Splunk.SPLK-1001.v2024-04-13.q147

Exam Code:	SPLK-1001
Exam Name:	Splunk Core Certified User
Certification Provider:	Splunk
Free Question Number:	147
Version:	v2024-04-13
# of views:	1941
# of Questions views:	1470
https://www.freeqas.com/qa/Splunk/SPLK-1001/Splunk.SPLK-1001.v2024-04-13.q147.html	

NEW QUESTION: 1
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. Any change to the underlying report will affect every dashboard that utilizes that report.
D. It makes the dashboard more efficient because it only has to run one search string.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
How many minutes, by default, is the time to live (ttl) for an ad-hoc search job?
A. 5 minutes
B. 1 minute
C. 10 minutes
D. 60 minutes
Answer: C (LEAVE A REPLY)
Explanation
The default time to live (ttl) for an ad-hoc search job is 10 minutes. This means that if no one views the results of a search within 10 minutes, the search job is canceled and the results are deleted. You can change this setting in the limits.conf file1.

NEW QUESTION: 3
What is the primary use for the rare command?
A. To sort field values in descending order.
B. To find the fields with the fewest number of values across a dataset.
C. To return only fields containing five of fewer values.
D. To find the least common values of a field in a dataset.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which search matches the events containing the terms "error" and "fail"?
A. index=security error OR fail
B. index=security Error Fail
C. index=security NOT error NOT fail
D. index=security "error failure"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
By default, which of the following fields would be listed in the fields sidebar under interesting Fields?
A. sourcetype
B. source
C. index
D. host
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
It is no possible for a single instance of Splunk to manage the input, parsing and indexing of machine data.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Query - status != 100:
A. Will return event where status field exist but value of that field is not 100.
B. Will get different results depending on data
C. Will return event where status field exist but value of that field is not 100 and all events where status field doesn't exist.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
How can search results be kept longer than 7 days?
A. By changing the time range picker to more than 7 days.
B. By creating a link to the job.
C. By changing the job settings.
D. By scheduling a report.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
When editing a dashboard, which of the following are possible options? (Choose all that apply.)
A. Add an output.
B. Modify the chart type displayed in a dashboard panel.
C. Drag a dashboard panel to a different location on the dashboard.
D. Export a dashboard panel.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Splunk extracts fields from event data at index time and at search time.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 11
The command shown here does witch of the following: Command: |outputlookup products.csv
A. Writes search results to a file named products.csv
B. Returns the contents of a file named products.csv
Answer: (SHOW ANSWER)

NEW QUESTION: 12
What is the main requirement for creating visualizations using the Splunk UI?
A. Your search must transform event data into statistical data tables first
B. Your search must transform event data into JSON formatted data first
C. Your search must transform event data into XML formatted data first
D. Your search must transform event data into Excel file format first
Answer: (SHOW ANSWER)

NEW QUESTION: 13
What syntax is used to link key/value pairs in search strings?
A. Parentheses
B. Quotation marks
C. @ or # symbols
D. Relational operators such as =, <, or >
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
What are the two most efficient search filters?
A. _time and host
B. _time and index

C. host and sourcetype
D. index and sourcetype
Answer: B (LEAVE A REPLY)
Explanation
This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1. The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2. The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.

NEW QUESTION: 15
Which of the following is the best description of Splunk Apps?
A. Built only by Splunk employees.
B. A collection of files.
C. Only available for download on Splunkbase.
D. Available on iOS and Android.
Answer: (SHOW ANSWER)
Explanation
The best description of Splunk Apps is a collection of files that provide specific functionality or views of your data. Splunk Apps can be built by anyone, not only by Splunk employees. Splunk Apps are not only available for download on Splunkbase, but also can be created or customized by users. Splunk Apps are not available on iOS and Android, but rather on Splunk Enterprise or Splunk Cloud platforms.

NEW QUESTION: 16
In the fields sidebar, what indicates that a field is numeric?
A. A # symbol to the left of the field name.
B. A number to the right of the field name.
C. A lowercase n to the right of the field name.
D. A lowercase n to the left of the field name.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
What is Search Assistant in Splunk?
A. It is only available to Admins.
B. Shows options to complete the search string
C. Such feature does not exist in Splunk.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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) AND index=netops warn OR critical
C. (index=netfw failure) OR index=netops OR (warn OR critical)
D. (index=netfw failure) OR (index=netops (warn OR critical))
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following statements describes a search job?
A. Once a search job begins, it cannot be stopped
B. A search job can only be paused when less than 50% of events are returned
C. A search job can only be stopped when less than 50% of events are returned
D. Once a search job begins, it can be stopped or paused at any point in time
Answer: (SHOW ANSWER)
Explanation/Reference: Reference: https://answers.splunk.com/answers/329699/why-does-my-search-head-cluster-captain-start-dele- 1.html

NEW QUESTION: 20
What syntax is used to link key/value pairs in search strings?
A. action equal purchase
B. action=purchase
C. action I purchase
D. action+purchase
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following is the most efficient filter for running searches in Splunk?
A. Selected Fields
B. Sourcetype
C. Fast mode
D. Time
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Which command is used to review the contents of a specified static lookup file?
lookup
A. outputlookup
B. inputlookup
C. csvlookup
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
Which search string matches only events with the status_code of 4:4?
A. status code>403 status_code<405
B. status_code !=404
C. status_code<=404
D. status_code>=400
Answer: C (LEAVE A REPLY)

NEW QUESTION: 24
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: C (LEAVE A REPLY)

NEW QUESTION: 25
Which search will return the 15 least common field values for the dest_ip field?
A. sourcetype=firewall | rare count=15 dest_ip
B. sourcetype=firewall | rare limit=15 dest_ip
C. sourcetype=firewall | rare last=15 dest_ip
D. sourcetype=firewall | rare num=15 dest_ip
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
What is the default lifetime of every Splunk search job?
A. All search jobs are saved for 10 weeks
B. All search jobs are saved for 10 hours
C. All search jobs are saved for 10 minutes
D. All search jobs are saved for 10 days
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which command automatically returns percent and count columns when executing searches?
A. table
B. top
C. stats
D. percent
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
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: 29
Splunk shows data in _____.
A. Chronological order.
B. Reverse chronological order.
C. Alphanumeric order.
D. ASCII Character order.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
When running searches command modifiers in the search string are displayed in what color?
A. Highlighted
B. Red
C. Orange
D. Blue
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
What must be done before an automatic lookup can be created? (select all that apply)
A. The lookup definition must be created.
B. The lookup file must be verified using the inputlookup command.
C. The lookup command must be used.
D. The lookup file must be uploaded to Splunk.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
Universal forwarder is recommended for forwarding the logs to indexers.
A. False
B. True
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 33
What are the steps to schedule a report?
What are the steps to schedule a report?
A. After saving the report, click Dashboard Panel.
B. After saving the report, click Schedule.
C. After saving the report, click Event Type.
D. After saving the report, click Scheduling.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
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
Answer: C (LEAVE A REPLY)
A best practice when writing a search string is to include the search terms at the beginning of the search string. This helps Splunk narrow down the events that match your search criteria and improve the search performance. Formatting commands and functions can be added later in the search pipeline to manipulate and display the results. Reference: Splunk Core User Certification Exam Study Guide, page 13.

NEW QUESTION: 35

What are the steps to schedule a report?
A. After saving the report, click Dashboard Panel
B. After saving the report, click Event Type
C. After saving the report, click Scheduling
D. After saving the report, click Schedule
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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:

NEW QUESTION: 37
Which of the statements is correct regarding click and drag option in timeline?
A. This doesn't execute a new query
B. The new result after selecting the range by dragging filters the events and displays the most recent first.
C. There is no functionality like click and drag in Splunk's timeline.
D. Using this option executes a new query.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
Uploading local files though Upload options index the file only once.
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
Uploading local files though Upload options index the file only once.
A. No
B. Yes
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 40
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: 41
What are Splunk alerts based on?
A. Dashboards
B. Searches
C. Webhooks
D. Reports
Answer: B (LEAVE A REPLY)
Splunk alerts are based on searches that run on a schedule or in real time. You can use alerts to monitor for and respond to specific events or conditions in your dat a. Alerts use a saved search to look for events in real time or on a schedule. Alerts trigger when search results meet specific conditions. You can use alert actions to respond when alerts trigger, such as sending an email, running a script, or creating a ticket1.
You can create alerts from the Search app, the Alerts page, or the Dashboards app. You can also use the Splunk Web framework to create custom alert actions using Python or JavaScript1.
Dashboards, webhooks, and reports are not the basis for Splunk alerts, although they can be related to them. Dashboards are collections of views that display data visually in a variety of ways. You can add alert panels to dashboards to show the status of your alerts2. Webhooks are a type of alert action that send HTTP POST requests to a specified URL when an alert triggers. You can use webhooks to integrate Splunk alerts with external systems or applications3. Reports are saved searches that include additional attributes such as a visualization type, permissions, and an optional description. You can create reports from search results and add them to dashboards as panels. You can also use reports as the basis for scheduled or real-time alerts.
Reference
Getting started with alerts
Add an alert panel to a dashboard
Use webhooks with Splunk Enterprise
[Create and edit reports]

NEW QUESTION: 42
Query - status != 100:
A. Will return event where status field exist but value of that field is not 100.

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 get different results depending on data.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 43
Select the answer that displays the accurate placing of the pipe in the following search string:
index=security sourcetype=access_w status=200 stats count by price
A. index=security sourcetype=access_" status=200 I stats count I by price
B. index=security sourcetype=access_* status=200 | stats count by price
C. index=security sourcetype=access_* I status=200 I stats count by price
D. index=security sourcetype=access_* status=200 stats I count by price
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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)
Explanation/Reference: Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-indiffe.html

NEW QUESTION: 45
Select the best options for "search best practices" in Splunk:
(Choose five.)
A. Try to specify index values.
B. Include as many search terms as possible.
C. Try to keep specific search terms.
D. Never select time range.
E. Try to use * with every search term.
F. Inclusion is generally better than exclusion.
G. Select the time range always.
Answer: A,B,C,F,G (LEAVE A REPLY)

NEW QUESTION: 46
Which command will rename action to Customer Action?
A. | rename action = CustomerAction
B. | rename Action as "Customer Action"

C. | rename Action to "Customer Action"
D. | rename action as "Customer Action"
Answer: D (LEAVE A REPLY)
Explanation/Reference: Reference:
https://answers.splunk.com/answers/610038/understanding-command-in-search.html

NEW QUESTION: 47
Which of the following Splunk components typically resides on the machines where data originates?
A. Forwarder
B. Deployment server
C. Indexer
D. Search head
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
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: C (LEAVE A REPLY)

NEW QUESTION: 49
What determines the scope of data that appears in a scheduled report?
A. All data accessible to the owner of the report will appear in the report.
B. All data accessible to all users will appear in the report until the next time the report is run.
C. 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.
D. All data accessible to the User role will appear in the report.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
What is a quick, comprehensive way to learn what data is present in a Splunk deployment?
A. Review Splunk reports
B. Run ./splunk show
C. Click Data Summary in Splunk Web
D. Search index=* sourcetype=* host=*
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata

NEW QUESTION: 51
Which of the following is the best way to create a report that shows the last 24 hours of events?
A. Use earliest=-1d@d latest=@d
B. Set a real-time search over a 24-hour window
C. Use the time range picket to select "Yesterday"
D. Use the time range picker to select "Last 24 hours"
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/153100/how-to-get-the-event-count-for-the-last-24-hours-as- a-scheduled-report.html

NEW QUESTION: 52
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.
Answer: (SHOW ANSWER)
Explanation/Reference: https://answers.splunk.com/answers/65/are-field-values-case-sensitive.html

NEW QUESTION: 53
Which of the statements are correct about HF? (Choose three.)
A. Searching
B. Forwarding
C. Parsing
D. Masking
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 54

The new data uploaded in Splunk are shown in _____.

A. 30 Minutes

B. 10 Minutes

C. Real-time

D. Overnight Download

Answer: C (LEAVE A REPLY)

NEW QUESTION: 55

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

A. (index=web OR index=sales)

B. index=web OR index=s"

C. *index=sales AND index= web

D. index=*

Answer: A (LEAVE A REPLY)

NEW QUESTION: 56

Splunk indexes the data on the basis of timestamps.

A. True

B. False

Answer: A (LEAVE A REPLY)

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/7.2.3/Data/Aboutdefaultfields

NEW QUESTION: 57

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

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

B. It only gives us search functionality.

C. Provides default interface for searching and analyzing logs.

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

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

NEW QUESTION: 58

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: (SHOW ANSWER)

Explanation/Reference:

https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline

NEW QUESTION: 59
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. All non-indexed events to which the user has access will be returned.
B. Events from every index searched by default to which the user has access will be returned.
C. No events will be returned.
D. Splunk will prompt you to specify an index.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
Which search matches the events containing the terms "error" and "fail"?
A. index=security error OR fail
B. index=security Error Fail
C. index=security NOT error NOT fail
D. index=security "error failure"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 61
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
B. $SPLUNK_HOME/bin/scripts
C. $SPLUNK_HOME/etc/scripts/bin
D. $SPLUNK_HOME/bin/etc/scripts
Answer: (SHOW ANSWER)

NEW QUESTION: 62
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. Export the results of the search to an XML file and use the file as the basis of the dashboards

C. Save the search as a dashboard panel for each dashboard that needs the data
D. Save the search as a scheduled alert and use it in multiple dashboards as needed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
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 | stats table action, src, dest
D. error | table column=action column=src column=dest
Answer: C (LEAVE A REPLY)
Explanation/Reference: Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/search

NEW QUESTION: 64
Which statement is true about Splunk alerts?
A. Alerts are based on searches and require cron to run on scheduled interval
B. Alerts are based on searches and when triggered will only send an email notification.
C. Alerts are based on searches that are either run on a scheduled interval or in real-time
D. Alerts are based on searches that are run exclusively as real-time
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following index searches would provide the most efficient search performance?
A. index=*
B. *index=sales AND index=web*
C. index=web OR index=s*
D. (index=web OR index=sales)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
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. Splunk will prompt you to specify an index.
B. Events from every index searched by default to which the user has access will be returned.
C. No events will be returned.
D. All non-indexed events to which the user has access will be returned.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67

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

NEW QUESTION: 68
In the fields sidebar, which character denotes alphanumeric field values?
A. a#
B. a
C. %
D. #
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
How do you add or remove fields from search results?
A. Use field +to add and field -to remove.
B. Use table +to add and table -to remove.
C. Use fields +to add and fields -to remove.
D. Use fields Plusto add and fields Minusto remove.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Fields

NEW QUESTION: 70
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
Answer: C (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Selecttimerangestoapply

NEW QUESTION: 71
Which of the following fields is stored with the events in the index?
A. user
B. sourcelp
C. source
D. location

Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
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 automatically discovers many fields based on sourcetype and key/value pairs found in the data.
C. Splunk only extracts fields users have manually specified in their data.
D. Splunk automatically extracts any fields that generate interesting visualizations.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
In monitor option you can select the following options in GUI.
A. Only HTTP Event Collector (HEC) and TCP/UDP
B. Only TCP/UDP
C. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts
D. Only Scripts
E. None of the above
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
Following are the time selection option while making search:
(Choose all that apply.)
A. Presets
B. Date & Time Range
C. Relative
D. Advanced
E. Date Range
Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 75
Which all time unit abbreviations can you include in Advanced time range picker? (Choose seven.)
A. week
B. h
C. w
D. y
E. mon
F. m
G. yr
H. day

I. d
J. s
Answer: B,C,D,E,F,I,J (LEAVE A REPLY)

NEW QUESTION: 76
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: 77
In the Fields sidebar, what does the number directly to the right of the field name indicate?
A. The numeric non-unique values of the field
B. The number of values for the field
C. The value of the field
D. The number of unique values for the field
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
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: 79
How can results from a specified static lookup file be displayed?
A. lookupcommand
B. inputlookupcommand
C. Settings > Lookups > Input
D. Settings > Lookups > Upload
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/30376/how-to-display-the-contents-of-a-lookup-file.html

NEW QUESTION: 80
Select the statements that are true for timeline in Splunk (Choose four.):
A. Single click to see the result for particular time period.
B. You can click and drag across the bar for selecting the range.
C. You can hover your mouse for details like total events, time and date.
D. This is default view and you can't make any changes to it.
E. Timeline shows distribution of events specified in the time range in the form of bars.
Answer: A,B,C,E (LEAVE A REPLY)

NEW QUESTION: 81
You are able to create new Index in Data Input settings.
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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 !=404
D. status_code>=400
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 84
In the Search and Reporting app, which is a default selected field?
A. index
B. action
C. _time
D. host
Answer: C (LEAVE A REPLY)
In the Search and Reporting app, _time is a default selected field. This means that it is always displayed in the events list and table views, unless explicitly deselected. Other default selected fields are host, source, and sourcetype. Index and action are not default selected fields, but they can be added to the list of selected fields by clicking on All Fields4.

NEW QUESTION: 85
In the Search and Reporting app, which tab displays timecharts and bar charts?
A. Patterns
B. Visualization
C. Statistics
D. Events
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
Which of the following constraints can be used with the top command?
A. limit
B. useperc
C. fieldcount
D. addtotals
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
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: 88
Which time range picker configuration would return real-time events for the past 30 seconds?
A. Preset - Relative: 30-seconds ago

B. Real-time - Earliest: 30-seconds ago, Latest: Now
C. Advanced - Earliest: 30-seconds ago, Latest: Now
D. Relative - Earliest: 30-seconds ago, Latest: Now
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
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: 90
Which of the following is an accurate definition of fields within Splunk?
A. Inherent entities that exist in event data.
B. A searchable key/value pair in event data.
C. Values pulled exclusively from lookup tables.
D. A non-searchable name/value pair used while indexing data.
Answer: A (LEAVE A REPLY)
Explanation
Fields are searchable key/value pairs in event data. They allow you to specify criteria for your searches and filter out unwanted events. Fields can be extracted automatically by Splunk software during indexing or searching, or manually by users using various methods. Fields are not inherent entities that exist in event data, but rather interpretations of data by Splunk software or users. Fields are not values pulled exclusively from lookup tables, although lookup tables can be used to add fields to events based on existing fields. Fields are not non-searchable name/value pairs used while indexing data, but rather searchable attributes that can be used to refine searches5.

NEW QUESTION: 91
By default, all users have DELETE permission to ALL knowledge objects.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
Which of the following is a Splunk internal field?
A. _raw
B. index
C. host
D. _host
Answer: A (LEAVE A REPLY)

NEW QUESTION: 93
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: 94
Which of the following is a Splunk search best practice?
A. Filter as early as possible.
B. Use wildcards to return more search results.
C. Never specify more than one index.
D. Include as few search terms as possible.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following is an accurate definition of fields within Splunk?
A. Inherent entities that exist in event data.
B. A searchable key/value pair in event data.
C. Values pulled exclusively from lookup tables.
D. A non-searchable name/value pair used while indexing data.
Answer: (SHOW ANSWER)

Fields are searchable key/value pairs in event data. They allow you to specify criteria for your searches and filter out unwanted events. Fields can be extracted automatically by Splunk software during indexing or searching, or manually by users using various methods. Fields are not inherent entities that exist in event data, but rather interpretations of data by Splunk software or users. Fields are not values pulled exclusively from lookup tables, although lookup tables can be used to add fields to events based on existing fields. Fields are not non-searchable name/value pairs used while indexing data, but rather searchable attributes that can be used to refine searches5.

NEW QUESTION: 96
What will always appear in the Selected Fields list?
A. action
B. sourcetype
C. clientip
D. index
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
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: (SHOW ANSWER)
The search query sourcetype=access_combined would return events from the access_combined sourcetype, which is a predefined sourcetype in Splunk that matches the access-common or access-combined Apache logging formats1. The sourcetype field is case-sensitive, so using different capitalization such as Access_Combined or ACCESS_COMBINED would not match the exact sourcetype name2. The sourcetype field is also a default field that is added by the indexer when it indexes the data, so it does not need to be enclosed in quotation marks3.
Reference
List of pretrained source types
Search command syntax details
Basic searches and search results

NEW QUESTION: 98
Lookups allow you to overwrite your raw event.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Snapping rounds down to the nearest specified unit.
A. Yes
B. No
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 100
Which of the following file types is an option for exporting Splunk search results?
A. JSON
B. RTF
C. PDF
D. XLS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
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)

NEW QUESTION: 102
This search will return 20 results. SEARCH: error | top host limit = 20
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
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: 104
How can another user gain access to a saved report?
A. The owner of the report must clone the original report and save it to their user account
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 can edit permissions from the Edit dropdown
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following are functions of the stats command?
A. sum, avg. values
B. count, sum, less
C. count, sum, add
D. sum, values, table
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
Search Language Syntax in Splunk can be broken down into the following components. (Choose all that apply.)
A. Arguments
B. Pipe
C. Clause
D. Search term
E. Command
F. Functions
Answer: A,B,C,D,E,F (LEAVE A REPLY)

NEW QUESTION: 107
What is the main requirement for creating visualizations using the Splunk UI?
A. Your search must transform event data into Excel file format first.
B. Your search must transform event data into XML formatted data first.
C. Your search must transform event data into statistical data tables first.

D. Your search must transform event data into JSON formatted data first.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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: B (LEAVE A REPLY)
Explanation/Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-in- diffe.html

NEW QUESTION: 109
When writing searches in Splunk, which of the following is true about Booleans?
A. They must be in parentheses.
B. They must be in quotations.
C. They must be lowercase.
D. They must be uppercase.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following fields is stored with the events in the index?
A. sourcelp
B. location
C. source
D. user
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
You can view the search result in following format (Choose three.):
A. Raw
B. Pie Chart
C. Table
D. List
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Which statement is true about the topcommand?
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.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.0/SearchReference/Top

NEW QUESTION: 113
Which of the following is a metadata field assigned to every event in Splunk?
A. host
B. owner
C. bytes
D. action
Answer: A (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically

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

NEW QUESTION: 115
Snapping rounds down to the nearest specified unit.
A. Yes
B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Monitor option in Add Data provides _____.
A. Only continuous monitoring.
B. None of the above.
C. Only One-time monitoring.
D. Both One-time and continuous monitoring
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
All components are installed and administered in Splunk Enterprise on-premise.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 118
These users can create global knowledge objects. (Select all that apply.)
A. users
B. administrators
C. power users
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Splunk indexes the data on the basis of timestamps.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
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: B (LEAVE A REPLY)
Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Exportsearchresults

NEW QUESTION: 121
What user interface component allows for time selection?
A. Data source time statistics
B. Time range picker
C. Time summary
D. Search time picker
Answer: (SHOW ANSWER)

NEW QUESTION: 122
Which of the following is a false statement about Splunk dashboards?
A. Dashboards must have a unique dashboard ID within a permission's context.
B. Splunk dashboards consist of one or more panels displaying data visually in a useful way.
C. Splunk dashboards may not be directly created from search results without first creating a report.
D. Splunk dashboard panels can be populated by reports.
Answer: (SHOW ANSWER)
According to the Splunk documentation, dashboards are collections of views that you can use to visually analyze your dat a. You can create dashboards using simple XML, or use the Splunk Web framework to build custom dashboards using HTML, CSS, and JavaScript. Dashboards consist of one or more panels that display data in a variety of ways. You can use charts, tables, maps, single value indicators, and other visualizations to display your data. You can also add interactive elements to your dashboards, such as filters, drilldowns, and time range pickers, to make them more dynamic and user-friendly.
To create a dashboard panel from a search result, you can use the Save As button in the Search app and select Dashboard Panel. This will open a dialog box where you can choose an existing dashboard or create a new one, and specify the panel title and visualization type. You can also edit the panel properties and permissions before saving it to the dashboard. Alternatively, you can create a report from a search result and then add it to a dashboard as a panel. Reports are saved searches that include additional attributes such as a visualization type, permissions, and an optional description. You can create reports using the Save As button in the Search app and select Report. To add a report to a dashboard, you can use the Add to Dashboard button in the Reports listing page or in the report itself.
Dashboards must have a unique dashboard ID within a permission's context. This means that you cannot have two dashboards with the same ID in the same app or user space. The dashboard ID is used to reference the dashboard in URLs and XML files. You can specify the dashboard ID when you create a new dashboard using simple XML or the Splunk Web framework. If you do not specify an ID, Splunk software will generate one based on the dashboard title.

NEW QUESTION: 123
Which search string only returns events from hostWWW3?

A. host=WWW3
B. Host=WWW3
C. host=WWW*
Answer: (SHOW ANSWER)

NEW QUESTION: 124
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: 125
Which of the following searches would return only events that match the following criteria?
* Events are inside the main index
* The field status exists in the event
* The value in the status field does not equal 200
A. index==main status!==200
B. index=main NOT status=200
C. index==main NOT status==200
D. index-main status!=200
Answer: (SHOW ANSWER)
The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. It's a powerful language that allows you to perform advanced queries and extract meaningful insights from your data.
To query for events that match the criteria you specified, you would use the following KQL query:
index==main NOT status==200
This query will return all events that are inside the main index and have a status field, but the value of the status field does not equal 200. It is important to note that the "NOT" operator must be used in order to exclude events with a status value of 200.
By using the "NOT" operator, the query will return only events that do not match the specified criteria. This is useful for narrowing down search results to only those events that are relevant to the query.

NEW QUESTION: 126
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: A (LEAVE A REPLY)
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: 127
Which of the following searches will show the number of categoryId used by each host?
A. Sourcetype=access_* |sum(bytes) by host
B. Sourcetype=access_* |stats sum(categorylD) by host
C. Sourcetype=access_* |stats sum by host
D. Sourcetype=access_* |sum bytes by host
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following are Splunk premium enhanced solutions? (Choose three.)
A. Splunk User Behavior Analytics (UBA)
B. Splunk Enterprise Security (ES)
C. Splunk Analytics Security (AS)
D. Splunk IT Service Intelligence (ITSI)
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 129
What can be included in the All Fields option in the sidebar?
A. Dashboards
B. Field descriptions
C. Metadata only
D. Non-interesting fields
Answer: D (LEAVE A REPLY)

NEW QUESTION: 130
What type of search can be saved as a report?
A. Any search can be saved as a report
B. Only searches that generate visualizations
C. Only searches containing a transforming command
D. Only searches that generate statistics or visualizations
Answer: D (LEAVE A REPLY)
Only searches that generate statistics or visualizations can be saved as a report. These are searches that contain a transforming command, such as stats, chart, timechart, top, rare, etc.

Transforming commands create a data table from the events and enable various types of visualizations. Searches that do not contain a transforming command can only be saved as an alert or a dashboard panel. Reference: Splunk Core User Certification Exam Study Guide, page 35.

NEW QUESTION: 131
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. count-by(field)
C. count(field)
D. dc(field)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
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/etc/scripts
B. $SPLUNK_HOME/etc/scripts/bin
C. $SPLUNK_HOME/bin/scripts
D. $SPLUNK_HOME/etc/scripts
Answer: C (LEAVE A REPLY)

NEW QUESTION: 133
Selected fields are a set of configurable fields displayed for each event.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following statements about case sensitivity is true?
A. Both field names and field values ARE NOT case sensitive.
B. Field values ARE case sensitive; field names ARE NOT.
C. Field names ARE case sensitive; field values are NOT.
D. Both field names and field values ARE case sensitive.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
Prefix wildcards might cause performance issues.
A. True
B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following file types is an option for exporting Splunk search results?
A. RTF
B. XLS
C. JSON
D. PDF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
You can change the App context in Input setting.
A. No
B. Yes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Snapping rounds down to the nearest specified unit.
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 139
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: 140
How do you add or remove fields from search results?
A. Use fields +to add and fields -to remove.
B. Use table +to add and table -to remove.
C. Use fields Plus to add and fields Minus to remove.
D. Use field +to add and field -to remove.
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Put query into separate lines where | (Pipes) are used by selecting following options.
A. Shift + Enter
B. Space + Enter
C. ALT + Enter
D. CTRL + Enter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
Which of the following is a metadata field assigned to every event in Splunk?
A. host
B. bytes
C. owner
D. action
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
Which of the following is the best way to create a report that shows the last 24 hours of events?
A. Use earliest=-1d@d latest=@d
B. Use the time range picket to select "Yesterday"
C. Set a real-time search over a 24-hour window
D. Use the time range picker to select "Last 24 hours"
Answer: D (LEAVE A REPLY)

NEW QUESTION: 144
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: 145
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: 146
What are the two most efficient search filters?
A. _time and host
B. _time and index
C. host and sourcetype
D. index and sourcetype
Answer: B (LEAVE A REPLY)
This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1. The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2. The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.

NEW QUESTION: 147
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 at least 20% of the events
C. A field that appears in every event
D. A field that appears in the top 10 events
Answer: (SHOW ANSWER)