DUMPSBOSS.

Splunk Core Certified User

Splunk SPLK-1001

Version Demo

Total Demo Questions: 15

Total Premium Questions: 243

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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 C

QUESTION NO: 2

When an alert action is configured to run a script, Splunk must be able to locate the script.

Which is one of the directories Splunk will look in to find the script?

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/scripts

C. $SPLUNK_HOME/bin/etc/scripts

D. $SPLUNK_HOME/etc/scripts/bin

ANSWER: A

Explanation:

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

QUESTION NO: 3

Interesting fields are the fields that have at least 20% of resulting fields.

A. True

B. False

ANSWER: A

QUESTION NO: 4

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

A. Zoom to selection

B. Format Timeline

C. Deselect

D. Delete

E. Zoom Out

ANSWER: A B C E

QUESTION NO: 5

Splunk apps are used for following (Choose three.):

A. Designed to cater numerous use cases and empower Splunk.

B. We can not install Splunk App.

C. Allows multiple workspaces for different use cases/user roles.

D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

ANSWER: A C D

QUESTION NO: 6

What are the two most efficient search filters?

A. _time and host

B. _time and index

C. host and sourcetype

D. index and sourcetype

ANSWER: B

QUESTION NO: 7

Which command is used to review the contents of a specified static lookup file?

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

ANSWER: C

QUESTION NO: 8

What is the primary use for the rare command?

A. To sort field values in descending order.

B. To return only fields containing five of fewer values.

C. To find the least common values of a field in a dataset.

D. To find the fields with the fewest number of values across a dataset.

ANSWER: C

Explanation:

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

QUESTION NO: 9

Which all time unit abbreviations can you include in Advanced time range picker? (Choose seven.)

A. h

B. day

C. mon

D. yr

E. y

F. w

G. week

H. d

I. s

J. m

ANSWER: A C E F H I J

QUESTION NO: 10

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.

ANSWER: A

QUESTION NO: 11

Select the best options for "search best practices" in Splunk: (Choose five.)

A. Select the time range always.

B. Try to specify index values.

C. Include as many search terms as possible.

D. Never select time range.

E. Try to use * with every search term.

F. Inclusion is generally better than exclusion.

G. Try to keep specific search terms.

ANSWER: A B C F G

QUESTION NO: 12

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”

ANSWER: C

QUESTION NO: 13

You can also specify a time range in the search bar. You can use the following for beginning and ending for a time range (Choose two.):

A. Not possible to specify time manually in Search query

B. end=

C. start=

D. earliest=

E. latest=

ANSWER: D E

QUESTION NO: 14

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.

ANSWER: A B D

QUESTION NO: 15

Selected fields are a set of configurable fields displayed for each event.

A. True

B. False

ANSWER: A