Splunk

Terms in this set (196)

1. Which search string only returns events from host WWW3? A. host=* B. host=WWW3 C. host=WWW* D. Host=WWW3	B. 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	A.10 Minutes
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.	B. They must be uppercase.

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.	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_Description	C. 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	A. Filter as early as possible.

7. Which of the following are common constraints of the top command? A. limit, count B. limit, showpercent C. limits, countfield D. showperc, countfield	D. showperc, countfield
8. 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.	B. Filters current search results.

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.	C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
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. ,	D. ,

Splunk

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	C. Real-time - 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)	C. stats count (vendor_action)

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.	B. Field names ARE case sensitive; field values are NOT.
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.	A. Returns the least common 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	A. $SPLUNK_HOME/bin/scripts
16. Which Boolean operator is always implied between two search terms, unless otherwise specified? A. OR B. NOT C. AND D. XOR	C. AND
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)	A. dc(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.

A. Alerts are based on searches that are either run on a scheduled interval or in 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.	A. Click All Fields and select the field to add it to Selected Fields.
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	B. action=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	B. Time range picker
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 +	A. dedup
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 >	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"	B. index=security failure | stats 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**	C. (index=web OR index=sales)

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.	B. Use a consistent naming convention so they are easily separated by characteristics such as group and object.
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.	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	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.	B. A # symbol to the left 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

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.	C. Include the search terms at the beginning of the search string.
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.	A. Any search can be saved as a report.

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	A. index=security Error Fail
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.	B. All events with a host of www3 that also have a status of 503.

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.	C. Calculates statistics on data that matches the search criteria.
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.	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.	D. Change Job Lifetime from 10 minutes to 7 days.
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.	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.

D. The selected field and its corresponding values will appear underneath the events in the search results.

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

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

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**	C. fail*
42. Which command automatically returns percent and count columns when executing searches? A. top B. stats C. table D. percent	A.top
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.	C. Lookups add more fields to results returned by a search.

44. _____ transforms raw data into events and distributes the results into an index. A. Index B. Search Head C. Indexer D. Forwarder	C. Indexer
45. Which component of Splunk is primarily responsible for saving data? A. Search Head B. Heavy Forwarder C. Indexer D. Universal Forwarder	C. Indexer
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.	A. Designed to cater numerous use cases and empower Splunk. 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	A. Forwarders C. Indexer 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.	A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
49. We should use heavy forwarder for sending event-based data to Indexers. A. False B. True	B. True
50. Splunk Enterprise is used as a Scalable service in Splunk Cloud. A. True B. False	A.True

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	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)	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	B. Searching and Reporting

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	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.	B. Reverse chronological order.
56. Which of the following can be used as wildcard search in Splunk? A. = B. > C. ! D. *	D. *

Splunk

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	C. the_questionnaire_pedia
58. Prefix wildcards might cause performance issues. A. False B. True	B. True
59. Machine data can be in structured and unstructured format. A. False B. True	B. True
60. How many main user roles do you have in Splunk? A. 2 B. 4 C. 1 D. 3	D. 3

61. Fields are searchable name and value pairings that differentiates one event from another. A. False B. True	B. True
62. Field values are case sensitive. A. True B. False	B. False
63. Splunk indexes the data on the basis of timestamps. A. True B. False	A.True
64. _____ is the default web port used by Splunk. A. 8089 B. 8000 C. 8080 D. 443	B. 8000
65. Parsing of data can happen both in HF and Indexer. A. Only HF	C. Yes

66. License Meter runs before data compression. A. No B. Yes	B. Yes
67. Forward Option gather and forward data to indexers over a receiving port from remote machines. A. False B. True	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	B. CLI C. Splunk Web E. Splunk apps and add-ons G. inputs.conf
69. Data sources being opened and read applies to: A. Indexing Phase B. Parsing Phase C. Input Phase D. License Metering	C. Input Phase

70. Select the correct option that applies to Index time processing (Choose three.). A. Indexing B. Searching C. Parsing D. Settings E. Input	A. Indexing C. Parsing E. Input
71. Splunk automatically determines the source type for major data types. A. False B. True	B. True
72. Upload option creates inputs.conf A. Yes B. No	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	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	A. Parsing B. Masking D. Forwarding
75. Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses. A. No B. Yes	B. Yes
76. Zoom Out and Zoom to Selection re-executes the search. A. No B. Yes	B. Yes
77. Every Search in Splunk is also called _____. A. Job B. Search Only C. None of the above	A.Job

78. Search Assistant is enabled by default in the SPL editor with compact settings. A. No B. Yes	B. Yes
79. @ Symbol can be used in advanced time unit option. A. No B. Yes	B. Yes
80. The new data uploaded in Splunk are shown in _____. A. Real-time B. 10 Minutes C. Overnight Download D. 30 Minutes	A. Real-time
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	A. earliest= B. latest=

82. The default host name used in Inputs general settings can not be changed. A. False B. True	A. False
83. Events in Splunk are automatically segregated using data and time. A. Yes B. No	A. Yes
84. You are able to create new Index in Data Input settings. A. No B. Yes	B.Yes
85. Splunk Parses data into individual events, extracts time, and assigns metadata. A. False B. True	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.	A. The new result after selecting the range by dragging filters the events and displays the most recent first.
87. Which symbol is used to snap the time? A. @ B. & C. * D. #	A.@
88. There are three different search modes in Splunk (Choose three.): A. Automatic B. Smart C. Fast D. Verbose	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.

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.
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. None of the above.

A. Open new search.
B. Exclude the item from search.
C. Add the item to search.

Splunk

91. You can view the search result in following format (Choose three.): A. Table B. Raw C. Pie Chart D. List	A. Table B. Raw D. List
92. Snapping rounds down to the nearest specified unit. A. Yes B. No	A.Yes
93. Data summary button just below the search bar gives you the following (Choose three.): A. Hosts B. Sourcetypes C. Sources D. Indexes	A. Hosts B. Sourcetypes C. Sources
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	A.Yes

95. Interesting fields are the fields that have at least 20% of resulting fields. A. True B. False	A.True
96. Field names are case sensitive and field value are not. A. True B. False	A.True
97. != and NOT are same arguments. A. True B. False	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.	A. Will return event where status field exist but value of that field is not 100.

Splunk

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.

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.

A. Select the time range always.
B. Try to specify index values.
C. Include as many search terms as possible.
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 I (Pipes) are used by selecting following options. A. CTRL + Enter B. Shift + Enter C. Space + Enter D. ALT + Enter	B. Shift + Enter
103. Fields are searchable key value pairs in your event data. A. True B. False	A.True
104. Selected fields are a set of configurable fields displayed for each event. A. True B. False	A. True

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	A. Search term B. Command 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	C. Report 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	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	A. error | table action, src, 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	A. Top values by time
110. In the Search and Reporting app, which tab displays timecharts and bar charts? A. Events B. Patterns C. Statistics D. Visualization	D. Visualization
111. What will always appear in the Selected Fields list? A. index B. action C. clientip D. sourcetype	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	B. earliest=-2h
113. Which of the following is a Splunk internal field? A. _raw B. host C. _host D. index	A. _raw
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"	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=*	C. Click Data Summary in Splunk Web
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	B. _time and index
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"	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	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	B. index=Security

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. C. The lookup file must be uploaded to Splunk. D. The lookup file must be verified using the inputlookup command.	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.
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	B. Forwarder

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)

B. (index=netfw failure) OR (index=netops (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	B. 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	A.Limit

125.When running searches, command modifiers in the search string are displayed in what color? A. Red B. Blue C. Orange D. Highlighted	C. Orange
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.	C. You cannot modify the search string in the panel, but you can change and configure the visualization.

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.	A. Line charts are optimal for single and multiple series.
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.	C. In reverse chronological order.

129.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.

D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

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.

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	C. inputlookup
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.	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	B. index
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.	B. Lists unique values of a given field.
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	A.An App

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.	C. Use fields +to add and fields -to remove.
137.In the fields sidebar, which character denotes alphanumeric field values? A. # B. % C. a D. a#	C. a

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.	C. Your search must transform event data into statistical data tables 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	A. error AND (fail AND 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	A.Time
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.	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	B. JSON
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	C. 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.	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.	A. After saving the report, click Schedule.

146.At index time, in which field does Splunk store the timestamp value? A. time B. _time C. EventTime D. timestamp	B. _time
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	C. Non-interesting fields
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.	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	B. 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.	B. Adding the item to the search.