Splunk.SPLK-1001.v2023-06-17.q114

Exam Code:	SPLK-1001
Exam Name:	Splunk Core Certified User
Certification Provider:	Splunk
Free Question Number:	114
Version:	v2023-06-17
# of views:	2688
# of Questions views:	1140
https://www.exam-tests.com/SPLK-1001-exam/Splunk.SPLK-1001.v2023-06-17.q114.html	

NEW QUESTION: 1
Select the answer that displays the accurate placing of the pipe in the following search string:
A. index=security sourcetype=access_* | status=200 | stats count by price
B. index=security sourcetype=access_* status=200 stats count by price
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: D (LEAVE A REPLY)

NEW QUESTION: 2
Splunk index time process can be broken down into _____ phases.
A. 3
B. 4
C. 1
D. 2
Answer: (SHOW ANSWER)

NEW QUESTION: 3
What are the three main Splunk components?
A. Search head, indexer, forwarder
B. Search head, SSD, heavy weight agent
C. Search head, GPU, streamer
D. Search head, SQL database, forwarder
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Which stats command function provides a count of how many unique values exist for a given field in the result set?
A. distinct-count(field)
B. dc(field)
C. count-by(field)
D. count(field)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
Splunk indexes the data on the basis of timestamps.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.3/Data/Aboutdefaultfields

NEW QUESTION: 6
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.
Answer: C (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline

NEW QUESTION: 7
Snapping rounds down to the nearest specified unit.
A. No
B. Yes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
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: 9
How can another user gain access to a saved report?
A. The owner of the report can edit permissions from the Edit dropdown.
B. Only users with an Admin or Power User role can access other users' reports.
C. Anyone can access any reports marked as public within a shared Splunk deployment.
D. The owner of the report must clone the original report and save it to their user account.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Report/Managereportpermissions

NEW QUESTION: 10
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: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Stats

NEW QUESTION: 11
Which of the following are common constraints of the top command?
A. limit, showpercent
B. showperc, countfield
C. limit, count
D. limits, countfield
Answer: (SHOW ANSWER)

NEW QUESTION: 12
It is mandatory for the lookup file to have this for an automatic lookup to work.
A. Timestamp
B. At least five columns
C. Source type
D. Input filed
Answer: (SHOW ANSWER)

NEW QUESTION: 13

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/bin/etc/scripts

C. $SPLUNK_HOME/etc/scripts

D. $SPLUNK_HOME/etc/scripts/bin

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

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

A. limit

B. fieldcount

C. addtotals

D. useperc

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

Which of the following are not true about lookups? (Select all that apply.)

A. Lookup have a 10mg maximum size limit

B. Lookups can be time based

C. Search results can be used to populate a lookup table

D. Splunk DB Connect can be used to populate a lookup table from relational databases

D .Output from a script can be used to populate a lookup table

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Clicking a SEGMENT on a chart, _____.

A. adds the highlighted value to the search criteria

B. highlights the field value across the chart

C. drills down for that value

Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
This function of the stats command allows you to return the middle-most value of field X.
A. Values(X)
B. Fields(X)
C. Median(X)
D. Eval by X
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
Lookups allow you to overwrite your raw event.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
Creating Data Models:
Fields associated with a data set are known as _____.
A. Attributes
B. Constraints
Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following is an option after clicking an item in search results?
A. Adding the item to a dashboard
B. Adding the item to the search.
C. Saving the search to a JSON file.
D. Saving the item to a report
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Which command is used to validate a lookup file?
A. | lookup definition products.csv
B. I inputlookup products.csv
C. inputlookup products.csv
D. | lookup products.csv
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
What is a quick, comprehensive way to learn what data is present in a Splunk deployment?
A. Search index=* sourcetype=* host=*
B. Click Data Summary in Splunk Web
C. Review Splunk reports
D. Run ./splunk show
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23
Which component of Splunk let us write SPL query to find the required data?
A. Forwarders
B. Indexer
C. Search head
D. Heavy Forwarders
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following constraints can be used with the topcommand?
A. limit
B. useperc
C. addtotals
D. fieldcount
Answer: (SHOW ANSWER)
Explanation/Reference: https://answers.splunk.com/answers/339141/how-to-use-top-command-or-stats-with-sort- results.html

NEW QUESTION: 25
Which all time unit abbreviations can you include in Advanced time range picker? (Choose seven.)
A. w
B. yr
C. h
D. day
E. s
F. y
G. mon
H. week
I. m
J. d
Answer: A,C,E,F,G,I,J (LEAVE A REPLY)

NEW QUESTION: 26
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.
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Drilldownonstatisticaltablerowsandcells

NEW QUESTION: 27
Select the best options for "search best practices" in Splunk:
(Choose five.)
A. Select the time range always.
B. Include as many search terms as possible.
C. Try to keep specific search terms.
D. Inclusion is generally better than exclusion.
E. Try to specify index values.
F. Never select time range.
G. Try to use * with every search term.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Upload option creates inputs.conf
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
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
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

NEW QUESTION: 30

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

NEW QUESTION: 31
By default, how long does Splunk retain a search job?
A. 10 Minutes
B. 7 Days
C. 15 Minutes
D. 1 Day
Answer: (SHOW ANSWER)

NEW QUESTION: 32
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: C (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/41928/add-a-lookup-csv-colum-information-to-the-results-of- a-inputlookup-search.html

NEW QUESTION: 33
By default, which of the following fields would be listed in the fields sidebar under interesting Fields?
A. source
B. sourcetype

C. host
D. index
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
In the Fields sidebar, what does the number directly to the right of the field name indicate?
A. The value of the field
B. The number of values for the field
C. The number of unique values for the field
D. The numeric non-unique values of the field
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch

NEW QUESTION: 35
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 OR (warn OR critical)
C. (index=netfw failure) AND index=netops warn OR critical
D. (index=netfw failure) OR (index=netops (warn OR critical))
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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: 37
At index time, in which field does Splunk store the timestamp value?
A. timestamp
B. time
C. _time
D. EventTime
Answer: (SHOW ANSWER)

NEW QUESTION: 38
When looking at a statistics table, what is one way to drill down to see the underlying events?
A. Viewing your report in a dashboard.
B. Clicking on the visualizations tab.
C. Clicking on any field value in the table.
D. Creating a pivot table.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
Monitor option in Add Data provides _____.
A. Only One-time monitoring.
B. Both One-time and continuous monitoring
C. None of the above.
D. Only continuous monitoring.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
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. Events from every index searched by default to which the user has access will be returned.
D. All non-indexed events to which the user has access will be returned.
Answer: (SHOW ANSWER)

NEW QUESTION: 41
By default, which of the following is a Selected Field?
A. sourcetype
B. action
C. clientip
D. categoryId
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
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. Raw Events, XML, JSON

C. CSV, XML JSON
D. Raw Events, CSV, XML, JSON
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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: (SHOW ANSWER)

NEW QUESTION: 44
Universal forwarder is recommended for forwarding the logs to indexers.
A. False
B. True
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 45
Which of the following is true about user account settings and preferences?
A. Search & Reporting is the only app that can be set as the default application.
B. Full names can only be changed by accounts with a Power User or Admin role.
C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 46
After running a search, what effect does clicking and dragging across the timeline have?
A. Filters current search results.
B. Moves to past or future events.
C. Executes a new search.
D. Expands the time range of the search.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
Field names are case sensitive and field value are not.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Splunk Enterprise is used as a Scalable service in Splunk Cloud.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
How are events displayed after a search is executed?
A. In chronological order.
B. In reverse chronological order.
C. Randomly by default.
D. Alphabetically according to field name.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
What syntax is used to link key/value pairs in search strings?
A. action equal purchase
B. action I purchase
C. action+purchase
D. action=purchase
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
In automatic lookup definitions, the _____ fields are those that are not in the event data.
A. output
B. input

Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
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: D (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports

NEW QUESTION: 53
You can use the following options to specify start and end time for the query range:
A. latest=
B. All the above
C. Only 3rd and 4th
D. beginning=
E. earliest=
F. ending=
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Fields are searchable key value pairs in your event data.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 55
What will always appear in the Selected Fields list?
A. clientip
B. index
C. sourcetype
D. action
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
Which search would return events from the access_combinedsourcetype?
A. Sourcetype=access_combined
B. sourcetype=Access_Combined

C. SOURCETYPE=access_combined
D. Sourcetype=Access_Combined
Answer: (SHOW ANSWER)

NEW QUESTION: 57
When viewing results of a search job from the Activity menu, which of the following is displayed?
A. New events in addition to the same events from the original search
B. The same events from when the original search was executed
C. The same events based on the current time range picker
D. New events based on the current time range picker
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
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: D (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Wildcards

NEW QUESTION: 59
Which of the following are Splunk premium enhanced solutions? (Choose three.)
A. Splunk Enterprise Security (ES)
B. Splunk IT Service Intelligence (ITSI)
C. Splunk User Behavior Analytics (UBA)
D. Splunk Analytics Security (AS)
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 60
What can be included in the All Fields option in the sidebar?
A. Non-interesting fields
B. Field descriptions
C. Metadata only
D. Dashboards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
When is an alert triggered?
A. When a trigger action meets the predefined conditions
B. When results of a search meet a specifically defined condition
C. When Splunk encounters a syntax error in a search
D. When an event in a search matches up with a data model
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
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: (SHOW ANSWER)
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: 63
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: 64
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: 65
Selected fields are a set of configurable fields displayed for each event.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation/Reference:

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

NEW QUESTION: 67
You can on-board data to Splunk using following means (Choose four.):
A. Splunk apps and add-ons
B. Props
C. CLI
D. inputs.conf
E. savedsearches.conf
F. metadata.conf
G. Splunk Web
H. indexes.conf
Answer: A,C,D,G (LEAVE A REPLY)

NEW QUESTION: 68
Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.
A. lookup
B. inputlookup
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69

Which of the following commands will show the maximum bytes?
A. sourcetype=access_* | stats max(bytes)
B. sourcetype=access_* | maximum totals by bytes
C. sourcetype=access_* | avg (bytes)
D. sourcetype=access_* | max(bytes)
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following searches will return results where fail, 400, and error exist in every event?
A. error AND (fail OR 400)
B. error OR (fail and 400)
C. error OR fail OR 400
D. error AND (fail AND 400)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
This function of the stats command allows you to return the sample standard deviation of a field.
A. by standarddev
B. dev
C. count deviation
D. stdev
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
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: (SHOW ANSWER)
Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels

NEW QUESTION: 73

Which is primary function of the timeline located under the search bar?
A. To differentiate between structured and unstructured events in the data.
B. To sort the events returned by the search command in chronological order.
C. To zoom in and zoom out, although this does not change the scale of the chart.
D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Startsearching

NEW QUESTION: 74
What is the correct syntax to count the number of events containing a vendor_actior field?
A. count stats(vendor_action)
B. stats vendor action(count)
C. stats count(vendor_action)
D. count stats vendor_action
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
Which search string matches only events with the status_code of 4:4?
A. status_code<=404
B. status code>403 status_code<405
C. status_code>=400
D. status_code !=404
Answer: (SHOW ANSWER)

NEW QUESTION: 76
This search will return 20 results. SEARCH: error | top host limit = 20
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 77
In the fields sidebar, which character denotes alphanumeric field values?
A. a#
B. #
C. a
D. %
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
Every Search in Splunk is also called _____.
A. Job
B. Search Only
C. None of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 79
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: 80
Which search string returns a filed containing the number of matching events and names that field Event Count?
A. index=security failure | stats count by "Event Count"
B. index=security failure | stats sum as "Event Count"
C. index=security failure | stats dc(count) as "Event Count"
D. index=security failure | stats count as "Event Count"
Answer: (SHOW ANSWER)

NEW QUESTION: 81

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.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Managereportpermissions

NEW QUESTION: 82
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
Answer: A (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Configuringscriptedalerts

NEW QUESTION: 83
Which events will be returned by the following search string?
host=www3 status=503
A. We need more information: we cannot tell without knowing the time range
B. All events that either have a host of www3 or a status of 503.
C. We need more information a search cannot be run without specifying an index
D. All events with a host of www3 that also have a status of 503
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following is a correct way to limit search results to display the 5 most common values of a field?
A. | rare limit=5
B. | rare top=5
C. | top limit=5
D. | top rare=5
Answer: (SHOW ANSWER)

NEW QUESTION: 85

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 number of values for the field
C. The value of the field
D. The numeric non-unique values of the field
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which search matches the events containing the terms "error" and "fail"?
A. index=security NOT error NOT fail
B. index=security error OR fail
C. index=security Error Fail
D. index=security "error failure"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 87
The new data uploaded in Splunk are shown in _____.
A. 10 Minutes
B. Overnight Download
C. Real-time
D. 30 Minutes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
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 fields directly related to the search results
D. Splunk automatically discovers only manually configured fields
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
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 72 hours up to one day ago
C. Look back 3 days ago and prior
D. Look back 72 hours, up to the end of today
Answer: (SHOW ANSWER)

NEW QUESTION: 90

Which search string matches only events with the status_code of 4:4?
A. status_code>=400
B. status_code !=404
C. status code>403 status_code<405
D. status_code<=404
Answer: (SHOW ANSWER)

NEW QUESTION: 91
What can be included in the All Fields option in the sidebar?
A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/ExtractfieldsinteractivelywithIFX#Access_the_field_extractor_from_the_All_Fields_dialog_box

NEW QUESTION: 92
Interesting fields are the fields that have at least 20% of resulting fields.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following is the most efficient filter for running searches in Splunk?
A. Sourcetype
B. Selected Fields
C. Time
D. Fast mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
What can be included in the All Fields option in the sidebar?
A. Non-interesting fields
B. Metadata only
C. Dashboards
D. Field descriptions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
Data sources being opened and read applies to:
A. None of the above
B. License Metering
C. Indexing Phase
D. Input Phase
E. Parsing Phase
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
What is Search Assistant in Splunk?
A. Such feature does not exist in Splunk.
B. Shows options to complete the search string
C. It is only available to Admins.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
Can you stop or pause the searching?
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
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: 99

How can search results be kept longer than 7 days?
A. By changing the time range picker to more than 7 days.
B. By scheduling a report.
C. By creating a link to the job.
D. By changing the job settings.
Answer: (SHOW ANSWER)

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

NEW QUESTION: 101
Which command is used to validate a lookup file?
A. | lookup definition products.csv
B. I inputlookup products.csv
C. | lookup products.csv
D. inputlookup products.csv
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
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: 103
Splunk automatically determines the source type for major data types.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104

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

NEW QUESTION: 105
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. Events from every index searched by default to which the user has access 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. No events will be returned.
Answer: (SHOW ANSWER)

NEW QUESTION: 106
What is the main requirement for creating visualizations using the Splunk UI?
A. Your search must transform event data into JSON formatted data first.
B. Your search must transform event data into Excel file format first.
C. Your search must transform event data into statistical data tables first.
D. Your search must transform event data into XML formatted data first.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
What is the primary use for the rare command?
A. To sort field values in descending order.
B. To find the least common values of a field in a dataset.
C. To return only fields containing five of fewer values.

D. To find the fields with the fewest number of values across a dataset.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 108
The better way of writing search query for index is:
A. index=a index=b
B. index=(a & b)
C. (index=a OR index=b)
D. index = a, b
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
Which of the following statements describes a search job?
A. A search job can only be paused when less than 50% of events are returned
B. Once a search job begins, it cannot be stopped
C. Once a search job begins, it can be stopped or paused at any point in time
D. A search job can only be stopped when less than 50% of events are returned
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following is the most efficient filter for running searches in Splunk?
A. Sourcetype
B. Selected Fields
C. Time
D. Fast mode
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
Three basic components of Splunk are (Choose three.):
A. Forwarders
B. Deployment Server
C. Indexer
D. Knowledge Objects
E. Index
F. Search Head
Answer: A,C,F (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 112
Which search matches the events containing the terms "error" and "fail"?
A. index=security NOT error NOT fail

B. index=security Error Fail
C. index=security error OR fail
D. index=security "error failure"
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
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 automatically extracts any fields that generate interesting visualizations.
C. Splunk only extracts the most interesting data from the last 24 hours.
D. Splunk only extracts fields users have manually specified in their data.
Answer: (SHOW ANSWER)

NEW QUESTION: 114
What does the following specified time range do?
earliest=-72h@h latest=@d
A. Look back 3 days ago and prior.
B. Look back 72 hours, up to one day ago.
C. Look back 72 hours, up to the end of today.
D. Look back from 3 days ago, up to the beginning of today.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/149904/find-earliest-and-latest-event-per-day-for-a-time- range.html