Splunk Core Certified User
SPLK-1001

1 In the Search and Reporting app, which is a default selected field?

A. index

B. action

C. _time

D. host

Answer: C

Explanation

:

In the Search and Reporting app, _time is a default selected field. This means that it is always displayed in the events list and table views, unless explicitly deselected. Other default selected fields are host, source, and sourcetype. Index and action are not default selected fields, but they can be added to the list of selected fields by clicking on All Fields4.

2 What are Splunk alerts based on?

A. Dashboards

B. Searches

C. Webhooks

D. Reports

Answer: B

Explanation

:

Splunk alerts are based on searches that run on a schedule or in real time. You can use alerts to monitor for and respond to specific events or conditions in your dat a. Alerts use a saved search to look for events in real time or on a schedule. Alerts trigger when search results meet specific conditions. You can use alert actions to respond when alerts trigger, such as sending an email, running a script, or creating a ticket1.

You can create alerts from the Search app, the Alerts page, or the Dashboards app. You can also use the Splunk Web framework to create custom alert actions using Python or JavaScript1.

Dashboards, webhooks, and reports are not the basis for Splunk alerts, although they can be related to them. Dashboards are collections of views that display data visually in a variety of ways. You can add alert panels to dashboards to show the status of your alerts2. Webhooks are a type of alert action that send HTTP POST requests to a specified URL when an alert triggers. You can use webhooks to integrate Splunk alerts with external systems or applications3. Reports are saved searches that include additional attributes such as a visualization type, permissions, and an optional description. You can create reports from search results and add them to dashboards as panels. You can also use reports as the basis for scheduled or real-time alerts.

Reference

Getting started with alerts

Add an alert panel to a dashboard

Use webhooks with Splunk

Enterprise [Create and edit reports]

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

A. False

B. True

Answer: A

4 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

Answer: A

5 Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts

B. Sourcetypes

C. Sources

D. Indexes

Answer: A,B,D

6 This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev

B. dev

C. count deviation

D. by standarddev

Answer: A

7 Which is a 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

Answer: D

8 The stats command will create a_____by default.

A. Table

B. Report

C. Pie chart

Answer: A

9 Field names are case sensitive and field value are not.

A. True

B. False

Answer: A

10 Matching of parentheses is a feature of Splunk Assistant.

A. No

B. Yes

Answer: B

11 When refining search results, what is the difference in the time picker between real-time and relative time ranges?

A. Real-time searches happen instantly, while relative searches happen at a scheduled time.

B. Real-time searches display results from a rolling time window, while relative searches display results from a set length of time.

C. Real-time searches run constantly in the background, while relative searches only run when certain criteria are met.

D. Real-time represents events that have happened in a set time window, while relative will display results from a rolling time window.

Answer: B

Explanation

:

The difference between real-time and relative time ranges in the time picker is that real-time searches display results from a rolling time window, such as the last 15 minutes, while relative searches display results from a set length of time, such as yesterday or last week. Real-time searches do not happen instantly, but rather update periodically based on the refresh interval. Relative searches do not happen at a scheduled time, but rather when the user runs them. Real-time searches do not run constantly in the background, but rather when the user starts them. Real-time searches do not represent events that have happened in a set time window, but rather events that are happening now.

12 Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes

B. sourcetype=access_* | avg (bytes)

C. sourcetype=access_* | stats max(bytes)

D. sourcetype=access_* | max(bytes)

Answer: C

13 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. ,

Answer: D

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

A. All data accessible to the User role will appear in the report.

B. All data accessible to the owner of the report will appear in the report.

C. All data accessible to all users will appear in the report until the next time the report is run.

D. 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.

Answer: D

15 When editing a dashboard, which of the following are possible options? (select 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.
Answer: D

16 Splunk shows data in_____.
A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.
Answer: B

17 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
Answer: C

18 Prefix wildcards might cause performance issues.
A. False
B. True
Answer: B

19 How many main user roles do you have in Splunk?
A. 2
B. 4
C. 1
D. 3
Answer: D

20 What is Search Assistant in Splunk?
A. It is only available to Admins.
B. Such feature does not exist in Splunk.
C. Shows options to complete the search string
Answer: C

21 Splunk indexes the data on the basis of timestamps.

A. True
B. False
Answer: A

22_____transforms raw data into events and distributes the results into an index.
A. Index
B. Search Head

C. Indexer
D. Forwarder
Answer: C

23 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
Answer: A
Explanation
:
The search query sourcetype=access_combined would return events from the access_combined sourcetype, which is a predefined sourcetype in Splunk that matches the access-common or access-combined Apache logging formats1. The sourcetype field is case-sensitive, so using different capitalization such as Access_Combined or ACCESS_COMBINED would not match the exact sourcetype name2. The sourcetype field is also a default field that is added by the indexer when it indexes the data, so it does not need to be enclosed in quotation marks3.
Reference
List of pretrained source types
Search command syntax details
Basic searches and search results

24 Fields are searchable name and value pairings that differentiates one event from another.
A. False
B. True
Answer: B

25 Which search will return only events containing the word "error" and display the results as a table that includes the fields named action, src, and dest?
A. error | table action, src, dest
B. error | tabular action, src, dest
C. error | stats table action, src, dest
D. error | table column=action column=src column=dest
Answer: C
Explanation
:
Explanation/Reference: Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/search

26 Universal forwarder is recommended for forwarding the logs to indexers.
A. False
B. True
Answer: B

27 36. Lookups can be private for a user.