

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

When looking at a dashboard panel that is based on a report, which of the following is true?

- A. You can modify the search string in the panel, and you can change and configure the visualization.
- B. You can modify the search string in the panel, but you cannot change and configure the visualization.
- C. You cannot modify the search string in the panel, but you can change and configure the visualization.
- D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Answer: C

NEW QUESTION 3

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 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

Which statement is true about Splunk alerts?

- A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
- B. Alerts are based on searches and when triggered will only send an email notification.
- C. Alerts are based on searches and require cron to run on scheduled interval.
- D. Alerts are based on searches that are run exclusively as real-time.

Answer: A

NEW QUESTION 6

How do you add or remove fields from search results?

- A. Use field +to add and field -to remove.
- B. Use table +to add and table -to remove.
- C. Use fields +to add and fields -to remove.
- D. Use fields Plus to add and fields Minus to remove.

Answer: C

NEW QUESTION 7

What is the main requirement for creating visualizations using the Splunk UI?

- A. Your search must transform event data into Excel file format first.
- B. Your search must transform event data into XML formatted data first.
- C. Your search must transform event data into statistical data tables first.
- D. Your search must transform event data into JSON formatted data first.

Answer: B

NEW QUESTION 8

What syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

Answer: B

NEW QUESTION 9

What user interface component allows for time selection?

- A. Time summary
- B. Time range picker
- C. Search time picker
- D. Data source time statistics

Answer: B

NEW QUESTION 10

When placed early in a search, which command is most effective at reducing search execution time?

- A. dedup
- B. rename
- C. sort -
- D. fields +

Answer: A

NEW QUESTION 10

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 13

What can be included in the All Fields option in the sidebar?

- A. Dashboards
- B. Metadata only
- C. Non-interesting fields
- D. Field descriptions

Answer: D

NEW QUESTION 17

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 22

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 23

Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

- A. Save the search as a report and use it in multiple dashboards as needed.
- B. Save the search as a dashboard panel for each dashboard that needs the data.
- C. Save the search as a scheduled alert and use it in multiple dashboards as needed.
- D. Export the results of the search to an XML file and use the file as the basis of the dashboards.

Answer: D

NEW QUESTION 27

What does the following specified time range do?
earliest=-72h@h latest=@d

- A. Look back 3 days ago and prior.
- B. Look back 72 hours, up to one day ago.
- C. Look back 72 hours, up to the end of today.
- D. Look back from 3 days ago, up to the beginning of today.

Answer: C

NEW QUESTION 30

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 33

How can another user gain access to a saved report?

- A. The owner of the report can edit permissions from the Edit dropdown.
- B. Only users with an Admin or Power User role can access other users' reports.
- C. Anyone can access any reports marked as public within a shared Splunk deployment.
- D. The owner of the report must clone the original report and save it to their user account.

Answer: A

NEW QUESTION 34

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 37

Three basic components of Splunk are (Choose three.):

- A. Forwarders
- B. Deployment Server
- C. Indexer
- D. Knowledge Objects
- E. Index
- F. Search Head

Answer: ACF

NEW QUESTION 40

What is Splunk?

- A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
- B. Database management tool.
- C. Security Information and Event Management (SIEM).
- D. Cloud based application that help in analyzing logs.

Answer: A

NEW QUESTION 41

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

- A. True
- B. False

Answer: A

NEW QUESTION 45

Log filtering/parsing can be done from _____.

- A. Index Forwarders (IF)
- B. Universal Forwarders (UF)
- C. Super Forwarder (SF)
- D. Heavy Forwarders (HF)

Answer: D

NEW QUESTION 48

Which is the default app for Splunk Enterprise?

- A. Splunk Enterprise Security Suite
- B. Searching and Reporting
- C. Reporting and Searching
- D. Splunk apps for Security

Answer: B

NEW QUESTION 49

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 54

Upload option creates inputs.conf

- A. Yes
- B. No

Answer: B

NEW QUESTION 55

Which of the statements are correct about HF? (Choose three.)

- A. Parsing
- B. Masking
- C. Searching
- D. Forwarding

Answer: ABD

NEW QUESTION 60

Where does Licensing meter happen?

- A. Indexer
- B. Parsing
- C. Heavy Forwarder
- D. Input

Answer: A

NEW QUESTION 61

You are able to create new Index in Data Input settings.

- A. No
- B. Yes

Answer: B

NEW QUESTION 64

Splunk Parses data into individual events, extracts time, and assigns metadata.

- A. False
- B. True

Answer: B

NEW QUESTION 66

Which symbol is used to snap the time?

- A. @
- B. &
- C. *
- D. #

Answer: A

NEW QUESTION 71

You can view the search result in following format (Choose three.):

- A. Table
- B. Raw
- C. Pie Chart
- D. List

Answer: ABD

NEW QUESTION 73

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1001 Practice Test Here](#)