SPLK-1001.68q

Number: SPLK-1001
Passing Score: 800
Time Limit: 120 min

SPLK-1001

Splunk Core Certified User

Exam A

QUESTION 1
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels **QUESTION 3**
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports

QUESTION 5
After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.
B. Filters current search results.
C. Moves to past or future events.
D. Expands the time range of the search.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline

QUESTION 6
Which command is used to review the contents of a specified static lookup file?

A. `lookup`
B. `csvlookup`
C. `inputlookup`
D. `outputlookup`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: (none)
Explanation

Explanation/Reference:

QUESTION 8
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethestatscommandandfunctions

QUESTION 10
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: (none)
Explanation

Explanation/Reference:

QUESTION 11
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: (none)
Explanation

Explanation/Reference:

QUESTION 12
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Stats#1._Compare_the_difference_between_using_the_stats_and_chart_commands

QUESTION 13
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Fields

QUESTION 14
In the fields sidebar, which character denotes alphanumeric field values?

A. #
B. %
C. a
D. a#

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 16
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: (none)
Explanation

Explanation/Reference:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

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: (none)
Explanation

Explanation/Reference:

QUESTION 20

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Aboutsavingandsharingreports#Save_a_search_as_a_report

QUESTION 24
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/ExtractfieldsinteractivelywithIFX#Access_the_field_extractor_from_the_All_Fields_dialog_box

QUESTION 25
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

QUESTION 26
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: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Exportsearchresults

QUESTION 27
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: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

QUESTION 28
Which of the following fields is stored with the events in the index?

A. `user`
B. `source`
C. `location`
D. `sourceIp`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/609626/is-there-a-way-to-check-if-makeresults-stored-the.html

QUESTION 29
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/231429/can-i-have-multiple-panels-using-the-same-inline-s.html

QUESTION 30
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
Section: (none)

Reference: https://answers.splunk.com/answers/149904/find-earliest-and-latest-event-per-day-for-a-time-range.html

QUESTION 31
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: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/617772/why-am-i-getting-a-http-503-error-when-using-threa.html

QUESTION 32
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Stats

QUESTION 33
Which is primary function of the timeline located under the search bar?

Explanation

Explanation/Reference:
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Startsearching

QUESTION 34
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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
Section: (none) Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Inputlookup

QUESTION 36
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Report/Managereportpermissions

QUESTION 37
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Rare

QUESTION 38

Explanation

Explanation/Reference:
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

QUESTION 39
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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: (none)
QUESTION 41
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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: (none)
Explanation

Explanation/Reference:

QUESTION 43
All components are installed and administered in Splunk Enterprise on-premise.

A. True

Explanation

Explanation/Reference:
B. False

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
A

QUESTION 44
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: (none)
Explanation

Explanation/Reference:

QUESTION 45
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: (none)
Explanation
Explanation/Reference:

QUESTION 46
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Splunk shows data in _____.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

A. the_questionnaire _pedia
B. the_questionnaire pedia
C. the_questionnaire_pedia
D. the_questionnaire Pedia

C

QUESTION 49
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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
Section: (none)
Explanation

Explanation/Reference:
QUESTION 51
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: (none)
Explanation

Explanation/Reference:

QUESTION 52
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
Section: (none)
Explanation

Explanation/Reference:

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
QUESTION 53
Parsing of data can happen both in HF and UF.

A. Yes
B. No

B

QUESTION 54
Upload option creates inputs.conf

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Splunk index time process can be broken down into _____ phases.

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the statements are correct about HF? (Choose three.)

A. Parsing
B. Masking
C. Searching
D. Forwarding

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
QUESTION 58
Where does Licensing meter happen?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Matching search terms are highlighted.

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
The default host name used in Inputs general settings can not be changed.

A. False
B. True

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
You are able to create new Index in Data Input settings.

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Splunk Parses data into individual events, extracts time, and assigns metadata.

A. False
B. True

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which symbol is used to snap the time?

A. @
B. &
C. *
D. #

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
There are three different search modes in Splunk (Choose three.):

A. Automatic
B. Smart
C. Fast

D. Verbose

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
You can view the search result in following format (Choose three.):

A. Table
B. Raw
C. Pie Chart
D. List

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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
Section: (none)
Explanation

Explanation/Reference: