Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

NEW QUESTION 1
Which of the following is a Splunk search best practice?
Splunk Core Certified User

A. Filter as early as possible.
B. Never specify more than one index.
C. Include as few search terms as possible.
D. Use wildcards to return more search results.

Answer: A

NEW QUESTION 2
Which of the following is true about user account settings and preferences?

A. Search & Reporting is the only app that can be set as the default application.
B. Full names can only be changed by accounts with a Power User or Admin role.
C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Answer: B

NEW QUESTION 3
Which command is used to review the contents of a specified static lookup file?

A. lookup
B. csvlookup
C. inputlookup
D. outputlookup

Answer: C

NEW QUESTION 4
What must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.
B. The contents of the lookup file must be copied and pasted into the search bar.
C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer: C

NEW QUESTION 5
What does the values function of the stats command do?

A. Lists all values of a given field.
B. Lists unique values of a given field.
C. Returns a count of unique values for a given field.
D. Returns the number of events that match the search.

Answer: C

NEW QUESTION 6
How does Splunk determine which fields to extract from data?

A. Splunk only extracts the most interesting data from the last 24 hours.
B. Splunk only extracts fields users have manually specified in their data.
C. Splunk automatically extracts any fields that generate interesting visualizations.
D. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data.

Answer: D

NEW QUESTION 7
What type of search can be saved as a report?

A. Any search can be saved as a report.
B. Only searches that generate visualizations.
C. Only searches containing a transforming command.
D. Only searches that generate statistics or visualizations.

Answer: A

NEW QUESTION 8
When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event.
B. A field that appears in every event.
C. A field that appears in the top 10 events.
D. A field that appears in at least 20% of the events.

Answer: D

NEW QUESTION 9
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

Answer: B

NEW QUESTION 10
What does the stats command do?

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

Answer: C

NEW QUESTION 10
Which is primary function of the timeline located under the search bar?

A. To differentiate between structured and unstructured events in the data.
B. To sort the events returned by the search command in chronological order.
C. To zoom in and zoom out, although this does not change the scale of the chart.
D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.

Answer: D

NEW QUESTION 14
What happens when a field is added to the Selected Fields list in the fields sidebar?

A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
D. The selected field and its corresponding values will appear underneath the events in the search results.

Answer: D

NEW QUESTION 15
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 18
Splunk shows data in _____ .

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Answer: B

NEW QUESTION 20
What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

A. the_questionnaire _pedia
B. the_questionnaire pedia
C. the_questionnaire_pedia
D. the_questionnaire Pedia

Answer: C

NEW QUESTION 21
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 24
You can on-board data to Splunk using following means (Choose four.):

A. Props
B. CLI
C. Splunk Web
D. savedsearches.conf
E. Splunk apps and add-ons
F. indexes.conf
G. inputs.conf
H. metadata.conf

Answer: BCEG

NEW QUESTION 28
Data sources being opened and read applies to:

A. None of the above
B. Indexing Phase
C. Parsing Phase
D. Input Phase
E. License Metering

Answer: D

NEW QUESTION 31
Select the correct option that applies to Index time processing (Choose three.).

A. Indexing
B. Searching
C. Parsing
D. Settings
E. Input

Answer: ACE

NEW QUESTION 34
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 35
In monitor option you can select the following options in GUI.

A. Only HTTP Event Collector (HEC) and TCP/UDP
B. None of the above
C. Only TCP/UDP
D. Only Scripts
E. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

NEW QUESTION 39
Matching search terms are highlighted.

A. Yes
B. No

Answer: A

NEW QUESTION 43
Which symbol is used to snap the time?

A. @

B. &
C. *
D. #

Answer: A

NEW QUESTION 46
Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

A. Open new search.
B. Exclude the item from search.
C. None of the above.
D. Add the item to search.

Answer: ABD

NEW QUESTION 47
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-1001 Practice Exam Features:

* SPLK-1001 Questions and Answers Updated Frequently

* SPLK-1001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-1001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-1001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year