SPLK-1001

Number: SPLK-1001
Passing Score: 800
Time Limit: 120 min
File Version: 1

SPLK-1001

Exam A

QUESTION 1
Which search string only returns events from `hostWWW3?`

A. `host=*`

B. `host=WWW3`

C. `host=WWW*`

D. `Host=WWW3`

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes **QUESTION 3**
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:

QUESTION 5

Which of the following constraints can be used with the `top` command?

A. `limit`

B. `useperc`

C. `addtotals`

D. `fieldcount`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/339141/how-to-use-top-command-or-stats-with-sort-results.html

QUESTION 6
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/Developnamingconventionsforknowledgeobjecttitles

QUESTION 8
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 9
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 10
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 11
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/LineAreaCharts

QUESTION 12
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 13
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 14
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/185864/selected-fields-in-fields-side-bar.html **QUESTION 16**
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/65/are-field-values-case-sensitive.html

QUESTION 17
Which Boolean operator is always implied between two search terms, unless otherwise specified?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 18
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 19
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 20
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
In the fields sidebar, which character denotes alphanumeric field values?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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: (none)
Explanation

Explanation/Reference:

QUESTION 23
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 24
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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: (none)
Explanation

Explanation/Reference:

QUESTION 26
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

QUESTION 28

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: (none)
Explanation

Explanation/Reference:
QUESTION 29
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: (none)
Explanation

Explanation/Reference:

QUESTION 30
At index time, in which field does Splunk store the timestamp value?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Data/HowSplunkextractstimestamps

QUESTION 31
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 32
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 33
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 34
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 35
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 36
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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 38
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 39
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 40
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 41
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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Startsearching

QUESTION 42
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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)
Explanation

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

QUESTION 44
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: (none)
Explanation

Explanation/Reference:

QUESTION 45
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 46
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 47
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: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which command automatically returns percent and count columns when executing searches?

A. top
B. stats

C. `table`

D. `percent`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 49
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: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/Aboutlookupsandfieldactions

QUESTION 50
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: (none)
Explanation

Explanation/Reference:

QUESTION 51
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
_______________ 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: (none)
Explanation

Explanation/Reference:

QUESTION 53
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: (none)
Explanation

Explanation/Reference:

QUESTION 54
Three basic components of Splunk are (Choose three.):

A. Forwarders
B. Deployment ServerC. Indexer
D. Knowledge Objects
E. Index
F. Search Head

Correct Answer: ACF
Section: (none)
Explanation
Explanation/Reference:

QUESTION 55
We should use heavy forwarder for sending event-based data to Indexers.

A. False
B. True

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
All components are installed and administered in Splunk Enterprise on-premise.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 58
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 59
Which of the following can be used as wildcard search in Splunk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
How many main user roles do you have in Splunk?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Splunk extracts fields from event data at index time and at search time.

A. True
B. False

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.3/SearchTutorial/Usefieldstosearch

QUESTION 62
Splunk indexes the data on the basis of timestamps.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.3/Data/Aboutdefaultfields

QUESTION 63
_______________ is the default web port used by Splunk.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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: (none)
Explanation

Explanation/Reference:
QUESTION 66
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 67
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 68
Splunk automatically determines the source type for major data types.
A. False
B. True

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Upload option creates inputs.conf

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Uploading local files though Upload options index the file only once.

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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:

QUESTION 73
Where does Licensing meter happen?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Zoom Out and Zoom to Selection re-executes the search.

A. No

B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Search Assistant is enabled by default in the SPL editor with compact settings.

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
@ Symbol can be used in advanced time unit option.
A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
The new data uploaded in Splunk are shown in ________________.

A. Real-time
B. 10 Minutes

C. Overnight Download
D. 30 Minutes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 80
Events in Splunk are automatically segregated using data and time.

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82

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 83

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 84
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 85
Snapping rounds down to the nearest specified unit.

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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:

QUESTION 87
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 will enable it.
D. Click Settings -> 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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 88
Field names are case sensitive and field value are not.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
!= and NOT are same arguments.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Query - status != 100:

A. Will 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. Will get different results depending on data.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 91
Will 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Put query into separate lines where | (Pipes) are used by selecting following options.

A. CTRL + Enter
B. Shift + Enter
C. Space + Enter
D. ALT + Enter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Fields are searchable key value pairs in your event data.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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: ABCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Search Language Syntax in Splunk can be broken down into the following components. (Choose all that apply.)

A. Search term
B. Command
C. Pipe
D. Functions
E. Arguments
F. Clause

Correct Answer: ABCDEF
Section: (none)
Explanation
Explanation/Reference:

QUESTION 96
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: (none)
Explanation

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Savingsearches

QUESTION 97
What will always appear in the Selected Fields list?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 98
Which of the following is a Splunk internal field?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Splexicon:Internalfield

QUESTION 99
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: (none)
Explanation

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

QUESTION 100
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: (none)
Explanation

Explanation/Reference:

QUESTION 101
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: (none)
Explanation

Explanation/Reference:

QUESTION 102
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: (none)
Explanation

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

QUESTION 103
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: (none)
Explanation

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

QUESTION 104
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: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/153100/how-to-get-the-event-count-for-the-last-24-hours-as-a-scheduled-report.html

QUESTION 105
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: (none)
Explanation

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

QUESTION 106
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: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/30376/how-to-display-the-contents-of-a-lookup-file.html

QUESTION 107
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Rare#:~:text=The%20rare%20command%20is%20a,the%20limit%20argument%20is%2010

QUESTION 108
What are the three main Splunk components?

A. Search head, GPU, streamer
B. Search head, indexer, forwarder
C. Search head, SQL database, forwarderD. Search head, SSD, heavy weight agent

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.edureka.co/blog/splunk-architecture/

QUESTION 109
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: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-in-diffe.html