**Searching and Reporting**

1. Which search will return the same events as the search in the searchbar? **“password AND failed”**
2. What is the most efficient way to filter events in Splunk? **By Time**
3. Which is not a comparison operator in Splunk? **?=**
4. How is the asterick used in Splunk Search? **As a wild card**
5. As a general practice, inclusion is better than exclusion in a Splunk Search. **True**
6. Field names are? **Case sensitive**
7. What command would you use to remove the status field from the returned events? **Fields –**
8. Finish the rename command to change the name of the status field to HTTP Status. Status as “HTTP Status”
9. Would the client ip column be removed in the results of this search? No the name was changed
10. What is missing from the search? Quotation marks around user ID
11. Which command removes results with duplicate field values? Dedup
12. To display the most common values in a specific field what command would be used? Top
13. How many events are shown by default when using top or rare command? 10
14. Unlimited results? **Limit=0**
15. Which one of these is not a stats function? **Addtotals**
16. Which clause would you use to rename the count field? **AS**
17. Which stats function would you use to find the average value of a field? AVG
18. If a search returns this you can view the results as a chart? Statistical values
19. When using the chart command the x axis should always be numeric? False
20. The time chart command clusters data in time intervals dependent on. Time range selected
21. Finish this search to remove any results that do not contain a value in the product\_name field. Usenull=f
22. When using the search below, what axis would time be on? **X**
23. The trendline command requires this many arguments? 3
24. In the following search, what should the empty argument contain? **An IP address**
25. The Geostats command requires both latitude and longitude data to use on a map? True
26. Data created using the IP location command cannot be used with the Geostats command. False
27. Which command do you used when creating a choropleth map? Geom
28. Which Splunk search command allows you to perform mathematical functions on field values? Eval
29. Which is the correct argument order when using the eval if function? If (Boolean, Is True, Is False)
30. If you want to format values without changing their characteristics which would you use? The Field format command
31. By default, the fillnull command replaces null values with this: 0
32. You can only use one Eval command per search? False
33. This command allows you to correlate related events on a field or list of fields that span time. **transaction**
34. Which of these is not a field created with the transaction command. Max count
35. \_\_\_\_\_ Should be used when you want to see results of a calculation, or you need to group events on a field value. Stats
36. \_\_\_\_\_ Should be used when you want to see results of a correlated together, or you need to grouped on start and end values. Transactions
37. What should you use with the transaction command to set the maximum total time between the earliest and latest events returned? Maxspan
38. Three main processing components? Forwarder, Indexers, Search Heads
39. Raw data in an index is stored in a Compressed Form? TRUE
40. Forwarders are typically installed on? Machines where the data originates
41. The SEARCH HEADS handle search management while INDEXERS perform the searches.
42. A Group of indexers configured to replicate each other’s data is called Index cluster
43. DISK I/O is often the biggest bottle neck in the Splunk Indexing pipeline
44. Search heads do not require as much disk space as indexers but require more CPU Power
45. Adding more machines no matter the hardware will make your deployment perform better. FALSE
46. Splunk indexers and Search heads on virtual machines should have 100% of vCPU reserved for them.
47. Keeping \_\_\_\_\_\_\_ synchronized across your deployment makes sure events are returned in the proper order. **TIME**
48. What command is used to start the Splunk Enterprise service? **./splunk start**
49. This command can be used to make Splunk start each time the server is booted.  **./splunk enable boot-start**
50. When logging into Splunk the user name is admin and changeme
51. The folder inside the splunk enterprise installation directory contains licenses and configuration files. **ETC**
52. Splunk Enterprise commands are executed from the directory. **BIN**
53. The following are Splunk Enterprise processing tiers. **Data Input, Indexing, Search Management**
54. Event separation happens during the \_\_\_\_\_\_ segment of the data pipeline. **Parsing**
55. Events are written to disk during the segment of the data pipeline.  **Indexing**
56. The functions of the data pipeline vary drastically depending on the deployment.  **FALSE**
57. Splunk Enterprise licenses specify how much data you can index per. **DAY**
58. Any editing done to .conf files should be done in the \_\_\_\_ directory. **LOCAL**
59. The MAIN index is used when an index is not specified at input time.
60. Having multiple indexes allows. Multiple retention, access limiting and faster searches
61. As data is input into Splunk Enterprise it is first placed into a \_\_\_\_\_\_\_\_\_ bucket HOT
62. Differences between hot and warm buckets. Hot buckets are writeable, searched first and naming convention.
63. When a bucket is frozen by default it is moved to a different location before deleting. FALSE
64. The time zone setting in a user’s account will affect the timestamp shown in events. TRUE
65. Define what users can do in Splunk. Roles
66. Only the \_\_\_\_\_\_\_\_\_\_ role can use the delete command by default. Can\_delete
67. The \_\_\_\_\_\_\_\_\_\_ role has the most capabilities of the predefined splunk roles ADMIN
68. When mixing authentication sources, scripted authentication will always take precedence. FALSE
69. In most production environments, \_\_\_\_\_\_\_\_\_ will be used as your main source of data input. Forwarders
70. Splunk uses \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to categorize the type of data being indexed. Source Types
71. The server that data is forwarded to is called the? Receiver
72. Indexing on a Heavy forwarder does not affect your license. False
73. The following can be used to build apps for Splunk. Simple XML, Simple Javascript and SDK
74. When migrating from a single instance deployment to a distributed environment, you will want to use the existing instance as an? INDEXER
75. An indexer in a distributed search environment is called a? SEARCH PEER
76. It is best practice to \_\_\_\_\_\_\_\_ forwarder across all indexers in a search peer group. Load balance
77. The management port is required when adding a search peer to a search head. TRUE
78. DMC stands for Distributed Management console
79. **What are some of the components installed from the Splunk enterprise package**

Splunk SDK are wrappers around the Rest API that do a log of the work for you, except authentication T/F - FALSE

Select the three types of requests the REST API uses to interact with SPLUNK **POST DELETE UPDATE GET REMOVE**

Using Simple XML Extensions you can customize the layout of a dashboard and add custom visualizations TRUE

Splunk data inputs can be categorized as which of the following types.

Splunk configuration information is stored in files with the .conf True

An add-on is similar to an app, but it does not contain a user facing view with dashboard True

Select the item that is NOT a major component of the Splunk platform **Data Input, Dashboard, Forwarder, Indexer, Search Head**

Select the item that is NOT a knowledge object **Field Lookup Transform Macro Element**

Which of the following is a phase in the Splunk data life cycle Collect and Index, search and investigate, add knowledge, monitor and alert, report and anlyze

**USING SPLUNK**

1. Machine data is always structured. FALSE
2. Machine data makes up for more than \_\_\_\_ of the data accumulated by organizations. 90%
3. Machine data can give you insights into. ALL
4. Machine data is only log files on web servers. False
5. Which of these is not a main component of Splunk? Compress and archive
6. The index does not play a major role in Splunk? False
7. Data is broken into single events by? Source type
8. Time stamps are stored? In a consistent format
9. Which role defines what apps a user will see by default? ADMIN
10. Which two apps sh8ip with Splunk Enterprise? Search and Reporting and Home App
11. There are 7 components to the Search and Reporting app’s default interface.
12. What is the most efficient way to filter events in Splunk? By time
13. When a search is run, events are returned in? reverse chronological order
14. Commands that create statistics or visualizations are called? Transforming commands
15. The Search & Reporting App has how many search modes? 3
16. Which character acts as a wildcard in the Splunk Search Language \*
17. What are the Boolean operators in Splunk. OR, NOT, AND
18. Which is not a comparison operator? &=
19. Field names are case sensitive.
20. What could be said of the circled field below? It contains string values, it was extracted at search time, It contains four values
21. After a report is saved, you can longer edit the search? False
22. These searches will return the same result? False
23. Which is not a valid option when editing a report? Rename
24. Wildcards can be used with field value searches? True
25. A power user can allow read/write permissions on a report? True
26. Search command can be used with search terms to do the following? Create charts, compute statistics, format data
27. If we want to see events after running a transforming command, we need to switch to this mode. Verbose
28. Any search that returns these values can be viewed as a chart. Statistical
29. Charts can be based on numbers, time or location. True
30. **Dashboards** are searches gathered together into a single pane of glass.
31. An alert is an action triggered by a Saved search.
32. Alerts can send an email. True
33. These are knowledge objects that provide the data structure for pivot. Data models
34. Which roles can create data models. **Power**
35. You can think of adding child data model objects as an \_\_\_\_ Boolean in the Splunk Search language. **AND**
36. Pivots cannot be saved as reports or dashboard panels. **FALSE**
37. The instant pivot button is displayed in the statistics and visualization tabs when a \_\_\_\_\_\_\_\_ search is used. Non-transforming
38. Unlike pivot, reports created with instant pivot cannot be saved. False

**Creating Knowledge Objects**

1. Which roles can create private knowledge objects? **User, Power and Admin**
2. Which Roles can create knowledge objects shared across all apps. **Admin**
3. Knowledge objects can be used to normalize data? **True**
4. A common information model is supported by splunk? **True**
5. What are the predefined ways knowledge objects can be shared? **All Apps, Private, Specific app**
6. When using a .csv file for lookups the first row in the file represents this. **Field Names**
7. Which is the correct order to use when creating a lookup?  **Define a Lookup Table, Define a Lookup, create an automatic lookup.**
8. Finish this search command so that it displays data from the http status.csv lookup file. **inputlookup**
9. Finish this search so that it uses the http\_\_status lookup to return events. **Lookup**
10. Field Aliases are used to **normalize** data.
11. You can only have one field alias per field. **False**
12. Field Aliases. Can be referenced by lookup tables, are applicable to a specified app context, make correlation easier
13. Calculated Fields are shortcuts for. **Eval commands**
14. Calculated fields can use lookup tables. False
15. The easiest way to extract a filed is from \_\_\_\_\_\_\_ Allowing you to skip a few steps. The event actions menu
16. When editing a Field Extraction, you will be working with. The regular expressions.
17. You can extract multiple fields with the Field extractor. True
18. \_\_\_\_\_\_\_\_\_\_ is a field extraction method for events that contain fields separated by a character. Delimiter
19. Fields extracted with the field extractor. Are persistent, are specific to a host, source or source type, are reusable in multiple searches.
20. You can only add one tag per field value pair. **False**
21. Which search would limit an “alert” Tag to the “host” field? **Tag::host=alert**
22. Allow you to categorize events based on search terms. **Event types**
23. Tags can be added to event types. True
24. Event Types do not show up in the field lists. **False**
25. Splunk suggests naming your knowledge objects using **6** segmented keys.  **6**
26. A workflow action can. Send field values to external resources, pass variables to a URL, execute a secondary search
27. This workflow action sends field values to external resources. POST
28. This workflow Action passes variables in a URL? GET
29. To escape the “Fieldname” Value which command would your use? $\_\_\_\_! \_fieldname$ **!**
30. Are based on Searches that run on a schedule interval or in real time. Alerts
31. Which Actions can be triggered by an alert? List in triggered alerts, send email, run a script
32. Alerts can be shared to all apps? True
33. Once an alert is created you can no longer edit its defining search. False
34. A real time alert type is useful when you want to know as soon as your trigger condition is met. True
35. Search Macros. Allow store entire search string, time range independent, pass arguments to the search.
36. What is the proper syntax for Using a Macro called “dostuff”? ` dostuff`
37. You can pipe the results of a macro to other commands. TRUE
38. What is the correct way to name a Macro with two arguments? Dostuff(2)
39. Validating macro arguments can be done with which type of command. Boolean expressions, eval expressions
40. After creating your data model, the next step is to? Add root objects
41. Root search objects benefit from acceleration. FALSE
42. Objects can be added to a root event object to narrow down the search. Child
43. What attributes can be added to an object? Auto-Extracted, Eval Expressions, lookup, regular expression, geo IP.
44. You can add additional child objects to either existing objects or the root object. True
45. The external data used by a lookup can come from sources like. CSV File, Scripts, Geospatial data
46. Input fields are automatically generated with a lookup command. False
47. You can extract multiple fields from overlapping values using the field extractor. True
48. Root events are the most commonly used type of root data model object. True

This Boolean operator is implied between search terms unless otherwise specified AND

Selecting a series of bars in the timeline to drill down runs a new search. False

From the Search Jobs page, you can click the job link to

In order to be a selected field, the field must exist in every event

This search user= \* **displays only events that contain a value for user**

Tag names are case insensitive.

Alerts are knowledge objects and have a name.

Reports are \_\_\_\_\_\_\_\_\_\_ .

Which of the following are responsible for conducting the actual search for results in the index files

A time range picker on a report can be used to override the specified time range for the report.

Pivots can be saved as

The following searches will return the same results. SEARCH 1: web error SEARCH 2: web AND error

Search terms are case \_\_\_\_\_\_\_\_\_\_ .

The fields command has a + and - option. The fields + command

This command allows you to extract fields at search time; these fields do not persist as knowledge objects

The 'as' clause can be used with this command

When a search returns \_\_\_\_\_\_\_\_\_\_, you can view the results as a chart

Hovering over a SEGMENT on a chart,

Which of the following null formatting options with the timechart command flattens the trendline to zero where the data value is NULL

The license meter runs during the \_\_\_\_\_\_\_\_\_\_ segment of the data flow pipeline

The if function used with the eval command takes \_\_\_\_\_\_\_\_\_\_ arguments.

Lookups allow you to augment your event data with fields that do not exist in the source file

Which of the following are true about lookups? (Select all that apply.)

|  |
| --- |
| **search results can be used to populate a lookup table** |
| **output from a script can be used to populate a lookup table** |
| **Splunk DB Connect can be used to populate a lookup table from relational databases.** |
| **lookups can be time based** |
| **lookups can be configured to run automatically** |

Field aliases are applicable to a specified app context

These knowledge objects apply to a SET OF FIELDS with similar data.

Use this method to extract fields that persist as knowledge objects.