Quiz 200.9.2 - Splunk Certification Qualification 02

Due No due date **Points** 60 **Questions** 60
Available until Oct 27 at 11:59pm **Time Limit** 60 Minutes **Allowed Attempts** 4

Instructions

Instructor Home
(https://perscholas.instructure.com/courses/1639/pages/instructor-

Please open the quiz in a new tab to complete.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
KEPT	Attempt 2	40 minutes	56.5 out of 60
LATEST	Attempt 2	40 minutes	56.5 out of 60
	Attempt 1	53 minutes	48 out of 60

ⓘ Correct answers are hidden.

Score for this attempt: **56.5** out of 60
Submitted Oct 27 at 2:48pm
This attempt took 40 minutes.

Incorrect

Question 1

0 / 1 pts

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

- (selected) dedup
- rename
- sort -
- fields +

Incorrect

Question 2

0 / 1 pts

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

- (selected) inputlookup
- lookup
- uselookup
- lookupfield

Question 3

1 / 1 pts

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

- Executes a new search.
- Filters current search results.
- Moves to past or future events.
- Expands the time range of the search.

Question 4

1 / 1 pts

All users by default have WRITE permission to ALL knowledge objects.

- True
- False

Question 5

1 / 1 pts

The stats command will create a _____ by default.

- Table
- Report
- Pie chart
- Dashboard

Question 6

1 / 1 pts

What type of search can be saved as a report?

- (selected) Any search can be saved as a report.
- Only searches that generate visualizations.
- Only searches containing a transforming command.
- Only searches that generate statistics or visualizations.

Question 7

1 / 1 pts

What is the primary use for the rare command?

- To sort field values in descending order.
- To return only fields containing five or fewer values.
- (selected) To find the least common values of a field in a dataset.
- To find the fields with the fewest number of values across a dataset.

Question 8

1 / 1 pts

Splunk Components:
Which of the following are responsible for parsing incoming data and storing data on disc?

- forwarders
- (selected) indexers

- search heads
- lookups

Question 9

1 / 1 pts

According to Splunk best practices, which placement of the wildcard results in the most efficient
search?

- f*il
- *fail
- fail* (selected)
- *fail*

Question 10

1 / 1 pts

It is mandatory for the lookup file to have this for an automatic lookup to work.

- Source type
- At least five columns
- Timestamp
- Input filed (selected)

Question 11

1 / 1 pts

Which command is used to validate a lookup file?

- | lookup products.csv
- inputlookup products.csv
- [x] | inputlookup products.csv
- | lookup definition products.csv

Question 12

1 / 1 pts

What can be included in the All Fields option in the sidebar?

- Dashboards.
- Metadata only.
- [x] Non-interesting fields.
- Field descriptions.

Question 13

1 / 1 pts

What must be done before an automatic lookup can be created? (select all that apply)

- [ ] The lookup command must be used.
- [x] The lookup definition must be created.
- [x] The lookup file must be uploaded to Splunk.

- [ ] The lookup file must be verified using the inputlookup command.

Question 14

1 / 1 pts

What can be configured using the Edit Job Settings menu?

- ○ Export the results to CSV format.
- ○ Add the Job results to a dashboard.
- ○ Schedule the Job to re-run in 10 minutes.
- ◉ Change Job Lifetime from 10 minutes to 7 days.

Question 15

1 / 1 pts

What is the purpose of using a by clause with the stats command?

- ◉ To group the results by one or more fields.
- ○ To compute numerical statistics on each field.
- ○ To specify how the values in a list are delimited.
- ○ To partition the input data based on the split-by fields.

Question 16

1 / 1 pts

When looking at a dashboard panel that is based on a report, which of the following is true?

You can modify the search string in the panel, and you can change and configure the visualization.

You can modify the search string in the panel, but you cannot change and configure the visualization.

You cannot modify the search string in the panel, but you can change and configure the visualization.

You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Question 17

1 / 1 pts

Which of the following searches will show the number of categoryID used by each host?

sourcetype=access_* | sum bytes by host

sourcetype=access_* | stats sum(categoryID) by host

sourcetype=access_* | sum(bytes) by host

sourcetype=access_* | stats sum by host

Question 18

1 / 1 pts

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

- Red
- Blue
- Orange
- Highlighted

Question 19

1 / 1 pts

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

- index=*
- index=web OR index=s*
- (index=web OR index=sales)
- *index=sales AND index=web*

Question 20

1 / 1 pts

Which search string only returns events from host WWW3?

- host=WWW3
- HOST=www3
- host=www*
- Host=WWW3

Question 21

1 / 1 pts

This is what Splunk uses to categorize the data that is being indexed.

- (●) sourcetype
- ( ) index
- ( ) source
- ( ) host

In Splunk, the `sourcetype` is used to categorize the data that is being indexed. It specifies the format of the data and determines how the data will be processed, such as what field extractions and transformations to apply, which timestamp to use, and which parsing rules to use. For example, if you have log data from different sources such as Apache, Syslog, or Windows Event Logs, you can use different sourcetypes to categorize and process each type of log data differently. The sourcetype can be set manually when indexing data, or it can be automatically assigned using props.conf and transforms.conf configuration files.

Question 22

1 / 1 pts

By default, which of the following fields would be listed in the fields sidebar under interesting Fields?

- ( ) host
- (●) index
- ( ) source
- ( ) sourcetype

Partial

Question 23

0.5 / 1 pts

When editing a dashboard, which of the following are possible options? (select all that apply)

- [ ] Add an output.
- [x] Export a dashboard panel.
- [x] Modify the chart type displayed in a dashboard panel.
- [x] Drag a dashboard panel to a different location on the dashboard.

Question 24

1 / 1 pts

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

- ( ) action+purchase
- (•) action=purchase
- ( ) action | purchase
- ( ) action equal purchase

Question 25

1 / 1 pts

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

CSV, JSON, PDF

CSV, XML JSON

When a Splunk search generates calculated data that appears in the Statistics tab, the results can be exported in CSV, XML, and JSON formats. These formats can be selected by clicking the "Export" button in the Statistics tab, and then selecting the desired format from the drop-down menu.

Raw Events, XML, JSON

Raw Events, CSV, XML, JSON

Question 26

1 / 1 pts

It is not possible for a single instance of Splunk to manage the input, parsing, and indexing of machine
data.

True

False

Question 27

1 / 1 pts

Which of the following represents the Splunk recommended naming convention for dashboards?

Description_Group_Object

Group_Description_Object

Group_Object_Description

- Object_Group_Description

Question 28

1 / 1 pts

Lookups can be private for a user.

- True
- False

Question 29

1 / 1 pts

An online retailer has a daily goal of 500 sales. What should an admin configure to notify the retailer every day at 23:00 about the sales status?

- A scheduled alert
- A real-time alert
- A throttled alert
- An indexed alert

Question 30

1 / 1 pts

What is a suggested Splunk best practice for naming reports?

- Reports are best named using many numbers so they can be more easily sorted.

- [x] Use a consistent naming convention so they are easily separated by characteristics such as group and object.
- [ ] Name reports as uniquely as possible with no overlap to differentiate them from one another.
- [ ] Any naming convention is fine as long as you keep an external spreadsheet to keep track.

Question 31

1 / 1 pts

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

- [ ] Cloned panel
- [x] Inline panel
- [ ] Report panel
- [ ] Prebuilt panel

Question 32

1 / 1 pts

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

- [x] Forwarders
- [ ] Deployment Server

- [x] Indexer
- [ ] Knowledge Objects
- [ ] Index
- [x] Search Head

Incorrect

Question 33

0 / 1 pts

Splunk shows data in _____.

- ( ) ASCII Character order.
- (•) Reverse chronological order.
- ( ) Alphanumeric order.
- ( ) Chronological order.

Question 34

1 / 1 pts

Assuming a user has the capability to edit reports, which of the following are editable?

- (•) Acceleration, schedule, permissions
- ( ) he report’s name, schedule, permissions
- ( ) The report’s name, acceleration, schedule
- ( ) The report’s name, acceleration, permissions

Question 35

1 / 1 pts

What does the values function of the stats command do?

- Lists all values of a given field.
- Lists unique values of a given field.
- Returns a count of unique values for a given field.
- Returns the number of events that match the search.

Question 36

1 / 1 pts

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

- Splunk User Behavior Analytics (UBA)
- Splunk IT Service Intelligence (ITSI)
- Splunk Enterprise Security (ES)
- Splunk Analytics Security (AS)

Question 37

1 / 1 pts

How many main user roles do you have in Splunk?

- 2
- 4

- [x] 3
- [ ] 1

Question 38

1 / 1 pts

Which search will return the 15 least common field values for the dest_ip field?

- [ ] sourcetype=firewall | rare num=15 dest_ip
- [ ] sourcetype=firewall | rare last=15 dest_ip
- [ ] sourcetype=firewall | rare count=15 dest_ip
- [x] sourcetype=firewall | rare limit=15 dest_ip

Question 39

1 / 1 pts

By default. what will always appear in the Selected Fields list?

- [ ] index
- [ ] action
- [ ] clientip
- [x] sourcetype

Question 40

1 / 1 pts

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

- No
- Yes

Question 41

1 / 1 pts

What is the correct way to use a time range specifier in the search bar so that the search looks back 2 hours?

- latest=-2h
- earliest=-2h
- latest=-2hour@d
- earliest=-2hour@d

Question 42

1 / 1 pts

Matching of parentheses is a feature of Splunk Assistant.

- No
- Yes

Question 43

1 / 1 pts

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

- (●) True
- ( ) False

Question 44

1 / 1 pts

Field names are case sensitive.

- (●) True
- ( ) False

Question 45

1 / 1 pts

When looking at a statistics table, what is one way to drill down to see the underlying events?

- ( ) Creating a pivot table.
- ( ) Clicking on the visualizations tab.
- ( ) Viewing your report in a dashboard.
- (●) Clicking on any field value in the table.

Question 46

1 / 1 pts

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

- [x] True
- [ ] False

Question 47

1 / 1 pts

Which is the default app for Splunk Enterprise?

- [ ] Splunk Enterprise Security Suite.
- [x] Searching and Reporting.
- [ ] Reporting and Searching.
- [ ] Splunk apps for Security.

Question 48

1 / 1 pts

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

- [ ] OR
- [ ] NOT
- [x] AND
- [ ] XOR

Question 49

1 / 1 pts

Parsing of data can happen both in HF (Hevy Forwarders) and Indexer.

- ○ Only HF
- ○ No
- ◉ Yes

Question 50

1 / 1 pts

In the Fields sidebar, what does the number directly to the right of the field name indicate?

- ○ The value of the field.
- ○ The number of values for the field.
- ◉ The number of unique values for the field.
- ○ The numeric non-unique values of the field.

Question 51

1 / 1 pts

Which of the statements are correct? (Choose three).

- ☑ Zoom to selection: Narrows the time range and re-executes the search.
- ☐ Zoom to selection: Narrows the time range and doesn't re-executes the search.
- ☑ Format Timeline: Hides or shows the timeline in different views.

- [ ] Zoom-Out: Expands the time focus and doesn't re-executes the search.
- [x] Zoom-out: Expands the time focus and re-executes the search.

Question 52

1 / 1 pts

_____ is the default web port used by Splunk.

- [ ] 8089
- [x] 8000
- [ ] 8080
- [ ] 443

Question 53

1 / 1 pts

What is the primary use for the rare command?

- [ ] To sort field values in descending order.
- [ ] To return only fields containing five of fewer values.
- [x] To find the least common values of a field in a dataset.
- [ ] To find the fields with the fewest number of values across a dataset.

Question 54

1 / 1 pts

Fields are searchable key value pairs in your event data.

- True
- False

Question 55

1 / 1 pts

A field exists in search results, but isn't being displayed in the fields sidebar. How can it be added to
the fields sidebar?

- Click All Fields and select the field to add it to Selected Fields.
- Click Interesting Fields and select the field to add it to Selected Fields.
- Click Selected Fields and select the field to add it to Interesting Fields.
- This scenario isn't possible because all fields returned from a search always appear in the fields sidebar.

Question 56

1 / 1 pts

Which of the following is the most efficient filter for running searches in Splunk?

- Time
- Fast mode
- Sourcetype
- Selected Fields

Question 57

1 / 1 pts

Data sources being opened and read applies to:

- Reporting phase
- Indexing Phase
- Parsing Phase
- Input Phase
- License Metering

Question 58

1 / 1 pts

Which of the following is a Splunk internal field?

- _raw
- host
- _host
- index

Question 59

1 / 1 pts

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

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

Question 60

1 / 1 pts

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

- Before clauses. For example: stats sum(bytes) | by host
- Before commands. For example: | stats sum(bytes) by host
- Before arguments. For example: stats sum| (bytes) by host
- Before functions. For example: stats |sum(bytes) by host

Quiz Score: **56.5** out of 60