1)which of these is not a main component of splunk?
A)Compress and archive
2)What are the three main processing components of splunk?
A)Search head, indexers, forwarders
3)_____define what users can do in splunk.
A)Roles
4)This role will only see their own knowledge objects and those that have been shared with them.
A)User
5)What are three main default roles in splunk enterprise?
A)power, admin, user
6)Which apps with splunk enterprise?
A)Home App, Search & Reporting
7)The default username and password for a newly installed splunk instance is:
A)Admin and changeme
8)Files indexed using the upload input option get indexed____
A)Once
9)Splunk knows where to break the event, where the time stamp is located and how to automatically create field valu e pairs using these.
A)Source types
10)A search job will remain active for ____ minutes after it is run.
A)10
11)Which are reusable chunks of spl that can be inserted into other searches?
A)Search Macros
12)To acess splunk web interface, use
A)https://hostname:8000
13)How many search types that affect splunk enterprise performance do we have?
A)4
14)After a report is saved, it can be added to a new or existing dashboard
A)Correct
15)When a knowledge object is created, it can be shared to other users.
A)Correct
16)Which type of search gives indexer throughput of up to 10-50 index bucket per sec?
A)Rare
17)Which of the following tool is used to get a closer look at what your search is doing and see where the splunk sof twere is spending most of its time?
A)Splunk job inspector
18)Which command creates new fields in the events by using existing fields and an arbitary expression
A)eval
19)As a best practice, it is recommended to have naming conventions for knowledge objects.
A)Correct
20)Which chart shows trends in the relationships between discrete data values?
A)Scatter chart
21)There are how many types of data model Acceleration?
A)2
22)Splunk software knowledge can be grouped into how many categories?
A)5
23)Data model editor groups datasets fields into the how many categories?
A)3
24)Contents of macro can be checked using the following keyboard shortcut in linux
A)ctrl+Shift+E
25)We can use multiple aliases to a single field.
A)Correct
26)when the fields are seperated by spaces, use the folowing field extractor method
A)Delimeters
27)Which command performs aggregate statistcs such as average, count and sum over the result set

A)stats
28)Transactions and macro searches are a powerful combination that allow substitution in your transaction searches
A)correct
29)Transaction command adds the following two fiels to the raw event
A)duration, event code
30)5 tags make data more understandable and less ambiguous
A)Correct
31)Which chart provides a visual way to view a three dimensional series?
A)Bubble
32)Which search mode return best results for whatever search you run.
A)smart
33)These are used to manage and normalize sets of field informations
A)Aliases, tags
34)Which command computes the moving averages of a field?
A)trendline
35)Which command is used to replace Null values in a field?
A)fillnull
36)Transaction command can create a single event from group of events.
A)correct
37)How many field extractor methods do we have?
A)2
38)eventcount under transaction command tells about the number of events in the transaction.
A)correct
39)Timechart command is a statistical aggregation aplied to a field to product chary.
A)correct
40)iplocation command supports.
A)ipv4 and ipv6 (both)
41)Which command enables searching existing data models and their datasets from the search interface?
A)datamodel
42)geom adds a field named geom to each search result.
A)correct
43)Which command helps to report on a specific dataset without SPL?
A)Pivot
44)By default, what is the number of events per transaction.
A)1000
45)What are the various types of data model acceleration?
A)Both (Persistent data model acce, Ad-hoc data model acceleration
46)When a search macro is inserted in a search string, it is necessary to place this symbol before and after the macro
?
A)backstick"`"
47)Event type comes seventh in the ssearch time operations order.
A)Correct
48)All dataset fields are hidden and required by default.
A)incorrect
49)Transforming commands include.
A)chart, timechart, top, stat
50)Search macros can take arguments dynamically and the search result will be updated as per new values.
A)correct
51)Which command creates a time series chart with corresponding value of statistics?
A)timechart
52)It is a must to specify a statistical function when you use the chart command.
A)Correct
53)An alias removes and replaces the original field name
A)Incorrect
54)For a chart, by default only these number of values are returned.

A)There is no limit
55)Constraints for transaction include.
A)All of these. (maxpause, startwith, maxspan, endswith)
56)which is a representation of statistical information without showing the axes?
A)Sparkline
57)Which of the following search type affect splunk enterprise performace?
A)Sparse, Super Sparse, Rare, dense
58)To count frequency of a field(s), use the folowing commands.
A)Top, rare
59)Timecharts are best represented in'
A)line chart, Area chart
60)The best way to use wildcard is.
A)At the end of the search term
61)What are the different types of data model dataset fields?
A)All of these (eval expression, regular expression, geo ip, auto extracted, lookup)
62)Which of the following is a shared semantic model focused on extracting value from data?
A)Splunk common information model
63)WHich tool is used to speed up data models that represent extremely large dataset?
A)Data model acceleration
64)For splunk, booleans must be in
A)Uppercase
65)Which command adds field values from external source?
A)lookup
66)How many kinds of workflow actions can be set up?
A)3
67)An alias removes original field name
A)Incorrect
68)General naming convention for a knowledge object includes.\
A)Group->search type->platform->category->time interval->description
69)By default, what is the number of events per transaction?
A)1000
70)Data models can contain multiple hierarchies which are divided into ____.
A)search, event, transaction
71)What is a hierarchically structured search time mapping of semantic knowledge about one or more datasets?
A)Data model
72)What are the various workflow actions?
A)Post, Search, Get
73)What allows to filter the large amounts of data, find similar patterns, create reports and alerts?
A)Event Types
74)Tags are
A)Case sensitive
75)Time is the most efficient filter.
A)Correct
76)The field extractor provides the following field extraction methods.
A)Both Regular Expression and Delimeters
77)A group of related events over a duration of time is a transaction
A)Correct
78)Search terms are
A)Case insensitive
79)The eval command evaluates the following expressions.
A)All of these (String Expression, Mathematical Expression, Boolean Expression,Comparison Expression)
80)What are inline charts that appear within table cells in search results?
A)Sparklines
81)6 period for the trendline command must be an integer between.
A)2 and 10000

82)Which type of search give indexer throughput of up to 2 seconds per index bucket?
A)Super Sparse
83)Any Currently running search job can be inspected?
A)Correct
84)Which option of chart is used to limit the number of values to appear in the output
A)limit
85)Which command is used to lookup and add location information to an event?
A)iplocation
86)It is not possible to chain multiple 'eval' expressions in one search using a comma to seperate the subsequent expr essions
A)Incorrect
87)Which app provides the primary interface for using splunk to run reports, save searvhes and create dashboards?
A)Search and Reporting
88)A power user can share and promote knowledge objects.
A)correct
89)What are the macros with the same name but different number of required arguments?
A)Overloaded macros
90)How many map types do we have?
A)2
91)Which are used to assign names to specific field and value combinations?
A)tags
92)To seperate multiple 'eval' expressions in a single search, use.
A)comma (",")
93)Transaction command adds two new fields to the raw events.
A)Duration, Eventcount
94)Knowledge objects can be kept to private, in other words, it need not be shared.
A)correct
95)It is not a best practice tp have knowledge objects of a single type with unique names.
A)incorrect
96)Which symbol represents the start and end of a search macro definition in search processing language?
A)backstick"`"
97)where is the occurrence of tags in the sequence of search-time operation?
A)Last
98)chart command returns in a tabular format.
A)Correct
99)Splunk knowledge is categorized into how many categories?
A)5
100)What are various chart types?
A)bar, scatter, bubble, line, pie (All of these)
101)Which chart shows the relationship of parts of your data to the entire set of data as a whole?
A)pie
102)We can apply statistical functions to
A)All of these (timechart, chart, stats)
103)Private data models cannot be accelerated.
A)Incorrect
104)Accelerated data models can be edited.
A)Incorrect
105)Data model editor groups datasets fields into the folowing categories?
A)Inherited, Extracted, Calculated
106)Contents of macro can be checked using the following keyboard shortcut in windows.
A)Ctrl+Shift+E
107)How many types of data model acceleration we have?
A)2
108)A calculated field may be based on which of the following?
A)Extracted fields

109)Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search
A)Events will be returned from the data model named Application_State
110)Which of the following actions can be eval command perform?
A)Create or replace an existing field
111)The field extractor (FX) is used to extract a custom field. A report can be created using this custom field. The cr eated report can then be shared with other people in the organization.
If another person in the organization runs the shared report and no results are returned, why might this be?
A)The extraction is private-
The person in the organization running the report does not have access to the index.
112)Which of the following statements describes this search? sourcetype=access_combined|transaction JESSIONID| timechart avg (duration)
A)This is a valid search and will display a timechart of the average duration, of each transaction event.
113)What does the following search do?
index=corndog type=mysterymeat action=eaten |stats count as corndog_count by user
A)Creates a table of the total count of mysterymeat corndogs split by user
114)A user wants to convert field values to string and also to sort on those value. Which command should be used fi rst, the eval or the sort?
A)Covert the numeric to a string with eval first, then sort.
115)Which delimeters can the field extractor (FX) detect? (select all that apply)
A)Pipe character, spaces, commas
116)To identify all of the contributing events within a transaction that contains at least one Reject event, which synta x is correct?
A)index=main |transaction sessionid|search REJECT
117)When should you use the transaction command, instead of the stats command?
A)When unique alone is not sufficient to discriminate between two transactions.
118)Which of the following knowledge objects represents the output of an eval expression?
A)Calculated fields
119)Which of the following data model are included in the splunk common information model (CIM) add-on? (Sele ct all that apply)
A)Alerts, database, email
120)In large environments, which of the following statements is/are correct.
A)The stats command is faster and more efficient than the transaction command
121)Which of the folowing statements describe the common information model (CIM)?
A)CIM can correlate data from different sources.
CIM is a methodology for normalizing data.
122)Which of the following statements about event types is true?
A)Event types can be a useful method for capturing and sharing knowledge
Event types can be tagged.
Event types categorize events based on a search.
Event types categorize events based on a search.
123)Which of the following is the correct way to use the data model command to search field in the data model withi n the web dataset?
A)|datamodel web search |field web*
124)Which one of the following statements about the search command is true?
A)It can only be used at the beginning of the search pipeline.
125)When using the field extractor (fx), which of the following delimiters will work?
A)Pipes, Spaces
101)When using the field extractor (FX). which of the following delimiters will work?
A)Spaces, Pipes
102)WHich of the following describes the Splunk common information model (CIM) add-on?
A)The CIM add-on contains data models to help you normalize data
103)Which of the Following statements described the search beloow?(select all that apply) index =main | transaction client host maxspan=30s maxpause=5s
A)It group event taht share client and host

The First and last event are no more than 30seconds apart
104)When creating a search workflow action,filed required?
A) Searching String
105) Data model are composad of one more of which of following datasets
A)Events datasets, Transaction datasets, search datasets
106)Which of the following statements about data models and pivot are true?
A)Pivot allows the creation of data visualizations that present different aspects of a data model
Data models are created out of datasets called pivots
107)In what order are the following knowledge objects/configurations applied?
A)Field Extractions, Field Aliases, Lookups
108)Which of the following statements describes field aliases?
A)Field alias names are alternate name that you assign to a field
109)Selected fields are displayed_____each event in the search results.
A)below
110)what is the relationship between data models and pivots?
A)Data models provide the datasets for pivots.
111)If a search returns_____it can be viewed as a chart.
A)Statistics
112)Which of these search strings is not valid:
A)index=web status=50*|chart count over host,status
113)which of the folowing are valid timechart options with the chart command?
A)useother=f, usenull=f
114)When you mouse over and click to add a search term which boolean operator is not implied
A)()
115)Select this in the fields sidebar to automatically pipe you search results
A)Interesting fields
116)A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being_____
A)Skipped or deferred
117)The splunk CIm add-on includes data models in a _____format.
A)JSON
118)Splunk alerts can be based on search that run _____
A)on a regular schedule
In real-time
119)In the field extractor utility, this button wil display events that do not contain extracted fields.
A)Non-matches
120)_____datasets can be added to root dataset to narrow down the search
A)Child
121)When using a field value variable with a workflow action, which punctuation mark will escape the data
A)!
122)Use the dedup command to ____.
A)Remove duplicate values
123)Which of the folowing are valid options to speed up reports?
A)Edit acceleration
124)The time range specified for a historial search defines the _____questionable on ans.
A)Amount of data fetched from index matching that time range
125)In this search, _____will appear on the y-axis. SEARCH:sourcetype=access_combined status!=200 |chart cou
nt over host.
A)Count
126)What is the only writeable bucket type?
A)Hot bucket
127)By what filter are indexes divided into buckets?
A)by time
128)What are the 4 types of searches in splunk (by performance)
A)rare, dense, sparse, super sparse
129)You can only split chart results over two dimensions.

A)correct
130)Null values are not shown by default by chart and timechart.
A)Incorrect.
131)Functions and arguments used with stats and chart can not be used with timechart.
A)Incorrect
132)As with chart, it is possible to split timechart by two fields.
A)Incorrect
133)A sparkline is an inline chart, that can be added to timechart.
A)Correct
134)Automatically totaling of every columns can be done by using format option.
A)Incorrect
135)Results of eval can be written to existing field.
A)Correct
136)Indexed data get modified after field values are overwritten by the eval command
A)Incorrect
137)The tostring function can be used with eval.
A)Correct
138)The search command treats values in a case-insensitive manner
A)Correct
139)The where command treats field values in a case insensitive manner.
A)Incorrect
140)Unquoted or single-quoted strings are treated as fields.
A)Correct
141)Transaction command creates a single event from a group of events.
A)correct
142)Knowledge objects are shareable, reusable and searchable.
A)correct
143)The power user role can create an object that persists globally across all apps
A)incorrect
144)The power user role can create an object that persists in the context of a specific app.
A)correct
145)Field aliases are applied after field extraction, before lookups.
A)Correct
146)It is not possible to apply field aliases to lookups.
A)Incorrect
147)Multiple aliases can be applied to one field.
A)correct
148)After a field alias have been made, the field alias can be used as an ordinary field in SPL
A)correct
149)Tags are case sensitive.
A)Correct
150)you can only create one tag for any field/value combination.
A)Incorrect
151)Knowledge objects like tags, field aliases and calulated fields are searchable.
A)Correct
152)Events types names can contain spaces.
A)Incorrect
153)It is not possible to add tag to an event type.
A)Incorrect
154)Event types does not include a time range, while a saved report does.
A)correct
155)Macros are shareable.
A)Correct
156)This is a valid search:|'monthly_sales(euro,E,0.79)'.
A)incorrect

157)A workflow action can be applied to both fields and event types.
A)correct
158)Datamodels are hierarchical structures where childern datasets inherit constraints and field from their parent dat aset(s)
A)correct
159)A private data model can be accelerated.
A)Incorrect
160)Accelerated data models can be edited
A)Incorrect
161)Only root events can be accelerated.
A)correct
162)The data models included in the CIM add-on are configured with data model acceleration turned off.
A)correct
163)Data model name and dataset name are case sensitive.
A)correct
164)Field values are case sensitive.
A)Incorrect
165)Matching search terms are hightlighted.
A)Correct
166)Events in splunk are automaticaly segregated using data and time.
A)Correct
167)The new data uploaded in splunk are shown in _____
A)Real-time
168)Splunk extracts fields from event data at index time and at search time.
A)Correct
169)What are the steps to schedule a report?
A)After saving the report, click schedule.
170)Which of the folowing constraints can be used with the top command?
A)limit
171)A field exist in search results, but isn't being displayed in the fields sidebar. How can it be added to the fields si debar?
A)Click all fields and select the field to add it to selected fields.
172)Which search matches the events containing the terms "error" and "fail"?
A)index=security Error Fail
173)What is Splunk?
A)Splunk is a softwere platform to search, analyze and visualize the machine generated data.
174)What user interface component allows for time selection?
A)time range picker
175)Which of the following searches will return results where fail, 400, and error exist in every event?
A)error AND (fail AND 400)
176)which of the statement is correct regarding click and drag option in timeline?
A)The new result after selecting the range by dragging filters the events and display the most recent first.
177)what types of search can be saved as a report?
A)Any search can be saved ad a report.
178)Which command automatically returns percent and count columns when executing searches?
A)top
179)By default, how long does splunk retain a search job?
A)10 minutes
180)In the splunk interface, the list of alerts can be filtered based on which characteristics?
A)App, Owner, Severity, and Type
181)When writing searches in splunk, which of the following is true about booleans?
A)They must be uppercase.
182)Which of the following statements about case sensitivity is true?
A)Field names ARE case sensitive, field values are NOt.
183)How can another user gain access to saved report?

A)The owner of the report can edit permissions from the Edit dropdown.
184)What does the values function of the stats command do?
A)List unique values of a given field.
185)Which of the following splunk components typically resides on the machines where data originates?
A)Forwarder
186)Splunk enterprise is used as a scalable service in splunk cloud.
A)correct
187)Splunk index time process can be broken down into phases.
A)3
188)Which symbol is used to snap the time?
A)@
189)Field names are case sensitive.
A)correct
190)Which of the following is the recommended way to create multiple dashboards displaying data from the same se arch?
A)Save the search as a report and use it in multiple dashboards as needed.
191)Which stats command function provides a count of how many unique value exist for a given field in the result s et?
A)dc(field)
192)Which of the following is the most efficient filter for running searches in splunk?
A)time
193)The default host name used in inputs general settings can not be changed.
A)Incorrect.
194)BY default, which of the following fields would be listed in the fields sidebar under interesting fields?
A)Index
195)Which of the following in a splunk search best practice?
A)Filter as early as possible.
196)Documentations for splunk can be found at docs.splunk.com
A)correct
197)Splunk indexed the data on the basis of timestamps.
A)Correct
198)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.
199)All components are installed and admistrered in splunk enterprise on-premise.
A)Correct
200)Which search string returns a field containing the number of matching events and names that field event count?
A)index=security failure|stats count as "Event Count"
201)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.
202)WHat is the purpose of using a by clause with the stats command?
A)To group the results by one or more fields.
203)which of the folowing searches would return events with failure in index netfw or warm or critical in index neto ps?
A)(index=netfw failure) OR (Index=netops (warm OR critical))
204)Select the answer that display the accurate placing of the pipe in the following search string : index=security sou rcetype=access_*status=200 stats count by price
A)index=security sourcetype=access_*status=200|stats count by price
205)Where does licensing meter happen?
A)Indexer
206)When an alert option is configured to run a script, splunk must be able to locate the script. which is one of the di rectories splunk will look into find the script?
A)$SPLUNK_Home/bin/scripts
207)Splunk internal fields contains general information about events and starts from underscore i.e.__
A)Correct
208)Which search string only returns events from host WWW3?

A)host=WWW3
209)After running a search, what effect does clicking and dragging across the timeline have?
A)Filters current search results.
210)What does the rare command do?
A)Returns the least common field values of a given field in the results.
211)How can search results be kept longer than 7 days?
A)By scheduling a report.
212)Zoom out and zoom to selection re-executes the search.
A)Correct.
213)When running searches, command modifiers in the search string are displayed in what color?
A)Orange
214)Splunk show data in _____
A)Reverse chronological order.
215)You can change the APP context in input setting.
A)Correct
216)When a splunk search generates calculated data that appears in the statistics tab, in what formats can the results be exported?
A)CSV,XML,JSON
217)What is a suggested splunk best practice for naming report?
A)Use a consistent naming convention so they are easily seperated by characteristics such as a group and object.
218)Upload options creates inputs.conf
A)Incorrect
219)Which of the following are functions of the stats command?
A)sum, avg, values
220)Universal forwarder is recommended for forwarding the logs to indexers.
A)Correct
221)What must be done in order to use a lookup table in splunk?
A)The lookup file must be uploaded to splunk and a lookup definition must be created.
222)License meter runs before data compression.
A)Correct
223)Fields are searchable name and value pairings that differentiates one event from another.
A)Correct
224)which is the default app for splunk enterprise?
A)Searching and Reporting
225)When looking at a dashboard panel that is based on a report, which of the following is true?
A)you cannot modify the searcg string in the panel, but you can change and configure the visualization.
226)Forward option gather and forward data indexers over a recieving port from remote machines.
A)Corect
227)Every search is splunk is also called
A)Job
228)___is the default webport used by Splunk.
A)8000
229)Uploading local files though upload options index the files only once.
A)Correct
230)Which of the following represents the splunk recommended naming convention for dashboards.
A)Group_object_description
231)In the field sidebar,which character denotes alphanumeric field value.
A)a
232)@ symbol can be used in advanced time unit option.
A)Correct
233)Which boolean operation is always implied between two search terms, otherwise specified.
A)AND
234)How do you add or remove fields from search results.
A)Use fields+to add and fields-to remove.
235)At index time, in which field does splunk store the timestamp value.

A)_Time
236)We should use heavy forwarder for sending eventbased data to indexers.
A)Correct
237)Which of the following file types is an option for exporting splunk search result.
A)JSON
238)How are events displayed after a search is executed.
A)in reverse chronological order.
239)Which command is used to review the contents of a specified static lookup fiel.
A)inputlookup
240)Which search would return events from the access-combined sourcetype.
A)Source=Access_Combined
241)Which time range picker configuration would return real-time events for the past 30 seconds.
A)Real-time_earliest:30-seconds ago,Latest:Now
242)Which of the following fields is stored with the events in the index.
A)Source
243)what is the main requirement for creating visualizations using the splunk UI?.
A) Your search must transform event data into statistical data tables first.
244)Splunk automatically determines the source type for major data types.
A)Correct
245)Splunk parses data into individual events, extracts time,and assigns metadata.
A)Correct
246)In the fields sidebar,what indicates that a fields is numeric?
A)A#symbol to the left of the field name.
247)Search assistant is enabled by default in the SPL editor with compact setting.
A)Correct
248)Which events will be returned by the following search string? host=www3 status=503
A)All events with a host of www3 that also have a status of 503.
249)What can be include in the all fields option in the sidebar?
A)Non-interesting fields.
250)Portal for splunl apps can be accessed through www.splunkbase.com
A)Correct
251)Parsing of data can happen both in HF and UF.
A)Incorrect
252)Prefix wildcards might cause performance issues.
A)Correct
253)Which of the following index searches would provide the most efficient search performance?
A)(index=web OR index=sales)
254)You are able to create new index in data input settings
A)Correct
255)Which ist the correct syntax to count the number of events containing a vendor_action field?
A)Stats count (vendor_action)
256)Which of the following is an option after clicking an item in search reasults
A)Adding the item to the search.
257)Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.
A)Correct
258)Machine data can be in structured and unstructtured format.
A)Correct
259)What does the stats command do
A)Calculates statistics on data that matches the search criteria
260)What is a primary function of a sheduled report?
A)Triggering an alert in your splunk instance when certain conditions are met.
261)What is search assistant in splunk?
A)Shows options to complete the search string
262)What syntax is used to link key/value pairs in search strings?
A)Relational operators such as=,<,or>

263)In monitor option you can select the following options in GUI
A)Files & directories,HTTP event collector (hEC),TCP/UDP and scripts
264)By default ,which of the following is a selected field?
A)Sourcetype
265)You can use the folloeing options to specify start and end time for the query range:
A)latest
earliest
266)Three basics components of splunk are(choose three)
A) search head
indexer
forwarders
267)When viewing the results of a search,what is an interesting field?
A)A field that appears in at least 20% of the evnets
268)According to splunk best practices , which placement of the wildcard resuts in the most efficient search?
A)fail*
269)Parsing of data can happen both in HF and indexer.
A)yes
270)Which of the statements are correct?(Choose three)
A)Zoom-out:expands the time focus and re-executes the search.
Format timeline:hides or shows the timelines in differents view.
Zoom to selection:narrows the time range and re-executes the search
271)Which of the following describes lookup files?
A)Lookups contain static data available in the index.
Lookups add more fields t results returned by a search
272)How does splunk determine which fields to extract from data?
A)Splunk automatically discovers many fields based on sourcetype and key/value paris found in data.
273)Which search string is the most efficient?
A)index=security"failed password"
274)What sorting on multiple fields with the sort command,what delimiter can be used between the field names in th
e serach?
A),
275)Which component of splunk is primarily responsible for saving data?
A)Indexer
276)What determines the scope of data that appears in a scheduled report?
A)the owner of the report csn configure permissions so that the report uses either the user roler or the owners profile
at run time.
277)When editing a dashboard,which of the following are possible options?
A)Drag a dashboard panel to a different loaction on the dashboard
modify the chart type displayed in a dashoard panel.
278)what happens when a field is added to the selected fields list in the fields sidebar?
A)The selected field and its corresponding values will appear underneath the events in the search results.
279)You can on-board to splunk using following means(choose four)
A)Splunk
splunk apps and add-ons
indexes.conf
CLI
280)Which of the statements are correct about HF?(choose three)
A)parsing
masking
Forwarding
281)Which of the following can be used as wildcard search in splunk?
A)*
282)In a deployment with multiple indexes,what will happen when a search is run and an index is not specified in th
e search string?
A)Event from every index searched by default to which the user has access will be returned

283)Monitor option in add data provides_____
A)Both one-time and continuous monitoring
284)When looking at a statistics table,what is one way to drill down to see the underlying events?
A)Clicking on any field value in the table.
285)select the satatement taht are true for timeline in splunk(choose four)
A)Timeline shows distribution of events specified in the time range in the form of bars.
You can click and drag across the bar for selecting the range
single click to see the result for particular time period
You can hover your mouse for details like total events,time and date
286)How many main user roles do you have in splunk?
A)3
287)What is one benefit of creating dashboard panels from reports?
A)Any change to the underlying report will affect every dashboard that utilize that report
288)which search string matches only events with the status_code of 404?
A)status_code>403 status_code<405
289)Splunk apps are used for following(choose three)
A)Designed to cater numerous use cases and empower splunk
It is collection of different splunk config likes data inputs,UI and knowledge object.
Allows multiple workspaces for different use cases/user roles
290)There are three different search modes in splunk(choose three)
A)Fast
verbose
Smart
291)What is the primary use for the rare command?
A)To find the fields with the fewest number of values across a dataset
292)Which statement is true about the top command
A)All of these
293)Which of the following is a best practice when writing a serach string
A)Avoid using formatting causes as they add too much aoverhead
294)Which component of splunk let us write SPL query to find the required data?
A)Search head
295)What does the following specified time range do?
Earliest=-72h@h latest=@d
A)Look back from 3days ago,up to the beginning of today
296)When placed early in a search,which command is most effective at reducing saerch execution time?
A)field+
297)Which of the following ate common constraints of the top command
A)Showperc,countfield
298)What can be configured using the edit job settings menu
A)Change job lifetime from 10 minutes to 7 days
299)What result will you get with following search index=test sourcetype="The_Questionnaire_p*"?
A)the_questionnaire_pedia
300)Which of the following are splunk premium enchanced solutions?
A)Splunk IT service intelligence(ITSI)
Splunk enterprise security(ES)
Splunk User Behavior Analytics(UBA)
301) which of the following statement are correctabout search & Reporting App?
A)Enable the user to creat knowledge object, reports, alerts and dashbord.
Can be accessed by apps> search & Reporting.
provides default interface for searching and analyzing logs.
302)select the correct option that applies to index time processing
A)Input
Indexing
parsing
303)Which of the following is true about user account setting and preferences?

A)Fullname, time zone, and default app can be defined by cliking the login name in the splunk bar.
304) Data sources being opened and read applies to:
A)Input Phase
305)What kind of long can splunk index?
A)All firewall, web server,database, router and swich logs.
306)Which is primary function of the timeline located under the search bar?
A) To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.
307)Log filtering/ oarsing can be done form_____.
A) Heavy Forwarers(HF)
308)Alert throttling is used to_____.
A)Stop spamming yourself with alerts
309)Highlighted search terms indicates_____search result in splunk.
A)Matching
310)The Field Extractor (FX) is used to extract a custom field.A report can be created using this custom feild. The cr eated report can then be shared with other people in the organization.
If another person in the organization runs the shared report and no result are returned, why might this be?(slect all th at apply)
A)The person in the organization running thge report does not have access to the index.
The Extraction is private-
311) The fileds sidebar does not show_____.(selectr all that apply.)
A)All Extracted fileds
312)What does the follwing search do?
Index+condlog type=mysterymear action=eaten i stats count as cornlog_count by us:
A)Creates a Tables of the total count of mysterymeat corndogs split by user.
313) A space is an implied_____ in a search sting.
A)AND
314)Which of the follwing data model are included in the splunk common information Model(CIM) add-on?(select a ll theat apply)
A) Alerts
Database
Email
315)When a search returns_____.you can view the result as a list.
A)Statistical values
316)When extracting fields,we may choose to use our own regular expressions
A)Incorrects
317)Using the exprt function, you can export search result as_____.(select all the apply)
A)Json
Xml
318)A field alias has been created based on an orginal filed.A search whithout any transforming commands is than e xecuted in smart mode.Which filed name appears in the result?
A)Both will appear in the interesting Fields list, but only if they appear in at least 20 percent of events.
319)When performing a regular expression (reger) field extraction using the field Extractor(FX),what happens when the require option is used?
A)Only events with the required string will be included in the extraction.
320)Which of the following statement describes POST workflow action?
A)POst workflow action can open a web page in either the same window or a new.
321)Which of the following statement describe GET workflow action?
A)The variables passed in URIs for GET action are URL encoded during transmission.
322)Which of the following statement des cribes this search?
sourcetype+access_combined I trasaction JSESSIONID timechart avg duration
A) This is a valid search and will display a timechart of the average duration, of each transaction event
323) Which of the folowing about reports is/are true?
A) all of these
324) Whcih of the following statements describe calculated fields (select all that apply)
A) calculated fields can be based on extracted field.

calculated fields are shortcuts for performing calculations using the eval command.
325) _____transforms raw data into events and distributes the results into an index.
A) Indexer
326) After manually editing; a regular expression (regex), which of the following statements is true?
A) The field extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.
327) These users can create global knowledge objects.(select all that apply.)
A) power users
Administrators
328) clicking a SEGMENT on a chart,_____
A) adds the highlighted value to the search criteria.
329) This is what splunk uses to categorize the data that is being indexed.
A) sourcetype
330) When should you use the transaction command instead of the states command?
A) When you have over 1000 events in a transaction.
331) Which of the following are valid options to speed up reports?
A) Edit acceleration
332) What is required for a macro to accept three arguments?
A) The macro's name ends with (3)
333) Which of the following commands will show the maximum bytes?
A) sourcetype=access_*| stats max (bytes)
334) Which of the following eval command function is valid?
A) Tostring()
335) Which of the following search modes automatically returns all extracted fields in the fields sidebar?
A) Verbose
336) Which of the following commands are used when creating visualizations(select all that apply.)
A) Geom
iplocation
Geostats
337) Which of the following statements describe data model acceleration? (select all that apply)
A) private data ,odels cannot be accelerated
accelerated data models cannot be edited.
You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.
338) It is mandatory for the lookup file to have this for an automatic lookup to work.
A) Input field
339) Which group of users would most likely use pivots?
A) Knowledge managers
340) We can use the rename command to ---- (select all that apply.)
A) Give a field a new name at search time
341) Which of the following statements describe macros?
A) A macro is reusable search string that may have a flexible time range.
342) Which is not a comparison opeartor in splunk
A) ?=
343) Which of the following statements about tags is true?
A) Tags can make your data more understandable.
344) The transaction command allows you to ---- events across multiple sources.
A) correlate
345) Which of the following searches will return events contains a tag name privileged?
A) Tag=Privileged
346) This function of the state command allows you to return the middle-most value of field X.
A) Median(X)
347) In what order are the following knowledge objects/configurations applied?
A) Field extractions, field aliases, lookups
348) The stats command will create a --- by default.
A) Table

349) _____datasets can be added to root dataset to narrow down the search
A) child
350) Field aliases are used to ---data
A) normalize
376) which of the following file formats can be extracted using a delimiter field extraction?
A)CSV
377)This role is required to install the CIM Add-on.Select your answer
A)Admin
378)When using the Field Extractor (FX),Which of the following delimiters will work?(select all the apply)
A)Tabs
spaces
pipes
379)For choropleth maps,splunk ships with th following KMZ files(select all the apply)
A)countries of the world
states of the united states
380)What will you learn from the results of the following search?sourcetype=cisco_esa |transaction mid,dcd,icid|tim echat avg(duration)
A)The average time elapsed during each transaction for all transactions
381)Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.
A)lookup
382)The time range specified for a historical search defines the_____
A)Amount of data fetched from index matching that time range
383)In which of the following scenarios in an event type more effective than a saved search?
A)When formatting needs to be included with the search string
384)When using a split series on a chart,the series MUST be displayed using the stacked option.
A)Incorrect
385)What are the two parts of a root event dataset?
A)constraints and fields
386)Which of the following statements is true, especially in large environments?
A)The stats command is faster and more efficient than the stats command
387)This function of the stats command allows you to return the sample standard deviation of a field.
A)stdev
388)Which of the following statements are true for this search?(select all the apply.)
SEARCH:sourcetype=access*|fields action productld status
A)limit the fields are extracted
users the table command to improve preformance
389)During the validation step of the field extractor workflow:select your answer.
A)You can remove values that aren't a mantch for the field you want to define
390)Which are valid waysto create an event type?(select all the apply)
A)By going to the setting memu and clicking event type>new.
By selecting an event in search result and clicking event action >Build event type.
391)These kinds of charts represent a series in a single br with multiple sections
A)split-series
392)when multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?
A)Priority
393)Calculated fields can be based on which of the following?
A)Extracted fields
394)Data model fields can be added using the auto-extracted method.which of the following statements describe Aut o-extracted fields?(select all the apply)
A)Auto-Extracted fields can be added if they already exist in the dataset with constraints
Auto-extracted fields can be given a friendly name for use in pivot
Auto-extracted fields can be hidden in pivot
395)which of the following are required to create a POST workflow action?
A)XMI attributes,URI,name.

396)What dies the fillnull command replace null values with,it the value argument is not specified?
A)Zero
397)Howdoes a user display a chart in stack mode?
A)By changing stack model in the format menu.
398)Which of the following can be used with the eval command tostring function(select all the apply)
A)commas"
"hex"
duration"
399)Which of the following search control will not re-rerun the search?(select all the apply)
A)select a range of bars on the timelines
select a bar on the timeline
deselect
340)Which of the following statements describes search workflo actions?
A)the user can define the time range of the search when created the workflow action.
341)What do events in a transaction have in common?
A)All events in a transaction must have the same sourcetype
342)a real-time alert is_____
A)constantly running n the background
343)The limit attribute will_____
A)override default of 10
344)What does the splunk common information model (CIM) add-on include?(select all the apply)
A)pre-configured data models
custom visualizations
fields and event category tags
345)which of the following search will show the number of categoryld used by each host?
A)sourcetype=access_*|stat sum(categoryID)by host
346)which of the following statement describe the command below(select all that apply)
A)An additional field named eventcount is created
event with the same JSESSIONID wil be grouped together ito a single event
An additional fields named duration is created.
347)What is the correct syntax to search for a tag associated with a value on the spacific fields?
A)Tag::<field>=<tagname>
348)A calculated fields maybe based on which of the following?
A)extracted fields
349)What does the transcation command do?
A)Creates a single event a group of events.
350)Which of the following workflow actions can be executed from search results(select all the apply)
A)Get
post
search
351)Which of the folliwing statement about macros is true?(select all the apply)
A)Argument values are used to resolve the search string at execution time
Argument are dedfined at execution time
352)This tab shows you the event patterns in the results of a specific search.
A)Patterns
353)What functionality does the splunk common information model(CIM) rely on to normalize fields with different names?
A)Fields
354)Complete the search,....|_____Failure>successes
A)where
355)Select this in the fields sidebar to automatically pipe you search results to the rare command.
A)rare values
356)These allow you to categorize events based on search terms.select your answer.
A)Events types
357)The_____axis should always be numeric.

A)Y
358)Field aliases can only be applied to a single source type,source,or host.
A)Incorrect
359)Which seearch would limit an "alert" tag to the "host"field?
A)tag::host=alert
360)Required fields in a data model:
A)constrains thev dataset to only return events that include that field
361)A workflow action can:
A)all of these
362)Tags can be added to event types.
A)Correct
363)A field can only have one field alias.
A)incorrect
364)What is the correct way to name a macro withtwo arguments?
A)US_sales(2)
365)If a search return _____it can be viewed as a chart.
A)statistics
366)Workflow action can only be applied to a single field.
A)Incorrect
367)This role is required to install the CIM Add-on.
A)admin
368)Field aliases are used to_____data
A)normalize
369)This workflow Action type directs users to a specified URI
A)GET
370)You can pipe the results of a macro to other commands.
A)Correct
371)Which of these are NOT data model dataset types:
A)lookups
372)The srach expansion tool:
A)allows you to see what a macro will expand to before you a search
373)Tags are descriptive names for_____
A)key value pairs
374)Event type do not show up in the fields list
A)incorrect
375)When using a field value variable with a workflow action,which punctuation mark will escape the data ?
A)!
376)This workflow action type sends field values to external resources.
A) post
377) Calculated fields are based on underlying:
A) eval expressions
378) --------datasets can be added to a root dataset to narrow down the search
A) child
379) The CIM add-on indexes extra data and will affect license usage.
A) incorrect
380) The number of arguments in a macro must be included in the macro name.
A) correct
381) Fields used in data models must already be extracted before creating the datasets.
A) incorrect
382) Once a field alias is created:
A) you can still use the original field name to search
383)These allows you to categorize events based on search terms
A)Events types
384)the splunk CIM add-on include data models in a _____format
A)json

385)Search macros:
A) can pass arguments to the search
are time-range independent
allow you to store entire search string ,including pipes and eval statements
386)what is the proper syntax for using a macro named "us_sales"
A)'us_sales'
387)You can only add one tag per field value pair.
A)incorrect
388)The only way to access and use a dataset is form the pivot interface.
A)incorrect
389)Which of the following are vaild option with the chat command?
A)usenull
useother
390)To use field value data from an event in a workflow action ,we need to:
A)wrap the field in dollar signs
391)By default,data models in the CID add-on will search across all indexes
A)correct
451)Hidden fields in a data model:
A)will not be displayed to a pivot user, but can be used to define other datasets
452)You can normalize data for CIM use:
A)Using Knowledge Objects, at index time
453)The data models in the CIM Add-on are accelerated by default.
A)Incorrect
454)You can only use one eval commands per search.
A)Incorrect
454)You can only use one eval command per search.
A)Incorect
455)During the validation step of the field extractor workflow:
A)You can remove values that aren't a match for the field you want to define.
456)Which function should you use with the transaction command to set the maximum total time between the earlies t and latest events returned?
A)maxspan
457)If you want to format values without changing their characteristics which would you use?
A)the fieldformat command
458)Which of these is not a field that is automatically created with the transaction command?
A)maxcount
459)The eval command if command requires the following three arguments (in order):
A)Boolean expression, result if true, result if false
460)Which users can create private knowledge objects?
A)admin, power, user
461)Mark the terms that fill in the blanks in the correct order: use___to see results of a calculation, or group events o n a field value. Use____to see events correlated together, or grouped by start and end values.
A)Stats,transaction
462)When a user creates a knowledge object it is automatically set to ___.
A)private
463)The eval command overwrites field values in the splunk index.
A)Incorrect
464)In the field extractor utility, this button will display events that do not contain extracted fields.
A)Non-matches
465)___can share a knowledge object across all apps.
A)administrators
466)The field extarctor utility allows you to extract fields using the following two methods:
A)regex and delimiter
467)Users with this role can reassign knowledge objects.
A)admin

468)Knowledge objects are automatically shared with all users.
A)Incorrect
469)The transaction command allows you to _____events across multiple sources.
A)Correlate
470)Once a field is created using the regex method, you cannot modify the underlying regular expression.
A)Incorrect
471)Knowledge objects can be used to normalize data.
A)Correct
472)You can create a transaction based on multiple fields.
A)Correct
473)Knowledge objects should be named as generically as possible.
A)Incorrect
474)The trendline command requires the following three arguments.
A)trend type, time period, and field
475)The maxpause definition.
A)Finds group of events where the span of time between included events does not exceed a specific value.
476)It is suggested that you name your knowledge objects using____segmented keys.
A)6
477)If the destination field for the eval command already exists, it is:
A)Overwritten by the new field defined in the eval command
478)After editing your regular expression from the field extractor utility, you will be returned to the utility.
A)Incorrect
479)By default, the fillnull command replaces null values with:
A)zero
480)Fields extracted with the field extractor:
A)are specific to a host, source, or source type
481)How many ways are there to acess the field extractor utility?
A)3
482)How is the astrick used in splunk search?
A)as awildcard
483)Which option is NOT available with the chart and timechart commands?
A)usefill
484)When searching, field values are cases:
A)Case insensitive
485)Which command removes results with duplicate field values?
A)dedup
486)The_____clause allows you ti define which field is represented on the X axis of a chart
A)over
487)Warm buckets in splunk indexes are named by:
A)the timestamp of first and last event in the bucket
488)By default, the top command returns the top___values of agiven field.
A)10
489)The timechart command buckets data in time intervals depending on:
A)the selected time range
490)The iplocation and geostats commands can be used together.
A)Correct
491)WHich of the following is NOT a stats function?
A)addtotals
492)In this search____will appear on the y axis.
SEARCH:sourcetype=access_combined status!=200|chart count over host
A)count
493)What is wrong with the following search syntax:
A)Asia is not in double quotes
494)The iplocation command:
A)Returns location information for events that includes external IP addresses

495)The geom command allows you to create.
A)choropleth maps
496)Bucket names in splunk indexes are used to:
A)determine if the bucket should be searched based on the time range of the search
497)The search job inspector shows you how long a given search took to run.
A)Correct
498)Time is the most efficient filter you can apply to a search.
A)Correct
499)The____function of the eval command can take multiple boolean arguments.
A)Case
500)This command will compute the sum of numeric fields within events and place the result in a new field
A)addtotals
501)Which command is used to create choropleth maps?
A)geom
502)These are booleans in the splunk search language.
A)AND, NOT, OR
503)Which type of visualization allows you to show a third dimension of data?
A)bubble chart
504)The gauge command:
A)allow you to set colored ranges for a single value visualization
505)How many results are shown by default when using a Top or Rare command?
A)10
506)The trendline command requires the folowing three arguments.
A)trend type, time period, and field
507)Which is not a comparison operator in splunk?
A)?=