SPLK-1001.27q

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

SPLK-1001

Splunk Core Certified User

Exam A

QUESTION 1
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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: (none)
Explanation

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

QUESTION 3
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: A
Section: (none)
Explanation

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

QUESTION 4
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 5
How can search results be kept longer than 7 days?

A. By scheduling a report.
B. By creating a link to the job.
C. By changing the job settings.
D. By changing the time range picker to more than 7 days.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 6
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 7
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 8
How are events displayed after a search is executed?
A. In chronological order.
B. Randomly by default.
C. In reverse chronological order.
D. Alphabetically according to field name.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 9
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 10
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 11
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 12
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: (none)
Explanation
Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Sort

QUESTION 13
Which time range picker configuration would return real-time events for the past 30 seconds?

A. Preset - Relative: 30-seconds ago
B. Relative - Earliest: 30-seconds ago, Latest: Now
C. Real-time - Earliest: 30-seconds ago, Latest: Now
D. Advanced - Earliest: 30-seconds ago, Latest: Now

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 14
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 15
What does the `rare` command do?

A. Returns the least common field values of a given field in the results.
B. Returns the most common field values of a given field in the results.
C. Returns the top 10 field values of a given field in the results.
D. Returns the lowest 10 field values of a given field in the results.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 16
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 17

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 18**
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 19
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 20
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 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
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: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which search string returns a filed containing the number of matching events and names that field `Event Count`?

A. `index=security failure | stats sum as "Event Count"`
B. `index=security failure | stats count as "Event Count"`
C. `index=security failure | stats count by "Event Count"`
D. `index=security failure | stats dc(count) as "Event Count"`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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: (none)
Explanation

Explanation/Reference:

QUESTION 26
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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

https://www.vceplus.com/