

## Splunk.SPLK-1001.v2023-04-21.q138

□□□□:	SPLK-1001
□□□□:	Splunk Core Certified User
□□□:	Splunk
□□ □□ □□□:	138
□□:	v2023-04-21
# □□ □:	1747
# □□ □□□:	1380
<a href="https://www.krdump.com/Splunk.SPLK-1001.v2023-04-21.q138.html">https://www.krdump.com/Splunk.SPLK-1001.v2023-04-21.q138.html</a>	

### NEW QUESTION: 1

□□ □□□□ □□ □□□ □□□□□□?

- A. □□ □□□ □□□□ □□□□□□.
- B. □□ □□□ □□□ □□ □□ □□ PDF □□□.
- C. □□□ □□ □□□□ □□ □□□□ □□ □□□□□ □□□ □□□□.
- D. □□ □□□ □□□ □ Splunk □□□□□□ □□□ □□□□□□.

Answer: D ([LEAVE A REPLY](#))

□□

□□/□□: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports>

### NEW QUESTION: 2

□□□□□ □□□ □ □□ □ □□□ □□□ □□□□□□? (□□□□ □□ □□ □□□□□□.)

- A. □□□ □□□□□.
- B. □□□□ □□□ □□□□□ □□ □□□ □□□□□□.
- C. □□□□ □□□ □□□□□.
- D. □□□□ □□□ □□□□ □□ □□□ □□□□□.

Answer: D ([LEAVE A REPLY](#))

### NEW QUESTION: 3

□□□ □□ |□ □□ □□□□ □□ □□□□□□?

- A. □ □. □: stats sum(bytes) | □□□□ □□
- B. □□ □. □: □□□□ □□ |□□(□□□)
- C. □□ □. □: □□ □□ |(□□□) □□□□
- D. □□ □. □: | □□□□ □□ □□(□□□)

Answer: ([SHOW ANSWER](#))

### NEW QUESTION: 4

Which of the following is a valid Splunk search command? (Select all that apply)

- A. search inputlookup
- B. search inputlookup
- C. search inputlookup
- D. search Splunk

Answer: (SHOW ANSWER)

**NEW QUESTION: 5**

Which of the following is a valid Splunk search command? (Select all that apply)

- A. search=-2h
- B. search=-2@d
- C. search=-2h
- D. search=-2hour@d

Answer: C (LEAVE A REPLY)

**NEW QUESTION: 6**

Which of the following is a valid Splunk search command? (Select all that apply)

- A. search + search
- B. search search
- C. search + search - search
- D. search + search - search

Answer: (SHOW ANSWER)

**NEW QUESTION: 7**

Splunk search command: search

- A. 4
- B. 3
- C. 2
- D. 1

Answer: B (LEAVE A REPLY)

**NEW QUESTION: 8**

Which of the following is a valid Splunk search command? (Select all that apply)

- A. search
- B. search
- C. search
- D. search

Answer: (SHOW ANSWER)

Source: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usesthetimeline>

**NEW QUESTION: 9**

□□□ □□□ □□ □□ □□ □□□□ □□□ □ □□ □□□□□□.

A. □

B. □□□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 10**

Splunk □□□□□□□ □□ □□□ □□□□ □ □□ □□□ □□□□□?

A. □, □□, □□ □ □□□

B. □, □□□, □□□□ □ □□

C. □, □□□□, □□□ □ □□

D. □, □□□, □□□ □ □□

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 11**

□□ □ □□□ □□□ □□□□ □□□□ □□ □□□□□ □□□ □ □□□□ □□□ □□□□□?

A. □□□ □□□□ □□□□ □□□ □□ □□ □□□□□□ □□

B. □□□ □□□ □□□□ □□□□ □□□ □□ □□ □□□□□□ □□

C. □□□□ □□□ □□□□□□ □□□ □□□□ □□□ □□

D. □□ □□□ XML □□□ □□□□ □□ □□□□ □□□□ □□

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 12**

□□□ □□□ input.conf□ □□□□□.

A. □□□

B. □

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 13**

□□□□□ Splunk□ □□ □□□ □□□ □□ □□□□□?

A. 10□

B. 15□

C. 1□

D. 7□

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 14**

topcommand□ □□ □□□□ □□ □□?

A. □□ 10□ □□□ □□□□□.

B. □□□ □□□ □□□□ □□□□□.

C. □□ □□ □ □□□ □□ □□□□□.



Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 19**

!= NOT NOT NOT NOT.

- A. NOT
- B. NOT

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 20**

NOT NOT | NOT NOT NOT NOT NOT NOT NOT?

- A. NOT NOT. NOT: stats sum(bytes) | NOT NOT NOT NOT
- B. NOT NOT. NOT: | NOT NOT NOT NOT NOT (NOT NOT)
- C. NOT NOT. NOT: NOT NOT (NOT NOT) NOT NOT
- D. NOT NOT. NOT: NOT NOT NOT NOT | NOT (NOT NOT)

Answer: B ([LEAVE A REPLY](#))

NOT/NOT:

[https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes\\_and\\_escaping\\_characters](https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes_and_escaping_characters)

**NEW QUESTION: 21**

Splunk NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT.

- A. NOT
- B. NOT

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 22**

NOT NOT NOT NOT Splunk NOT NOT NOT NOT NOT NOT (4 NOT NOT).

- A. NOT
- B. Splunk NOT NOT NOT NOT
- C. indexes.conf
- D. savesearches.conf
- E. Splunk Web
- F. NOT NOT NOT NOT.conf
- G. input.conf
- H. CLI

Answer: B,E,G,H ([LEAVE A REPLY](#))

**NEW QUESTION: 23**

NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT.

NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT?

- A. Selected Fields NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT.
- B. NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT NOT.





- B. `src | eval src=src`
- C. `src | eval src=src`
- D. `src | eval src=src`

Answer: [\(SHOW ANSWER\)](#)

**NEW QUESTION: 33**

`search dest_ipfield=15 dest_ip`

- A. `search dest_ip=15 dest_ip`
- B. `search dest_ip=15 dest_ip`
- C. `search dest_ip=15 dest_ip`
- D. `search dest_ip=15 dest_ip`

Answer: D [\(LEAVE A REPLY\)](#)

`search`:

<https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Rare#:~:text=The%20rare%20command%20is%20a,the%20limit%20argument%20is%2010>

**NEW QUESTION: 34**

`search`

- A. `#`
- B. `%`
- C. `#`
- D.

Answer: [\(SHOW ANSWER\)](#)

**NEW QUESTION: 35**

`Splunk`

- A. `search`
- B. `search`
- C. `search`
- D. `search`

Answer: A [\(LEAVE A REPLY\)](#)

**NEW QUESTION: 36**

`Splunk` `docs.splunk.com`

- A. `search`
- B. `search`

Answer: [\(SHOW ANSWER\)](#)

**NEW QUESTION: 37**

`search`

- A. `search`



C. `vendor_action()`

D. `vendor_action()`

Answer: (SHOW ANSWER)

#### NEW QUESTION: 43

Which of the following is a valid Splunk search command?

A. `search * | eval a=1`

B. `search * | eval a=1 | eval b=2`

C. `search * | eval a=1 | eval b=2 | eval c=3`

D. `search * | eval a=1 | eval b=2 | eval c=3 | eval d=4`

Answer: C (LEAVE A REPLY)

#### NEW QUESTION: 44

Which of the following is a valid Splunk search command?

A. `search *`

B. `search !*`

C. `search *`

D. `search >*`

Answer: C (LEAVE A REPLY)

#### NEW QUESTION: 45

Which of the following is a valid Splunk search command?

A. `search *`

B. `search *`

Answer: A (LEAVE A REPLY)

URL: <https://docs.splunk.com/Documentation/Splunk/7.2.3/SearchTutorial/Usefieldstosearch>

#### NEW QUESTION: 46

Which of the following is a valid Splunk search command?

A. `search host=WWW3`

B. `search host=WWW*`

C. `search host=WWW3`

Answer: B (LEAVE A REPLY)

**SPLK-1001** Splunk dumps, DumpTop Splunk SPLK-1001! DumpTop Splunk

**SPLK-1001** Splunk dumps, DumpTop Splunk SPLK-1001 Splunk dumps, DumpTop Splunk. Splunk

Splunk dumps, DumpTop Splunk SPLK-1001 Splunk dumps. [https://www.dumptop.com/Splunk/SPLK-1001-](https://www.dumptop.com/Splunk/SPLK-1001-dump.html)

[dump.html](https://www.dumptop.com/Splunk/SPLK-1001-dump.html) (245 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

**NEW QUESTION: 47**

□□ □□ □□□□ \_\_\_\_\_ □□□ □□□ □□□□ □□ □□□□□□.

A. □□

B. □□

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 48**

stats □□□ values □□□ □□□ □□□?

A. □□□ □□□ □□ □□ □□□□□□.

B. □□□ □□□□ □□□ □□ □□□□□□.

C. □□□ □□□ □□ □□ □□ □□□ □□□□□□.

D. □□□ □□□ □□□ □□ □□□□□□.

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 49**

□□□ □□ □□□ □□□□ □□□ □□□ □□□□□□(3□ □□).

A. □□

B. □□ □

C. □□

D. □□

E. □□□

Answer: C,D,E ([LEAVE A REPLY](#))

**NEW QUESTION: 50**

Splunk □□□ □□ □□□□ □□ □□?

A. □□□ □□□ □□ □□ □□□□□ □□□□ □□□ □□□□ □□□.

B. □□□ □□□ □□□□ □□ □□□□□ □□□ □□□ □□□□.

C. □□□□□□ □□□□ □□□ □□□□ □□□ □□□□□.

D. □□□ □□□ □□□□ □□ cron□ □□□ □□□□ □□□□□ □□□.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 51**

□□ □□ □□□□□ □□□□ □□□ □□□ □□□□ □□□ □□□□□□□.

index=security sourcetype=access\_\* status=200 □□ □□□□ □□

A. □□□=□□ □□ □□=□□□\_\* | □□=200 | □□□ □□□□ □□

B. □□□=□□ □□ □□=□□□\_\* □□=200 | □□ □ | □□□□

C. □□□=□□ □□ □□=□□□\_\* □□=200 □□ | □□□□ □□

D. □□□=□□ □□ □□=□□□\_\* □□=200 | □□□ □□□□ □□

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 52**

□□□ □□ □□ □□□ □□□ □□□ □ □□□□?

- A. □□ □□
- B. □□ □□ □□
- C. □□ > □□ > □□
- D. □□ > □□ > □□□

Answer: B ([LEAVE A REPLY](#))

□□/□□: <https://answers.splunk.com/answers/30376/how-to-display-the-contents-of-a-lookup-file.html>

**NEW QUESTION: 53**

□□ □ □□ □□□ □□ □□□ □□□□□?

- A. □□□□ 50% □□□ □□□ □□□□ □□ □□□ □□ □□□□.
- B. □□ □□□ □□□□ □□□□ □□□□□ □□ □□□ □ □□□□.
- C. □□ □□□ □□□□ □□□ □ □□□□.
- D. □□□□ 50% □□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 54**

□□□□□ □□□□ □□□ □□□ □□ □□□ □□□□?

- A. □□□ □□ □□□□ □□□□ □□□ □□□□□ □□ □□□□□ □□□□.
- B. □□ □□□□ □□□□ □□ □□□□ □□□□ □□ □□□□□ □□□ □□□□.
- C. □□ □□□ □□ □□□□□□ □□ □□□□ □□□□□.
- D. □□□□□ □□□□ □□□ □□□□ □□□ □□□□.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 55**

"□□" □ "□□"□□ □□□ □□□ □□□□ □□□□ □□□ □□□□□?

- A. index=security NOT □□ NOT □□
- B. index=security "□□ □□"
- C. □□□=□□ □□ □□ □□
- D. □□□=□□ □□ □□

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 56**

□□ □ security□□ □□□□□ □□ □□□□ □□□□ □□/□ □□ □□□□□?

- A. □□=□□
- B. □□□=□□
- C. □□□=□□
- D. □□□!=□□

Answer: B ([LEAVE A REPLY](#))

□□/□□: <https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-in-diffe.html>

**NEW QUESTION: 57**

□□□ □□□ □ □□□□ □□□ □□□□□?

- A. □□□.
- B. □□□□.
- C. □□□□□ □□□□□□.
- D. □□ □□□ □□ □□□□□□□.

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 58**

□□ □□□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□ □ □□ □ □□□□ □□ □□□□□?

- A. □□□ □□
- B. □□□ □□
- C. □□ □□□ □□
- D. □□□ □□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 59**

□□ □□ □□ □ Splunk □□ □□□ □□□□ □□ □□□ □□□□□?

- A. JSON
- B. XLS
- C. PDF
- D. RTF

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 60**

□□ □ Splunk□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□□□?

- A. □□\_□□\_□□
- B. Group\_Object\_Description
- C. Group\_Description\_Object
- D. □□\_□□\_□□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 61**

□□ □ status\_code□ 4:4□ □□□□ □□□□ □□ □□□□ □□□□□?

- A. □□ □□ !=404
- B. status\_code<=404
- C. □□ □□>403 status\_code<405
- D. status\_code>=400

Answer: C ([LEAVE A REPLY](#))



C. □□□

Answer: B,C ([LEAVE A REPLY](#))

**NEW QUESTION: 67**

□□ □□□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□ □ □□ □ □□□□ □□ □□□□□?

A. □□□ □□

B. □□□ □□

C. □□□ □□

D. □□ □□□ □□

Answer: C ([LEAVE A REPLY](#))

□□

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Savingsearches>

**NEW QUESTION: 68**

Splunk □□□□□^□□ □□ □□□ □□□□ □ □□ □□□ □□□□□?

A. □, □□□, □□□ □ □□

B. □, □□□, □□□□ □ □□

C. □, □□□□ □□□ □ □□

D. □, □□, □□ □ □□□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 69**

rarecommand □ □□□ □□□?

A. □□□□ □□□ □□□ □□ □□ □□ □□□□□.

B. □□□□ □□□ □□□ □□ □□□□ □□ □□ □□□□□.

C. □□□□ □□□ □□□ □□ 10□ □□ □□ □□□□□.

D. □□□□ □□□ □□□ □□ □□ 10□ □□ □□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

□□/□□:

□□: <https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Rare>

**NEW QUESTION: 70**

HF□ □□ □□□□ □□ □□? (3□□ □□□□□.)

A. □□□

B. □□ □

C. □□

D. □□□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 71**

□□ □□ □□□□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□□?

- A. `count=dc count | count count "count" count.`
- B. `count=dc count | stats dc(count) count "count" count`
- C. `count=dc count | "count" count count count`
- D. `count=dc count | count "count" count count count.`

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 72**

- count count count count count count count count count?
- A. count count count count count count count count count count count count count count count.
  - B. count count count count count count count count count.
  - C. count count count count count count count count count count count count count count count.
  - D. count count count count count count count count count.

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 73**

- count count count count count count.
- A. count
  - B. count

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 74**

- count count count count count count count count count count count count count count count?
- A. count count count count count.
  - B. count count count count count.
  - C. count count count count count.
  - D. count count count count count count count.

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 75**

- count count count count count count count count count count count count count count count?
- A. count count
  - B. count count
  - C. count count
  - D. count count count

Answer: C ([LEAVE A REPLY](#))

count/count: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Savingsearches>

**NEW QUESTION: 76**

- count count index=test sourcetype="The\_Questionnaire\_P\*" count count count count count count?
- A. the\_questionnaire pedia
  - B. the\_questionnaire \_pedia



D. 30 00 0 000 00000.

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 81**

000 000 00 00000. | (000)0 00 000 0000 00000.

- A. Ctrl + Enter
- B. Shift + Enter
- C. 00000 + 00
- D. Alt + Enter

Answer: B ([LEAVE A REPLY](#))

00/00:

**NEW QUESTION: 82**

00 0 top 000 00 000 0 00 00 000 00000?

- A. 00 0
- B. 00
- C. 00
- D. userperc

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 83**

00000 Splunk0 00 000 000 00 00000?

- A. 100
- B. 150
- C. 10
- D. 70

Answer: ([SHOW ANSWER](#))

00/00: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes>

**NEW QUESTION: 84**

stats 000 000 000?

- A. 00 000 0000 0000 00 000 00000.
- B. 00 00 000 0000 000 00 00 000 00000.
- C. 00 000 0000 000000.
- D. 00 00 00 000 00

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 85**

00 000 000 0 00 00 000 000 0 00 0000 000 00000?

- A. 00 +
- B. 00 00



Answer: A,B,C,E ([LEAVE A REPLY](#))

□□/□□:

**NEW QUESTION: 91**

□□ □□□ □□□ □□□ □□ □□□□□ □□□□ □□□□. □□ □□□□□ □□□ □□□ □ □□□□?

A. □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□□□.

B. □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□□□.

C. Selected Fields □ □□□□ □□□□□ □□□ □□□ □□□□□.

D. □□□□ □□□ □□ □□□ □□ □□ □□□□□ □□□□ □□□ □ □□□□□ □□□□□□.

Answer: A ([LEAVE A REPLY](#))

□□/□□:

**SPLK-1001** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1001 □□! DumpTop □ □□

**SPLK-1001** □□ □□□ □□□□□□, DumpTop SPLK-1001 □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □

□□□ □□□ □□□□ □□ DumpTop SPLK-1001 □□□ □□□□□. <https://www.dumptop.com/Splunk/SPLK-1001-dump.html> (245 Q&As Dumps, **30%OFF Special Discount: KrDump**)

**NEW QUESTION: 92**

□□ □□□ □□□□□ □□□□□ □□□ □□ Splunk□ □□□□□ □□ □ □□□ □□□. Splunk□ □□□□□ □□ □

□ □□□ □□□□ □ □□□ □□□□□?

A. \$SPLUNK\_HOME/bin/scripts

B. \$SPLUNK\_HOME/etc/scripts

C. \$SPLUNK\_HOME/bin/etc/scripts

D. \$SPLUNK\_HOME/etc/scripts/bin

Answer: A ([LEAVE A REPLY](#))

□□/□□:

□□: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Configuringscriptedalerts>

**NEW QUESTION: 93**

□□ □ Splunk□ □□ □□□□ □□□ □□□□□ □□□ □□□□□?

A. □□□

B. □□

C. □□□

D. □□□

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 94**

□□ □□ □ □ □□□□□ □□□□ categoryId□ □□ □□□□ □□ □□□□□?

A. Sourcetype=access\_\* |□□□□ □□ □□□

- B. Sourcetype=access\_\* |stats sum( categoryD.
- C. Sourcetype=access\_\* | ( )
- D. Sourcetype=access\_\* |

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 95**

?  
 =www3 =503

- A. www3 503
- B. www3 503
- C. . .
- D. . .

Answer: B ([LEAVE A REPLY](#))

/: <https://answers.splunk.com/answers/617772/why-am-i-getting-a-http-503-error-when-using-threa.html>

**NEW QUESTION: 96**

Splunk \_\_\_\_\_

- A. 2
- B. 4
- C. 3
- D. 1

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 97**

30 ?

- A. - : 30
- B. - , :
- C. - : , :
- D. - , :

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 98**

?

- A. \* = \*
- B. ( = OR = )
- C. = \*
- D. = s \*

Answer: C ([LEAVE A REPLY](#))

**NEW QUESTION: 99**

.





D. | □□ □□=5

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 109**

□□□ □□□ □□ □□□□□ □□ □□□ □□□□□?

A. □□□□□ □□□□ □□□□ □□□□□ □□ □□□□ □□□□□.

B. □□ □□□ □□ □□□ □□□□ □□□□□ □□□□□.

C. □□□ □□□ □□□□ □□□ □□ □ □□□□□.

D. □□ □□ □□□□□ □□□ □□□ □ □□ □□□□□ □□□ □/□□ □□□□ □□□□□.

Answer: D ([LEAVE A REPLY](#))

□□/□□: <https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Startsearching>

**NEW QUESTION: 110**

□□□ □□□ □ □□□□□ □□□□ □□□□□ □□ □□□ □□□□?

A. □□□ □□□ □□□□□.

B. □□ □□ □□□ □□□□□□.

C. □□ □□ □□ □□□□ □□□□□.

D. □□ □□ □□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

□□/□□: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usesthetimeline>

**NEW QUESTION: 111**

Splunk□ □□ □□□□ □□ □□?

A.

B. >

C. <

D. ?

E. !

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 112**

□□ Splunk □□ □□□ □□ □□□ □□□ □□□?

A. □□ □□ □□□ 10□ □□ □□□□□.

B. □□ □□ □□□ 10□ □□ □□□□□.

C. □□ □□ □□□ 10□□ □□ □□□□□.

D. □□ □□ □□□ 10□ □□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 113**

□□ □ □□□ □□ □□□□ □□ □□ □□? (□□□□ □□ □□□ □□□□.)

A. □□ □□□ □□□□ □□ □□□□ □□ □ □□□□.

B. 10mg

C. Splunk DB Connect

D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 114

A.

B.

C.

D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 115

A.

B.

C.

D. XML

Answer: D (LEAVE A REPLY)

https://answers.splunk.com/answers/231429/can-i-have-multiple-panels-using-the-same-inline-s.html

NEW QUESTION: 116

A. Splunk

B. Splunk

C.

D.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 117

stats

A.

B.

C.

D.

Answer: (SHOW ANSWER)

NEW QUESTION: 118



Answer: D ([LEAVE A REPLY](#))

□□/□□: <https://answers.splunk.com/answers/610038/understanding-command-in-search.html>

**NEW QUESTION: 123**

□ □□□ 20□□ □□□ □□□□□. □□: □□ | □□ □□□ □□ = 20

A. □□

B. □□

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 124**

□□ command1□ □□ □□□ □□□□□?

A. □□□ □□□□ □□ □□ □□ □□□ □□□□

B. □□ □□ □□□□□□ □□□□□

C. 5□ □□□ □□ □□□□ □□□ □□□□□

D. □□□ □□□□ □□□ □□ □□ □ □□

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 125**

□□ □ top □□□ □□□□ □□ □□□ □□□□□?

A. □□, □□ □□

B. showperc, countfield

C. □□, □□

D. □□, □□□ □□

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 126**

□□ □□□□□ □/□ □□ □□□□ □ □□□□ □□□ □□□□□?

A. □□ □□ □□

B. □□=□□

C. □□ | □□

D. □□+□□

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 127**

□□ □ Splunk □□□□ □□ □□□□ □□□□□? (3□□ □□□□□.)

A. Splunk Enterprise □□(ES)

B. Splunk IT □□□ □□□□□(ITSI)

C. Splunk Analytics □□(AS)

D. Splunk □□□ □□ □□(UBA)

Answer: A,B,D ([LEAVE A REPLY](#))

**NEW QUESTION: 128**

Which of the following is a valid Splunk search for finding all events with a status code of 404?

- A. status\_code!=404
- B. status\_code>=400
- C. status\_code<=404
- D. status\_code>403 status\_code<405

**Answer: C (LEAVE A REPLY)**

Source: <https://docs.splunk.com/Documentation/SplunkLight/7.3.1/Examples/Searchforerrors>

**NEW QUESTION: 129**

Which of the following is a valid Splunk search for finding all events with a status code of 404?

- A. Splunk search status\_code=404
- B. status\_code=404
- C. status\_code=404 | Splunk search status\_code=404
- D. Splunk search status\_code=404 | status\_code=404

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 130**

Which of the following is a valid Splunk search for finding all events with a status code of 404?

- A. Splunk search status\_code=404
- B. status\_code=404
- C. status\_code=404 | Splunk search status\_code=404
- D. Splunk search status\_code=404 | status\_code=404

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 131**

Which of the following is a valid Splunk search for finding all events with a status code of 404?

(status\_code=404)

- A. status\_code=404
- B. status\_code=404 | Splunk search status\_code=404
- C. status\_code=404
- D. status\_code=404 | status\_code=404
- E. status\_code=404 | Splunk search status\_code=404

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 132**

Which of the following is a valid Splunk search for finding all events with a status code of 404?

- A. status\_code=404
- B. status\_code=404 | Splunk search status\_code=404
- C. status\_code=404 | status\_code=404
- D. status\_code=404 | Splunk search status\_code=404

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 133**

Which of the following is a valid CSV file name?

- A. | file.csv
- B. file.csv
- C. | file.csv
- D. | lookup\_definition file.csv

Answer: ([SHOW ANSWER](#))

Q/A: <https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Inputlookup>

**NEW QUESTION: 134**

Which of the following is a valid CSV file name?

- A. file
- B. file
- C. file
- D. file

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 135**

Which of the following is a valid CSV file name? (file.csv is a valid file name)

- A. lookup file.csv
- B. file.csv
- C. file Splunk file.csv
- D. inputlookup file.csv

Answer: B ([LEAVE A REPLY](#))

Q/A: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/DefineanautomaticlookupinSplunkWeb>

**NEW QUESTION: 136**

Which of the following is a valid CSV file name?

- A. HF
- B. file
- C. file

Answer: C ([LEAVE A REPLY](#))

**SPLK-1001** file.csv DumpTop file.csv SPLK-1001 file! DumpTop file.csv  
**SPLK-1001** file.csv, DumpTop SPLK-1001 file.csv file.csv file.csv. file

