[Q91-Q106 Real Splunk SPLK-1001 Exam Questions [Updated 2023

Real Splunk SPLK-1001 Exam Questions [Updated 2023]
SPLK-1001 Exam Dumps Pass with Updated 2023 Splunk Core Certified User

Q91. What must be done before an automatic lookup can be created? (select all that apply)
* The lookup command must be used.
* The lookup definition must be created.
* The lookup file must be uploaded to Splunk.
* The lookup file must be verified using the inputlookup command.

Q92. Which command is used to validate a lookup file?
* | lookup products.csv
* inputlookup products.csv
* I inputlookup products.csv
* | lookup definition products.csv

Q93. Which of the following is an option after clicking an item in search results?
* Saving the item to a report
* Adding the item to the search.

* Adding the item to a dashboard
* Saving the search to a JSON file.

Q94. By default, which of the following is a Selected Field?
* action
* clientip
* categoryId
* sourcetype

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch#Specify_additional_selected_fields

Q95. When looking at a statistics table, what is one way to drill down to see the underlying events?
* Creating a pivot table.
* Clicking on the visualizations tab.
* Viewing your report in a dashboard.
* Clicking on any field value in the table.

Q96. How can search results be kept longer than 7 days?
* By scheduling a report.
* By creating a link to the job.
* By changing the job settings.
* By changing the time range picker to more than 7 days.

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

Q97. Which of the following is a metadata field assigned to every event in Splunk?
* host
* owner
* bytes
* action

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically

Q98. Portal for Splunk apps can be accessed through www.splunkbase.com
* False
* True

Q99. Splunk apps are used for following (Choose three.):
* Designed to cater numerous use cases and empower Splunk.
* We can not install Splunk App.
* Allows multiple workspaces for different use cases/user roles.
* It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

Q100. Which of the following are functions of the stats command?
* count, sum, add
* count, sum, less
* sum, avg, values
* sum, values, table

Q101. How are events displayed after a search is executed?

* In chronological order.
* Randomly by default.
* In reverse chronological order.
* Alphabetically according to field name.

Q102. Which of the following represents the Splunk recommended naming convention for dashboards?
* Description_Group_Object
* Group_Description_Object
* Group_Object_Description
* Object_Group_Description

Q103. In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?
* No events will be returned.
* Splunk will prompt you to specify an index.
* All non-indexed events to which the user has access will be returned
* Events from every index searched by default to which the user has access will be returned

Q104. How can search results be kept longer than 7 days?
* By scheduling a report.
* By creating a link to the job.
* By changing the job settings.
* By changing the time range picker to more than 7 days.

Q105. Which statement is true about the topcommand?
* It returns the top 10 results.
* It displays the output in table format.
* It returns the count and percent columns per row.
* All of the above.

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/SearchReference/Top

Q106. When writing searches in Splunk, which of the following is true about Booleans?
* They must be lowercase.
* They must be uppercase.
* They must be in quotations.
* They must be in parentheses.

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Booleanexpressions