Splunk.SPLK-1001.v2022-09-26.q150

□□□□:	SPLK-1001
□□□□:	Splunk Core Certified User
□□□:	Splunk
□□ □□ □□□:	150
□□:	v2022-09-26
# □□ □:	2165
# □□ □□□:	1500
https://www.krdump.com/Splunk.SPLK-1001.v2022-09-26.q150.html	

NEW QUESTION: 1
In the Splunk interface^ the list of alerts can be filtered based on which characteristics?
A. App, Owner, Priority, and Status
B. App, Owner, Severity, and Type
C. App, Dashboard Severity, and Type
D. App, Time Window, Type, and Severity
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which statement describes field discovery at search time?
A. Splunk automatically discovers only numeric fields
B. Splunk automatically discovers only alphanumeric fields
C. Splunk automatically discovers only manually configured fields
D. Splunk automatically discovers only fields directly related to the search results
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
What user interface component allows for time selection?
A. Search time picker
B. Data source time statistics
C. Time range picker
D. Time summary
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Will the queries following below get the same result?
1. index=log sourcetype=error_log status !=100

2. index=log sourcetype=error_log NOT status =100

A. No

B. Yes

Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

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

A. Highlighted

B. Red

C. Blue

D. Orange

Answer: (SHOW ANSWER)

NEW QUESTION: 6

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*

Answer: (SHOW ANSWER)

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Wildcards

NEW QUESTION: 7

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

Answer: (SHOW ANSWER)

Explanation/Reference: https://answers.splunk.com/answers/185864/selected-fields-in-fields-side-bar.html

NEW QUESTION: 8

Which search will return the 15 least common field values for the dest_ipfield?

A. sourcetype=firewall | rare num=15 dest_ip

B. sourcetype=firewall | rare last=15 dest_ip

C. sourcetype=firewall | rare count=15 dest_ip

D. sourcetype=firewall | rare limit=15 dest_ip

Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Rare#:~:text=The%20rare%20command%20is%20a,the%20limit%20argument%20is%2010

NEW QUESTION: 9
Field names are case sensitive.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 10
These users can create global knowledge objects. (Select all that apply.)
A. administrators
B. users
C. power users
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Creating Data Models:
Object ATTRIBUTES do not define _____.
A. fields for the object
B. a base search for the object
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
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: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

NEW QUESTION: 13
Which of the following represents the Splunk recommended naming convention for dashboards?
A. Group_Object_Description
B. Object_Group_Description
C. Description_Group_Object

D. Group_Description_Object
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
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 (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 15
Which search string is the most efficient?
A. "failed password"*
B. index=security "failed password"
C. index=* "failed password"
D. "failed password"
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which Boolean operator is always implied between two search terms, unless otherwise specified?
A. NOT
B. OR
C. AND
D. XOR
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following is the best way to create a report that shows the last 24 hours of events?

A. Use the time range picket to select "Yesterday"
B. Use earliest=-1d@d latest=@d
C. Use the time range picker to select "Last 24 hours"
D. Set a real-time search over a 24-hour window
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
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. We need more information a search cannot be run without specifying an index
C. We need more information: we cannot tell without knowing the time range
D. All events with a host of www3 that also have a status of 503
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
Splunk Enterprise is used as a Scalable service in Splunk Cloud.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 20
By default, how long does Splunk retain a search job?
A. 10 Minutes
B. 15 Minutes
C. 1 Day
D. 7 Days
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

NEW QUESTION: 21
Put query into separate lines where | (Pipes) are used by selecting following options.
A. CTRL + Enter
B. Shift + Enter
C. Space + Enter
D. ALT + Enter
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 22

Which of the following can be used as wildcard search in Splunk?
A. *
B. !
C.
D. >
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
All components are installed and administered in Splunk Enterprise on-premise.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Which is a primary function of the timeline located under the search bar?
A. To differentiate between structured and unstructured events in the data
B. To zoom in and zoom out. although this does not change the scale of the chart
C. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime
D. To sort the events returned by the search command in chronological order
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
Which time range picker configuration would return real-time events for the past 30 seconds?
A. Relative - Earliest: 30-seconds ago, Latest: Now
B. Preset - Relative: 30-seconds ago
C. Real-time - Earliest: 30-seconds ago, Latest: Now
D. Advanced - Earliest: 30-seconds ago, Latest: Now
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
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
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Inputlookup

NEW QUESTION: 27

Snapping rounds down to the nearest specified unit.
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 28
When editing a dashboard, which of the following are possible options? (select all that apply)
A. Export a dashboard panel.
B. Add an output.
C. Modify the chart type displayed in a dashboard panel.
D. Drag a dashboard panel to a different location on the dashboard.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
Data summary button just below the search bar gives you the following (Choose three.):
A. Hosts
B. Sources
C. Indexes
D. Sourcetypes
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Splunk automatically determines the source type for major data types.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
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 Selected Fields and select the field to add it to Interesting Fields.
B. Click All Fields and select the field to add it to Selected Fields.
C. This scenario isn't possible because all fields returned from a search always appear in the fields sidebar.
D. Click Interesting Fields and select the field to add it to Selected Fields.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Which statscommand 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)
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethestatscommandandfunctions

NEW QUESTION: 33
How are events displayed after a search is executed?
A. In reverse chronological order.
B. In chronological order.
C. Alphabetically according to field name.
D. Randomly by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
It is mandatory for the lookup file to have this for an automatic lookup to work.
A. Source type
B. At least five columns
C. Input filed
D. Timestamp
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
By default, how long does Splunk retain a search job?
A. 10 Minutes
B. 15 Minutes
C. 1 Day
D. 7 Days
Answer: (SHOW ANSWER)

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

NEW QUESTION: 36
Assuming a user has the capability to edit reports, which of the following are editable?
A. The report's name, schedule, permissions
B. The report's name, acceleration, permissions
C. Acceleration, schedule, permissions
D. The report's name, acceleration, schedule
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
Which search string matches only events with the status_codeof 404?
A. status_code!=404
B. status_code>=400
C. status_code<=404
D. status_code>403 status_code<405
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/SplunkLight/7.3.1/Examples/Searchforerrors

NEW QUESTION: 38
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
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 39
_____ transforms raw data into events and distributes the results into an index.
A. Index
B. Search Head
C. Indexer
D. Forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following fields is stored with the events in the index?

A. user
B. source
C. location
D. sourceIp
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/609626/is-there-a-way-to-check-if-makeresults-stored- the.html

NEW QUESTION: 41
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.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 42
Which of the following can be used as wildcard search in Splunk?
A. =
B. *
C. !
D. >
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
What is the primary use for the rarecommand?
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.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Rare

NEW QUESTION: 44
Snapping rounds down to the nearest specified unit.
A. No
B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following searches would return events with failurein index netfwor warn or criticalin 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)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Aboutsubsearches

NEW QUESTION: 46
Which command is used to validate a lookup file?
A. I inputlookup products.csv
B. inputlookup products.csv
C. | lookup products.csv
D. | lookup definition products.csv
Answer: (SHOW ANSWER)

NEW QUESTION: 47
In the Search and Reporting app, which tab displays timecharts and bar charts?
A. Statistics
B. Events
C. Patterns
D. Visualization
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Parsing of data can happen both in HF and Indexer.
A. No
B. Only HF

C. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which is the default app for Splunk Enterprise?
A. Searching and Reporting
B. Splunk apps for Security
C. Splunk Enterprise Security Suite
D. Reporting and Searching
Answer: (SHOW ANSWER)

NEW QUESTION: 50
36. Lookups can be private for a user.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
A collection of items containing things such as data inputs, UI elements and knowledge objects is known as what?
A. JSON
B. A role
C. Anapp
D. An enhanced solution
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
Which of the statements is correct regarding click and drag option in timeline?
A. Using this option executes a new query.
B. This doesn't execute a new query
C. There is no functionality like click and drag in Splunk's timeline.
D. The new result after selecting the range by dragging filters the events and displays the most recent first.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Which of the following Splunk components typically resides on the machines where data originates?
A. Indexer
B. Search head
C. Deployment server

D. Forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
Which of the statements are correct about HF? (Choose three.)
A. Masking
B. Forwarding
C. Searching
D. Parsing
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 55
Documentations for Splunk can be found at docs.splunk.com
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which statement is true about the top command?
A. It displays the output in table format
B. It returns the count and percent columns per row
C. All of the above
D. It returns the top 10 results
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
How to make Interesting field into a selected field?
A. Click field in field sidebar -> click YES on the pop-up dialog on upper right side -> check now field should be visible in the list of selected fields.
B. Click Settings -> Find field option -> Drop down select field -> enable selected field -> check now field should be visible in the list of selected fields.
C. Only CLI changes will enable it.
D. Not possible.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
When running searches command modifiers in the search string are displayed in what color?
A. Highlighted
B. Orange
C. Blue
D. Red

Answer: (SHOW ANSWER)

NEW QUESTION: 59
At the time of searching the start time is 03:35:08.
Will it look back to 03:00:00 if we use -30m@h in searching?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 60
When placed early in a search, which command is most effective at reducing search execution time?
A. dedup
B. rename
C. fields +
D. sort -
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
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
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/Developnamingconventionsforknowledgeobjecttitles

NEW QUESTION: 62
!= and NOT are same arguments.
A. True
B. False

Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
The new data uploaded in Splunk are shown in _____.
A. Real-time
B. Overnight Download
C. 10 Minutes
D. 30 Minutes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
Universal forwarder is recommended for forwarding the logs to indexers.
A. False
B. True
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 65
Which of the following Splunk components typically resides on the machines where data originates?
A. Forwarder
B. Indexer
C. Deployment server
D. Search head
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
Splunk internal fields contains general information about events and starts from underscore i.e. _ .
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
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 (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

NEW QUESTION: 68
What will always appear in the Selected Fields list?
A. index
B. action
C. clientip
D. sourcetype
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch

NEW QUESTION: 69
Which of the following are not true about lookups? (Select all that apply.)
A. Lookups can be time based
B. Search results can be used to populate a lookup table
C. Lookup have a 10mg maximum size limit
D. Splunk DB Connect can be used to populate a lookup table from relational databases
E. Output from a script can be used to populate a lookup table
Answer: (SHOW ANSWER)

NEW QUESTION: 70
What determines the scope of data that appears in a scheduled report?
A. All data accessible to all users will appear in the report until the next time the report is run.
B. All data accessible to the User role will appear in the report.
C. All data accessible to the owner of the report will appear in the report.
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.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
What happens when a field is added to the Selected Fields list in the fields sidebar'?
A. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time
B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
C. The selected field and its corresponding values will appear underneath the events in the search results
D. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
What are the two most efficient search filters?
A. host and sourcetype
B. _time and host
C. _time and index
D. index and sourcetype
Answer: C (LEAVE A REPLY)

NEW QUESTION: 73
Following are the time selection option while making search:
(Choose all that apply.)
A. Relative
B. Advanced
C. Presets
D. Date Range
E. Date & Time Range
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following is a Splunk internal field?
A. _raw
B. _host
C. host
D. index
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
Which Field/Value pair will return only events found in the index named security?
A. index=Security
B. index!=Security
C. Index=Security
D. Index=security
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which Boolean operator is always implied between two search terms, unless otherwise specified?
A. OR
B. NOT
C. AND

D. XOR
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Booleanexpressions

NEW QUESTION: 77
How does Splunk determine which fields to extract from data?
A. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data.
B. Splunk only extracts the most interesting data from the last 24 hours.
C. Splunk only extracts fields users have manually specified in their data.
D. Splunk automatically extracts any fields that generate interesting visualizations.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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.
Answer: (SHOW ANSWER)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports

NEW QUESTION: 79
Fields are searchable key value pairs in your event data.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80

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.

Answer: (SHOW ANSWER)

Explanation

NEW QUESTION: 81

Which of the following searches will show the number of categoryId used by each host?

A. Sourcetype=access_* |stats sum by host

B. Sourcetype=access_* |stats sum(categorylD) by host

C. Sourcetype=access_* |sum(bytes) by host

D. Sourcetype=access_* |sum bytes by host

Answer: B (LEAVE A REPLY)

NEW QUESTION: 82

Which symbol is used to snap the time?

A. #

B. *

C. &

D. @

Answer: (SHOW ANSWER)

NEW QUESTION: 83

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

A. Saving the search to a JSON file.

B. Adding the item to the search.

C. Adding the item to a dashboard

D. Saving the item to a report

Answer: D (LEAVE A REPLY)

NEW QUESTION: 84

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

A. True

B. False

Answer: A (LEAVE A REPLY)

NEW QUESTION: 85

Which search will return only events containing the word "error" and display the results as a table that includes the fields named action, src, and dest?

A. error | table action, src, dest

B. error | tabular action, src, dest

C. error | table column=action column=src column=dest

D. error | stats table action, src, dest

Answer: (SHOW ANSWER)

NEW QUESTION: 86

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: (SHOW ANSWER)

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

NEW QUESTION: 87

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

A. Your search must transform event data into XML formatted data first.

B. Your search must transform event data into statistical data tables first.

C. Your search must transform event data into JSON formatted data first.

D. Your search must transform event data into Excel file format first.

Answer: (SHOW ANSWER)

NEW QUESTION: 88

NOT status = 100:

A. Will display result depending on the data.

B. Will return event where status field exist but value of that field is not 100 and all events where status field doesn't exist.

C. Will return event where status field exist but value of that field is not 100.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

Which of the following is the most efficient search?

A. index=security "failed password"

B. (index=* OR index=security) "failed password"

C. index=* "failed password"

D. "failed password" index=*

Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
What is the correct way to use a time range specifier in the search bar so that the search looks back 2 hours?
A. earliest=-2hour@d
B. earliest=-2h
C. latest=-2h
D. latest=-2hour@d
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
Which search string only returns events from hostWWW3?
A. host=WWW3
B. Host=WWW3
C. host=WWW*
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
What does the following specified time range do?
earliest=-72h@h latest=@d
A. Look back from 3 days ago up to the beginning of today
B. Look back 3 days ago and prior
C. Look back 72 hours, up to the end of today
D. Look back 72 hours up to one day ago
Answer: (SHOW ANSWER)

NEW QUESTION: 93
What is the default lifetime of every Splunk search job?
A. All search jobs are saved for 10 days
B. All search jobs are saved for 10 minutes
C. All search jobs are saved for 10 hours
D. All search jobs are saved for 10 weeks
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Which Boolean operator is implied between search terms, unless otherwise specified?
A. AND
B. OR
C. NOT
D. NAND
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
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
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Exportsearchresults

NEW QUESTION: 96
Which of the following are common constraints of the top command?
A. limits, countfield
B. limit, showpercent
C. showperc, countfield
D. limit, count
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
What are the three main Splunk components?
A. Search head, GPU, streamer
B. Search head, indexer, forwarder
C. Search head, SQL database, forwarder
D. Search head, SSD, heavy weight agent
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://www.edureka.co/blog/splunk-architecture/

NEW QUESTION: 98
In the fields sidebar, which character denotes alphanumeric field values?
A. %
B. #

C. a
D. a#
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Which of the following is a metadata field assigned to every event in Splunk?
A. host
B. owner
C. bytes
D. action
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically

NEW QUESTION: 100
Splunk shows data in _____.
A. Reverse chronological order.
B. Alphanumeric order.
C. ASCII Character order.
D. Chronological order.
Answer: (SHOW ANSWER)

NEW QUESTION: 101
When editing a dashboard, which of the following are possible options? (select all that apply)
A. Drag a dashboard panel to a different location on the dashboard.
B. Export a dashboard panel.
C. Add an output.
D. Modify the chart type displayed in a dashboard panel.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
Which command is used to validate a lookup file?
A. I inputlookup products.csv
B. | lookup definition products.csv
C. inputlookup products.csv
D. | lookup products.csv
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
When viewing results of a search job from the Activity menu, which of the following is displayed?

A. The same events based on the current time range picker
B. New events in addition to the same events from the original search
C. The same events from when the original search was executed
D. New events based on the current time range picker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
All users by default have WRITE permission to ALL knowledge objects.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 105
How can another user gain access to a saved report?
A. Only users with an Admin or Power User role can access other users' reports
B. The owner of the report can edit permissions from the Edit dropdown
C. The owner of the report must clone the original report and save it to their user account
D. Anyone can access any reports marked as public within a shared Splunk deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 106
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: B (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following is true about user account settings and preferences?
A. Time zones are automatically updated based on the setting of the computer accessing Splunk.

B. Full names can only be changed by accounts with a Power User or Admin role.
C. Search & Reporting is the only app that can be set as the default application.
D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
What is the primary use for the rare command1?
A. To return only fields containing five or fewer values
B. To find the fields with the fewest number of values across a dataset
C. To sort field values in descending order
D. To find the least common values of a field in a dataset
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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/etc/scripts/bin
B. $SPLUNK_HOME/bin/scripts
C. $SPLUNK_HOME/etc/scripts
D. $SPLUNK_HOME/bin/etc/scripts
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following constraints can be used with the top command?
A. limit
B. addtotals
C. fieldcount
D. useperc
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
At index time, in which field does Splunk store the timestamp value?
A. timestamp
B. EventTime
C. time
D. _time
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112

Which all time unit abbreviations can you include in Advanced time range picker? (Choose seven.)

A. h

B. m

C. day

D. yr

E. s

F. d

G. w

H. week

I. mon

J. y

Answer: A,B,E,F,G,I,J (LEAVE A REPLY)

NEW QUESTION: 113

Parsing of data can happen both in HF and UF.

A. Yes

B. No

Answer: B (LEAVE A REPLY)

NEW QUESTION: 114

What can be configured using the Edit Job Settings menu?

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

B. Add the Job results to a dashboard

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

D. Export the results to CSV format

Answer: A (LEAVE A REPLY)

NEW QUESTION: 115

Following are the time selection option while making search:

(Choose all that apply.)

A. Relative

B. Date & Time Range

C. Advanced

D. Date Range

E. Presets

Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 116

In the Fields sidebar, what does the number directly to the right of the field name indicate?

A. The number of unique values for the field

B. The value of the field
C. The numeric non-unique values of the field
D. The number of values for the field
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
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 "Event Count"
B. index=security failure | stats count by "Event Count"
C. index=security failure | stats count as "Event Count"
D. index=security failure | stats dc(count) as "Event Count"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
What does the rarecommand 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.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Rare

NEW QUESTION: 119
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 any field value in the table.
C. Viewing your report in a dashboard.
D. Clicking on the visualizations tab.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 120
Which of the following file types is an option for exporting Splunk search results?
A. PDF
B. JSON
C. XLS
D. RTF
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/ExportdatausingSplunkWeb

NEW QUESTION: 121
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 (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels

NEW QUESTION: 122
_____ is the default web port used by Splunk.
A. 8000
B. 8089
C. 443
D. 8080
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
By default, how long does Splunk retain a search job?
A. 7 Days
B. 10 Minutes
C. 1 Day
D. 15 Minutes
Answer: (SHOW ANSWER)

NEW QUESTION: 124

Log filtering/parsing can be done from _____.
A. Heavy Forwarders (HF)
B. Super Forwarder (SF)
C. Universal Forwarders (UF)
D. Index Forwarders (IF)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
Which of the following file types is an option for exporting Splunk search results?
A. PDF
B. JSON
C. RTF
D. XLS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
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 (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 127
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
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
By default, which of the following fields would be listed in the fields sidebar under interesting Fields?
A. source
B. sourcetype
C. index
D. host
Answer: (SHOW ANSWER)

NEW QUESTION: 129
What is the primary use for the rare command1?
A. To find the least common values of a field in a dataset
B. To sort field values in descending order
C. To find the fields with the fewest number of values across a dataset
D. To return only fields containing five or fewer values
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following reports is available in the Fields window?
A. Top values by time
B. Events with top value fields
C. Events with rare value fields
D. Rare values by time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 131
Which of the following is the recommended way to create multiple dashboards displaying data from the same search?
A. Export the results of the search to an XML file and use the file as the basis of the dashboards
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. Save the search as a report and use it in multiple dashboards as needed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following statements are correct about Search & Reporting App? (Choose three.)
A. Provides default interface for searching and analyzing logs.
B. It only gives us search functionality.
C. Enables the user to create knowledge object, reports, alerts and dashboards.
D. Can be accessed by Apps > Search & Reporting.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 133
What is the purpose of using a byclause with the statscommand?
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.

Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Stats#1._Compare_the_difference_between_using_the_stats_and_chart_commands

NEW QUESTION: 134
Search Language Syntax in Splunk can be broken down into the following components. (Choose all that apply.)
A. Command
B. Pipe
C. Clause
D. Functions
E. Search term
F. Arguments
Answer: (SHOW ANSWER)

NEW QUESTION: 135
What does the statscommand 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: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Stats

NEW QUESTION: 136
Which of the following fields is stored with the events in the index?
A. location
B. user
C. sourcelp
D. source
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
Which of the following searches will return results where fail, 400, and error exist in every event?
A. error OR fail OR 400
B. error AND (fail AND 400)
C. error AND (fail OR 400)
D. error OR (fail and 400)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Which Boolean operator is always implied between two search terms, unless otherwise specified?
A. OR
B. NOT
C. AND
D. XOR
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Booleanexpressions

NEW QUESTION: 139
Which of the following is a best practice when writing a search string?
A. Include at least one function as this is a search requirement.
B. Include the search terms at the beginning of the search string.
C. Include all formatting commands before any search terms.
D. Avoid using formatting clauses, as they add too much overhead.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
How can results from a specified static lookup file be displayed?
A. lookup command
B. Settings > Lookups > Input
C. Settings > Lookups > Upload
D. inputlookup command
Answer: D (LEAVE A REPLY)

NEW QUESTION: 141
When a search returns _____, you can view the results as a list.

A. a list of events
B. transactions
C. statistical values
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
What must be done in order to use a lookup table in Splunk?
A. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion
B. The lookup must be configured to run automatically
C. The lookup file must be uploaded to Splunk and a lookup definition must be created
D. The contents of the lookup file must be copied and pasted into the search bar.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
What are the three main Splunk components?
A. Search head, GPU, streamer
B. Search head, SSD, heavy weight agent
C. Search head, indexer, forwarder
D. Search head, SQL database, forwarder
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
When writing searches in Splunk, which of the following is true about Booleans?
A. They must be in quotations.
B. They must be lowercase.
C. They must be uppercase.
D. They must be in parentheses.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 146
When placed early in a search, which command is most effective at reducing search execution time?
A. fields +

B. rename
C. sort -
D. dedup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
What happens when a field is added to the Selected Fields list in the fields sidebar'?
A. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time
B. The selected field and its corresponding values will appear underneath the events in the search results
C. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
D. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
Which of the statements are correct? (Choose three.)
A. Zoom to selection: Narrows the time range and re-executes the search.
B. Zoom-out: Expands the time focus and re-executes the search.
C. Zoom to selection: Narrows the time range and doesn't re-executes the search.
D. Format Timeline: Hides or shows the timeline in different views.
E. Zoom-Out: Expands the time focus and doesn't re-executes the search.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 149
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
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 150
What does the values function of the stats command do?
A. Returns the number of events that match the search.
B. Lists all values of a given field.
C. Lists unique values of a given field.
D. Returns a count of unique values for a given field.
Answer: (SHOW ANSWER)

SPLK-1001 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1001 □ □! DumpTop □ □□ **SPLK-1001** □□ □□□ □□□□□□, DumpTop SPLK-1001 □□ □□□ □□□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1001 □□□ □□□□□. https://www.dumptop.com/Splunk/SPLK-1001-dump.html (**245** Q&As Dumps, **30%OFF** **Special Discount:** **KrDump**)