Splunk.SPLK-1001.vJul-2024.by.Alen.151q

Number: SPLK-1001
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: SPLK-1001
Exam Name: Splunk Core Certified User

Exam A

QUESTION 1
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
Section:

QUESTION 2
Which command automatically returns percent and count columns when executing searches?

A. top
B. stats
C. table
D. percent

Correct Answer: A
Section:

QUESTION 3
Select the correct option that applies to Index time processing (Choose three.).

A. Indexing
B. Searching
C. Parsing
D. Settings
E. Input

Correct Answer: A, C, E
Section:

QUESTION 4
Splunk automatically determines the source type for major data types.

A. False
B. True

Correct Answer: B
Section:

QUESTION 5
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 6
Splunk index time process can be broken down into ___________ phases.

A. 3
B. 2
C. 4
D. 1

Correct Answer: A
Section:

QUESTION 7
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
Section:

QUESTION 8
Uploading local files though Upload options index the file only once.

A. No
B. Yes

Correct Answer: B
Section:

QUESTION 9
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
Section:

QUESTION 10
When running searches command modifiers in the search string are displayed in what color?

A. Red
B. Blue
C. Orange
D. Highlighted

Correct Answer: B
Section:

QUESTION 11
How do you add or remove fields from search results?

A. Use field +to add and field -to remove.
B. Use table +to add and table -to remove.
C. Use fields +to add and fields –to remove.
D. Use fields Plus to add and fields Minus to remove.

Correct Answer: C
Section:

QUESTION 12
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: D
Section:
Explanation:

Only searches that generate statistics or visualizations can be saved as a report. These are searches that contain a transforming command, such as stats, chart, timechart, top, rare, etc. Transforming commands create a data table from the events and enable various types of visualizations. Searches that do not contain a transforming command can only be saved as an alert or a dashboard panel.

Reference:Splunk Core User Certification Exam Study Guide, page 35.

QUESTION 13
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: C
Section:

QUESTION 14
What syntax is used to link key/value pairs in search strings?

A. action+purchase

B. action=purchase

C. action | purchase

D. action equal purchase

Correct Answer: B
Section:

QUESTION 15
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
Section:

QUESTION 16
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
Section:

QUESTION 17
When a Splunk search generates calculated data that appears in the Statistics tab. in what formats can the results be exported?

A. CSV, JSON, PDF

B. CSV, XML JSON

C. Raw Events, XML, JSON

D. Raw Events, CSV, XML, JSON

Correct Answer: D
Section:

QUESTION 18
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
Section:

QUESTION 19
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
Section:

QUESTION 20
Which search matches the events containing the terms "error" and "fail"?

A. index=security Error Fail
B. index=security error OR fail
C. index=security "error failure"
D. index=security NOT error NOT fail

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

QUESTION 21
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: A
Section:

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

A. dedup
B. rename
C. sort -
D. fields +

Correct Answer: A
Section:

QUESTION 23
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
Section:

QUESTION 24
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
Section:

QUESTION 25
A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

A. An app
B. JSON
C. A role
D. An enhanced solution

Correct Answer: A
Section:

QUESTION 26
Which of the following fields is stored with the events in the index?

A. user
B. source
C. location
D. sourcelp

Correct Answer: B
Section:

QUESTION 27
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: A
Section:

QUESTION 28
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
Section:

QUESTION 29
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
Section:

QUESTION 30
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
Section:

QUESTION 31
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: D
Section:

QUESTION 32
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
Section:

QUESTION 33
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: B
Section:

QUESTION 34
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
Section:

QUESTION 35
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
Section:

QUESTION 36
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
Section:

QUESTION 37
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
Section:

QUESTION 38
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

Section:

QUESTION 39

Which is a 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
Section:

QUESTION 40

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
Section:

QUESTION 41

What can be configured using the Edit Job Settings menu?

A. Export the results 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
Section:

QUESTION 42

Which command is used to validate a lookup file?

A. | lookup products.csv

B. inputlookup products.csv

C. I inputlookup products.csv

D. | lookup definition products.csv

Correct Answer: C
Section:

QUESTION 43

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
Section:

QUESTION 44
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
Section:

QUESTION 45
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
Section:

QUESTION 46
When editing a dashboard, which of the following are possible options? (select 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: D
Section:

QUESTION 47
Which of the following index searches would provide the most efficient search performance?

A. index=*

B. index=web OR index=s*
C. (index=web OR index=sales)
D. *index=sales AND index=web*

Correct Answer: C
Section:

QUESTION 48
At index time, in which field does Splunk store the timestamp value?

A. time
B. _time
C. EventTime
D. timestamp

Correct Answer: B
Section:

QUESTION 49
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
Section:

QUESTION 50
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
Section:

QUESTION 51
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: C
Section:

QUESTION 52
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
Section:

QUESTION 53
What is the primary use for the rare command1?

A. To sort field values in descending order
B. To return only fields containing five or 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
Section:

QUESTION 54
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
Section:

QUESTION 55
By default, which of the following is a Selected Field?

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

Correct Answer: D
Section:

QUESTION 56
What are the steps to schedule a report?

A. After saving the report, click Schedule.
B. After saving the report, click Event Type.
C. After saving the report, click Scheduling.
D. After saving the report, click Dashboard Panel.

Correct Answer: A
Section:

QUESTION 57
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
Section:

QUESTION 58
Which Boolean operator is implied between search terms, unless otherwise specified?

A. OR
B. AND
C. NOT
D. NAND

Correct Answer: B
Section:

QUESTION 59
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
Section:

QUESTION 60
When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?

A. |
B. $
C. !
D. ,

Correct Answer: D
Section:

QUESTION 61
Which search string is the most efficient?

A. "failed password"
B. ''failed password"*
C. index=* "failed password"
D. index=security "failed password"

Correct Answer: D
Section:

QUESTION 62
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: B
Section:

QUESTION 63
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
Section:

QUESTION 64
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
Section:

QUESTION 65
_________________ transforms raw data into events and distributes the results into an index.

A. Index
B. Search Head
C. Indexer
D. Forwarder

Correct Answer: C
Section:

QUESTION 66
Documentations for Splunk can be found at docs.splunk.com

A. True
B. False

Correct Answer: A
Section:

QUESTION 67
Which component of Splunk is primarily responsible for saving data?

A. Search Head
B. Heavy Forwarder
C. Indexer
D. Universal Forwarder

Correct Answer: C
Section:

QUESTION 68
Universal forwarder is recommended for forwarding the logs to indexers.

A. False
B. True

Correct Answer: B
Section:

QUESTION 69
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: A, C, D
Section:

QUESTION 70
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: A, C, F
Section:

QUESTION 71
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
Section:

QUESTION 72
We should use heavy forwarder for sending event-based data to Indexers.

A. False
B. True

Correct Answer: B
Section:

QUESTION 73
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Correct Answer: B
Section:

QUESTION 74
Splunk shows data in ___________________.

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Correct Answer: B
Section:

QUESTION 75
Which of the following can be used as wildcard search in Splunk?

A. =
B. >
C. !
D. *

Correct Answer: D
Section:

QUESTION 76
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
Section:

QUESTION 77
Prefix wildcards might cause performance issues.

A. False
B. True

Correct Answer: B
Section:

QUESTION 78
Machine data can be in structured and unstructured format.

A. False
B. True

Correct Answer: B
Section:

QUESTION 79
Field names are case sensitive.

A. True
B. False

Correct Answer: A
Section:

QUESTION 80
Splunk internal fields contains general information about events and starts from underscore i.e. _ .

A. True
B. False

Correct Answer: A
Section:

QUESTION 81
How many main user roles do you have in Splunk?

A. 2
B. 4
C. 1
D. 3

Correct Answer: D
Section:

QUESTION 82
Which of the following are Splunk premium enhanced solutions? (Choose three.)

A. Splunk User Behavior Analytics (UBA)
B. Splunk IT Service Intelligence (ITSI)
C. Splunk Enterprise Security (ES)
D. Splunk Analytics Security (AS)

Correct Answer: A, B, C
Section:

QUESTION 83

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

A. False
B. True

Correct Answer: B
Section:

QUESTION 84
Splunk extracts fields from event data at index time and at search time.

A. True
B. False

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.3/SearchTutorial/Usefieldstosearch
Explanation:

QUESTION 85
Field values are case sensitive.

A. True
B. False

Correct Answer: B
Section:

QUESTION 86
Splunk indexes the data on the basis of timestamps.

A. True
B. False

Correct Answer: A
Section:

QUESTION 87
_______________ is the default web port used by Splunk.

A. 8089
B. 8000
C. 8080
D. 443

Correct Answer: B

Section:

QUESTION 88
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: A, B, C
Section:

QUESTION 89
Parsing of data can happen both in HF and Indexer.

A. Only HF
B. No
C. Yes

Correct Answer: C
Section:

QUESTION 90
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
Section:

QUESTION 91
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Correct Answer: B
Section:

QUESTION 92
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: B, C, E, G
Section:

QUESTION 93
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
Section:

QUESTION 94
Where does Licensing meter happen?

A. Indexer
B. Parsing
C. Heavy Forwarder
D. Input

Correct Answer: A
Section:

QUESTION 95
Matching search terms are highlighted.

A. Yes
B. No

Correct Answer: A
Section:

QUESTION 96
Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.

A. No

B. Yes

Correct Answer: B
Section:

QUESTION 97
Zoom Out and Zoom to Selection re-executes the search.

A. No
B. Yes

Correct Answer: B
Section:

QUESTION 98
Every Search in Splunk is also called _______________.

A. None of the above
B. Job
C. Search Only

Correct Answer: B
Section:

QUESTION 99
Matching of parentheses is a feature of Splunk Assistant.

A. No
B. Yes

Correct Answer: B
Section:

QUESTION 100
Search Assistant is enabled by default in the SPL editor with compact settings.

A. No
B. Yes

Correct Answer: B
Section:

QUESTION 101
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
Section:

QUESTION 102
Fields are searchable key value pairs in your event data.

A. True
B. False

Correct Answer: A
Section:

QUESTION 103
Selected fields are a set of configurable fields displayed for each event.

A. True
B. False

Correct Answer: A
Section:

QUESTION 104
Following are the time selection option while making search:
(Choose all that apply.)

A. Date & Time Range
B. Advanced
C. Date Range
D. Presets
E. Relative

Correct Answer: B
Section:

QUESTION 105
When saving a search directly to a dashboard panel instead of saving as a report first, which of the following is created?

A. Cloned panel
B. Inline panel
C. Report panel
D. Prebuilt panel

Correct Answer: C
Section:

QUESTION 106
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
Section:
Explanation:
Reference:
https://answers.splunk.com/answers/329699/why-does-my-search-head-cluster-captain-start-dele-1.html

QUESTION 107
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/search
Explanation:

QUESTION 108
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
Section:

QUESTION 109
In the Search and Reporting app, which tab displays timecharts and bar charts?

A. Events
B. Patterns
C. Statistics
D. Visualization

Correct Answer: D
Section:

Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Aboutreportingcommands
Explanation:

QUESTION 110
What will always appear in the Selected Fields list?

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

Correct Answer: D
Section:

QUESTION 111
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Specifytimemodifiersinyoursearch
Explanation:

QUESTION 112
Which of the following is a Splunk internal field?

A. _raw
B. host
C. _host
D. index

Correct Answer: A
Section:

QUESTION 113
Which command will rename action to Customer Action?

A. | rename action = CustomerAction
B. | rename Action as "Customer Action"

C. | rename Action to "Customer Action"
D. | rename action as "Customer Action"

Correct Answer: D
Section:
Explanation:
Reference:
https://answers.splunk.com/answers/610038/understanding-command-in-search.html

QUESTION 114
Which of the following is the most efficient search?

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

Correct Answer: A
Section:

QUESTION 115
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
Section:

QUESTION 116
When viewing results of a search job from the Activity menu, which of the following is displayed?

A. New events based on the current time range picker
B. The same events based on the current time range picker
C. The same events from when the original search was executed
D. New events in addition to the same events from the original search

Correct Answer: C
Section:

QUESTION 117
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata
Explanation:

QUESTION 118
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Report/Createandeditreports
Explanation:

QUESTION 119
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Assignmetadatatoeventsdynamically
Explanation:

QUESTION 120
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
Section:
Explanation:

This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1.The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2.The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.

QUESTION 121
Which of the following is the best way to create a report that shows the last 24 hours of events?

A. Use earliest=-1d@d latest=@d
B. Set a real-time search over a 24-hour window
C. Use the time range picket to select "Yesterday"
D. Use the time range picker to select "Last 24 hours"

Correct Answer: D
Section:

QUESTION 122
When is the pipe character, I, used in search strings?

A. Before clauses. For example: stats sum(bytes) | by host
B. Before commands. For example: | stats sum(bytes) by host
C. Before arguments. For example: stats sum| (bytes) by host
D. Before functions. For example: stats |sum(bytes) by host

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes_and_escaping_characters
Explanation:

QUESTION 123
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
Section:

QUESTION 124
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch
Explanation:

QUESTION 125
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Extendjoblifetimes
Explanation:

QUESTION 126
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: C
Section:
Explanation:
Reference:
https://answers.splunk.com/answers/41928/add-a-lookup-csv-colum-information-to-the-results-ofainputlookup-search.html
Explanation:

QUESTION 127
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
Section:
Explanation:
Reference:
https://books.google.com.pk/books?id=sNwkBQAAQBAJ&pg=PT525&lpg=PT525&dq=splunk+alert+triggered+When+results+of+a+search+meet+a+specifically+defined+condition&source=bl&ots=avtEx5luxo&sig=ACfU3U1ZVob_j9nU243Te2vhqwxI3YvJuA&hl=en&sa=X&ved=2ahUKEwjm48rmkfXoAhUlMewKHb_FAbkQ6AEwB3oECBYQJg
Explanation:

QUESTION 128
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
Section:
Explanation:
Reference:
https://www.edureka.co/blog/splunk-architecture/
Explanation:

QUESTION 129
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
Section:
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Changethesearchmode
Explanation:

QUESTION 130
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
Section:
Explanation:
Reference:
https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexingindiffe.html
Explanation:

QUESTION 131
Which of the following searches would return only events that match the following criteria?
• Events are inside the main index
• The field status exists in the event
• The value in the status field does not equal 200

A. index==main status!==200
B. index=main NOT status=200
C. index==main NOT status==200
D. index-main status!=200

Correct Answer: C
Section:
Explanation:
The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. It's a powerful language that allows you to perform advanced queries and extract meaningful insights from your data.
To query for events that match the criteria you specified, you would use the following KQL query:
index==main NOT status==200
This query will return all events that are inside the main index and have a status field, but the value of the status field does not equal 200. It is important to note that the "NOT" operator must be used in order to exclude events with a status value of 200.
By using the "NOT" operator, the query will return only events that do not match the specified criteria. This is useful for narrowing down search results to only those events that are relevant to the query.

QUESTION 132
Given the following SPL search, how many rows of results would you expect to be returned by default? index=security sourcetype=linux_secure (fail* OR invalid) I top src__ip

A. 10
B. 50
C. 100
D. 20

Correct Answer: A
Section:
Explanation:
The SPL search specified above will return 10 rows of results by default, as the "top" command specifies a limit of 10 results. The query will search for all events in the security index with a sourcetype of linuxsecure that contain either the terms fail* or invalid and will display the top 10 results according to the src_ip field.

QUESTION 133
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: D
Section:
Explanation:
The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. To query for events that are found in the index named security, you would use the following KQL query:
index=Security
This query will return all events that are found in the security index. It is important to note that the "=" operator must be used in order to match the exact index name.

QUESTION 134
How many minutes, by default, is the time to live (ttl) for an ad-hoc search job?

A. 5 minutes
B. 1 minute
C. 10 minutes
D. 60 minutes

Correct Answer: C
Section:
Explanation:
The default time to live (ttl) for an ad-hoc search job is 10 minutes. This means that if no one views the results of a search within 10 minutes, the search job is canceled and the results are deleted. You can change this setting in the limits.conf file1.

QUESTION 135
When using the top command in the following search, which of the following will be true about the results?
index="main" sourcetype="access_*" action="purchase" | top 3 statusCode by user showperc=f countfield=status_code_count

A. The search will fail. The proper top command format is top limit=3 instead of top 3.
B. The top three most common values in statusCode will be displayed for each user.
C. Only the top three overall most common values in statusCode will be displayed.
D. The percentage field will be displayed in the results.

Correct Answer: B
Section:
Explanation:
The top command returns the most common values of a field and their count. By using the by clause, you can group the results by another field. In this case, the top command will return the top three most common values in statusCode for each user. The showperc=f option will suppress the percentage column in the output. The countfield option will rename the count column to status_code_count2.

QUESTION 136
By default, which role contains the minimum permissions required to have write access to Splunk alerts?

A. User
B. Alerting
C. Power
D. Admin

Correct Answer: C
Section:

Explanation:
The Power role contains the minimum permissions required to have write access to Splunk alerts.
The User role can only view alerts created by others, but cannot create or modify them. The Alerting role is not a default role in Splunk, but a custom one that can be created by an administrator. The Admin role has write access to Splunk alerts, but also has many other permissions that are not necessary for alerting3.

QUESTION 137
In the Search and Reporting app, which is a default selected field?

A. index
B. action
C. _time
D. host

Correct Answer: C
Section:
Explanation:
In the Search and Reporting app, _time is a default selected field. This means that it is always displayed in the events list and table views, unless explicitly deselected. Other default selected fields are host, source, and sourcetype. Index and action are not default selected fields, but they can be added to the list of selected fields by clicking on All Fields4.

QUESTION 138
Which of the following is an accurate definition of fields within Splunk?

A. Inherent entities that exist in event data.
B. A searchable key/value pair in event data.
C. Values pulled exclusively from lookup tables.
D. A non-searchable name/value pair used while indexing data.

Correct Answer: A
Section:
Explanation:
Fields are searchable key/value pairs in event data. They allow you to specify criteria for your searches and filter out unwanted events. Fields can be extracted automatically by Splunk software during indexing or searching, or manually by users using various methods. Fields are not inherent entities that exist in event data, but rather interpretations of data by Splunk software or users. Fields are not values pulled exclusively from lookup tables, although lookup tables can be used to add fields to events based on existing fields. Fields are not non-searchable name/value pairs used while indexing data, but rather searchable attributes that can be used to refine searches5.

QUESTION 139
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. File-based
C. Total
D. Segmented

Correct Answer: B
Section:
Explanation:
The four types of lookups that Splunk provides out-of-the-box are file-based, external, KV Store, and geospatial. File-based lookups use CSV files to map fields from your data to fields in the external table. External lookups use Python scripts or binary executables to populate your events with field values from an external source. KV Store lookups use a key-value store to map fields from your data to fields in the external table. Geospatial lookups use

KMZ or KML files to match location coordinates in your events to geographic feature collections1.

QUESTION 140
When refining search results, what is the difference in the time picker between real-time and relative time ranges?

A. Real-time searches happen instantly, while relative searches happen at a scheduled time.
B. Real-time searches display results from a rolling time window, while relative searches display results from a set length of time.
C. Real-time searches run constantly in the background, while relative searches only run when certain criteria are met.
D. Real-time represents events that have happened in a set time window, while relative will display results from a rolling time window.

Correct Answer: B
Section:
Explanation:
The difference between real-time and relative time ranges in the time picker is that real-time searches display results from a rolling time window, such as the last 15 minutes, while relative searches display results from a set length of time, such as yesterday or last week. Real-time searches do not happen instantly, but rather update periodically based on the refresh interval. Relative searches do not happen at a scheduled time, but rather when the user runs them. Real-time searches do not run constantly in the background, but rather when the user starts them. Real-time searches do not represent events that have happened in a set time window, but rather events that are happening now.

QUESTION 141
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Correct Answer: A
Section:

QUESTION 142
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
Section:

QUESTION 143
All components are installed and administered in Splunk Enterprise on-premise.

A. True
B. False

Correct Answer: A
Section:

QUESTION 144

Log filtering/parsing can be done from ______________.

A. Index Forwarders (IF)
B. Universal Forwarders (UF)
C. Super Forwarder (SF)
D. Heavy Forwarders (HF)

Correct Answer: D
Section:

QUESTION 145
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
Section:

QUESTION 146
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
Section:

QUESTION 147
Which of the following is the best description of Splunk Apps?

A. Built only by Splunk employees.
B. A collection of files.
C. Only available for download on Splunkbase.
D. Available on iOS and Android.

Correct Answer: B
Section:
Explanation:
The best description of Splunk Apps is a collection of files that provide specific functionality or views of your data. Splunk Apps can be built by anyone, not only by Splunk employees. Splunk Apps are not only available for download on Splunkbase, but also can be created or customized by users. Splunk Apps are not available on iOS and Android, but rather on Splunk Enterprise or Splunk Cloud platforms.

QUESTION 148
What is the proper SPL terminology for specifying a particular index in a search?

A. indexer---index_name
B. indexer name---index_name
C. index=index_name
D. index name=index_name

Correct Answer: C
Section:
Explanation:
This means that you can use the index field to filter your search results by the name of the index that contains the events you want to see.
For example, if you want to search for events in the index named ''gcp_logs'', you can use the following SPL:
index=gcp_logs
You can also specify multiple indexes by using the OR operator, such as:
index=gcp_logs OR index=oswin

QUESTION 149
Which of the following is the appropriately formatted SPL search?

A. index=security sourcetype=linux secure (invalid OR failed) | stats count as 'Potential Issues'
B. index=security sourcetype=linux secure (invalid OR failed) | stats 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) | count as 'Potential Issues'

Correct Answer: A
Section:
Explanation:
This is the appropriately formatted SPL search because it follows the SPL syntax rules12, such as:
Using the=operator to specify field-value pairs, such asindex=securityandsourcetype=linux.
Using theORoperator to combine multiple values for the same field, such as(invalid OR failed).
Using the|character to separate commands, such asstats count as 'Potential Issues'.
Using theaskeyword to rename fields, such ascount as 'Potential Issues'.

QUESTION 150
How are the results of the following search sorted?
... | sort action, ---file, +bytes

A. In descending order by action, then descending order by file, and lastly by ascending order of bytes.
B. In ascending order by action, then descending order by file, and lastly by ascending order of bytes.
C. In descending order by action if it exists. If not, then in descending order by file, and if both action and file do not exist, by ascending order of bytes.
D. In ascending order by action if it exists. If not, then in descending order by file, and if both action and file do not exist, by ascending order of bytes.

Correct Answer: B
Section:
Explanation:

Using a minus sign (-) for descending order and a plus sign (+) for ascending order. If no sign is specified, the default order is ascending.
Sorting by multiple fields in the order they are specified. If there are duplicate values in one field, the next field is used to break the tie.
Sorting by field values according to their types. If the field type is not specified, the sort command tries to automatically determine it.

QUESTION 151
Splunk users are assigned roles. Which of the following do roles determine?

A. Password
B. Port number
C. Username
D. Data access

Correct Answer: D
Section:
Explanation:
This is the correct answer because roles determine the level of access that users have to the Splunk platform and the tasks that they can perform on the platform1.Roles can contain one or more capabilities that provide access to specific parts of the Splunk platform, such as searching, indexing, alerting, and so on2.Roles can also specify which indexes that a user can search and which indexes are searched by default1.