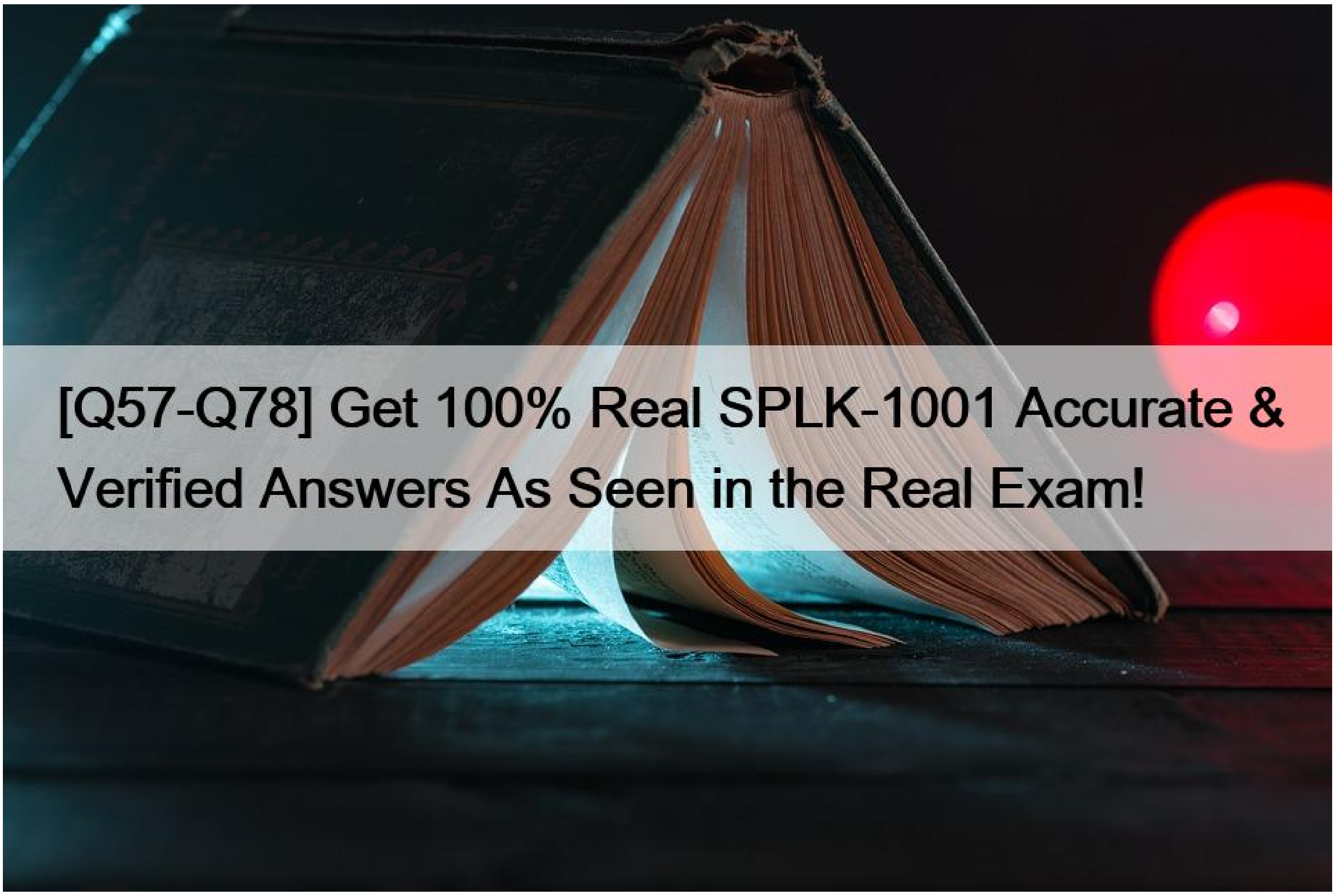
[Q57-Q78 Get 100% Real SPLK-1001 Accurate & Verified Answers As Seen in the Real Exam!


[Q57-Q78] Get 100% Real SPLK-1001 Accurate & Verified Answers As Seen in the Real Exam!

Get 100% Real SPLK-1001 Exam Questions, Accurate & Verified Answers As Seen in the Real Exam! SPLK-1001 Premium Files Updated Jul-2022 Practice Valid Exam Dumps Question

Designing & Using Lookups (6%) **As you may probably guess, this area will exclusively focus on your ability to use lookups. And to do so, it will address these skills:** - Taking advantage of the lookup when it comes to searches.- Checking a lookup file instance;- Describing lookups;- Creating a lookup file and dealing with a lookup notion;- Configuring an automatic lookup; **Q57.** Parsing of data can happen both in HF and Indexer.

* Only HF
* No
* Yes

Q58. What does the stats command do?

* Automatically correlates related fields
* Converts field values into numerical values
* Calculates statistics on data that matches the search criteria
* Analyzes numerical fields for their ability to predict another discrete field

Q59. Which stats command function provides a count of how many unique values exist for a given field in the result set?
* dc(field)
* count(field)
* count-by(field)
* distinct-count(field)

Q60. Which of the following represents the Splunk recommended naming convention for dashboards?
* Description_Group_Object
* Group_Description_Object
* Group_Object_Description
* Object_Group_Description

Q61. 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.

Q62. What can be included in the All Fields option in the sidebar?
* Dashboards
* Metadata only
* Non-interesting fields
* Field descriptions

Q63. @ Symbol can be used in advanced time unit option.
* No
* Yes

Q64. Which search will return the 15 least common field values for the dest_ipfield?
* sourcetype=firewall | rare num=15 dest_ip
* sourcetype=firewall | rare last=15 dest_ip
* sourcetype=firewall | rare count=15 dest_ip
* sourcetype=firewall | rare limit=15 dest_ip

Explanation/Reference: https://answers.splunk.com/answers/41928/add-a-lookup-csv-colum-information-to-the-results-of-a-inputlookup-search.html

Q65. Interesting fields are the fields that have at least 20% of resulting fields.
* True
* False

Q66. Clicking a SEGMENT on a chart, ________.
* drills down for that value
* highlights the field value across the chart
* adds the highlighted value to the search criteria

Q67. In the fields sidebar, what indicates that a field is numeric?
* A number to the right of the field name.
* A # symbol to the left of the field name.
* A lowercase nto the left of the field name.
* A lowercase nto the right of the field name.

Explanation

Q68. 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

Q69. What determines the scope of data that appears in a scheduled report?
* All data accessible to the User role will appear in the report
* All data accessible to the owner of the report will appear in the report
* All data accessible to all users will appear in the report until the next time the report is run
* The owner of the report can configure permissions so that the report uses either the User role or the owner&#8217;s profile at run time

Q70. A collection of items containing things such as data inputs, Ul elements and knowledge objects is known as what?
* Anapp
* JSON
* A role
* An enhanced solution

Q71. By default search results are not returned in ________ order.
* Chronological
* Reverser chronological
* ASCIE
* Alphabetical

Q72. 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.

Q73. What is the primary use for the rare command1?
* To sort field values in descending order
* To return only fields containing five or 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

Q74. When placed early in a search, which command is most effective at reducing search execution time?
* dedup
* rename
* sort &#8211;
* fields +

Q75. Which Boolean operator is implied between search terms, unless otherwise specified?
* OR
* AND

* NOT
* NAND

Q76. Which statscommand function provides a count of how many unique values exist for a given field in the result set?
* dc(field)
* count(field)
* count-by(field)
* distinct-count(field)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/ Usethestatscommandandfunctions

Q77. What does the values function of the stats command do?
* Lists all values of a given field.
* Lists unique values of a given field.
* Returns a count of unique values for a given field.
* Returns the number of events that match the search.

Q78. Universal forwarder is recommended for forwarding the logs to indexers.
* False
* True
Explanation/Reference:

REAL SPLK-1001 Exam Questions With 100% Refund Guarantee : https://www.vceprep.com/SPLK-1001-latest-vce-prep.html
]