# Quiz 200.9.1 - Splunk Certification Qualification 01

**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 3 | 49 minutes | 57 out of 60 |
| **LATEST** | Attempt 3 | 49 minutes | 57 out of 60 |
| | Attempt 2 | 60 minutes | 31.5 out of 60 |
| | Attempt 1 | 46 minutes | 49.33 out of 60 |

Correct answers are hidden.

Score for this attempt: **57** out of 60
Submitted Oct 27 at 2:04pm
This attempt took 49 minutes.

## Question 1

1 / 1 pts

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

- sourceIp
- location
- source
- user

## Question 2

1 / 1 pts

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

- False
- True

## Question 3

1 / 1 pts

Which stats command functions provide a count of how many unique values exist for a given field in
the result set (chose two)?

- [x] distinct-count(field)
- [x] dc(field)
- [ ] count(field)
- [ ] dedup(field)
- [ ] count-by(field)

## Question 4

1 / 1 pts

What does the stats command do?

- ( ) Converts field values into numerical values.
- ( ) Automatically correlates related fields.
- (•) Calculates statistics on data that matches the search criteria.
- ( ) Analyzes numerical fields for their ability to predict another discrete field.

## Question 5

1 / 1 pts

Which command is used to validate a lookup file?

- (•) | inputlookup products.csv
- ( ) | lookup definition products.csv
- ( ) inputlookup products.csv
- ( ) | lookup products.csv

## Question 6

1 / 1 pts

What can be configured using the Edit Job Settings menu?

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

## Question 7

1 / 1 pts

How are events displayed after a search is executed?

- In reverse chronological order.
- In chronological order.
- Alphabetically according to field name.
- Randomly by default.

## Question 8

1 / 1 pts

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

- Orange

- Blue
- Red
- Highlighted

## Question 9

1 / 1 pts

Creating Data Models:
Fields associated with a data set are known as _____.

- Constraints
- Attributes

## Question 10

1 / 1 pts

What are the steps to schedule a report?

- After saving the report, click Scheduling.
- After saving the report, click Dashboard Panel.
- After saving the report, click Event Type.
- After saving the report, click Schedule.

## Question 11

1 / 1 pts

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

- table
- stats
- (selected) top
- percent

## Question 12

**1 / 1 pts**

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

- (selected) Relational operators such as =, <, or >
- Quotation marks
- @ or # symbols
- Parentheses

## Question 13

**1 / 1 pts**

Lookups can be private for a user.

- False
- (selected) True

## Question 14

**1 / 1 pts**

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

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

## Question 15

1 / 1 pts

In a deployment with multiple indexes, what will happen when a search is run and an index is not
specified in the search string?

- (•) Events from every index searched by default to which the user has access will be returned.

In a deployment with multiple indexes, if an index is not specified in the search string, events from every index searched by default to which the user has access will be returned. This can lead to slower search performance and potentially overwhelming results if the user has access to a large number of indexes.

- ( ) Splunk will prompt you to specify an index.
- ( ) No events will be returned.
- ( ) All non-indexed events to which the user has access will be returned.

## Question 16

1 / 1 pts

What is the main requirement for creating visualizations using the Splunk UI?

- Your search must transform event data into XML formatted data first.
- Your search must transform event data into statistical data tables first.
- Your search must transform event data into JSON formatted data first.
- Your search must transform event data into Excel file format first.

## Question 17

1 / 1 pts

How can another user gain access to a saved report?

- Only users with an Admin or Power User role can access other users' reports.
- Anyone can access any reports marked as public within a shared Splunk deployment.
- The owner of the report can edit permissions from the Edit dropdown.
- The owner of the report must clone the original report and save it to their user account.

## Question 18

1 / 1 pts

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

- JSON
- An app
- An enhanced solution
- A role

## Question 19

1 / 1 pts

When viewing the results of a search, what is an Interesting Field?

- A field that appears in every event.
- A field that appears in any event.
- A field that appears in at least 20% of the events.

In Splunk, an Interesting Field is a field that appears in at least 20% of the events returned by a search. These fields are automatically identified by Splunk and are displayed on the left-hand side of the search results page. Interesting Fields can be useful in helping to identify patterns and trends in the data and can also be used to refine the search or create additional reports and dashboards.

- A field that appears in the top 10 events.

## Question 20

1 / 1 pts

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

- action=purchase
- action equal purchase

- action | purchase
- action+purchase

## Question 21

1 / 1 pts

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

- lookups
- forwarders
- indexers
- search heads

## Question 22

1 / 1 pts

What determines the scope of data that appears in a scheduled report?

- All data accessible to all users will appear in the report until the next time the report is run.
- All data accessible to the User role will appear in the report.
- 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.
- All data accessible to the owner of the report will appear in the report.

## Question 23

1 / 1 pts

How can search results be kept **longer** than 7 days?

- By changing the job settings.
- By scheduling a report.
- By creating a link to the job.
- By changing the time range picker to more than 7 days.

## Question 24

1 / 1 pts

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

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

## Question 25

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?

- An indexed alert

- A real-time alert
- A scheduled alert
- A throttled alert

Incorrect

## Question 26

0 / 1 pts

This search will return 20 results. SEARCH: error | top host limit = 20

- True
- False

## Question 27

1 / 1 pts

What is the correct syntax to count the number of events containing a vendor_action field?

- stats vendor_action (count)
- stats count (vendor_action)
- count stats vendor_action
- count stats (vendor_action)

## Question 28

1 / 1 pts

Which of the following Splunk components typically resides on the machines where data originates?

- Search head
- [x] Forwarder
- Indexer
- Deployment server

## Question 29

1 / 1 pts

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

- f*il
- *fail
- [x] fail*
- *fail*

## Question 30

1 / 1 pts

What user interface component allows for time selection?

- Data source time statistics
- Time summary
- Search time picker
- [x] Time range picker

## Question 31

1 / 1 pts

Machine data can be in structured and unstructured format.

- (selected) True
- False

## Question 32

1 / 1 pts

Which of the following reports is available in the Fields window?

- Events with rare value fields
- Events with top value fields
- (selected) Top values by time
- Rare values by time

## Question 33

1 / 1 pts

Matching search terms are highlighted.

- No
- (selected) Yes

## Question 34

1 / 1 pts

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

- (selected) Yes
- No

## Question 35

1 / 1 pts

Which of the following statements describes a search job?

- Once a search job begins, it cannot be stopped.
- A search job can only be paused when less than 50% of events are returned.
- A search job can only be stopped when less than 50% of events are returned.
- (selected) Once a search job begins, it can be stopped or paused at any point in time.

## Question 36

1 / 1 pts

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

- sourcetype=firewall | rare last=15 dest_ip
- (selected) sourcetype=firewall | rare limit=15 dest_ip

- sourcetype=firewall | rare num=15 dest_ip
- sourcetype=firewall | rare count=15 dest_ip

## Question 37

1 / 1 pts

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

- The report’s name, acceleration, schedule
- he report’s name, schedule, permissions
- The report’s name, acceleration, permissions
- [x] Acceleration, schedule, permissions

## Question 38

1 / 1 pts

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

- [x] Format Timeline: Hides or shows the timeline in different views.
- [ ] Zoom to selection: Narrows the time range and doesn't re-executes the search.
- [x] Zoom to selection: Narrows the time range and re-executes the search.
- [ ] 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 39

1 / 1 pts

Prefix wildcards might cause performance issues.

- False
- True

## Question 40

1 / 1 pts

Where does Licensing meter happen?

- Heavy Forwarder
- Parsing
- Indexer
- Input

## Question 41

1 / 1 pts

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

- sourcetype
- index
- clientip
- action

## Question 42

1 / 1 pts

What does the values function of the stats command do?

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

## Question 43

1 / 1 pts

What is a quick, comprehensive way to learn what data is present in a Splunk deployment?

- Review Splunk reports
- Run ./splunk show
- Click Data Summary in Splunk Web
- Search index=* sourcetype=* host=*

## Question 44

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

## Question 45

1 / 1 pts

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

- False
- True

## Question 46

1 / 1 pts

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

- index=security failure | stats count as “Event Count”
- index=security failure | stats dc(count) as “Event Count”
- ndex=security failure | stats sum as “Event Count”
- index=security failure | stats count by “Event Count”

## Question 47

1 / 1 pts

Uploading local files through Upload options index the file only once.

- (●) Yes
- ( ) No

## Question 48

1 / 1 pts

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

- (●) True
- ( ) False

## Question 49

1 / 1 pts

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

- (●) True
- ( ) False

## Question 50

1 / 1 pts

Which symbol is used to snap the time?

- * 
- @ 
- & 
- # 

## Question 51

1 / 1 pts

Which of the following searches will return results where fail, 400, and error exist in every event?

- error AND (fail OR 400)
- error OR (fail and 400)
- error AND (fail AND 400)
- error OR fail OR 400

## Question 52

1 / 1 pts

How can results from a specified static lookup file be displayed?

- lookup command
- Settings > Lookups > Upload
- Settings > Lookups > Input
- inputlookup command

Incorrect

## Question 53

0 / 1 pts

Splunk shows data in _____.

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

## Question 54

1 / 1 pts

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

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

## Question 55

1 / 1 pts

What options do you get after selecting timeline? (Choose four):

- [x] Zoom to selection
- [x] Zoom Out

- [x] Deselect
- [ ] Delete
- [x] Format Timeline

Incorrect

## Question 56

0 / 1 pts

!= and NOT are the same arguments.

- (•) True
- ( ) False

## Question 57

1 / 1 pts

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

- ( ) Use the time range picket to select “Yesterday”
- (•) Use the time range picker to select “Last 24 hours”
- ( ) Set a real-time search over a 24-hour window
- ( ) Use earliest=-1d@d latest=@d

## Question 58

1 / 1 pts

Which of the following file types is an option for exporting Splunk search results?

- RTF
- XLS
- PDF
- JSON

## Question 59

1 / 1 pts

Field values are case sensitive.

- True
- False

## Question 60

1 / 1 pts

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

- True
- False

Quiz Score: **57** out of 60