Actual exam question from Splunk's SPLK-1001

Question #: 1

Topic #: 1

[All SPLK-1001 Questions]

Which search string only returns events from hostWWW3?

A. host=*

B. host=WWW3

C. host=WWW*

D. Host=WWW3

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 2

Topic #: 1

[All SPLK-1001 Questions]

By default, how long does Splunk retain a search job?

A. 10 Minutes

B. 15 Minutes

C. 1 Day

D. 7 Days

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 3

Topic #: 1

[All SPLK-1001 Questions]

What must be done before an automatic lookup can be created? (Choose all that apply.)

A. The lookup command must be used.

B. The lookup definition must be created.

C. The lookup file must be uploaded to Splunk.

D. The lookup file must be verified using the inputlookup command.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 4

Topic #: 1

[All SPLK-1001 Questions]

Which of the following Splunk components typically resides on the machines where data originates?

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 5

Topic #: 1

[All SPLK-1001 Questions]

What determines the scope of data that appears in a scheduled report?

A. All data accessible to the User role will appear in the report.

B. All data accessible to the owner of the report will appear in the report.

C. All data accessible to all users will appear in the report until the next time the report is run.

D. The owner of the report can configure permissions so that the report uses either the User role or the owner's profile at run time.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 6

Topic #: 1

[All SPLK-1001 Questions]

When writing searches in Splunk, which of the following is true about Booleans?

A. They must be lowercase.

B. They must be uppercase.

C. They must be in quotations.

D. They must be in parentheses.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 7

Topic #: 1

[All SPLK-1001 Questions]

Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

A. (index=netfw failure) AND index=netops warn OR critical

B. (index=netfw failure) OR (index=netops (warn OR critical))

C. (index=netfw failure) AND (index=netops (warn OR critical))

D. (index=netfw failure) OR index=netops OR (warn OR critical)

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 8

Topic #: 1

[All SPLK-1001 Questions]

Select the answer that displays the accurate placing of the pipe in the following search string: index=security sourcetype=access_* status=200 stats count by price

A. index=security sourcetype=access_* status=200 stats | count by price

B. index=security sourcetype=access_* status=200 | stats count by price

C. index=security sourcetype=access_* status=200 | stats count | by price

D. index=security sourcetype=access_* | status=200 | stats count by price

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 9

Topic #: 1

[All SPLK-1001 Questions]

Which of the following constraints can be used with the top command?

A. limit

B. useperc

C. addtotals

D. fieldcount

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 10

Topic #: 1

[All SPLK-1001 Questions]

When editing a dashboard, which of the following are possible options? (Choose all that apply.)

A. Add an output.

B. Export a dashboard panel.

C. Modify the chart type displayed in a dashboard panel.

D. Drag a dashboard panel to a different location on the dashboard.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 11

Topic #: 1

[All SPLK-1001 Questions]

When running searches, command modifiers in the search string are displayed in what color?

A. Red

B. Blue

C. Orange

D. Highlighted

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 12

Topic #: 1

[All SPLK-1001 Questions]

Which of the following represents the Splunk recommended naming convention for dashboards?

A. Description_Group_Object

B. Group_Description_Object

C. Group_Object_Description

D. Object_Group_Description

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 13

Topic #: 1

[All SPLK-1001 Questions]

How can search results be kept longer than 7 days?

A. By scheduling a report.

B. By creating a link to the job.

C. By changing the job settings.

D. By changing the time range picker to more than 7 days.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 14

Topic #: 1

[All SPLK-1001 Questions]

Which of the following is a Splunk search best practice?

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 15

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 16

Topic #: 1

[All SPLK-1001 Questions]

Which of the following are common constraints of the top command?

A. limit, count

B. limit, showpercent

C. limits, countfield

D. showperc, countfield

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 17

Topic #: 1

[All SPLK-1001 Questions]

When displaying results of a search, which of the following is true about line charts?

A. Line charts are optimal for single and multiple series.

B. Line charts are optimal for single series when using Fast mode.

C. Line charts are optimal for multiple series with 3 or more columns.

D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 18

Topic #: 1

[All SPLK-1001 Questions]

How are events displayed after a search is executed?

A. In chronological order.

B. Randomly by default.

C. In reverse chronological order.

D. Alphabetically according to field name.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 19

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 20

Topic #: 1

[All SPLK-1001 Questions]

What is a primary function of a scheduled report?

A. Auto-detect changes in performance.

B. Auto-generated PDF reports of overall data trends.

C. Regularly scheduled archiving to keep disk space use low.

D. Triggering an alert in your Splunk instance when certain conditions are met.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 21

Topic #: 1

[All SPLK-1001 Questions]

After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.

B. Filters current search results.

C. Moves to past or future events.

D. Expands the time range of the search.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 22

Topic #: 1

[All SPLK-1001 Questions]

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

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 23

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 24

Topic #: 1

[All SPLK-1001 Questions]

When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?

A. |

B. $

C. !

D. ,

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 25

Topic #: 1

[All SPLK-1001 Questions]

Which time range picker configuration would return real-time events for the past 30 seconds?

A. Preset - Relative: 30-seconds ago

B. Relative - Earliest: 30-seconds ago, Latest: Now

C. Real-time - Earliest: 30-seconds ago, Latest: Now

D. Advanced - Earliest: 30-seconds ago, Latest: Now

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 26

Topic #: 1

[All SPLK-1001 Questions]

What is the correct syntax to count the number of events containing a vendor_action field?

A. count stats vendor_action

B. count stats (vendor_action)

C. stats count (vendor_action)

D. stats vendor_action (count)

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 27

Topic #: 1

[All SPLK-1001 Questions]

What is one benefit of creating dashboard panels from reports?

A. Any newly created dashboard will include that report.

B. There are no benefits to creating dashboard panels from reports.

C. It makes the dashboard more efficient because it only has to run one search string.

D. Any change to the underlying report will affect every dashboard that utilizes that report.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 28

Topic #: 1

[All SPLK-1001 Questions]

By default, which of the following fields would be listed in the fields sidebar under interesting Fields?

A. host

B. index

C. source

D. sourcetype

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 29

Topic #: 1

[All SPLK-1001 Questions]

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 30

Topic #: 1

[All SPLK-1001 Questions]

What does the rare command do?

A. Returns the least common field values of a given field in the results.

B. Returns the most common field values of a given field in the results.

C. Returns the top 10 field values of a given field in the results.

D. Returns the lowest 10 field values of a given field in the results.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 31

Topic #: 1

[All SPLK-1001 Questions]

When an alert action is configured to run a script, Splunk must be able to locate the script.

Which is one of the directories Splunk will look in to find the script?

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/scripts

C. $SPLUNK_HOME/bin/etc/scripts

D. $SPLUNK_HOME/etc/scripts/bin

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 32

Topic #: 1

[All SPLK-1001 Questions]

Which Boolean operator is always implied between two search terms, unless otherwise specified?

A. OR

B. NOT

C. AND

D. XOR

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 33

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 34

Topic #: 1

[All SPLK-1001 Questions]

Which stats command function provides a count of how many unique values exist for a given field in the result set?

A. dc(field)

B. count(field)

C. count-by(field)

D. distinct-count(field)

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 35

Topic #: 1

[All SPLK-1001 Questions]

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

A. An app

B. JSON

C. A role

D. An enhanced solution

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 36

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 37

Topic #: 1

[All SPLK-1001 Questions]

What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.

B. To compute numerical statistics on each field.

C. To specify how the values in a list are delimited.

D. To partition the input data based on the split-by fields.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 38

Topic #: 1

[All SPLK-1001 Questions]

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 ג€"to remove.

D. Use fields Plus to add and fields Minus to remove.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 39

Topic #: 1

[All SPLK-1001 Questions]

A field exists in search results, but isn't being displayed in the fields sidebar.

How can it be added to the fields sidebar?

A. Click All Fields and select the field to add it to Selected Fields.

B. Click Interesting Fields and select the field to add it to Selected Fields.

C. Click Selected Fields and select the field to add it to Interesting Fields.

D. This scenario isn't possible because all fields returned from a search always appear in the fields sidebar.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 40

Topic #: 1

[All SPLK-1001 Questions]

In the fields sidebar, which character denotes alphanumeric field values?

A. #

B. %

C. a

D. a#

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 41

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 42

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 43

Topic #: 1

[All SPLK-1001 Questions]

What user interface component allows for time selection?

A. Time summary

B. Time range picker

C. Search time picker

D. Data source time statistics

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 44

Topic #: 1

[All SPLK-1001 Questions]

Which of the following searches will return results where fail, 400, and error exist in every event?

A. error AND (fail AND 400)

B. error OR (fail and 400)

C. error AND (fail OR 400)

D. error OR fail OR 400

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 45

Topic #: 1

[All SPLK-1001 Questions]

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

A. dedup

B. rename

C. sort -

D. fields +

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 46

Topic #: 1

[All SPLK-1001 Questions]

Which of the following is the most efficient filter for running searches in Splunk?

A. Time

B. Fast mode

C. Sourcetype

D. Selected Fields

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 47

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 48

Topic #: 1

[All SPLK-1001 Questions]

Which of the following file types is an option for exporting Splunk search results?

A. PDF

B. JSON

C. XLS

D. RTF

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 49

Topic #: 1

[All SPLK-1001 Questions]

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

A. Parentheses

B. @ or # symbols

C. Quotation marks

D. Relational operators such as =, <, or >

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 50

Topic #: 1

[All SPLK-1001 Questions]

Which search string returns a filed containing the number of matching events and names that field Event Count?

A. index=security failure | stats sum as ɹ€Event Countɹ€

B. index=security failure | stats count as ɹ€Event Countɹ€

C. index=security failure | stats count by ɹ€Event Countɹ€

D. index=security failure | stats dc(count) as ɹ€Event Countɹ€

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 51

Topic #: 1

[All SPLK-1001 Questions]

Which search would return events from the access_combined sourcetype?

A. Sourcetype=access_combined

B. Sourcetype=Access_Combined

C. sourcetype=Access_Combined

D. SOURCETYPE=access_combined

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 52

Topic #: 1

[All SPLK-1001 Questions]

Which of the following index searches would provide the most efficient search performance?

A. index=*

B. index=web OR index=s*

C. (index=web OR index=sales)

D. *index=sales AND index=web*

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 53

Topic #: 1

[All SPLK-1001 Questions]

What is a suggested Splunk best practice for naming reports?

A. Reports are best named using many numbers so they can be more easily sorted.

B. Use a consistent naming convention so they are easily separated by characteristics such as group and object.

C. Name reports as uniquely as possible with no overlap to differentiate them from one another.

D. Any naming convention is fine as long as you keep an external spreadsheet to keep track.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 54

Topic #: 1

[All SPLK-1001 Questions]

In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

A. No events will be returned.

B. Splunk will prompt you to specify an index.

C. All non-indexed events to which the user has access will be returned.

D. Events from every index searched by default to which the user has access will be returned.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 55

Topic #: 1

[All SPLK-1001 Questions]

When looking at a statistics table, what is one way to drill down to see the underlying events?

A. Creating a pivot table.

B. Clicking on the visualizations tab.

C. Viewing your report in a dashboard.

D. Clicking on any field value in the table.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 56

Topic #: 1

[All SPLK-1001 Questions]

In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type

B. App, Owner, Priority, and Status

C. App, Dashboard, Severity, and Type

D. App, Time Window, Type, and Severity

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 57

Topic #: 1

[All SPLK-1001 Questions]

What are the steps to schedule a report?

A. After saving the report, click Schedule.

B. After saving the report, click Event Type.

C. After saving the report, click Scheduling.

D. After saving the report, click Dashboard Panel.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 58

Topic #: 1

[All SPLK-1001 Questions]

In the fields sidebar, what indicates that a field is numeric?

A. A number to the right of the field name.

B. A # symbol to the left of the field name.

C. A lowercase n to the left of the field name.

D. A lowercase n to the right of the field name.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 59

Topic #: 1

[All SPLK-1001 Questions]

Which of the following are functions of the stats command?

A. count, sum, add

B. count, sum, less

C. sum, avg, values

D. sum, values, table

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 60

Topic #: 1

[All SPLK-1001 Questions]

At index time, in which field does Splunk store the timestamp value?

A. time

B. _time

C. EventTime

D. timestamp

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 61

Topic #: 1

[All SPLK-1001 Questions]

Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms.

B. Include at least one function as this is a search requirement.

C. Include the search terms at the beginning of the search string.

D. Avoid using formatting clauses, as they add too much overhead.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 62

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 63

Topic #: 1

[All SPLK-1001 Questions]

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

A. Dashboards

B. Metadata only

C. Non-interesting fields

D. Field descriptions

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 64

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 65

Topic #: 1

[All SPLK-1001 Questions]

When a Splunk search generates calculated data that appears in the Statistics tab, in what formats can the results be exported?

A. CSV, JSON, PDF

B. CSV, XML, JSON

C. Raw Events, XML, JSON

D. Raw Events, CSV, XML, JSON

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 66

Topic #: 1

[All SPLK-1001 Questions]

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 ɹ€error failureɹ€

D. index=security NOT error NOT fail

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 67

Topic #: 1

[All SPLK-1001 Questions]

Which of the following is an option after clicking an item in search results?

A. Saving the item to a report.

B. Adding the item to the search.

C. Adding the item to a dashboard.

D. Saving the Search to a JSON file.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 68

Topic #: 1

[All SPLK-1001 Questions]

Which of the following fields is stored with the events in the index?

A. user

B. source

C. location

D. sourceIp

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 69

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 70

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 71

Topic #: 1

[All SPLK-1001 Questions]

Which events will be returned by the following search string? host=www3 status=503

A. All events that either have a host of www3 or a status of 503.

B. All events with a host of www3 that also have a status of 503.

C. We need more information; we cannot tell without knowing the time range.

D. We need more information; a search cannot be run without specifying an index.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 72

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 73

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 74

Topic #: 1

[All SPLK-1001 Questions]

What can be configured using the Edit Job Settings menu?

A. Export the result to CSV format.

B. Add the Job results to a dashboard.

C. Schedule the Job to re-run in 10 minutes.

D. Change Job Lifetime from 10 minutes to 7 days.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 75

Topic #: 1

[All SPLK-1001 Questions]

Which command is used to validate a lookup file?

A. | lookup products.csv

B. inputlookup products.csv

C. | inputlookup products.csv

D. | lookup_definition products.csv

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 76

Topic #: 1

[All SPLK-1001 Questions]

Which statement is true about the top command?

A. It returns the top 10 results.

B. It displays the output in table format.

C. It returns the count and percent columns per row.

D. All of the above.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 77

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 78

Topic #: 1

[All SPLK-1001 Questions]

What is the primary use for the rare command?

A. To sort field values in descending order.

B. To return only fields containing five of fewer values.

C. To find the least common values of a field in a dataset.

D. To find the fields with the fewest number of values across a dataset.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 79

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 80

Topic #: 1

[All SPLK-1001 Questions]

By default, which of the following is a Selected Field?

A. action

B. clientip

C. categoryId

D. sourcetype

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 81

Topic #: 1

[All SPLK-1001 Questions]

According to Splunk best practices, which placement of the wildcard results in the most efficient search?

A. f*il

B. *fail

C. fail*

D. *fail*

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 82

Topic #: 1

[All SPLK-1001 Questions]

Which command automatically returns percent and count columns when executing searches?

A. top

B. stats

C. table

D. percent

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 83

Topic #: 1

[All SPLK-1001 Questions]

Which of the following describes lookup files?

A. Lookup fields cannot be used in searches.

B. Lookups contain static data available in the index.

C. Lookups add more fields to results returned by a search.

D. Lookups pull data at index time and add them to search results.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 84

Topic #: 1

[All SPLK-1001 Questions]

Which search string is the most efficient?

A. ɹ€failed passwordɹ€

B. ɹ€failed passwordɹ€*

C. index=* ɹ€failed passwordɹ€

D. index=security ɹ€failed passwordɹ€

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 85

Topic #: 1

[All SPLK-1001 Questions]

Which search string matches only events with the status_code of 404?

A. status_code!=404

B. status_code>=400

C. status_code<=404

D. status_code>403 status_code<405

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 86

Topic #: 1

[All SPLK-1001 Questions]

_____ transforms raw data into events and distributes the results into an index.

A. Index

B. Search Head

C. Indexer

D. Forwarder

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 87

Topic #: 1

[All SPLK-1001 Questions]

Documentations for Splunk can be found at docs.splunk.com

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 88

Topic #: 1

[All SPLK-1001 Questions]

Which component of Splunk is primarily responsible for saving data?

A. Search Head

B. Heavy Forwarder

C. Indexer

D. Universal Forwarder

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 89

Topic #: 1

[All SPLK-1001 Questions]

Universal forwarder is recommended for forwarding the logs to indexers.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 90

Topic #: 1

[All SPLK-1001 Questions]

Splunk apps are used for following (Choose three.):

A. Designed to cater numerous use cases and empower Splunk.

B. We can not install Splunk App.

C. Allows multiple workspaces for different use cases/user roles.

D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 91

Topic #: 1

[All SPLK-1001 Questions]

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

A. Forwarders

B. Deployment Server

C. Indexer

D. Knowledge Objects

E. Index

F. Search Head

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 92

Topic #: 1

[All SPLK-1001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 93

Topic #: 1

[All SPLK-1001 Questions]

We should use heavy forwarder for sending event-based data to Indexers.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 94

Topic #: 1

[All SPLK-1001 Questions]

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

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 95

Topic #: 1

[All SPLK-1001 Questions]

Which component of Splunk let us write SPL query to find the required data?

A. Forwarders

B. Indexer

C. Heavy Forwarders

D. Search head

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 96

Topic #: 1

[All SPLK-1001 Questions]

All components are installed and administered in Splunk Enterprise on-premise.

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 97

Topic #: 1

[All SPLK-1001 Questions]

Log filtering/parsing can be done from _____.

A. Index Forwarders (IF)

B. Universal Forwarders (UF)

C. Super Forwarder (SF)

D. Heavy Forwarders (HF)

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 98

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 99

Topic #: 1

[All SPLK-1001 Questions]

What kind of logs can Splunk Index?

A. Only A, B

B. Router and Switch Logs

C. Firewall and Web Server Logs

D. Only C

E. Database logs

F. All firewall, web server, database, router and switch logs

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 100

Topic #: 1

[All SPLK-1001 Questions]

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

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 101

Topic #: 1

[All SPLK-1001 Questions]

Splunk shows data in _____.

A. ASCII Character order.

B. Reverse chronological order.

C. Alphanumeric order.

D. Chronological order.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 102

Topic #: 1

[All SPLK-1001 Questions]

Which of the following can be used as wildcard search in Splunk?

A. =

B. >

C. !

D. *

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 103

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 104

Topic #: 1

[All SPLK-1001 Questions]

Prefix wildcards might cause performance issues.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 105

Topic #: 1

[All SPLK-1001 Questions]

Machine data can be in structured and unstructured format.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 106

Topic #: 1

[All SPLK-1001 Questions]

Field names are case sensitive.

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 107

Topic #: 1

[All SPLK-1001 Questions]

Splunk internal fields contains general information about events and starts from underscore i.e. _ .

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 108

Topic #: 1

[All SPLK-1001 Questions]

How many main user roles do you have in Splunk?

A. 2

B. 4

C. 1

D. 3

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 109

Topic #: 1

[All SPLK-1001 Questions]

Which of the following are Splunk premium enhanced solutions? (Choose three.)

A. Splunk User Behavior Analytics (UBA)

B. Splunk IT Service Intelligence (ITSI)

C. Splunk Enterprise Security (ES)

D. Splunk Analytics Security (AS)

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 110

Topic #: 1

[All SPLK-1001 Questions]

Fields are searchable name and value pairings that differentiates one event from another.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 111

Topic #: 1

[All SPLK-1001 Questions]

Splunk extracts fields from event data at index time and at search time.

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 112

Topic #: 1

[All SPLK-1001 Questions]

Field values are case sensitive.

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 113

Topic #: 1

[All SPLK-1001 Questions]

Splunk indexes the data on the basis of timestamps.

A. True

B. False

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 114

Topic #: 1

[All SPLK-1001 Questions]

_____ is the default web port used by Splunk.

A. 8089

B. 8000

C. 8080

D. 443

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 115

Topic #: 1

[All SPLK-1001 Questions]

Which of the following statements are correct about Search & Reporting App? (Choose three.)

A. Can be accessed by Apps > Search & Reporting.

B. Provides default interface for searching and analyzing logs.

C. Enables the user to create knowledge object, reports, alerts and dashboards.

D. It only gives us search functionality.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 116

Topic #: 1

[All SPLK-1001 Questions]

Parsing of data can happen both in HF and Indexer.

A. Only HF

B. No

C. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 117

Topic #: 1

[All SPLK-1001 Questions]

Monitor option in Add Data provides _____.

A. Only continuous monitoring.

B. Only One-time monitoring.

C. None of the above.

D. Both One-time and continuous monitoring.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 118

Topic #: 1

[All SPLK-1001 Questions]

License Meter runs before data compression.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 119

Topic #: 1

[All SPLK-1001 Questions]

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

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 120

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 121

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 122

Topic #: 1

[All SPLK-1001 Questions]

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

A. Indexing

B. Searching

C. Parsing

D. Settings

E. Input

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 123

Topic #: 1

[All SPLK-1001 Questions]

Splunk automatically determines the source type for major data types.

A. False

B. True

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 124

Topic #: 1

[All SPLK-1001 Questions]

Parsing of data can happen both in HF and UF.

A. Yes

B. No

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 125

Topic #: 1

[All SPLK-1001 Questions]

Upload option creates inputs.conf

A. Yes

B. No

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 126

Topic #: 1

[All SPLK-1001 Questions]

Splunk index time process can be broken down into _____ phases.

A. 3

B. 2

C. 4

D. 1

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 127

Topic #: 1

[All SPLK-1001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 128

Topic #: 1

[All SPLK-1001 Questions]

Uploading local files though Upload options index the file only once.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 129

Topic #: 1

[All SPLK-1001 Questions]

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

A. Parsing

B. Masking

C. Searching

D. Forwarding

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 130

Topic #: 1

[All SPLK-1001 Questions]

Where does Licensing meter happen?

A. Indexer

B. Parsing

C. Heavy Forwarder

D. Input

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 131

Topic #: 1

[All SPLK-1001 Questions]

Matching search terms are highlighted.

A. Yes

B. No

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 132

Topic #: 1

[All SPLK-1001 Questions]

Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 133

Topic #: 1

[All SPLK-1001 Questions]

Zoom Out and Zoom to Selection re-executes the search.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 134

Topic #: 1

[All SPLK-1001 Questions]

Every Search in Splunk is also called _____.

A. None of the above

B. Job

C. Search Only

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 135

Topic #: 1

[All SPLK-1001 Questions]

Matching of parentheses is a feature of Splunk Assistant.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 136

Topic #: 1

[All SPLK-1001 Questions]

Search Assistant is enabled by default in the SPL editor with compact settings.

A. No

B. Yes

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 137

Topic #: 1

[All SPLK-1001 Questions]

What is Search Assistant in Splunk?

A. It is only available to Admins.

B. Such feature does not exist in Splunk.

C. Shows options to complete the search string.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1001

Question #: 138

Topic #: 1

[All SPLK-1001 Questions]

@ Symbol can be used in advanced time unit option.

A. No

B. Yes

Show Suggested Answer