ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

A. count stats vendor_action
B. count stats (vendor_action)
C. stats count (vendor_action)
D. stats vendor_action (count)

Answer: C

Explanation:

The stats command calculates statistics based on fields in the events. The count function counts the number of events that match the criteria. The syntax is stats count (field_name), where field_name is the name of the field that contains the value to be counted. In this case, vendor_action is the field name, so stats count (vendor_action) is the correct syntax. Reference: Splunk Core User Certification Exam Study Guide, page 23.

Question: 2

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: D

Explanation:

The fields sidebar in Splunk shows the default fields and the interesting fields for the events that match your search. The default fields are host, source, and sourcetype, which are extracted for every event at index time. The interesting fields are fields that appear in at least 20% of the events in your search results. You can also select additional fields to display in the fields sidebar1.

By default, the index field is not listed in the fields sidebar, because it is not a default field nor an interesting field. The index field is a metadata field that indicates which index the event belongs to. Metadata fields are not extracted from the event data, but are added by the indexer as part of the indexing process. Metadata fields are not shown in the fields sidebar, but you can use them in your search queries2.

Therefore, among the four options, only sourcetype would be listed in the fields sidebar under interesting fields by default.

Reference

Use fields to search

About default fields

Question: 3

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

Explanation:

When looking at a dashboard panel that is based on a report, you cannot modify the search string in the panel, but you can change and configure the visualization. This is because the dashboard panel inherits the search string from the report, and any changes to the search string will affect the report as well. However, you can customize the visualization settings for the dashboard panel without affecting the report. Reference: Splunk Core User Certification Exam Study Guide, page 37.

Question: 4

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

Explanation:

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.

Question: 5

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

Explanation:

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.

Question: 6

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: C

Explanation:

Question: 7

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

A. action+purchase
B. action=purchase
C. action | purchase
D. action equal purchase

Answer: B

Explanation:

Question: 8

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: D

Explanation:

Question: 9

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

A. Parentheses
B. @ or # symbols
C. Quotation marks
D. Relational operators such as =, <, or >

Answer: D

Explanation:

Question: 10

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: D

Explanation:

Question: 11

Which of the following are functions of the stats command?

A. count, sum, add
B. count, sum, less
C. sum, avg, values
D. sum, values, table

Answer: C

Explanation:

Question: 12

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: D

Explanation:

Question: 13

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: A

Explanation:

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

Question: 14

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

A. Saving the item to a report
B. Adding the item to the search.
C. Adding the item to a dashboard
D. Saving the search to a JSON file.

Answer: A

Explanation:

Question: 15

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

A. dedup
B. rename
C. sort -
D. fields +

Answer: A

Explanation:

Question: 16

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: D

Explanation:

Question: 17

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

A. Line charts are optimal for single and multiple series.
B. Line charts are optimal for single series when using Fast mode.
C. Line charts are optimal for multiple series with 3 or more columns.
D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Answer: C

Explanation:

Question: 18

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

Explanation:

Question: 19

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

A. user
B. source
C. location
D. sourcelp

Answer: B

Explanation:

Question: 20

Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

A. Save the search as a report and use it in multiple dashboards as needed
B. Save the search as a dashboard panel for each dashboard that needs the data
C. Save the search as a scheduled alert and use it in multiple dashboards as needed
D. Export the results of the search to an XML file and use the file as the basis of the dashboards

Answer: A

Explanation:

Question: 21

What must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.
B. The contents of the lookup file must be copied and pasted into the search bar.
C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer: C

Explanation:

Question: 22

What is a suggested Splunk best practice for naming reports?

A. Reports are best named using many numbers so they can be more easily sorted.
B. Use a consistent naming convention so they are easily separated by characteristics such as group and object.
C. Name reports as uniquely as possible with no overlap to differentiate them from one another.
D. Any naming convention is fine as long as you keep an external spreadsheet to keep track.

Answer: B

Explanation:

Question: 23

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

A. Indexer
B. Forwarder
C. Search head
D. Deployment server

Answer: B

Explanation:

Question: 24

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: D

Explanation:

Question: 25

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

Explanation:

Question: 26

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

A. limit, count
B. limit, showpercent
C. limits, countfield
D. showperc, countfield

Answer: B

Explanation:

Question: 27

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

A. To group the results by one or more fields.
B. To compute numerical statistics on each field.
C. To specify how the values in a list are delimited.
D. To partition the input data based on the split-by fields.

Answer: A

Explanation:

Question: 28

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

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

C. We need more information: we cannot tell without knowing the time range
D. We need more information a search cannot be run without specifying an index

Answer: B

Explanation:

Question: 29

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

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

Answer: B

Explanation:

Question: 30

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: B

Explanation:

Question: 31

What does the stats command do?

A. Automatically correlates related fields
B. Converts field values into numerical values
C. Calculates statistics on data that matches the search criteria
D. Analyzes numerical fields for their ability to predict another discrete field

Answer: C

Explanation:

Question: 32

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 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

Explanation:

Question: 33

Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
B. Alerts are based on searches and when triggered will only send an email notification.
C. Alerts are based on searches and require cron to run on scheduled interval.
D. Alerts are based on searches that are run exclusively as real-time.

Answer: A

Explanation:

Question: 34

What can be configured using the Edit Job Settings menu?

A. Export the results to CSV format
B. Add the Job results to a dashboard
C. Schedule the Job to re-run in 10 minutes
D. Change Job Lifetime from 10 minutes to 7 days.

Answer: D

Explanation:

Question: 35

Which command is used to validate a lookup file?

A. | lookup products.csv
B. inputlookup products.csv
C. I inputlookup products.csv
D. | lookup definition products.csv

Answer: C

Explanation:

Question: 36

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

result set?

A. dc(field)
B. count(field)
C. count-by(field)
D. distinct-count(field)

Answer: A

Explanation:

Question: 37

What user interface component allows for time selection?

A. Time summary
B. Time range picker
C. Search time picker
D. Data source time statistics

Answer: B

Explanation:

Question: 38

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

Explanation:

Question: 39

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

A. Add an output.
B. Export a dashboard panel.
C. Modify the chart type displayed in a dashboard panel.
D. Drag a dashboard panel to a different location on the dashboard.

Answer: D

Explanation:

Question: 40

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

A. index=*
B. index=web OR index=s*
C. (index=web OR index=sales)
D. *index=sales AND index=web*

Answer: C

Explanation:

Question: 41

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

A. time

B. _time
C. EventTime
D. timestamp

Answer: B

Explanation:

Question: 42

Which statement is true about the top command?

A. It returns the top 10 results
B. It displays the output in table format
C. It returns the count and percent columns per row
D. All of the above

Answer: D

Explanation:

Question: 43

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: D

Explanation:

Question: 44

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: C

Explanation:

Question: 45

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: A

Explanation:

Question: 46

What is the primary use for the rare command1?

A. To sort field values in descending order
B. To return only fields containing five or 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: C

Explanation:

Question: 47

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

Explanation:

Question: 48

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

A. action
B. clientip
C. categoryId
D. sourcetype

Answer: D

Explanation:

Question: 49

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

Explanation:

Question: 50

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

A. top
B. stats
C. table
D. percent

Answer: A

Explanation:

Question: 51

Which of the following describes lookup files?

A. Lookup fields cannot be used in searches
B. Lookups contain static data available in the index

C. Lookups add more fields to results returned by a search
D. Lookups pull data at index time and add them to search results

Answer: B

Explanation:

Question: 52

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

A. Red
B. Blue
C. Orange
D. Highlighted

Answer: B

Explanation:

Question: 53

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 Plus to add and fields Minus to remove.

Answer: C

Explanation:

Question: 54

What are the steps to schedule a report?

A. After saving the report, click Schedule.
B. After saving the report, click Event Type.
C. After saving the report, click Scheduling.
D. After saving the report, click Dashboard Panel.

Answer: A

Explanation:

Question: 55

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

A. 10 Minutes

B. 15 Minutes
C. 1 Day
D. 7 Days

Answer: A

Explanation:

Question: 56

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

A. OR
B. AND
C. NOT
D. NAND

Answer: B

Explanation:

Question: 57

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

Explanation:

Question: 58

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

A. |
B. $
C. !
D. ,

Answer: D

Explanation:

Question: 59

Which search string is the most efficient?

A. "failed password"
B. ''failed password"*
C. index=* "failed password"
D. index=security "failed password"

Answer: D

Explanation:

Question: 60

Which search string matches only events with the status_code of 4:4?

A. status_code !=404
B. status_code>=400
C. status_code<=404
D. status code>403 status_code<405

Answer: D

Explanation:

Question: 61

This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev
B. dev
C. count deviation
D. by standarddev

Answer: A

Explanation:

Question: 62

Which of the following commands will show the maximum bytes?

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

Answer: C

Explanation:

Question: 63

This search will return 20 results. SEARCH: error | top host limit = 20
A.True
B.False

Answer: A

Explanation:

Question: 64

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_* |sum(bytes) by host
D.Sourcetype=access_* |stats sum by host

Answer: B

Explanation:

Question: 65

This clause is used to group the output of a stats command by a specific name.

A.Rex
B.As
C.List
D.By

Answer: D

Explanation:

Question: 66

This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)
B. Eval by X
C. Fields(X)
D. Values(X)

Answer: A

Explanation:

Question: 67

When a search returns ¸ you can view the results as a list.

A. a list of events
B. transactions
C. statistical values

Answer: C

Explanation:

Question: 68

Clicking a SEGMENT on a chart, .

A. drills down for that value

B. highlights the field value across the chart
C. adds the highlighted value to the search criteria

Answer: C

Explanation:

Question: 69

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

A. inputlookup
B. lookup

Answer: B

Explanation:

Question: 70

C. . Lookups can be private for a user.

A. True
B. False

Answer: A

Explanation:

Question: 71

In automatic lookup definitions, the fields are those that are not in the event data.

A. input
B. output

Answer: B

Explanation:

Question: 72

What is the correct order of steps for creating a new lookup?

1. Configure the lookup to run automatically
2. Create the lookup table

3. Define the lookup

A. 2, 1, 3
B. 1, 2, 3
C. 2, 3, 1
D. 3, 2, 1

Answer: C

Explanation:

Question: 73

The command shown here does witch of the following: Command: |outputlookup products.csv

A.Writes search results to a file named products.csv

A. Returns the contents of a file named products.csv

Answer: A

Explanation:

Question: 74

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. 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
E. Lookup have a 10mg maximum size limit

Answer: E

Explanation:

Question: 75

Lookups allow you to overwrite your raw event.

A.True

B.False

Answer: A

Explanation:

Question: 76

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.Timestamp

D.Input filed

Answer: D

Explanation:

Question: 77

By default, all users have DELETE permission to ALL knowledge objects.

A. True
B. False

Answer: B

Explanation:

Question: 78

These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Answer: B, C

Explanation:

Question: 79

All users by default have WRITE permission to ALL knowledge objects.

A.True
B.False

Answer: B

Explanation:

Question: 80

Creating Data Models:
Object ATTRIBUTES do not define

A. a base search for the object
B. fields for the object

Answer: A

Explanation:

Question: 81

Creating Data Models:
Fields associated with a data set are known as

A. Attributes

B. Constraints

Answer: A

Explanation:

Question: 82

Splunk Components:

Which of the following are responsible for reducing search results?

A. search heads
B. indexers
C. forwarders

Answer: B

Explanation:

Question: 83

Splunk Components:

Which of the following are responsible for parsing incoming data and storing data on disc?

A. forwarders
B. indexers
C. search heads

Answer: B

Explanation:

Question: 84

This is what Splunk uses to categorize the data that is being indexed.

A. sourcetype
B. index
C. source
D. host

Answer: A

Explanation:

Question: 85

This is what Splunk uses to categorize the data that is being indexed.

A.Host
B.Sourcetype
C.Index
D.Source

Answer: B

Explanation:

Question: 86

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: B

Explanation:

Question: 87

It is not possible for a single instance of Splunk to manage the input, parsing and indexing of machine.

A. True
B.False

Answer: B

Explanation:

Question: 88

By default search results are not returned in order.

A.Chronological
B. Reverser chronological
C.ASCIE
D.Alphabetical

Answer: A, D

Explanation:

Question: 89

The stats command will create a by default.

A.Table
B.Report

C.Pie chart

Answer: A

Explanation:

Question: 90

Which is not a comparison operator in Splunk

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

Answer: E

Explanation:

Question: 91

Which search string only returns events from hostWWW3?

A. B. host=WWW3
B. C. host=WWW*
C. D. Host=WWW3

Answer: B

Explanation:

Question: 92

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

A. The lookup command must be used.
B. The lookup definition must be created.
C. The lookup file must be uploaded to Splunk.
D. The lookup file must be verified using the inputlookup command.

Answer: B

Explanation:

Question: 93

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

A. They must be lowercase.

B. They must be uppercase.
C. They must be in quotations.
D. They must be in parentheses.

Answer: B

Explanation:

Question: 94

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

A. limit
B. useperc
C. addtotals
D. fieldcount

Answer: A

Explanation:

Question: 95

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

Explanation:

Question: 96

How can search results be kept longer than 7 days?

A. By scheduling a report.
B. By creating a link to the job.
C. By changing the job settings.
D. By changing the time range picker to more than 7 days.

Answer: A

Explanation:

Question: 97

Which of the following is a Splunk search best practice?

A. Filter as early as possible.
B. Never specify more than one index.
C. Include as few search terms as possible.
D. Use wildcards to return more search results.

Answer: A

Explanation:

Question: 98

How are events displayed after a search is executed?

A. In chronological order.
B. Randomly by default.
C. In reverse chronological order.
D. Alphabetically according to field name.

Answer: C

Explanation:

Question: 99

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: B

Explanation:

Question: 100

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

A. lookup

B. csvlookup

C. inputlookup
D. outputlookup

Answer: C

Explanation:

Question: 101

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

Explanation:

Question: 102

What is one benefit of creating dashboard panels from reports?

A. Any newly created dashboard will include that report.
B. There are no benefits to creating dashboard panels from reports.
C. It makes the dashboard more efficient because it only has to run one search string.
D. Any change to the underlying report will affect every dashboard that utilizes that report.

Answer: C

Explanation:

Question: 103

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: B

Explanation:

Question: 104

What does the rare command do?

A. Returns the least common field values of a given field in the results.
B. Returns the most common field values of a given field in the results.
C. Returns the top 10 field values of a given field in the results.
D. Returns the lowest 10 field values of a given field in the results.

Answer: A

Explanation:

Question: 105

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

A. OR
B. NOT
C. AND
D. XOR

Answer: C

Explanation:

Question: 106

What does the values function of the stats command do?

A. Lists all values of a given field.
B. Lists unique values of a given field.
C. Returns a count of unique values for a given field.
D. Returns the number of events that match the search.

Answer: B

Explanation:

Question: 107

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

Explanation:

Question: 108

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

A. #
B. %
C. a
D. a#

Answer: B

Explanation:

Question: 109

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

Explanation:

Question: 110

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

A. Time
B. Fast mode
C. Sourcetype
D. Selected Fields

Answer: A

Explanation:

Question: 111

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

Explanation:

Question: 112

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

A. PDF
B. JSON
C. XLS
D. RTF

Answer: B

Explanation:

Question: 113

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 as “Event Count”
C. index=security failure | stats count by “Event Count”
D. index=security failure | stats dc(count) as “Event Count”

Answer: B

Explanation:

Question: 114

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: A

Explanation:

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

Question: 115

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

Explanation:

Question: 116

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

A. A number to the right of the field name.
B. A # symbol to the left of the field name.
C. A lowercase n to the left of the field name.
D. A lowercase n to the right of the field name.

Answer: B

Explanation:

Question: 117

What is the primary use for the rare command?

A. To sort field values in descending order.
B. To return only fields containing five of fewer values.
C. To find the least common values of a field in a dataset.
D. To find the fields with the fewest number of values across a dataset.

Answer: C

Explanation:

Question: 118

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

A. Index
B. Search Head
C. Indexer
D. Forwarder

Answer: C

Explanation:

Question: 119

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

A. True
B. False

Answer: A

Explanation:

Question: 120

Which component of Splunk is primarily responsible for saving data?

A. Search Head
B. Heavy Forwarder
C. Indexer
D. Universal Forwarder

Answer: C

Explanation:

Question: 121

Universal forwarder is recommended for forwarding the logs to indexers.

A. False
B. True

Answer: B

Explanation:

Question: 122

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

A. Designed to cater numerous use cases and empower Splunk.
B. We can not install Splunk App.
C. Allows multiple workspaces for different use cases/user roles.
D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

Answer: A, C, D

Explanation:

Question: 123

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

Explanation:

Question: 124

What is Splunk?

A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
B. Database management tool.
C. Security Information and Event Management (SIEM).
D. Cloud based application that help in analyzing logs.

Answer: A

Explanation:

Question: 125

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

A. False
B. True

Answer: B

Explanation:

Question: 126

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

A. True
B. False

Answer: A

Explanation:

Question: 127

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

A. Forwarders
B. Indexer
C. Heavy Forwarders
D. Search head

Answer: D

Explanation:

Question: 128

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

A. True
B. False

Answer: A

Explanation:

Question: 129

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

Explanation:

Question: 130

Which is the default app for Splunk Enterprise?

A. Splunk Enterprise Security Suite
B. Searching and Reporting
C. Reporting and Searching
D. Splunk apps for Security

Answer: B

Explanation:

Question: 131

What kind of logs can Splunk Index?

A. Only A, B
B. Router and Switch Logs
C. Firewall and Web Server Logs
D. Only C
E. Database logs
F. All firewall, web server, database, router and switch logs

Answer: F

Explanation:

Question: 132

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

A. False
B. True

Answer: B

Explanation:

Question: 133

Splunk shows data in

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Answer: B

Explanation:

Question: 134

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

A. =
B. >
C. !
D. *

Answer: D

Explanation:

Question: 135

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: C

Explanation:

Question: 136

Prefix wildcards might cause performance issues.

A. False
B. True

Answer: B

Explanation:

Question: 137

Machine data can be in structured and unstructured format.

A. False
B. True

Answer: B

Explanation:

Question: 138

Field names are case sensitive.

A. True
B. False

Answer: A

Explanation:

Question: 139

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

A. True
C. False

Answer: A

Explanation:

Question: 140

How many main user roles do you have in Splunk?

A. 2
B. 4
C. 1
D. 3

Answer: D

Explanation:

Question: 141

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

A. Splunk User Behavior Analytics (UBA)
B. Splunk IT Service Intelligence (ITSI)
C. Splunk Enterprise Security (ES)
D. Splunk Analytics Security (AS)

Answer: A, B, C

Explanation:

Question: 142

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

A. False
B. True

Answer: B

Explanation:

Question: 143

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

A. True
C. False

Answer: A

Explanation:

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.3/SearchTutorial/Usefieldstosearch

Question: 144

Field values are case sensitive.

A. True
B. False

Answer: B

Explanation:

Question: 145

Splunk indexes the data on the basis of timestamps.

A. True
B. False

Answer: A

Explanation:

Question: 146

is the default web port used by Splunk.

A. 8089
B. 8000
C. 8080

D. 443

Answer: B

Explanation:

Question: 147

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

A. Can be accessed by Apps > Search & Reporting.
B. Provides default interface for searching and analyzing logs.
C. Enables the user to create knowledge object, reports, alerts and dashboards.
D. It only gives us search functionality.

Answer: A, B, C

Explanation:

Question: 148

Parsing of data can happen both in HF and Indexer.

A. Only HF
B. No
C. Yes

Answer: C

Explanation:

Question: 149

Monitor option in Add Data provides

A. Only continuous monitoring.
B. Only One-time monitoring.
C. None of the above.
D. Both One-time and continuous monitoring

Answer: D

Explanation:

Question: 150

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

A. False
B. True

Answer: B

Explanation:

Question: 151

You can on-board data to Splunk using following means (Choose four.):

A. Props
B. CLI
C. Splunk Web
D. savedsearches.conf
E. Splunk apps and add-ons
F. indexes.conf
G. inputs.conf
H. metadata.conf

Answer: B C, E, G

Explanation:

Question: 152

Data sources being opened and read applies to:

A. None of the above
B. Indexing Phase
C. Parsing Phase
D. Input Phase
E. License Metering

Answer: D

Explanation:

Question: 153

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

A. Indexing
B. Searching
C. Parsing
D. Settings
E. Input

Answer: A, C, E

Explanation:

Question: 154

Splunk automatically determines the source type for major data types.

A. False
B. True

Answer: B

Explanation:

Question: 155

Parsing of data can happen both in HF and UF.

A. Yes
B. No

Answer: B

Explanation:

Question: 156

Splunk index time process can be broken down into phases.

A. 3
B. 2
C. 4
D. 1

Answer: A

Explanation:

Question: 157

In monitor option you can select the following options in GUI.

A. Only HTTP Event Collector (HEC) and TCP/UDP
B. None of the above
C. Only TCP/UDP
D. Only Scripts
E. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

Explanation:

Question: 158

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

A. No
B. Yes

Answer: B

Explanation:

Question: 159

Where does Licensing meter happen?

A. Indexer
B. Parsing
C. Heavy Forwarder
D. Input

Answer: A

Explanation:

Question: 160

Matching search terms are highlighted.

A. Yes
B. No

Answer: A

Explanation:

Question: 161

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

A. No
B. Yes

Answer: B

Explanation:

Question: 162

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

A. No
B. Yes

Answer: B

Explanation:

Question: 163

Every Search in Splunk is also called

A. None of the above
B. Job
C. Search Only

Answer: B

Explanation:

Question: 164

Matching of parentheses is a feature of Splunk Assistant.

A. No
B. Yes

Answer: B

Explanation:

Question: 165

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

A. No
B. Yes

Answer: B

Explanation:

Question: 166

What is Search Assistant in Splunk?

A. It is only available to Admins.
B. Such feature does not exist in Splunk.
C. Shows options to complete the search string

Answer: C

Explanation:

Question: 167

@ Symbol can be used in advanced time unit option.

A. No
B. Yes

Answer: B

Explanation:

Question: 168

The new data uploaded in Splunk are shown in

A. Real-time
B. 10 Minutes
C. Overnight Download
D. 30 Minutes

Answer: A

Explanation:

Question: 169

You can use the following options to specify start and end time for the query range:

A. earliest=
B. latest=
C. beginning=
D. ending=
E. All the above
F. Only 3rd and 4th

Answer: F

Explanation:

Question: 170

The default host name used in Inputs general settings can not be changed.

A. False
B. True

Answer: A

Explanation:

Question: 171

Events in Splunk are automatically segregated using data and time.

A. Yes
B. No

Answer: A

Explanation:

Question: 172

You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

Explanation:

Question: 173

Splunk Parses data into individual events, extracts time, and assigns metadata.

A. False
B. True

Answer: B

Explanation:

Question: 174

Which of the statements is correct regarding click and drag option in timeline?

A. The new result after selecting the range by dragging filters the events and displays the most recent first.
B. There is no functionality like click and drag in Splunk's timeline.
C. Using this option executes a new query.
D. This doesn't execute a new query

Answer: A

Explanation:

Question: 175

Which symbol is used to snap the time?

A. @
B. &
C. *
D. #

Answer: A

Explanation:

Question: 176

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

A. Zoom to selection: Narrows the time range and re-executes the search.
B. Zoom to selection: Narrows the time range and doesn't re-executes the search.
C. Format Timeline: Hides or shows the timeline in different views.
D. Zoom-Out: Expands the time focus and doesn't re-executes the search.
E. Zoom-out: Expands the time focus and re-executes the search.

Answer: A, C, E

Explanation:

Question: 177

There are three different search modes in Splunk (Choose three.):

A. Automatic
B. Smart
C. Fast
D. Verbose

Answer: B, C, D

Explanation:

Question: 178

Select the statements that are true for timeline in Splunk (Choose four.):

A. Timeline shows distribution of events specified in the time range in the form of bars.
B. Single click to see the result for particular time period.
C. You can click and drag across the bar for selecting the range.
D. This is default view and you can't make any changes to it.
E. You can hover your mouse for details like total events, time and date.

Answer: A, B, C, E

Explanation:

Question: 179

Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

A. Open new search.
B. Exclude the item from search.
C. None of the above.
D. Add the item to search

Answer: A, B, D

Explanation:

Question: 180

You can view the search result in following format (Choose three.):

A. Table
B. Raw
C. Pie Chart
D. List

Answer: A, B, D

Explanation:

Question: 181

Snapping rounds down to the nearest specified unit.

A. Yes
B. No

Answer: A

Explanation:

Question: 182

Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts
B. Sourcetypes
C. Sources
D. Indexes

Answer: A, B, D

Explanation:

Question: 183

What options do you get after selecting timeline? (Choose four.)

A. Zoom to selection
B. Format Timeline
C. Deselect
D. Delete
E. Zoom Out

Answer: A, B, C, E

Explanation:

Question: 184

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: A

Explanation:

Question: 185

Can you stop or pause the searching?

A. No
B. Yes

Answer: B

Explanation:

Question: 186

You can also specify a time range in the search bar. You can use the following for beginning and ending for a time range (Choose two.):

A. Not possible to specify time manually in Search query
B. end=
C. start=
D. earliest=

E. latest=

Answer: D, E

Explanation:

Question: 187

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

A. h
B. day
C. mon
D. yr
E. y
F. w
G. week
H. d
I. s
J. m

Answer: A, C, E, F, H, I, J

Explanation:

Question: 188

Interesting fields are the fields that have at least 20% of resulting fields.

A. True
B. False

Answer: A

Explanation:

Question: 189

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. Not possible.
C. Only CLI changes will enable it.
D. Click Settings -> Find field option -> Drop down select field -> enable selected field -> check now field should be visible in the list of selected fields.

Answer: A

Explanation:

Question: 190

Field names are case sensitive and field value are not.

A. True
B. False

Answer: A

Explanation:

Question: 191

!= and NOT are same arguments.

A. True
B. False

Answer: B

Explanation:

Question: 192

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

Explanation:

Question: 193

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.
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: C

Explanation:

Question: 194

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. Yes
B. No

Answer: B

Explanation:

Question: 195

Select the best options for "search best practices" in Splunk: (Choose five.)

A. Select the time range always.
B. Try to specify index values.
C. Include as many search terms as possible.
D. Never select time range.
E. Try to use * with every search term.
F. Inclusion is generally better than exclusion.
G. Try to keep specific search terms.

Answer: A, B, C, F, G

Explanation:

Question: 196

The better way of writing search query for index is:

A. index=a index=b
B. (index=a OR index=b)
C. index=(a & b)
D. index = a, b

Answer: B

Explanation:

Question: 197

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

Explanation:

Question: 198

Fields are searchable key value pairs in your event data.

A. True
B. False

Answer: A

Explanation:

Question: 199

Selected fields are a set of configurable fields displayed for each event.

A. True
B. False

Answer: A

Explanation:

Question: 200

Following are the time selection option while making search: (Choose all that apply.)

A. Date & Time Range
B. Advanced
C. Date Range
D. Presets
E. Relative

Answer: B

Explanation:

Question: 201

When saving a search directly to a dashboard panel instead of saving as a report first, which of the following is created?

A. Cloned panel
B. Inline panel
C. Report panel
D. Prebuilt panel

Answer: C

Explanation:

Question: 202

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: D

Explanation:

Explanation/Reference:

Reference: https://answers.splunk.com/answers/329699/why-does-my-search-head-cluster-captain- start-dele-1.html

Question: 203

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

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/search

Question: 204

Which of the following reports is available in the Fields window?

A. Top values by time
B. Rare values by time
C. Events with top value fields
D. Events with rare value fields

Answer: C

Explanation:

Question: 205

In the Search and Reporting app, which tab displays timecharts and bar charts?

A. Events
B. Patterns
C. Statistics
D. Visualization

Answer: D

Explanation:

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Aboutreportingcommands

Question: 206

What will always appear in the Selected Fields list?

A. index
B. action
C. clientip
D. sourcetype

Answer: D

Explanation:

Question: 207

What is the correct way to use a time range specifier in the search bar so that the search looks back 2 hours?

A. latest=-2h
B. earliest=-2h
C. latest=-2hour@d
D. earliest=-2hour@d

Answer: B

Explanation:

Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Specifytimemodifiersinyoursearch

Question: 208

Which of the following is a Splunk internal field?

A. _raw
B. host
C. _host

D. index

Answer: A

Explanation:

Question: 209

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

Explanation:

Explanation/Reference:

Reference: https://answers.splunk.com/answers/610038/understanding-command-in-search.html

Question: 210

Which of the following is the most efficient search?

A. index=* “failed password”
B. “failed password” index=*
C. (index=* OR index=security) “failed password”
D. index=security “failed password”

Answer: A

Explanation:

Question: 211

Which of the following is a correct way to limit search results to display the 5 most common values of a field?

A. | rare top=5
B. | top rare=5
C. | top limit=5
D. | rare limit=5

Answer: C

Explanation:

Question: 212

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

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

Answer: C

Explanation:

Question: 213

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: C

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata

Question: 214

Assuming a user has the capability to edit reports, which of the following are editable?

A. Acceleration, schedule, permissions
B. The report's name, schedule, permissions
C. The report's name, acceleration, schedule
D. The report's name, acceleration, permissions

Answer: B

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Report/Createandeditreports

Question: 215

Which of the following is a metadata field assigned to every event in Splunk?

A. host
B. owner
C. bytes
D. action

Answer: A

Explanation:

Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically

Question: 216

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

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.

Question: 217

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

Explanation:

Question: 218

When is the pipe character, I, used in search strings?

A. Before clauses. For example: stats sum(bytes) | by host
B. Before commands. For example: | stats sum(bytes) by host
C. Before arguments. For example: stats sum| (bytes) by host
D. Before functions. For example: stats |sum(bytes) by host

Answer: B

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes_and_escaping_characters

Question: 219

How can results from a specified static lookup file be displayed?

A. lookup command
B. inputlookup command
C. Settings > Lookups > Input
D. Settings > Lookups > Upload

Answer: B

Explanation:

Question: 220

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: C

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch

Question: 221

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 hours
C. All search jobs are saved for 10 weeks
D. All search jobs are saved for 10 minutes

Answer: D

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Extendjoblifetimes

Question: 222

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

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

Explanation:

Explanation/Reference:

Reference: https://answers.splunk.com/answers/41928/add-a-lookup-csv-colum-information-to-the-results-ofa-inputlookup-search.html

Question: 223

When is an alert triggered?

A. When Splunk encounters a syntax error in a search
B. When a trigger action meets the predefined conditions
C. When an event in a search matches up with a data model
D. When results of a search meet a specifically defined condition

Answer: D

Explanation:

Explanation/Reference:

Reference:

https://books.google.com.pk/books?id=sNwkBQAAQBAJ&pg=PT525&lpg=PT525&dq=splunk+alert+triggered+When+results+of+a+search+meet+a+specifically+defined+condition&source=bl&ots=avtEx5luxo&sig=ACfU3U1ZVob_j9nU243Te2vhqwxl3YvJuA&hl=en&sa=X &ved=2ahUKEwjm48rmkfXoAhUlMewKHb_FAbkQ6AEwB3oECBYQJg

Question: 224

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

Explanation:

Explanation/Reference:

Reference: https://www.edureka.co/blog/splunk-architecture/

Question: 225

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

Explanation:

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Changethesearchmode

Question: 226

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

Explanation:

Explanation/Reference:

Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-indiffe.html

Question: 227

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: C

Explanation:

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.

Question: 228

Given the following SPL search, how many rows of results would you expect to be returned by default? index=security sourcetype=linux_secure (fail* OR invalid) I top src ip

A. 10
B. 50
C. 100
D. 20

Answer: A

Explanation:

The SPL search specified above will return 10 rows of results by default, as the "top" command specifies a limit of 10 results. The query will search for all events in the security index with a sourcetype of linuxsecure that contain either the terms fail* or invalid and will display the top 10 results according to the src_ip field.

Question: 229

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: D

Explanation:

The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. To query for events that are found in the index named security, you would use the following KQL query: index=Security

This query will return all events that are found in the security index. It is important to note that the "=" operator must be used in order to match the exact index name.

Question: 230

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

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.

Question: 231

When using the top command in the following search, which of the following will be true about the results?

index="main" sourcetype="access_*" action="purchase" | top 3 statusCode by user showperc=f countfield=status_code_count

A. The search will fail. The proper top command format is top limit=3 instead of top 3.

B. The top three most common values in statusCode will be displayed for each user.

C. Only the top three overall most common values in statusCode will be displayed.

D. The percentage field will be displayed in the results.

Answer: B

Explanation:

The top command returns the most common values of a field and their count. By using the by clause, you can group the results by another field. In this case, the top command will return the top three most common values in statusCode for each user. The showperc=f option will suppress the percentage column in the output. The countfield option will rename the count column to status_code_count2.

Question: 232

By default, which role contains the minimum permissions required to have write access to Splunk alerts?

A. User

B. Alerting

C. Power

D. Admin

Answer: C

Explanation:

The Power role contains the minimum permissions required to have write access to Splunk alerts. The User role can only view alerts created by others, but cannot create or modify them. The Alerting role is not a default role in Splunk, but a custom one that can be created by an administrator. The Admin role has write access to Splunk alerts, but also has many other permissions that are not necessary for alerting3.

Question: 233

In the Search and Reporting app, which is a default selected field?

A. index

B. action

C. _time

D. host

Answer: C

Explanation:

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.

Question: 234

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

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.

Question: 235

The four types of Lookups that Splunk provides out-of-the-box are External, KV Store, Geospatial and which of the following?

A. Correlated

B. File-based

C. Total

D. Segmented

Answer: B

Explanation:

The four types of lookups that Splunk provides out-of-the-box are file-based, external, KV Store, and geospatial. File-based lookups use CSV files to map fields from your data to fields in the external table. External lookups use Python scripts or binary executables to populate your events with field values from an external source. KV Store lookups use a key-value store to map fields from your data to fields in the external table. Geospatial lookups use KMZ or KML files to match location coordinates in your events to geographic feature collections1.

Question: 236

When refining search results, what is the difference in the time picker between real-time and relative time ranges?

A. Real-time searches happen instantly, while relative searches happen at a scheduled time.

B. Real-time searches display results from a rolling time window, while relative searches display results from a set length of time.

C. Real-time searches run constantly in the background, while relative searches only run when certain criteria are met.

D. Real-time represents events that have happened in a set time window, while relative will display results from a rolling time window.

Answer: B

Explanation:

The difference between real-time and relative time ranges in the time picker is that real-time searches display results from a rolling time window, such as the last 15 minutes, while relative searches display results from a set length of time, such as yesterday or last week. Real-time searches do not happen instantly, but rather update periodically based on the refresh interval. Relative searches do not happen at a scheduled time, but rather when the user runs them. Real-time searches do not

run constantly in the background, but rather when the user starts them. Real-time searches do not represent events that have happened in a set time window, but rather events that are happening now.

Question: 237

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: B

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.

Question: 238

What is the proper SPL terminology for specifying a particular index in a search?

A. indexer—index_name

B. indexer name—index_name

C. index=index_name

D. index name=index_name

Answer: C

Explanation:

This means that you can use the index field to filter your search results by the name of the index that contains the events you want to see.

For example, if you want to search for events in the index named “gcp_logs”, you can use the following SPL: index=gcp_logs

You can also specify multiple indexes by using the OR operator, such as: index=gcp_logs OR index=oswin

Question: 239

Which of the following is the appropriately formatted SPL search?

A. index=security sourcetype=linux secure (invalid OR failed) | stats count as "Potential Issues"

B. index=security sourcetype=linux secure (invalid OR failed) | stats as "Potential Issues"

C. index—security sourcetype=linux secure (invalid OR failed) | count stats as "Potential Issues"

D. index—security sourcetype=linux secure (invalid OR failed) | count as "Potential Issues"

Answer: A

Explanation:

This is the appropriately formatted SPL search because it follows the SPL syntax rules12, such as: Using the = operator to specify field-value pairs, such as index=security and sourcetype=linux. Using the OR operator to combine multiple values for the same field, such as (invalid OR failed). Using the | character to separate commands, such as stats count as "Potential Issues".
Using the as keyword to rename fields, such as count as "Potential Issues".

Question: 240

How are the results of the following search sorted?

... | sort action, —file, +bytes

A. In descending order by action, then descending order by file, and lastly by ascending order of bytes.

B. In ascending order by action, then descending order by file, and lastly by ascending order of bytes.

C. In descending order by action if it exists. If not, then in descending order by file, and if both action and file do not exist, by ascending order of bytes.

D. In ascending order by action if it exists. If not, then in descending order by file, and if both action and file do not exist, by ascending order of bytes.

Answer: B

Explanation:

Using a minus sign (-) for descending order and a plus sign (+) for ascending order. If no sign is specified, the default order is ascending.
Sorting by multiple fields in the order they are specified. If there are duplicate values in one field, the next field is used to break the tie.
Sorting by field values according to their types. If the field type is not specified, the sort command tries to automatically determine it.

Question: 241

Splunk users are assigned roles. Which of the following do roles determine?

A. Password

B. Port number

C. Username

D. Data access

Answer: D

Explanation:

This is the correct answer because roles determine the level of access that users have to the Splunk platform and the tasks that they can perform on the platform1. Roles can contain one or more capabilities that provide access to specific parts of the Splunk platform, such as searching, indexing, alerting, and so on2. Roles can also specify which indexes that a user can search and which indexes are searched by default1.

Question: 242

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: C

Explanation:

According to the Splunk documentation, dashboards are collections of views that you can use to visually analyze your data. 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.

Question: 243

What is the result of the following search?

index=myindex source=c: \mydata. txt NOT error=*

A. Only data where the error field is present and does not contain a value will be displayed.

B. Only data with a value in the field error will be displayed.

C. Only data that does not contain the error field will be displayed.

D. Only data where the value of the field error does not equal an asterisk (*) will be displayed.

Answer: C

Explanation:

The search query index=myindex source=c: \mydata. txt NOT error=* specifies three criteria for the events to be returned:
The index must be myindex, which is a user-defined index that contains the data from a specific source or sources.
The source must be c: \mydata. txt, which is the name of the file or directory where the data came from.
The error field must not exist in the events, which is indicated by the NOT operator and the wildcard character (*).
The NOT operator negates the following expression, which means that it returns the events that do not match the expression.
The wildcard character () matches any value, including an empty value or a null value. Therefore, the expression NOT error= means that the events must not have an error field at all, regardless of its value.
The search query does not use quotation marks around the source value, which means that it is casesensitive and exact. If there are any variations in the source name, such as capitalization or spacing, they will not match the query.

Reference
Search command syntax details
Search command examples
Basic searches and search results

Question: 244

What are Splunk alerts based on?

A. Dashboards

B. Searches

C. Webhooks

D. Reports

Answer: B

Explanation:

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]