$Question #1 Which search string only returns events from hostWWW3?
A. host=*
B.host=WWW3
C.host=WWW*
D. Host=WWW3
^Correct Answer: B
Community vote distribution B (100%)

$Question #2 By default, how long does Splunk retain a search job?
A. 10 Minutes
B. 15 Minutes
C. 1 Day
D. 7 Days
^Correct Answer: A Reference: https://docs.splunk.com/D
ocumentation/Splunk/7.2.6/Search/Extendjoblifetimes

$Question #3 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.
^Correct Answer: B Reference: https://docs. splunk.com/Docume ntation/Splunk/7.2.6/
Knowledge/ Defineanauto naticlookupinSplunkWeb
Community vote distribution B (100%)

$Question #4 Which of the following Splunk components typically resides on the machines where data originates?
A. Indexer
B. Forwarder
C. Search head
D. Deployment server
^Correct Answer: B

$Question #5 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.

^Correct Answer: D Reference: https://docs.splunk.com/[ )ocumentation/Splunk/7.2.6/Report/Managereportpermissions
Community vote distribution B (67%) D (33%)

$Question #6 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.
^Correct Answer: B
Community vote distribution B (100%)

$Question #7 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)
^Correct Answer: B Reference: https:// docs.splunk. com/Documentation/ Splunk/7.2.6/Search/Aboutsubsearches
Community vote distribution B (100%)

$Question #8 Topic 1 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
^Correct Answer: B
Community vote distribution B (100%)

$Question #9 Topic 1 Which of the following constraints can be used with the top command?
A. limit
B. useperc
C. addtotals
D. fieldcount
^Correct Answer: A Reference: https://answers.splunk.com/answers/339141/how-to-use-top-com mand-or-stats-with-sort-results.html
Community vote distribution A (100%)

$Question #10 Topic 1 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.
^Correct Answer: C
Community vote distribution C (56%) D (44%)

$Question #11 When running searches, command modifiers in the search string are displayed in what color?
A. Red
B. Blue
C. Orange
D. Highlighted
^Correct Answer: C Reference: https:// docs.splunk.com/ Documentation/Splunk/7.2.6/ Search/Parsingsearches
Community vote distribution B (100%)

$Question #12 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
^Correct Answer: C Reference: https://docs.splunk.com/[ )ocumentation/Splunk/7.2.6/ Knowledge/Developnamingcon ventionsforknowledgeobjecttitles

$Question #13 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.
^Correct Answer: C Reference: https:// docs.splunk.com/ Documentation/Splunk/7.2.6 /Search/Extendjoblifetimes
Community vote distribution A (100%)

$Question #14 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.
^Correct Answer: A
Community vote distribution A (100%)

$Question #15 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.
^Correct Answer: C Reference: https://docs.splunk.cc m/ Documentation/Spl
unk/7.2.6/Viz/Working With DashboardPanels

$Question #16 Which of the following are common constraints of the top command?
A. limit, count
B. limit, showpercent
C. limits, countfield
D. showperc, countfield
^Correct Answer: A
Community vote distribution D (90%) 10%

$Question #17 When displaying results of a search, which of the following is true about line charts?
A. Line charts are optimal for single and multiple series.
B. Line charts are optimal for single series when using Fast mode.
C. Line charts are optimal for multiple series with 3 or more columns.
D. Line charts are optimal for multiseries searches with at least 2 or more columns.
^Correct Answer: C Reference: https://docs.splunk.com/Documentat ion/
Splunk/7.2.6/Viz/LineAreaCharts
Community vote distribution A (70%) C (30%)

$Question #18 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.
^Correct Answer: C
Community vote distribution C (100%)

$Question #19 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.
^Correct Answer: D
Community vote distribution D (100%)

$Question #20 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.
^Correct Answer: D Reference: https://docs.splunk.c com/Documentation/ Splunk/7.2.6/Report/ Schedulereports

$Question #21 After running a search, what effect does clicking and dragging across the timeline have ve?
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.
^Correct Answer: C Reference: https://docs. splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline
Community vote distribution B (92%) 8%

$Question #22
Which command is used to review the contents of a specified static lookup fle?
A. lookup
B.csvlookup
C. inputlookup
D. outputlookup
^Correct Answer: C

$Question #23 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.
^Correct Answer: C

$Question #24 When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?
A. I
B.$
C.!
D.
^Correct Answer: D Reference: https:// docs. splunk.com/Documentation/ Spl
unk/7.2.6/SearchReference/Sort

$Question #25 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
^Correct Answer: C Reference: https://docs.splunk. com/Documentation/Splunk/7.2.6/Search/
Selecttimerangestoapply

$Question #26 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)
^Correct Answer: C
Community vote distribution C (100%)

$Question #27 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.

^Correct Answer: C
Community vote distribution D (89%) 11%

$Question #28 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
^Correct Answer: A Reference: https:// answers.splunk.com/ answers/1858641 selected-fields-in-fields-side-bar.html
Community vote distribution B (100%)

$Question #29 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.
^Correct Answer: B Reference: https:// answers.splunk.com/ answers/65/ are-field-values-case-sensitive.html
Community vote distribution B (100%)

$Question #30 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.
^Correct Answer: A Reference: https:// docs.splunk.com/ Documentation/ Splunk/7.2.6/Sear chReference/Rare

$Question #31 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
^Correct Answer: A Reference: https:// docs.splunk. com/Documentation/Splunk/7.2.6/ Alert/Configuringscriptedalerts

$Question #32 Which Boolean operator is always implied between two search terms, unless otherwise specified?
A. OR
B.NOT
C. AND D.XOR
^Correct Answer: C Reference: https://docs. splunk.com/Documentati on/Splunk/7.2.6/Search/ Booleanexpressions

$Question #33 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.
^Correct Answer: C
Community vote distribution B (100%)

$Question #34 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)
^Correct Answer: A Reference: https://docs splunk. com/Documentation/Splunk/7.2.6/Search/Usethestatsc ommandandfunctions
Community vote distribution A (100%)

$Question #35 A collection of items containing things such as data inputs, Ul elements, and knowledge objects is known as what?
A. An app
B.JSON
C. A role
D. An enhanced solution
^Correct Answer: A

$Question #36 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.
^Correct Answer: A

$Question #37 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.
^Correct Answer: A Reference: https:// docs.splunk.com/ Documentation/Splunk/7.2.6/SearchReference/ Stats#1._Compare_the_ difference_between using_the_stats_and. chart_commands
Community vote distribution A(100%)

$Question #38 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 af ''to remove.
D. Use fields Plus to add and fields Minus to remove.
^Correct Answer: C Reference: https://docs.splunk com/Documentatio n/Splunk/7.2.6/Sear chReference/Fields
Community vote distribution C (54%) A (46%)

$Question #39 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.
^Correct Answer: A
Community vote distribution A (80%) B (20%)

$Question #40
In the fields sidebar, which character denotes alphanumeric field values?
A.#
B. %
C.a
D.a#
^Correct Answer: C

$Question #41 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.
^Correct Answer: B
Community vote distribution C (100%)

$Question #42
What syntax is used to link key/value pairs in search strings?
A. action+purchase
B. action=purchase
C.action I purchase
D. action equal purchase
^Correct Answer: B

$Question #43
What user interface component allows for time selection?
A. Time summary
B. Time range picker
C.Search time picker
D. Data source time statistics
^Correct Answer: B

$Question #44 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
^Correct Answer: C
Community vote distribution A (100%)

$Question #45 When placed early in a search, which command is most effective at reducing search execution time?
A. dedup
B. rename
C. sort-
D. fields +
^Correct Answer: A
Community vote distribution D (53%) A (47%)

$Question #46 Which of the following is the most efficient filter for running searches in Splunk?
A. Time
B. Fast mode
C. Sourcetype
D. Selected Fields
^Correct Answer: C
Community vote distribution A (100%)

$Question #47 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.
^Correct Answer: D

$Question #48 Which of the following file types is an option for exporting Splunk search results? A.PDF
B. JSON
C.XLS D.RTF
^Correct Answer: A Reference: https://docs. splunk.com/Documentati on/Splunk/7.2.6/Search/ExportdatausingSplunkWeb
Community vote distribution B (100%)

$Question #49 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 >
^Correct Answer: D

$Question #50 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 afEvent Countaf
B. index=security failure | stats count as 2fEvent Count2f
C. index=security failure | stats count by afEvent Countre
D. index=security failure | stats dc(count) as 2fEvent Countaf
^Correct Answer: C

Community vote distribution B (100%)

$Question #51 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
^Correct Answer: A
Community vote distribution C (100%)

$Question #52 Which of the following index searches would provide the most efficient search performance?
A. index=*
B. index=web OR index=s =s*
C. (index=web OR index=sales)
D. *index=sales AND index=web*
^Correct Answer: B
Community vote distribution C (90%) 10%

$Question #53 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.
^Correct Answer: B

$Question #54 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.
^Correct Answer: D
Community vote distribution D (100%)

$Question #55 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.
^Correct Answer: D
Community vote distribution D (63%) B (38%)

$Question #56 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
^Correct Answer: D Reference: https://docs.splunk.com/ Documentation/ Splunk/7.2.6/ Alert/ Reviewtriggeredalerts
Community vote distribution A (100%)

$Question #57 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 Pane nel.
^Correct Answer: A

$Question #58 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.
^Correct Answer: B

$Question #59
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
^Correct Answer: C

$Question #60 At index time, in which field does Splunk store the timestamp value?

A. time
B. _time
C. EventTime
D. timestamp
^Correct Answer: B Reference: https:// docs.splunk.com/ Documentation/ Splunk/7.2.6/Data/HowS plunkextractstimestamps

$Question #61 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.
^Correct Answer: D
Community vote distribution C (100%)

$Question #62 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.
^Correct Answer: A Reference: https://docs.splunk.com /Documentation/Splunk/ 7.3.1/SearchTutorial/ Aboutsavingandsharingreports#Save_ a_search_as_a_report

$Question #63 What can be included in the All Fields option in the sidebar?
A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions
^Correct Answer: D Reference: https://docs. splunk.com/Documentation /Splunk/7.3.1/Knowledge/ Extractfieldsinteract ivelywithIFX#Access. the. field_ extractor_from_the_ All_Fields_dialog_box
Community vote distribution C (100%)

$Question #64 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.
^Correct Answer: D Reference: https://docs.splunk.co m/ Documentation/Splu Ink/7.3.1/SearchTutor ial/Usefieldstosearch

$Question #65 When a Splunk search generates c alculated data that appears in the Statistics tab, in what formats can the re sults be exported?
A. CSV, JS0N,PDF
B.CSV,XML,JS0N
C. Raw Events, XML, JSON
D. Raw Events, CSV, XML, JSON
^Correct Answer: B Reference: https://docs.splunk.c com/Documentation/ Splunk/7.3.1/Search, Exportsearchresults
Community vote distribution B (100%)

$Question #66 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 afterror failurent
D. index=security NOT error NOT fail
^Correct Answer: B Reference: https://docs. splunk.com/Documentation/ Splu nk/7.3. 1/SearchReference/Search
Community vote distribution A (100%)

$Question #67 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.
^Correct Answer: B

$Question #68 Which of the following fields is stored with the events in the index?
A. user
B. source
C. location
D. sourcelp
^Correct Answer: B Reference: https:// answers.splunk.com/ answers/ 609626/is-there-a-way-to-check -if-makeresults-stored-the. Html

$Question #69 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.
^Correct Answer: D Reference: https://answers. splunk.com/ answers/231 429/ cani-have-multiple-panels s-using-the-same-inline-s.html
Community vote distribution A (100%)

$Question #70 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.
^Correct Answer: C Reference: https:// answers. splunk.com/answers/1 49904/ find-earliest-and-latest-event- per-day-for-a-time-range.html
Community vote distribution D (100%)

$Question #71 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.
^Correct Answer: B Reference: https:// answers.splunk.com/ answers/617772/why-am-i-getting-a- http-503-error-when-using-threa.html

$Question #72 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.
^Correct Answer: C Reference: https://docs.splunk .com/Documentatio n/Splunk/7.3.1/Sea rchReference/Stats

$Question #73 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.
^Correct Answer: D Reference: https://docs.splunk.c om/Documentation/S plunk/7.3.1/SearchTu torial/Startsearching

$Question #74 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.
^Correct Answer: D
Community vote distribution D (100%)

$Question #75 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
^Correct Answer: C Reference: https:// docs.splunk.com/ Documentation/Splunk/7.3.1 /SearchReference/ Inputlookup

$Question #76 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.
^Correct Answer: D
Community vote distribution D (100%)

$Question #77 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.
^Correct Answer: A Reference: https://docs.splunk.com/ Documentation/Splunk/ 7.3.1/Report/ Managereportpermissions

$Question #78 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.

^Correct Answer: C Reference: https://docs.splunk.com /Documentation/ Splunk/ 7.3. 1/SearchReference/Rare

$Question #79 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.
^Correct Answer: D Reference: https://docs. splunk.com/Documentation/ Splunk/7 3. 1/SearchTutorial/Usefieldstosearch
Community vote distribution D (100%)

$Question #80 By default, which of the following is a Selected Field?
A. action
B. clientip
C. categoryld
D. sourcetype
^Correct Answer: D Reference: https://docs.splunk.com/ Documentation/Splur 17.3.1/Search Tutorial/Usefieldstosearch#Specif additional__ selected__fields

$Question #81 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*
^Correct Answer: C

$Question #82 Which command automatically returns percent and count columns when executing searches? A.top
B. stats
C. table
D. percent
^Correct Answer: A Reference: https://docs.splunk.com/Docur nentation/Splunk/7.3. 1/Search/ Aboutsubsearches

$Question #83 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.
^Correct Answer: B Reference: https:// docs.splunk.com/Do cumentation/Splunk/ 7.3.1/Knowledge/ Aboutlookupsandfieldactions
Community vote distribution C (100%)

$Question #84 Which search string is the most efficient?
A. 2ffailed passwordie
B. affailed password
C. index=* affailed passwordle
D. index=security affailed passwordaf
^Correct Answer: D

$Question #85 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
^Correct Answer: D
Community vote distribution D (89%) 11%

$Question #86 transforms raw data into events and distributes the results into an index.
A. Index
B. Search Head
C. Indexer
D. Forwarder
^Correct Answer: C
Community vote distribution C (100%)

$Question #87
Documentations for Splunk can be found at docs.splunk.com
A. True
B. False
^Correct Answer: A

$Question #88
Which component of Splunk is primarily responsible for saving data?

A. Search Head
B. Heavy Forwarder
C. Indexer
D. Universal Forwarder
^Correct Answer: C

$Question #89
Universal forwarder is recommended for forwarding the logs to indexers.
A. False
B. True
^Correct Answer: B

$Question #90 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.
^Correct Answer: ACD

$Question #91
Three basic components of Splunk are (Choose three.):
A. Forwarders
B. Deployment Server
C. Indexer
D. Knowledge Objects
E. Index
F. Search Head
^Correct Answer:ACF

$Question #92 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.
^Correct Answer: A

$Question #93 We should use heavy forwarder for sending event-based data to Indexers.
A. False
B. True

^Correct Answer: B
Community vote distribution B (100%)

$Question #94 Splunk Enterprise is used as a Scalable service in Splunk Cloud.
A. True
B. False
^Correct Answer: A
Community vote distribution A (50%) B (50%)

$Question #95
Which component of Splunk let us write SPL query to find the required data?
A. Forwarders
B. Indexer
C. Heavy Forwarders
D. Search head
^Correct Answer: D

$Question #96
All components are installed and administered in Splunk Enterprise on-premise.
A. True
B. False
^Correct Answer: A

$Question #97
Log fltering/parsing can be done from
A. Index Forwarders (lF)
B. Universal Forwarders (UF)
C. Super Forwarder (SF)
D. Heavy Forwarders (HF)
^Correct Answer: D

$Question #98 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
^Correct Answer: B

$Question #99 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
^Correct Answer: F

$Question #100
Portal for Splunk apps can be accessed through www.splunkbase.com
A. False
B. True
^Correct Answer: B

$Question #101
Splunk shows data in
A. ASCIl Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.
^Correct Answer: B

$Question #102
Which of the following can be used as wildcard search in Splunk?
A.=
B.>
C.!
D.*
^Correct Answer: D

$Question #103 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
^Correct Answer: C

$Question #104
Prefix wildcards might cause performance issues.

A. False
B. True
^Correct Answer: B

$Question #105
Machine data can be in structured and unstructured format.
A. False
B. True
^Correct Answer: B

$Question #106
Field names are case sensitive.
A. True
B. False
^Correct Answer: A

$Question #107
Splunk internal fields contains general information about events and starts from underscore i.e. -.
A. True
B. False
^Correct Answer: A

$Question #108
How many main user roles do you have in Splunk?
A.2
B.4
C.1
D.3
^Correct Answer: D

$Question #109 Which of the following are Splunk premium enhanced solutions? (Choose three.)
A. Splunk User Behavior Analytics (UBA)
B. Splunk IT Service Intelligence (1TSI)
C. Splunk Enterprise Security (ES)
D. Splunk Analytics Security (AS)
^Correct Answer: ABC

$Question #110
Fields are searchable name and value pairings that differentiates one event from another.
A. False
B. True
^Correct Answer: B

$Question #111 Splunk extracts fields from event data at index time and at search time.
A. True
B. False
^Correct Answer: A Reference: https:// docs.splunk.com/D ocumentation/Splun k/7.2.3/SearchTutori al/Usefieldstosearch

$Question #112
Field values are case sensitive.
A. True
B. False
^Correct Answer: B
Community vote distribution
B (80%)   A(20%

$Question #113 Splunk indexes the data on the basis of timestamps.
A. True
B. False
^Correct Answer: A Reference: https:// docs.splunk.com/Do cumentation/Splunk/ 7.2.3/Data/ Aboutdefaultfields

$Question #114 is the default web port used by Splunk.
A. 8089
B. 8000
C. 8080
D. 443
^Correct Answer: B
Community vote distribution B (100%)

$Question #115 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.
^Correct Answer: ABC

$Question #116
Parsing of data can happen both in HF and Indexer.
A. Only HF
B.No
C. Yes
^Correct Answer: C

$Question #117
Monitor option in Add Data provides
A. Only continuous monitoring.
B. Only One-time monitoring.
C. None of the above.
D. Both One-time and continuous monitoring.
^Correct Answer: D

$Question #118
License Meter runs before data compression.
A. No
B. Yes
^Correct Answer: B

$Question #119 Forward Option gather and forward data to indexers over a receiving port from remote machines.
A. False
B. True
^Correct Answer: B
Community vote distribution B (80%) A (20%)

$Question #120 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
^Correct Answer: BCEG

$Question #121
Data sources being opened and read applies to:
A. None of the above
B. Indexing Phase
C. Parsing Phase
D. Input Phase
E. License Metering
^Correct Answer: D

$Question #122
Select the correct option that applies to Index time processing (Choose three.).
A. Indexing
B. Searching
C. Parsing
D. Settings
E. Input
^Correct Answer: ACE

$Question #123
Splunk automatically determines the source type for major data types.
A. False
B. True
^Correct Answer: B

$Question #124
Parsing of data can happen both in HF and UF.
A. Yes
B. No
^Correct Answer: B

$Question #125
Upload option creates inputs.conf
A. Yes
B. No
^Correct Answer: B

$Question #126
Splunk index time process can be broken down into phases.
A.3
B.2
C.4
D.1
^Correct Answer: A

$Question #127 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
^Correct Answer: E
Community vote distribution E (100%)

$Question #128
Uploading local fles though Upload options index the file only once.
A. No
B. Yes
^Correct Answer: B

$Question #129
Which of the statements are correct about HF? (Choose three.)
A. Parsing
B. Masking
C. Searching
D. Forwarding
^Correct Answer:ABD

$Question #130
Where does Licensing meter happen?
A. Indexer
B. Parsing
C. Heavy Forwarder
D. Input
^Correct Answer: A

$Question #131
Matching search terms are highlighted.

A. Yes
B. No
^Correct Answer: A

$Question #132 Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.
A. No
B. Yes
^Correct Answer: B
Community vote distribution A (83%) B (17%)

$Question #133
Zoom Out and Zoom to Selection re-executes the search.
A. No
B. Yes
^Correct Answer: B
Community vote distribution
B(100%)

$Question #134
Every Search in Splunk is also called
A. None of the above
B. Job
C. Search Only
^Correct Answer: B

$Question #135 Matching of parentheses is a feature of Splunk Assistant.
A. No
B. Yes
^Correct Answer: B
Community vote distribution A (50%) B (50%)

$Question #136
Search Assistant is enabled by default in the SPL editor with compact settings
A. No
B. Yes
^Correct Answer: B

$Question #137 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.
^Correct Answer: C
Community vote distribution C(100%)

$Question #138
@ Symbol can be used in advanced time unit option.
A. No
B.Yes
^Correct Answer: B

$Question #139
The new data uploaded in Splunk are shown in
A. Real-time
B.10 Minutes
C. Overnight Download
D.30 Minutes
^Correct Answer: A

$Question #140 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
^Correct Answer: F
Community vote distribution B (50%) A (50%)

$Question #141
You can change the App context in Input setting.
A. No
B. Yes
^Correct Answer: B

$Question #142
The default host name used in Inputs general settings can not be changed.
A. False
B. True
^Correct Answer: A

$Question #143
Events in Splunk are automatically segregated using data and time.
A.Yes
B. No
^Correct Answer: A

$Question #144 You are able to create new Index in Data Input settings.
A. No
B. Yes
^Correct Answer: B
Community vote distribution A (67%) B (33%)

$Question #145
Splunk Parses data into individual events,extracts time, and assigns metadata.
A. False
B. True
^Correct Answer: B

$Question #146 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.
^Correct Answer: A
Community vote distribution D (100%)

$Question #147
Which symbol is used to snap the time?
A. @
B.&
C.*

D.#
^Correct Answer:A

$Question #148 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.
^Correct Answer: ACE

$Question #149
There are three different search modes in Splunk (Choose three.):
A. Automatic
B. Smart
C. Fast
D. Verbose
^Correct Answer: BCD

$Question #150
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.
^Correct Answer: ABCE
Community vote distribution
ABCE (100%)

$Question #151
Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):
A. Open new search.
B. Exclude the item from search.
C. None of the above.
D. Add the item to search.
^Correct Answer: ABD

$Question #152
You can view the search result in following format (Choose three.):
A. Table

B. Raw
C. Pie Chart
D. List
^Correct Answer: ABD

$Question #153
Snapping rounds down to the nearest specified unit.
A. Yes
B. No
^Correct Answer: A

$Question #154
Data summary button just below the search bar gives you the following (Choose three.):
A. Hosts
B. Sourcetypes
C. Sources
D. Indexes
^Correct Answer: ABC

$Question #155
What options do you get after selecting timeline? (Choose four.)
A. Zoom to selection
B. Format Timeline
C. Deselect
D. Delete
E. Zoom Out
^Correct Answer: ABCE

$Question #156
At the time of searching the start time is 03:35:08.
Wil it look back to 03:00:00 if we use -30m@h in searching?
A. Yes
B. No
^Correct Answer: A

$Question #157
Can you stop or pause the searching?
A. No
B. Yes
^Correct Answer: B

$Question #158
You can also specify a time range in the search bar. You can use the following for beginning and ending for a time range (Choose two.):
A. Not possible to specify time manually in Search query
B. end=
C. start=
D. earliest=
E. latest=
^Correct Answer: DE
Community vote distribution
DE (100%)

$Question #159
Which al time unit abbreviations can you include in Advanced time range picker? (Choose seven.)
A. h
B. day
C. mon
D. yr
E. y
E w
G. week
H. d
I. S
J. M
^Correct Answer: ACEFH/J
Community vote distribution
ACEFHIJ (100%)

$Question #160
Interesting fields are the fields that have at least 20% of resulting fields
A. True
B. False
^Correct Answer: A

$Question #161
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 wil enable it.
D. Click Setings -> Find field option -> Drop down select field -> enable selected field -> check now field should be visible in the list of selected fields.
^Correct Answer: A
Community vote distribution
A (100%)

$Question #162
Field names are case sensitive and field value are not.
A. True
B. False
^Correct Answer: A

$Question #163
!= and NOT are same arguments.
A. True
B. False
^Correct Answer: B
Community vote distribution
B (100%)

$Question #164
Query - status != 100:
A. Wil 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. Wil get different results depending on data.
^Correct Answer: A

$Question #165
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 al events where status field doesn't exist.
^Correct Answer: C
Community vote distribution
C (88%)
13%

$Question #166

Wil 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
^Correct Answer: B

$Question #167
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.
^Correct Answer: ABCFG

$Question #168
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
^Correct Answer: B

$Question #169
Put query into separate lines where l (Pipes) are used by selecting following options.
A. CTRL + Enter
B. Shift + Enter
C. Space + Enter
D. ALT + Enter
^Correct Answer: B

$Question #170
Fields are searchable key value pairs in your event data.
A. True
B. False
^Correct Answer: A

$Question #171
Selected fields are a set of configurable fields displayed for each event.
A. True
B. False
^Correct Answer: A

$Question #172
Following are the time selection option while making search: (Choose al that apply.)
A. Date & Time Range
B. Advanced
C. Date Range
D. Presets
E. Relative
^Correct Answer: ABCDE
Community vote distribution
ABCDE (100%)

$Question #173
Search Language Syntax in Splunk can be broken down into the following components. (Choose al that apply.)
A. Search term
B. Command
C. Pipe
D. Functions
E. Arguments
F. Clause
^Correct Answer: ABCDEF

$Question #174 When saving a search dire ectly to a dashboard panel instead of saving as a report first, which of the fc pllowing is created?
A. Cloned panel
B. Inline panel
C. Report panel
D. Prebuilt panel
^Correct Answer: C Reference: https://docs.splunk.com/Documentatio
n/Splunk/8.0.3/Search/Savingsearches
Community vote distribution B (100%)

$Question #175 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
^Correct Answer: D Reference: https:// answers. splunk.com/
answers/329699/why-does-my-search head-cluster-captain-start-dele-1.html

$Question #176 Topic 1 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
^Correct Answer: C Reference: https://docs.splunk. com/Documentation /Splunk/8.0.3/Sear(
chReference/search
Community vote distribution A (100%)

$Question #177 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
^Correct Answer: C
Community vote distribution A (100%)

$Question #178 In the Search and Reporting app, which tab displays timecharts and bar charts?
A. Events
B. Patterns
C. Statistics
D. Visualization
^Correct Answer: D Reference: https://docs.splunk.com/Docur nentation/Splunk/8.0.2/Search/
Aboutreportingcommands

$Question #179 What will always appear in the Selected Fields list?
A. index
B. action
C. clientip
D. sourcetype
^Correct Answer: D Reference: https://docs.splunk.co m/ Documentation/Splu
Ink/8.0.3/SearchTutor ial/Usefieldstosearch

$Question #180 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
^Correct Answer: B Reference: https://docs.splunk.com/Docur nentation/Splunk/8.0.3/Search/ Specifytimemodifiersinyoursearch

$Question #181
Which of the following is a Splunk internal field?
A. raw
B. host
C. _host
D. index
^Correct Answer: A
Reference:
https:l//docs.splunk.com/Splexicon:Internalfield

$Question #182 Which command will rename action to Customer Action?
A. | rename action = CustomerAction
B. | rename Action as 2fCustomer Actionaf
C. I rename Action to afCustomer Actionaf
D. | rename action as afCustomer Actionaf
^Correct Answer: D Reference: https:// answers.splunk.com/ answers/ 610038/understanding-command-in-search.html
Community vote distribution D (100%)

$Question #183 Which of the following is the most efficient search?
A. index=* affailed password
B. affailed passwordif index=* :*
C. (index=* OR index=security) affailed password2f
D. index=security affailed passwordle
^Correct Answer: A
Community vote distribution D (83%) A (17%)

$Question #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
^Correct Answer: C Reference: https:// docs. splunk.com/Documentation/ SplunkCloud/latest/SearchReference/Top

$Question #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 ori
D. New events in addition to the same events from the original search
^Correct Answer: C
Community vote distribution C (60%) A (40%)

$Question # 186 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=*
^Correct Answer: C Reference: https://docs.splunk.cc m/ Documentation/Sp
lunk/8.0.3/InheritedD eployment/Yourdata
Community vote distribution C (100%)

$Question #187 Assuming a user has the capability to edit reports, which of the following are editable?
A. Acceleration, schedule, permissions
B. The report's name, schedule, permissions
C. The report's name, acceleration, schedule
D. The report's name, acceleration, permissions
^Correct Answer: B Reference: https://docs. splunk.com/Documentation/ Splunk/
8.0.3/Report/Createandeditreports
Community vote distribution A (100%)

$Question #188 Which of the following is a metadata field assigned to every event in Splunk?
A. host
B. owner
C. bytes
D. action

^Correct Answer: A Reference: https://docs. splunk.com/Documenta tion/Splunk/8.0.3/Data/ Assignmetadatatoeventsdynamically

$Question #189
What are the two most efficient search filters?
A. time and host
B. time and index
C. host and sourcetype
D. index and sourcetype
^Correct Answer: B

$Question #190 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 2f Yesterday
D. Use the time range picker to select afLast 24 hours2f
^Correct Answer: D Reference: https://answers. splunk.com/ answers/1 53100/how-to-get-the-6 event-count-for-the-last- 24-hours-as-a-scheduled-report.html

$Question #191 When is the pipe character, I, used in search strings?
A. Before clauses. For example: stats sum(bytes) I 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
^Correct Answer: B Reference: https://docs.splunk. com/Documentation/ Splunk/8.0.3/Search/ Aboutsearchlanguagesyntax#Quotes_ _and_escaping_characters
Community vote distribution B (100%)

$Question #192 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
^Correct Answer: B Reference: https:// answers.splunk.com/ answers/30376/how-to-display-th e-contents-of-a-lookup-file.html

$Question #193 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
^Correct Answer: C Reference: https:// docs. splunk.com/ Documentation/ Splunk/ 8.0.3/SearchTutoria I/Usefieldstosearch

$Question #194 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
^Correct Answer: D Reference: https://docs. splunk.com/ Documentation/ Splunk/8.0.3/Search/ Extendioblifetimes

$Question #195 Topic 1 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
^Correct Answer: D Reference: https://docs.splunk.com/Document ation/ Splunk/8.0.4/SearchReference /Rare#:~:text=The%20rare%20comr nand%20is%20a,the%20limit%20arg ument%20is% 2010
Community vote distribution D (100%)

$Question #196 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
^Correct Answer: D

$Question #197 What are the three main Splunk components?
A. Search head, GPU, streamer
B. Search head, indexer, forwarder
C. Search head, SQL database, forwarder
D. Search head, SSD, heavy weight agent

^Correct Answer: B Reference: https://www. edureka.co/blog/ splunk-architecture/

$Question #198 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
^Correct Answer: D Reference: https:// docs.splunk.com/D ocumentation/Splun k/8.0.2/Search/Cha ngethesearchmode
Community vote distribution D (100%)

$Question #199 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
^Correct Answer: B Reference: https:// answers.splunk.com/answers/7121 64/ why-are-the-wineventlogsse curity-indexing-in-diffe. Html

$Question #200 In the Search and Reporting app, which is a default selected field?
A. index
B. host
C. _time
D. action
^Correct Answer: A
Community vote distribution B (100%)

$Question #201 The four types of Lookups that Splunk provides out-of-the-box are External, KV Store, Geospatial and which of the following?
A. Correlated
B. Total
C. Segmented
D. File-based
^Correct Answer: D Reference: https://docs.splunk.com/Docun nentation/SplunkCloud/8.2220 2/ Knowledge/Usefieldlookupst oaddinformationtoyourevents

$Question #202 What is the result of the following search? index=myindex source=c:\mydata.txt NOT error=*

A. Only data where the value of the field error does not equal an asterisk (*) will be displayed.
B. Only data that does not contain the error field will be displayed.
C. Only data with a value in the field error will be displayed.
D. Only data where the error field is present and does not contain a value will be displayed.
^Correct Answer: B

$Question #203 When refining search results, what is the difference in the time picker between real-time and relative time ranges?
A. Real-time searches display results from a rolling time window, while relati ve searches display results from a set length of time.
B. Real-time searches happen instantly, while relative searches happen at a scheduled time.
C. Real-time represents events that have happened in a set time window, while relative will display results from a rolling time window.
D. Real-time searches run constantly in the background, while re lative searches only run when certain criteria are met.
^Correct Answer: A
Community vote distribution A (100%)

$Question #204 Topic 1 A SOC manager is complaining that a scheduled alert for failed login attempts triggered 150 emails. They still want to be alerted of failed logins via email, but they want less volume of alerts. Which of the following would resolve this for the SOC manager?
A. Change the schedule so the alert runs more frequently.
B. Disable the alert entirely.
C. Change the trigger from "For each result" to "Once".
D. Change the alert action from email to webhook.
^Correct Answer: A
Community vote distribution C (100%)

$Question #205 By default, which role contains the minimum permissions required to have write access to Splunk alerts?
A. Alerting
B. Admin
C. Power
D. User
^Correct Answer: D
Community vote distribution C (88%) 13%

$Question #206 Which of the following is the appropriately formatted SPL search?
A. index=security sourcetype=linux secure (invalid OR failed) I count as "Potential Issues"
B. index=security sourcetype=linux secure (invalid OR failed) | stats count as "Potential Issues"

C. index=security sourcetype=linux__ secure (invalid OR failed) | count stats as "Potential Issues"
D. index=security sourcetype=linux__ secure (invalid OR failed) | stats as "Potential Issues"
^Correct Answer: B

$Question #207 Topic 1 When using the top command in the following search, which of the following y will be true about the results? index="main" sourcetype="access__*" action="purchase" | top 3 statusCcde by user showperc=f countfield=status__code__count
A. The percentage field will be displayed in the results.
B. The top three most common values in statusCode will be displayed for each user.
C. The search will fail. The proper top command format is top limit=3 instead of top 3.
D. Only the top three overall most common values in statusCode will be displayed.
^Correct Answer: D
Community vote distribution B (100%)