

SPLK-1002 Dumps

Splunk Core Certified Power User Exam

<https://www.certleader.com/SPLK-1002-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

- A. Alerts
- B. Email
- C. Database
- D. User permissions

Answer: ABC

NEW QUESTION 2

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()
- C. Print ()
- D. ToString ()

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

Which of the following statements about event types is true? (select all that apply)

- A. Event types can be tagged.
- B. Event types must include a time range,
- C. Event types categorize events based on a search.
- D. Event types can be a useful method for capturing and sharing knowledge.

Answer: AC

NEW QUESTION 4

- (Exam Topic 1)

Which of the following statements describe the search string below?

dacamodel Application_State All_Application_State search

- A. Events will be returned from dataset named Application_state.
- B. Events will be returned from the data model named Application_State.
- C. Events will be returned from the data model named All_Application_state.
- D. No events will be returned because the pipe should occur after the datamodel command

Answer: C

NEW QUESTION 5

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (QM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

Answer: AC

NEW QUESTION 6

- (Exam Topic 1)

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases can be used in lookup file definitions.
- C. Field aliases only normalize data across sources and sourcetypes.
- D. Field alias names are not case sensitive when used as part of a search.

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

When creating a Search workflow action, which field is required?

- A. Search string
- B. Data model name
- C. Permission setting
- D. An eval statement

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

Answer: D

NEW QUESTION 9

- (Exam Topic 1)

Which of the following statements describes POST workflow actions?

- A. POST workflow actions are always encrypted.
- B. POST workflow actions cannot use field values in their URI.
- C. POST workflow actions cannot be created on custom sourcetypes.
- D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Answer: CD

NEW QUESTION 11

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

- A. CSV
- B. PDF
- C. XML
- D. JSON

Answer: A

NEW QUESTION 16

- (Exam Topic 1)

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

- A. Index-main | REJECT trans sessionid
- B. Index-main | transaction sessionid | search REJECT
- C. Index=main | transaction sessionid | whose transaction=reject
- D. Index=main | transaction sessionid | where transaction=reject"

Answer: D

NEW QUESTION 17

- (Exam Topic 1)

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.

D. The CIM add-on is automatically installed in a Splunk environment.

Answer: C

NEW QUESTION 19

- (Exam Topic 1)

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. Fast mode is enabled.
- B. The dashboard is private.
- C. The extraction is private
- D. The person in the organization running the report does not have access to the index.

Answer: BD

NEW QUESTION 23

- (Exam Topic 1)

Which of the following statements about data models and pivot are true? (select all that apply)

- A. They are both knowledge objects.
- B. Data models are created out of datasets called pivots.
- C. Pivot requires users to input SPL searches on data models.
- D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Answer: BD

NEW QUESTION 27

- (Exam Topic 1)

When should you use the transaction command instead of the scats command?

- A. When you need to group on multiple values.
- B. When duration is irrelevant in search result
- C. .
- D. When you have over 1000 events in a transaction.
- E. When you need to group based on start and end constraints.

Answer: C

NEW QUESTION 30

- (Exam Topic 1)

Selected fields are displayed _____ each event in the search results.

- A. below
- B. interesting fields
- C. other fields
- D. above

Answer: A

NEW QUESTION 35

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XMI attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: B

NEW QUESTION 39

- (Exam Topic 1)

In what order are the following knowledge objects/configurations applied?

- A. Field Aliases, Field Extractions, Lookups
- B. Field Extractions, Field Aliases, Lookups
- C. Field Extractions, Lookups, Field Aliases
- D. Lookups, Field Aliases, Field Extractions

Answer: B

NEW QUESTION 43

- (Exam Topic 1)

Which of the following statements describe the search below? (select all that apply) Index=main | transaction clientip host maxspan=30s maxpause=5s

- A. Events in the transaction occurred within 5 seconds.
- B. It groups events that share the same clientip and host.
- C. The first and last events are no more than 5 seconds apart.
- D. The first and last events are no more than 30 seconds apart.

Answer: B

NEW QUESTION 46

- (Exam Topic 1)

When using timechart, how many fields can be listed after a by clause? (Choose Two)

- A. because timechart doesn't support using a by clause.
- B. because _time is already implied as the x-axis.
- C. because one field would represent the x-axis and the other would represent the y-axis.
- D. There is no limit specific to timechart.

Answer: BD

NEW QUESTION 47

- (Exam Topic 1)

Which of the following statements describes this search? sourcetype=access_combined | transaction JSESSIONID | timechart avg (duration)

- A. This is a valid search and will display a timechart of the average duration, of each transaction event.
- B. This is a valid search and will display a stats table showing the maximum pause among transactions.
- C. No results will be returned because the transaction command must include the startswith and endswith options.
- D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Answer: A

NEW QUESTION 51

- (Exam Topic 1)

Which of the following statements describe data model acceleration? (select all that apply)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.

Answer: BCD

NEW QUESTION 53

- (Exam Topic 1)

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

- A. The regex can no longer be edited.
- B. The field being extracted will be required for all future events.
- C. The events without the required field will not display in searches.
- D. Only events with the required string will be included in the extraction.

Answer: D

NEW QUESTION 57

- (Exam Topic 1)

When using the Field Extractor (FX), which of the following delimiters will work? (select all that apply)

- A. Tabs
- B. Pipes
- C. Colons
- D. Spaces

Answer: ABD

NEW QUESTION 62

- (Exam Topic 1)

What does the transaction command do?

- A. Groups a set of transactions based on time.
- B. Creates a single event from a group of events.
- C. Separates two events based on one or more values.
- D. Returns the number of credit card transactions found in the event logs.

Answer: B

NEW QUESTION 64

- (Exam Topic 2)

Which of the following commands will show the maximum bytes?

- A. sourcetype=access_* | maximum totals by bytes
- B. sourcetype=access_* | avg (bytes)
- C. sourcetype=access_* | stats max(bytes)
- D. sourcetype=access_* | max(bytes)

Answer: C

NEW QUESTION 69

- (Exam Topic 2)

This tab shows you the event patterns in the results of a specific search.

- A. statistics
- B. visualization
- C. patterns

Answer: C

NEW QUESTION 72

- (Exam Topic 2)

The transaction command allows you to _____ events across multiple sources

- A. duplicate
- B. correlate
- C. persist
- D. tag

Answer: B

NEW QUESTION 76

- (Exam Topic 2)

Which of the following are valid options to speed up reports? (Select all the apply.)

- A. Edit permissions
- B. Edit description
- C. Edit acceleration
- D. Edit schedule

Answer: C

NEW QUESTION 77

- (Exam Topic 2)

We can use the rename command to _____ (Select all that apply.)

- A. Change indexed fields
- B. Exclude fields from our search results
- C. Extract new fields from our data using regular expressions
- D. Give a field a new name at search time

Answer: D

NEW QUESTION 79

- (Exam Topic 2)

Using the export function, you can export search results as _____.(Select all that apply)

- A. Xml
- B. Json
- C. Html
- D. A php file

Answer: AB

NEW QUESTION 84

- (Exam Topic 2)

When using the transaction command, what does the argument maxspan do?

- A. Sets the maximum total time between events in a transaction.
- B. Sets the maximum length of all events within a transaction.
- C. Sets the maximum total time between the earliest and latest events in a transaction.
- D. Sets the maximum length that any single event can reach to be included in the transaction.

Answer: B

NEW QUESTION 89

- (Exam Topic 2)
Clicking a SEGMENT on a chart, _____.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 92

- (Exam Topic 2)
Which of the following searches will show the number of categoryId used by each host?

- A. Sourcetype=access_* |sum bytes by host
- B. Sourcetype=access_* |stats sum(categoryId) by host
- C. by host
- D. Sourcetype=access_* |sum(bytes) by host
- E. Sourcetype=access_* |stats sum by host

Answer: B

NEW QUESTION 97

- (Exam Topic 2)
Which search would limit an "alert" tag to the "host" field?

- A. tag=alert
- B. host::tag::alert
- C. tag==alert
- D. tag::host=alert

Answer: D

NEW QUESTION 102

- (Exam Topic 2)
These allow you to categorize events based on search terms. Select your answer.

- A. Groups
- B. Event Types
- C. Macros
- D. Tags

Answer: B

NEW QUESTION 107

- (Exam Topic 2)
Which is not a comparison operator in Splunk

- A. <=
- B. =
- C. !=
- D. >
- E. ?=

Answer: E

NEW QUESTION 111

- (Exam Topic 2)
What will you learn from the results of the following search? sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

Answer: A

NEW QUESTION 113

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-1002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-1002-dumps.html>