Core User v1.0 (SPLK-1001)

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.

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.

1. Which search string only returns events from host WWW3?

A. host=*

B. host=WWW3

C. host=WWW* #exam4training

D. Host=WWW3

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

A. 10 Minutes

B. 15 Minutes

C. 1 Day

D. 7 Days

Reference:

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

3. 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.

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

A. Add an output.

B. Export a dashboard panel.

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

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

5. 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_DescriptionC. Group_Object_Description

6. 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.

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

A. limit, count

B. limit, showpercent

C. limits, countfield

D. showperc, countfield

9. 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.

10. 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. ,

11. 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

12. 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)

13. 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.

14. 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.

15. 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

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

A. OR

B. NOT

C. AND

D. XOR

17. 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)

18. 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.

19. 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.

20. 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

21. What user interface component allows for time selection?

A. Time summary

B. Time range picker

C. Search time picker

D. Data source time statistics

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

A. dedup

B. rename

C. sort -

D. fields +

23. 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 >

24. 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"

25. 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*

26. 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.

27. 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.

28. 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

29. 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.

30. 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

31. 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.

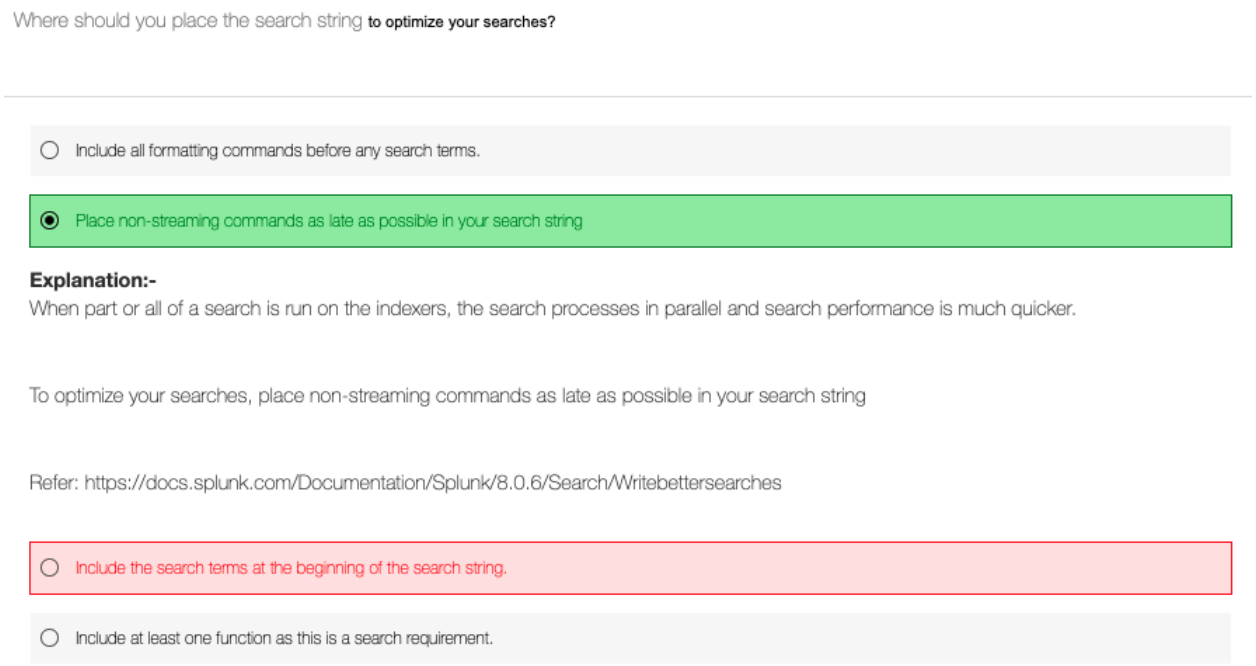
Where should you place the search string to optimize your searches?

A. Include all formatting commands before any search terms.

B. Place non-streaming commands as late as possible in your search string

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

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



https://docs.splunk.com/Documentation/Splunk/8.0.6/Search/Writebettersearches

32. 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.

33. 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

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

> The AND operator is always implied between terms and expressions. For example, `web error` is the same as `web AND error`. Specifying `clientip=192.0.2.255 earliest=-1h@h` is the same as `clientip=192.0.2.255 AND earliest=-1h@h`. So unless you want to include it for clarity reasons, you do not need to specify the AND operator.

34. 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.

35. 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.

36. 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.

37. What can be configured using the Edit Job Settings menu?

A. Export the result to CSV format.

B. Add the Job results to a dashboard.

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

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

Q. 44 What can be configured using the Edit Job Settings menu?

◉ Change Job Lifetime from 10 minutes to 7 days.

Explanation:-
Edit search job settings

You can open the Job Settings dialog when a search job is running, paused, or finalized. Just click Job and select Edit Job Settings

Sharing jobs - There are several ways to share a job with other Splunk users. You can change the job permissions or send a link to the job. This can be handy if you want another user to see the results returned by the job.

Job lifetimes - When you run a new search, a job is retained in the system for a period of time, called the job lifetime. The default lifetime is 10 minutes. The lifetime starts from the moment the job is run.

38. 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.

39. 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.

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

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

A. action

B. clientip

C. categoryId

D. sourcetype

41. 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*

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

A. top

B. stats

C. table

D. percent

43. 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.

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

A. Index

B. Search Head

C. Indexer

D. Forwarder

45. Which component of Splunk is primarily responsible for saving data?

A. Search Head

B. Heavy Forwarder

C. Indexer

D. Universal Forwarder

46. 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.

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

A. Forwarders

B. Deployment Server

C. Indexer

D. Knowledge Objects

E. Index

F. Search Head

48. 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.

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

A. False

B. True

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

A. True

B. False

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

A. Forwarders

B. Indexer

C. Heavy Forwarders

D. Search head

52. Log filtering/parsing can be done from _____.

A. Index Forwarders (IF)

B. Universal Forwarders (UF)

C. Super Forwarder (SF)

D. Heavy Forwarders (HF)

53. 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

54. 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.

55. Splunk shows data in _____.

A. ASCII Character order.

B. Reverse chronological order.

C. Alphanumeric order.

D. Chronological order.

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

A. =

B. >

C. !

D. *

57. 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

58. Prefix wildcards might cause performance issues.

A. False

B. True

59. Machine data can be in structured and unstructured format.

A. False

B. True

60. How many main user roles do you have in Splunk?

A. 2

B. 4

C. 1

D. 3

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

A. False

B. True

62. Field values are case sensitive.

A. True

B. False

63. Splunk indexes the data on the basis of timestamps.

A. True

B. False

64. _____ is the default web port used by Splunk.

A. 8089

B. 8000

C. 8080

D. 443

65. Parsing of data can happen both in HF and Indexer.

A. Only HF

B. No

C. Yes

66. License Meter runs before data compression.

A. No

B. Yes

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

A. False

B. True

###68. 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

69. Data sources being opened and read applies to:

A. Indexing Phase

B. Parsing Phase

C. Input Phase

D. License Metering

E. None of the above

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

A. Indexing

B. Searching

C. Parsing

D. Settings

E. Input

71. Splunk automatically determines the source type for major data types.

A. False

B. True

72. Upload option creates inputs.conf

A. Yes

B. No

73. 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

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

A. Parsing

B. Masking

C. Searching

D. Forwarding

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

A. No

B. Yes

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

A. No

B. Yes

77. Every Search in Splunk is also called _____.

A. Job

B. Search Only

C. None of the above

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

A. No

B. Yes

79. @ Symbol can be used in advanced time unit option.

A. No

B. Yes

80. The new data uploaded in Splunk are shown in _____.

A. Real-time

B. 10 Minutes

C. Overnight Download

D. 30 Minutes

81. 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

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

A. False

B. True

83. Events in Splunk are automatically segregated using data and time.

A. Yes

B. No

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

A. No

B. Yes

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

A. False

B. True

86. 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.

87. Which symbol is used to snap the time?

A. @

B. &

C. *

D. #

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

A. Automatic

B. Smart

C. Fast

D. Verbose

89. 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.

90. 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. Add the item to search.

D. Create a new search

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

A. Table

B. Raw

C. Pie Chart

D. List

92. Snapping rounds down to the nearest specified unit.

A. Yes

B. No

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

A. Hosts #exam4training

B. Sourcetypes #exam4training

C. Sources

D. Indexes #exam4training

94. 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

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

A. True

B. False

96. Field names are case sensitive and field value are not.

A. True

B. False

97. != and NOT are same arguments.

A. True

B. False

###98. 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.

99. 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.

100. 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.

101. 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 B. (index=a OR index=b)

102. 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

103. Fields are searchable key value pairs in your event data.

A. True

B. False

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

A. True

B. False

105. Search Language Syntax in Splunk can be broken down into the following components. (Choose all that apply.)

A. Search term

B. Command

C. Pipe

D. Functions

E. Arguments

F. Clause

106. 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

107. 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

108. 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

109. 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

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

A. Events

B. Patterns

C. Statistics

D. Visualization

111. What will always appear in the Selected Fields list?

A. index

B. action

C. clientip

D. sourcetype

112. 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

113. Which of the following is a Splunk internal field?

A. _raw

B. host

C. _host

D. index

114. 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"

115. 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=*

116. What are the two most efficient search filters?

A. _time and host

B. _time and index

C. host and sourcetype

D. index and sourcetype

117. 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"

118. 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

119. 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

#find the right answer#120.What must be done before an automatic lookup can be created? (Choose all that apply.)

A. The lookup command must be used.

B. The lookup definition must be created. #Exam4Training

C. The lookup file must be uploaded to Splunk. #Exam4Training

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/DefineanautomaticlookupinSplunkWeb

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

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

122.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)

123.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

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

A. limit

B. useperc

C. addtotals

D. fieldcount

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

A. Red

B. Blue

C. Orange

D. Highlighted

126.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.

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels

127.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.

128.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.

130.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.

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

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

###132.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.

133.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

###134.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.

135.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

136.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.

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

A. #

B. %

C. a

D. a#

Q. 20 In the fields sidebar, which character denotes alphanumeric field values?

Explanation:- https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchTutorial/Usefieldstosearch

https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchTutorial/Usefieldstosearch

138.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.

139.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

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

A. Time

B. Fast mode

C. Sourcetype

D. Selected Fields

Explanation: https://wiki.splunk.com/Community:Intro_to_Splunk_Search_Performance

141.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.

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

A. PDF

B. JSON

C. XLS

D. RTF

Explanation:- https://docs.splunk.com/Documentation/Splunk/8.1.0/Search/ExportdatausingSplunkWeb

https://docs.splunk.com/Documentation/Splunk/8.1.0/Search/ExportdatausingSplunkWeb

2. Click **Format** and select the format that you want the search results to be exported in.
The supported formats depend on the type of job artifact that you are working with.

Format	Ad hoc searches	Saved searches	Notes
CSV	X	X	
JSON	X	X	
PDF		X	If the search is a saved search, such as a Report, you can export using the PDF format.
Raw Events	X	X	If the search generates calculated data that appears on the Statistics tab, you cannot export using the Raw Events format.
XML	X	X	

143.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

144.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.

145.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.

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

A. time

B. _time

C. EventTime

D. timestamp

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

A. Dashboards

B. Metadata only

C. Non-interesting fields

D. Field descriptions

148.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.

149.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

150.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.

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

A. user

B. source

C. location

D. sourceIp

152.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.

153.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.

154.Which command is used to validate a lookup file?

A. | lookup products.csv

B. inputlookup products.csv

C. | inputlookup products.csv

D. | lookup_definition products.csv

155.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.

Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Report/Managereportpermissions

156.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.

157.Which search string is the most efficient?

A. "failed password"

B. "failed password"*

C. index=* "failed password"

D. index=security "failed password"

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

A. status_code!=404

B. status_code>=400

C. status_code<=404

D. status_code>403 status_code<405

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

A. True

B. False

160.Universal forwarder is recommended for forwarding the logs to indexers.

A. False

B. True

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

A. True

B. False

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

A. False

B. True

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

A. True

B. False

164.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)

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

A. True

B. False

166.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.

167.Monitor option in Add Data provides _____.

A. Only continuous monitoring.

B. Only One-time monitoring.

D. Both One-time and continuous monitoring.

C. None of the above.

168. Parsing of data can happen both in HF and UF.

A. Yes

B. No

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

A. 3

B. 2

C. 4

D. 1

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

A. No

B. Yes

171.Where does Licensing meter happen?

A. Indexer

B. Parsing

C. Heavy Forwarder

D. Input

172.Matching search terms are highlighted.

A. Yes

B. No

173.Matching of parentheses is a feature of Splunk Assistant.

A. No

B. Yes

174.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.

175.You can change the App context in Input setting.

A. No

B. Yes

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.

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

A. Zoom to selection

B. Format Timeline

C. Deselect

D. Delete

E. Zoom Out

178.Can you stop or pause the searching?

A. No

B. Yes

179.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

180.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.

181.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

###182.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

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

183.Which of the following is the most efficient search?

A. index=* "failed password" #gratisexam

B. "failed password" index=*

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

D. index=security "failed password" #quizlet #exam4training

184.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

185.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

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

A. Acceleration, schedule, permissions #exam4training

B. The report's name, schedule, permissions

C. The report's name, acceleration, schedule

D. The report's name, acceleration, permissions

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

A. host

B. owner

C. bytes

D. action

Explanation:

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

188.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

189.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

190.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

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

191.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

192.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

193.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

194.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.

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Managereportpermissions

195.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.

196.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.

WHIZLABS

The varicose Timeline controls under Search and Reporting App include

A. Zoom Out
B. Zoom to Selection
C. Deselect
D. Format Timeline
E. All of above

Any change to a report affects every Dashboard that utilizes that report.

A. True
B. False

Which kind of deployment removes infrastructure requirements from your plate?.

A. Splunk Enterprise deployment
B. Splunk Cloud deployment
C. Both
D. None

'Search Head' provides the following tools to assist search experience?

A. Dashboards
B. Reports
C. Visualixations
D. All of the above

Splunk naming format for a report is

A. Object_group_description
B. Group_object_description
C. There is no specific format
D. None

What will display matching terms, contextual matches and syntax documentation?

A. Apps
B. Search terms
C. Search assistant

D. None

The ‘fields -’ command will do the following

A. Subtract the values of two fields
B. Exclude the selected fields
C. Both
D. None

!= and **NOT** never yield the same results

A. True
B. False

Common constraints for top command are

A. Limit
B. Countfield
C. Showperc
D. All of the above

Which search mode emphasizes completeness over speed

A. Smart
B. Verbose
C. Fast
D. None

When hovering over a colume on timeline shows

A. Time range
B. Number of events
C. Both
D. None

Use the â€˜asâ€™ clause to rename the count field under stats count command.

A. True
B. False

Once a field is renamed, it can be accessed with the original name down further

A. True
B. False

If not specified, ‘index’ under search string defaults to

A. *
B. main
C. All-time
D. doesnâ€™t default to any

What are the ways to get the data into Splunk?

A. Download
B. Monitor
C. Pull
D. Forward
E. Upload

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.):

- Not possible to specify time manually in search query
- end=
- latest=
- start=
- earliest=

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)

Creating Data Models:

Object ATTRIBUTES do not define _____.

A . a base search for the object

B . fields for the object

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

All users by default have WRITE permission to ALL knowledge objects.
A . True
B . False

The stats command will create a _____ by default.
A . Table
B . Report
C . Pie chart

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

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

Creating Data Models: Fields associated with a data set are known as _____.
A . Attributes
B . Constraints