

Splunk.SPLK-1002.v2026-02-20.q238

□□□□:	SPLK-1002
□□□□:	Splunk Core Certified Power User Exam
□□□:	Splunk
□□ □□ □□□:	238
□□:	v2026-02-20
# □□ □:	110
# □□ □□□:	2380
https://www.krdump.com/Splunk.SPLK-1002.v2026-02-20.q238.html	

NEW QUESTION: 1

□□□□□ □□□ □□ Splunk□ □□ KMZ □□□ □□□□□(□□□□ □□ □□ □□).

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

Answer: A,D (LEAVE A REPLY)

Splunk□ □□□ □□ □□□□□ KMZ □□□ □□□□□. □□ □ □ □□ □□ □□. KMZ □□□ KML □□□ □□ □□□□ □□□□ □□ □□□□□. KML □□□ □□□ □□□ □ □□□ □□□□ XML □□□□□. Splunk□□ geom □□□ □□□□ KMZ □□□ □□□□ □□□□□ □□ □ □□□□. □□□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□□□□. Splunk□ □□□□□ □□□ □□□ □□□ □ □ □□ KMZ □□□ □□□□□. □□ □: □ KMZ □□□ □□ 50□ □□ □ □□□ □□□□□. □ KMZ □□□ □□□ us_states.kmz□□ \$SPLUNK_HOME/etc/apps/maps/appserver/static/geo □□□□□ □□□□. □ □□ □□: □ KMZ □□□ □ □□ □□□ □ □□□ □□□□□. □ KMZ □□□ □□□ world_countries.kmz □□ \$SPLUNK_HOME/etc/apps/maps/appserver/static/geo □□□□□ □□□□. Splunk□ □□, □□□ □□ □□ □□ □□□ KMZ □□□ □□□□ □□□□. □□□ KMZ □□□ □□ □□□□ □□ □□□□ □□□□□□ Splunk□□ □□□ □ □□□□.

NEW QUESTION: 2

□□□ □□□□□ □□□□ □□ □ □□ □□□ □□□□ □□□?

- A. □□□ □□□ □□:□ □□ □□□□□.
- B. □□□ Power □□□ □□□□ □□□.
- C. □□□ □□□□ □□ □□□ □□□ □ □□□□.
- D. □□□ □□□ □□□ □□ □□□ □□□ □□□.

Answer: D (LEAVE A REPLY)

Which of the following is a valid Splunk search command? (Select all that apply.)
A. search index=main
B. search index=main |
C. search index=main |
D. search index=main |

Splunk Search [] []

NEW QUESTION: 3

Which of the following is a valid Splunk search command? (Select all that apply.)
A. search index=main |
B. search index=main |
C. search index=main |
D. search index=main |

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

NEW QUESTION: 4

Which of the following is a valid Splunk search command? (Select all that apply.)
A. search index=main |
B. search index=main |
C. search index=main |
D. search index=main |

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

URL:

<https://www.edureka.co/blog/splunk-events-configuration-tips/>

NEW QUESTION: 5

Which of the following is a valid Splunk search command? (Select all that apply.)
A. eval sort
B. eval
C. sort eval
D. eval

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

NEW QUESTION: 6

Splunk Common Information Model (CIM) is a framework for organizing and analyzing data. Which of the following is a valid Splunk search command? (Select all that apply.)
A. search
B. search
C. search
D. search

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

123 A123. 123 123.

Splunk 12.1 Common Information Model (CIM) 12.1.

Splunk Common Information Model (CIM) 12.1.

(CIM)12.

CIM 12.1 Common Information Model (CIM) 12.1.

12.1 Common Information Model (CIM) 12.1.

12.1 Common Information Model (CIM) 12.1.

domain4. 12.1 Common Information Model (CIM) 12.1.

1. 12.1 Common Information Model (CIM) 12.1.

NEW QUESTION: 7

12.1 Common Information Model (CIM) 12.1.

A. 12.1

B. 12.1

C. 12.1

D. 12.1

Answer: B (LEAVE A REPLY)

12.1 Common Information Model (CIM) 12.1.

NEW QUESTION: 8

12.1 Common Information Model (CIM) 12.1.

12.1 Common Information Model (CIM) 12.1.

A. Index-main | REJECT trans sessionid

B. Index-main | 12.1 ID | 12.1 REJECT

C. Index=main | 12.1 ID | 12.1 12.1 12.1

D. Index=main | 12.1 ID | 12.1 12.1=12.1"

Answer: B (LEAVE A REPLY)

12.1 Common Information Model (CIM) 12.1.

transactions2. transaction 12.1 ID 12.1 12.1 12.1.

12.1 12.1, 12.1 12.1 12.1 12.1 12.1.

12.1 Common Information Model (CIM) 12.1.

12.1: index=main | transaction sessionid | search REJECT2. 12.1 12.1 12.1

sessionid 12.1 12.1 REJECT 12.1 12.1 12.1.

B 12.1 12.1 A, C 12.1 12.1 12.1 12.1 12.1.

12.1 12.1 12.1 12.1.

NEW QUESTION: 9

12.1 Common Information Model (CIM) 12.1.

A. 12.1= 12.1

Which of the following is a valid macro definition?

- A. `macro myMacro { mySource oldField=* | myField newField }`
- B. `macro myMacro { mySource oldField=* | myField newField }`
- C. `macro myMacro { mySource oldField=* | myField newField }`
- D. `macro myMacro { mySource oldField=* | myField newField }`

Answer: (SHOW ANSWER)

11

URL: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definereachmacros>

NEW QUESTION: 13

Which of the following is a valid macro definition?

| `Application_State All_Application_State`

- A. `Application_State`
- B. `Application_state`
- C. `All_Application_state`
- D. `Application_State`

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Which of the following is a valid macro definition?

```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

- A. `index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user`
- B. `index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user`
- C. `index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user`
- D. `index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user`

Answer: B (LEAVE A REPLY)

Which of the following is a valid macro definition?

| `corndog=mysterymeat`

`stats count as corndog_count by user`

`stats count as corndog_count by user`

where `corndog` `mysterymeat`

`corndog`

NEW QUESTION: 15

Which of the following is a valid macro definition? (Choose two)

- A. `corndog=mySource oldField=* | makeMyField(oldField) | newField`
- B. `corndog=mySource oldField=* | if('makeMyField(oldField)') | newField`
- C. `corndog=mySource oldField=* | newField='makeMyField(oldField)' | newField`

□□□□ □□□□□□ □□ □□□ □□□□ □□□ □□□□. 3. □□□ □□□□ □□□ □□ □□□□.

Which of the following is a valid Splunk search command? (Select all that apply.)
A. search 3. B. search 3. C. search 3. D. search 3.
Splunk3 is a valid Splunk search command. The other options are not valid Splunk search commands.

NEW QUESTION: 18

- Which of the following is a valid Splunk search command? (Select all that apply.)
- A. search 3.
 - B. search 3. C. search 3. D. search 3.
 - C. search 3.
 - D. search 3.

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

Which of the following is a valid Splunk search command? (Select all that apply.)
A. search 3. B. search 3. C. search 3. D. search 3.
Splunk3 is a valid Splunk search command. The other options are not valid Splunk search commands.

NEW QUESTION: 19

- Which of the following is a valid Splunk search command? (Select all that apply.)
- A. search 3.
 - B. search 3.
 - C. search 3.
 - D. search 3.

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

NEW QUESTION: 20

- Which of the following is a valid Splunk search command? (Select all that apply.)
- A. search 3.
 - B. search 3.
 - C. search 3.
 - D. search 3.

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

Splunk3 is a valid Splunk search command. The other options are not valid Splunk search commands.

NEW QUESTION: 23

□□□ weekly_sales(2)□□ □□ □□□□ □□□□ □□□□.

index-games | □□ □□ □□ = \$price\$ \$AmountS01d\$

□□ □ □□ □□ □□□ □□□□□?

A. '□□_□□□(3.99, 10) '

B. '□□_□□(\$3.99\$, \$10\$)

C. '□□_□□□ (3.99, 10)

D. '□□_□□(3)

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

□□□ C. 'weekly_sales (3.99, 10)'□□□. □□ □□ □□□□ □□□ □□□□ □□ □□□□□.

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

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

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

Splunk □□□□□ □□□ □□ □□□□ □□□□ □□1.

NEW QUESTION: 24

□□ □ eval □□ tostring □□□ □□ □□□ □ □□ □□ □□□□□? (□□□□ □□ □□□ □□□□□)

A. "16□□"

B. "□□"

C. "10□□"

D. "□□"

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

<https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29>

eval □□□ tostring □□□ □□ □□ □□□ □□□ □□□□□. □□□ □□ □□□ □□□□ □ □□ □□(□□ □□)□ □□□ □ □□□□. □□□ □□□ □□□ □□□□.

hex: □□ □□ 16□□ □□□□ □□□□□.

□□: □□ □□ □ □□□ □□□□ □□ □□□ □□□□□.

□□: □□ □□ "2□□ 3□ 4□"□ □□ □□□ □□ □ □□ □□ □□□□ □□□□□.

□□□ A, B, D □□□ tostring □□□ □□ □□□ □ □□□□.

NEW QUESTION: 25

□□ □□□ □□ □□□ □□□?

A. □□□ □□ □□□ □□□ □□□□□□.

B. □□□ □□□□ □□ □□□□ □□□□□.

C. □□ □□□ □□ □□□□ □ □□□□ □□□□□.

D. □□□ □□□□ □□□ □□□□ □□ □□ □□□□□.

Answer: ([SHOW ANSWER](#))

transaction □□□ □ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□□□.

transaction □□□ □□, □□ □□ □ □□ □□□□ □□□□ □□□□ □ □□□□. transaction □□□ □ □□

NEW QUESTION: 30

Which of the following is a valid Splunk transaction command?

- A. `transaction`
- B. `transact`
- C. `transact`
- D. `transact`

Answer: (SHOW ANSWER)

Splunk transaction command is used to group events into transactions. It is used to group events that are related to each other. It is used to group events that are related to each other. It is used to group events that are related to each other.

Example:

Splunk `transaction` command, `transaction` command

Splunk `transaction` command

"transaction command is used to group events into transactions."

NEW QUESTION: 31

Which of the following is a valid Splunk command to load a KMZ file into the geodata layer?

- A. `load`
- B. `load`
- C. `load`
- D. `load`

Answer: A,D (LEAVE A REPLY)

Example:

Splunk `load` command is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer.

Splunk `load` command is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer.

Example: `load` KMZ file into the geodata layer. `load` KMZ file into the geodata layer. `load` KMZ file into the geodata layer.

`$SPLUNK_HOME/etc/apps/maps/appserver/static/geo` command.

Example: `load` KMZ file into the geodata layer. `load` KMZ file into the geodata layer. `load` KMZ file into the geodata layer.

`$SPLUNK_HOME/etc/apps/maps/appserver/static/geo` command.

Splunk `load` command, `load` command is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer. It is used to load a KMZ file into the geodata layer.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

□□ □ □□ □□□ □□□ □□□□□?

A. SPL□ □□□□ □□ □□□ □□□□□.

B. □□□ □□□ □□□□ □□□□.

C. SPL□ □□□□ □□ □□□□ □□□□□.

D. □□□ □□□ □□□□ □□□□.

[illegible]

□□ □ □□ □□□ □□ □□ □□□□ □□□□ □□□?

| □□□□□ Application_State All_Application_State □□

A. Evenrches□ □□ □□ □□□□ □□□□□.

B. □□□□ Application_State□□ □□□ □□□□ □□□□□.

C. □□□□ All_Application_state□□ □□□ □□□□ □□□□□.

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

```

Application_State Application_State Application_State
| Application_State All_Application_State
Application_State Application_State
Splunk Application_State datamodel datamodel Application_State
. Application_State Application_State Application_State
Application_State Application_State Splunk Application_State, Application_State
Application_State
Application_State All_Application_State Application_State Application_State
Application_State Application_State

```


NEW QUESTION: 39

Which of the following is a valid HTTP method?

- A. GET
- B. HTTP
- C. POST
- D. Splunk

Answer: B (LEAVE A REPLY)

Explanation:

HTTP is a protocol for transferring data between a web client and a web server. It is a stateless protocol, meaning that each request from the client to the server is treated as an independent transaction. The client sends a request to the server, and the server responds with a response. The request and response are both in the form of text documents, called HTML documents. HTTP is a stateless protocol, meaning that each request from the client to the server is treated as an independent transaction. The client sends a request to the server, and the server responds with a response. The request and response are both in the form of text documents, called HTML documents.

Splunk Web is a web interface for Splunk. It is a stateful protocol, meaning that the server remembers the state of the client. The client sends a request to the server, and the server responds with a response. The request and response are both in the form of text documents, called HTML documents. GET is a valid HTTP method. It is used to retrieve data from the server. Google, WHOIS, and HTML are all valid HTTP methods.

POST is a valid HTTP method. It is used to send data to the server. URI is a valid HTTP method. It is used to send data to the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server. HTTP POST is a valid HTTP method. It is used to send data to the server. HTTP GET is a valid HTTP method. It is used to retrieve data from the server.

Splunk Web is a web interface for Splunk. It is a stateful protocol, meaning that the server remembers the state of the client. The client sends a request to the server, and the server responds with a response. The request and response are both in the form of text documents, called HTML documents.

Splunk Web is a web interface for Splunk. It is a stateful protocol, meaning that the server remembers the state of the client. The client sends a request to the server, and the server responds with a response. The request and response are both in the form of text documents, called HTML documents.

NEW QUESTION: 40

Which of the following is a valid HTTP method?

- A. macroname
- B. GET
- C. POST
- D. HTTP

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

□□
□□□ C□□□. □□□ □□□ □□ □□(□)□ □□□□.
□□□□ SPL □□□ □□ □□□□ □□□□□ □□□□□. □□□□ □□□ □□ □ □□□, □□□ □□□□
□□□ □ □□ □□□ □□□ □ □□ □□□□□. □□□□ □□□ □□ □□□□ □□□ □□ □□□, □□ □□
□□□□□ □□□.
□□□□ □□□□ □□□□□ □□□ □□□ □□ □□(□)□ □□□ □□□. □□ □□, □□□ □□□ □□
my_macro□□ □□□□ □□ □□, □□ □□□ □□□□ □□□□ □□ □□□□ □□□ □ □□□□.
| my_macro(□□) | ...
□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□ SPL □□□ □□□□□. □□ □□, □□□ □□□ □□
□ □□ □□:
[my_macro(argument)] □□ sourcetype=\$argument\$
□□□ □□□□ □□□ □□□□□.
index=main | my_macro(□) | □□□□ □□ □□
□□□ □□ □□□□ □□□□ □□ SPL □□□ □□□□□.
index=main | search sourcetype=web | □□□□ □□ □
□□□□:
□□□□ □□ □□□ □□

NEW QUESTION: 41

□□ eval □□□ □□□ 503□ □□ description□ □□ □□□□□? index=main | eval
□□=□□□(□□==200, "□□", □□==404, "□□ □ □□", □□==500, "□□ □□ □□")
A. □□ □□□ □□ □□□□.
B. □□ □□□□ □ 0□ □□□□□.
C. □□ □□□□ "□□ □□ □□" □□ □□□□□.
D. □ □□□ □□□□□ □□□ Splunk□□ □□□ □□□□□□.

Answer: ([SHOW ANSWER](#))

<https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/□□□ □□>

NEW QUESTION: 42

□□ □ □□□□ □□ □ □□□□ □□□ □□□□□?(□□□□ □□ □□□ □□□□□.)
A. □□□
B. □□□□□
C. □□
D. □□□□□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

□□ eval □□ □□ □ □□□ □□ □□□□□?
A. □□□□□()

- B.** $\square\square()$
C. $\square\square()$
D. $\square\square()$

Answer: A (LEAVE A REPLY)

NEW QUESTION: 44

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

- A.** GET
- B.** □□
- C.** □□
- D.** □□□□

Answer: A (LEAVE A REPLY)

11

[illegible]

NEW QUESTION: 45

□□ □□□□ □□□ □□□ □ □□ □□□ □□□□□?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 46

Which of the following is the correct Splunk query to join the email and employeeNumber fields from the acme table?

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrangers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

Which of the following is the correct Splunk query to join the email and employeeNumber fields from the acme table?

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

Which of the following is the correct Splunk query to join the email and employeeNumber fields from the acme table?

- A. email
- B. employeeNumber
- C. email
- D. employeeNumber

Answer: C (LEAVE A REPLY)

Which of the following is the correct Splunk query to join the email and employeeNumber fields from the acme table?

Splunk - Search

SPLK-1002 is a collection of Splunk questions and answers. DumpTop is a website that provides Splunk questions and answers. **SPLK-1002** is a collection of Splunk questions and answers. DumpTop is a website that provides Splunk questions and answers. <https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 47

Which of the following is the correct Splunk query to join the email and employeeNumber fields from the acme table?

B. ☐

Answer: A (LEAVE A REPLY)

NEW QUESTION: 48

```
eval 503 description index=main | eval
description=case(status==200, "", status==404, "", status==500, "")
```

A. □□ □□□ □□ □□□□.

B. 0 .

C. □□ □□□□ "□□ □□ □□" □□ □□□□□□.

D. □ □□□ □□□□□ □□□ Splunk□□ □□□ □□□□□□.

Answer: ([SHOW ANSWER](#))

11

<https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/>□□□ □□

NEW QUESTION: 49

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ |join ☐ ☐ ☐ ☐ ☐ ☐ . ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ .
☐ ☐ ☐ ☐ ☐ ☐

email	employeeNumber
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

□□□□ □□□□ □ □□□ SPL □□ □□□ □□□□. | join employeeNumber type=outer □ □□□□□ □ □
□ □□ □□□□□?

A. ☐ ☐

B. □□

C. ☐ ☐

D. ☐ ☐

Answer: C (LEAVE A REPLY)

□ □ □ □ :

Splunk ☐☐☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐.

□□ □□ □□□ □□ □□□ □ □ □□□?

A. ☐☐ ☐☐☐ ☐☐ ☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐

C. □ □□ □□□ □□ □□

□□ eval □□ □□ □ □□□ □□ □□□□□?

B. $\square\square\square()$

D. toString()

[https://docs.splunk.com/Documentation/Splunk/8.0/Getting started/Getting started](https://docs.splunk.com/Documentation/Splunk/8.0/Getting%20started/Getting%20started)

[illegible]

C. XML

Answer: A (LEAVE A REPLY)

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Extractfieldsfromfileswithstructureddata>

□□ □□□□ □□ □□ □□□□ 2□ □□□ □□□□□?

B. □□

C. 100

D. 100 100

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

100/100: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/CreateworkflowactionsinSplunkWeb>

NEW QUESTION: 54

Which of the following is a valid Splunk workflow action?

A. Add field: field, type, value.

B. Add field: field, type, value, action.

C. Add field: field, type, value, action, eventtype.

D. Add, field, type, value, action.

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

Which of the following is a valid Splunk workflow action?

1. Add field, sourcetype=access_combined, status=200, action=purchase

successful_purchase

2. Add field, sourcetype=access_combined, status=200, action=purchase, eventtype=successful_purchase

3. Add field, sourcetype=access_combined, status=200, action=purchase, eventtype=successful_purchase, info, warn, error

4. Add field, sourcetype=access_combined, status=200, action=purchase, eventtype=successful_purchase, info, warn, error, source type

5. Add field, sourcetype=access_combined, status=200, action=purchase, eventtype=successful_purchase, info, warn, error, source type, Splunk

6. Add field, sourcetype=access_combined, status=200, action=purchase, eventtype=successful_purchase, info, warn, error, source type, Splunk, action

NEW QUESTION: 55

Which of the following is a valid Splunk workflow action?

A. Add field: field, type, value, action.

B. Add field: field, type, value, action, eventtype.

C. Add field: field, type, value, action, eventtype, info, warn, error.

D. Add field: field, type, value, action, eventtype, info, warn, error, source type, Splunk.

Answer: (SHOW ANSWER)

NEW QUESTION: 56

Which of the following is a valid Splunk workflow action?

A. Add

B. Add field

C. Add field, type, value

D. Add field, type, value, action

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

100:

<https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields>

NEW QUESTION: 57

Which of the following is a valid Splunk workflow action? (Choose two)

- A. 1
- B. 222
- C. 22
- D. 2

Answer: B,C,D (LEAVE A REPLY)

11: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep> 11 111(FX)1
11 11 11 11 1111 1111 11111 111 1111 1 111 11 11111. 11 111 1
111 111 1111 11 11 111111. FX1 111(1), 11(), 11(,), 1111(;)
11 11 1111 11 111 11111. FX1 1(\t)1 11 111 1111 111 1 111, FX 11111
11 1111 111 1 1111.

NEW QUESTION: 58

11 1 111 111 111 111 1111 11 11 11111?

- A. 11 1111 1111 11 1111 11 111 11111.
- B. 11 1111 1 111 11 111 11111.
- C. 11 1111 1111 1111 11 1111 11 111 11111.
- D. 111 11 1111 11 111 11111.

Answer: C (LEAVE A REPLY)

111 111 11 111 11 111 11 11111.
11: "111 1111 111 1111 11111, 11 > 111 11 > 1 111 111 1111 111 1
11 111 1 1111." 11 1111 111 111 1111 11 111 11 111 11111. 111
11 C1 11111.

NEW QUESTION: 59

11 1 11 111(FX)1 1111 1111 11 11111?

- A. 11 1111 11 1 11 111 1111 11111.
- B. 11 1111 PERL1 1111 11 11111 111 11111.
- C. 11 1111 1111 111 111 11 111 11111.
- D. 11 1111 1111 111 111 1111 111 1 111 11 1111 111.

Answer: C (LEAVE A REPLY)

11

NEW QUESTION: 60

111 111 111 111 1, 1111 1111 11111 111 11 111 111 1111 111?

oidemo

Downloaded from <http://ajph.org/> on November 10, 2014

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$
| stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

- Answer: B (LEAVE A REPLY)**

<https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

□□ □ POST □□□□ □□□ □□□□ □□ □□□□□□?

- Answer: B (LEAVE A REPLY)**

□□□□ □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□□□. □□□
□ □□□ HTML □□□ □□□□□, HTTP POST □□□ □□□□□, □□ □□ □□□□ □□ □□□ □□□ □
□□□□.

* GET 0000 000 00 00 00 Google 000 000000 00 WHOIS 00000000 00 000 0
0 0000 00000 00 0000 00000 00 00000 HTML 000 000000.

* POST 0000 000 000 URI 00 HTTP POST 000 000000. 0 00 000 00000 00 00
0 0000 00000 00 00 00 00000 0000 00000 00 0000 0000 0 00000.

```
* 00 0000 000 0000 00 00 00 0000 20 000 00000. 00 00, 00 00 00 0
0 000000 ipaddress0 http status 00 00 00 0000 000000 00 0000 0000.
```

□□□ POST □□□□ □□□ □□□□ □□ B□□□. HTTP □□ □□□□ □□ □□ □□□□ □□ □□□□ □□ □□□□□□. □ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□□□ URI□ HTTP POST □□ □□□□ □□□.

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

* A. □□□□□ □□ □□□ □□ □□□□ □□ IP □□□ □□□□□. □ □□□□ GET □□□□ □□□ □□ □□ □□□ □□ □□□□□ □□□□ □□ IP □□ □□□□ □□ □□□ □□□□.

* C. □□□ □□□□ □□ □□□ □□ □□ □□□□ □□ Splunk □□ □□: □ □□□□ □□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□□ □□□□ □□ Splunk □□□ □□□□□.

* D. □ □□□□□ □□ HTTP □□ □□□ □□□□. □ □□□□□ GET □□□□ □□□ □□□□ HTTP □□ □□□ □□□ □□□□ □ □□□□ □□ □□□ □□□□.

□□□□:

* Splaxicon:□□□□ □□

* Splunk Web□ □□□□ □□□ □□□

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □ □ **SPLK-1002** □□ □□□ □□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□ □□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 62

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

A. □□ □□□ □□□ □□□□ □ □□□□.

B. □□□ □□□ □□□□□□ □□□ □□□□ accelerate_datamodelcapability□ □□□□□.

C. □□ □□□□ □□□□ □ □□□□.

D. □□ □□□ □□□ □□□ □ □□□□.

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

NEW QUESTION: 63

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

A. □□□ □□□ □□□□□□ □□□ □□□□ accelerate_dacamodel □□□ □□□ □□□.

B. □□ □□□ □□□ □□□ □ □□□□.

C. □□ □□□ □□□ □□□□ □ □□□□.

D. □□ □□□□ □□□□ □ □□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 64

□□ □ □□ □□□ □□□ □□□ □□□□ □□□?

A. □□ □□ □□: □□, □□, □□.

B. □□□ □□□□ □□ □□□□ □□ □□□□□.

C. □□ □□□□ □□□□ □□□□ □□□□ □□□□□.

D. $\square\square, \square\square\square \square\square \square\square\square\square\square.$

Answer: C (LEAVE A REPLY)

22

☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

□.□□ □□, sourcetype=access_combined, status=200, action=purchase□ □□□□ □□

successful_purchase□□ □□□ □□□ □□ □ □□□□.□□ □□ eventtype=successful_purchase□ □□□

[illegible]

□□□.Splunk □□□1□□ □□□ □□□ □□ □□□ □□□ □ □□□□.□□ □□□ □□□ □□□ □□□□

□□□□ □□□□ □□□□ □□□□.□□ □□ □□□ info, warn □□ error□ □□ □□□□ □□□□ □□□

☐ ☐☐☐☐☐.☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐☐ source type☐☐☐.

□□, □□□ □□ □□□ Splunk□ □□□□ □□□ □ □□ □□□ □□□□□ □□□ □□□ □□□□.

NEW QUESTION: 65

Splunk □ □ □ □ □ □ □ □ □ □ □ □ , □ □ □ □ □ □ □ □ □ □ .

A. ☐☐

B. ☐

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

NEW QUESTION: 66

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

A. "□□ □□ □□□ □□ □□ □□□□" □□□□ □□□□□.

B. "□□ □□□ □□□ □□□ □□□ □□ □□ □□" □□□□ □□□□□.

C. □□ □□□ □□□□ □□ □□ □□□ □□□□□.

D. □□ □□ □□□□□ □□□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

□□ □□□ □□□ □□ □□□ □□□□□ □□ □□□□ □□□ □□□□□ "□□ □□□ □□ □□□ □□□

□□ □□ □□" □□□ □□□□ □□□. □□□ □□ □□ □□□□ □□ □□□ □□□□□.

□ □ :

Splunk Docs - ☐ ☐ ☐ ☐ ☐ ☐

NEW QUESTION: 67

[illegible]

□?

A. ☐ ☐

B. ☐ ☐

C. ☐ ☐

D. ☐ ☐

Answer: D (LEAVE A REPLY)

NEW QUESTION: 71

Which of the following is a valid command to display the configuration of the interface? (Choose two)

- A. show interface
- B. show ip interface
- C. show ip interface brief
- D. show ip interface configuration

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Which of the following is a valid command to display the configuration of the interface? (Choose two)

- A. show interface
- B. show ip interface
- C. show ip interface brief
- D. show ip interface configuration

Answer: A (LEAVE A REPLY)

NEW QUESTION: 73

Which of the following is a valid command to display the configuration of the interface? (Choose two)

- A. show interface
- B. show ip interface
- C. show ip interface brief
- D. show ip interface configuration

Answer: C (LEAVE A REPLY)

Which of the following is a valid command to display the configuration of the interface? (Choose two)

2. show ip interface

3. show ip interface brief

4. show ip interface configuration

NEW QUESTION: 74

Which of the following is a valid command to display the configuration of the interface? (Choose two)

- A. show interface
- B. show ip interface
- C. show ip interface brief
- D. show ip interface configuration

Answer: (SHOW ANSWER)

Which of the following is a valid command to display the configuration of the interface? (Choose two)

(Choose two)

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

NEW QUESTION: 75

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

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

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

NEW QUESTION: 76

□□ □ □□ □□□ □□ □□□□ □□ □□ □□□□□?

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

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

□□: <https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usesearchcommand> □□ □□□
□□□□□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□□□ □□□□□ □ □□□□□.2. □□ □□□
□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □
□□□ □□□ □ □□□□.2. □□□ □□ D□ □□□ □□, □□ A, B, C□ □□ □□□ □□ □□ □□□□ □□
□□ □□□□.

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
□ **SPLK-1002** □□ □□□ □□□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 77

□□□□ □□□□ □□□□ □□ □□□□ □□□ □□□?

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

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

□□:

□□□ □□ □□□□ □□□ □□□ □ □□□□.

my_macro(□)

□□□ □□ □□□□ □□□□ □□ SPL □□□ □□□□□.

□□ sourcetype=web

□□□□ □□□□ □□□ □□□ □□□□□, □□□ □□□, □□□□ □□□, □□□□ □□□ □ □□□ □□ □ □□□□.

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

* A. □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□. □□□ □□□ □□ □□ □□□ □□□□ □ □□□ □□□□□. □□□ □□□ □□□□ □□□□ □□□ □ □□□□□, □□□ □□□□□, □□ □□ □□□ □ □□□□.

* B. □□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□□. □□ □□□ □□□ □□□□ □□□ □ □□□ □□□□ □□ □□□ □□□ □□□□□ □ □□□ □ □□□□. □□, □□□□□ □□□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□ □ □□□□.

* D. □□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□ □ □□ □□ □□□□ □. □□□ □□□□□ □□, □□ □□ □□ □□ □□□ □□□□□□ □□□ □□□ □□□ □ □□□ □□ □□ □□□□□ □□□ □ □□□ □ □□□□.

□□□□:

* □□□ □□□ □□□

* □□ □□□ □□□

* □□□ □□□

* □□□□ □□ □□□ □□

* □□□□ □□ □□□□ □□□□□

NEW QUESTION: 81

□□ □□□(FX)□ □□ □□□ □□□ □□ □□□□ □□□? (□□□□ □□ □□ □□)

A. □□, □□ □□ □□□ □□□ □□□□ □□□□□.

B. CSV(□□□ □□□ □) □□□ □□□□□□□.

C. □□□ □□□□ □□ □□ □□□ □□ □□□□ □□.

D. □□□ □□□□ □□.

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

□□ □□□(FX)□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□ □□ □□□ □ □□□□ □□□. □□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □ □□□, □□ □□□□ □□□ □□□□ □□□□ □□ □□□□ □□□□ □□ □□□□□ □□□ □□□□□.

□□

□□ □□□□ □□□□ □□ □□ □□ - Splunk □□ □ □□ □□□: □□□ □□ □□ - Splunk □□□ □□□ □□.

NEW QUESTION: 82

□□ □ □□ □□□, □□ □□□ □□□□ □□□□□?

- A. stats ☐☐☐ transaction ☐☐☐☐ ☐☐ ☐☐☐☐.
- B. transaction ☐☐☐ stats ☐☐☐☐ ☐☐ ☐☐☐☐.
- C. ☐☐ ☐☐☐ ☐☐ ☐ transaction ☐☐☐ ☐☐☐.
- D. ☐ ☐ ☐☐☐ ☐☐☐ ☐☐☐☐ stats ☐☐☐ ☐☐☐.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 83

☐☐ ☐☐☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐.

- A. ☐
- B. ☐☐

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

NEW QUESTION: 84

☐☐ ☐☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐☐? (☐☐☐☐ ☐☐ ☐☐ ☐☐)

- A. GET
- B. ☐☐
- C. ☐☐
- D. ☐☐

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

NEW QUESTION: 85

☐☐ ☐☐ ☐☐ ☐ src ☐☐ host ☐☐☐☐ ☐☐ ☐☐ host ☐☐ ☐☐ ☐☐ ☐☐☐☐?

- A. | ☐☐ ☐☐ = if (isnull(☐☐), ☐☐, ☐☐)
- B. | ☐☐ ☐☐ = if (☐☐ ☐☐, ☐☐, ☐☐☐ ☐☐)
- C. | ☐☐ ☐☐ = if (☐☐ = ☐☐, ☐☐, ☐☐)
- D. | ☐☐ ☐☐ = if (isnotnull(☐☐), ☐☐, ☐☐)

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

eval ☐☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐ Splunk ☐☐☐☐.

if ☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐☐. if ☐☐☐ ☐☐☐

if(X,Y,Z)☐☐☐. ☐☐☐ X ☐☐ ☐☐, Y ☐☐ X ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐☐.

isnotnull ☐☐☐ ☐☐☐ null ☐☐☐ true ☐☐☐☐☐☐, ☐☐☐ ☐☐☐ false ☐☐☐☐☐☐.

isnotnull ☐☐☐ ☐☐☐ isnotnull(X)☐☐, ☐☐☐ X ☐☐ ☐☐☐☐.

☐☐☐ if (isnotnull (src), src, host) ☐☐☐☐ src ☐☐☐ null ☐☐☐ src ☐☐ ☐☐☐☐, ☐☐☐ host ☐☐☐☐☐☐.

☐☐☐☐. ☐☐☐☐ src ☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐☐, ☐☐☐☐ host ☐☐☐☐☐☐.

NEW QUESTION: 86

☐☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐☐☐☐☐.

eval ☐☐☐☐ sort ☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐☐☐☐.

- A. eval☐☐ sort ☐☐ ☐☐ ☐☐ ☐☐☐☐☐☐.
- B. ☐☐ eval ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.
- C. ☐☐ ☐☐☐ ☐☐, eval ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

D. □□ □□□□ sort □□□ eval □□□ □□ □□□ □ □□□□.

Answer: ([SHOW ANSWER](#))

eval □□□ □□□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□ □ □□□□□.2. sort □□□ □□ □□
 □ □□□ □□□□ □□□ □□□□ □□ □□□□□□ □□□□ □ □□□□□.2. □□ □□ □□ □□□□ □□
 □□ □□ □□ □□□□ □□□□□ □□ sort □□□ □□□ □□ eval □□□ □□□□ □□ □□□□ □□□□
 □□□.2. □□□ □□ sort □□□ □□□ □□□ □□ □□ □□ □□ □□ □□□□ □□□□, □□□ □□□ □
 □ □□□ □□□□ □□ □ □□□□. □□□□ □□ C□ □□□ □□ □□ A, B, D□ □□□□ □□□□.

NEW QUESTION: 87

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

- A.** □□□□ □□□ □□
- B.** □□ □ □□□□ □□□ URI□□□.
- C.** □□ □ □□□ □□ □□□ □□□□ □□□□□□.
- D.** □□ □ □□□□ □□□ URI□ □□□□□.

Answer: A,B,C (LEAVE A REPLY)

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction> GET □□□□
 □□□ □□□□ □ □□□ □□□ □□□ □□□□. □□□□ □□ □□, □□ □ □□□□ □□□ URI, □□ □
 □□□ □□ □□□ □□□ □□□. GET □□□□ □□□ □□ □□□□ □□ □□ □□□□ GET □□□ □□□
 □ □□□□ □□ □□□□□. GET □□□□ □□□ □□□ □□ □□□ □□□□ □□□ □ □□□□.

□□□□ □□ □□: Splunk □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□□□. □□□□ □□□ □□□ □
□□□□ □□ □□ □□□□ □□□□ □□□□ □□□□.

11

URI: GET / HTTP/1.1
Host: 192.168.1.100:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0

`http://example.com/ip=$ip IP [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]`

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

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

□□□ □□ A, B, C□ □□□□.

NEW QUESTION: 88

eval 1 2 3 4 5 6 7 8 9 10?

- A.** □□ ()
B. □□ ()
C. □□ ()
D. □□□□ ()

Answer: D (LEAVE A REPLY)

eval [] [] [] [] [] [] [] [] [] [] [] [] [] [].

□□, □□, □□□ □□ □□ □□□□□. 2. eval □□ □□ □ □□□ □□□ □□□□.

toString() is a method of the Object class. It is used to convert the object into a string. The correct answer is A. B. C. D. eval is a function that evaluates the expression and returns the result.

NEW QUESTION: 89

- Which of the following is a valid Splunk search command? (Choose two.)
- A. search Pivot field
 - B. search field
 - C. search Pivot field
 - D. search field

Answer: (SHOW ANSWER)

Splunk search commands are used to search for data in the Splunk index. The correct answers are A and C. B and D are not valid search commands. A search command is used to search for data in the Splunk index. The correct answer is A. B. C. D. eval is a function that evaluates the expression and returns the result.

A: search Pivot field

B: search field

C: search Pivot field

D: search field

Splunk search commands are used to search for data in the Splunk index. The correct answers are A and C. B and D are not valid search commands. A search command is used to search for data in the Splunk index. The correct answer is A. B. C. D. eval is a function that evaluates the expression and returns the result.

NEW QUESTION: 90

- Which of the following is a valid Splunk search command? (Choose two.)
- A. search field
 - B. search field

D. ☐ ☐ ☐

NEW QUESTION: 91

A. NOT, $\square\square$, OR, AND

C. $\square\square$, NOT, AND, OR

Answer: C (LEAVE A REPLY)

* □□ : □□ □□ □□□ □□ □□□□□.

* AND: AND ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

☐ ☐☐☐ ☐☐ ☐☐ ☐☐ ☐, ☐ ☐☐☐ ☐☐ (NOT), ☐☐☐ (AND), ☐☐☐☐ ☐☐ (OR) ☐
☐☐☐ ☐☐ ☐☐☐.

* Splunk Docs - where ☐☐

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

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

B. ☐☐☐ ☐☐☐ ☐☐

D. □□□, □□□□ □ □□ □□□ □□□ □□ □□

□□□ □□ □□□ □□□ □□ □□□ □□□ □□□ □□□□ . □, □□-□□ □□□ □□□□.

□□ □□: □□□, □□, □□.

[https://docs.splunk.com/Splexicon:](https://docs.splunk.com/Splexicon)

NEW QUESTION: 93

□□ □□□(FX)□ □□□□ □□ □□□(regex) □□ □□□ □□□ □ □□ □□ □□□□□?
require □□□ □□ □□□□□?

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

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

□□ □□□(FX)□ □□□□ □□ □□□(regex)□ □□□□ □□□□□ □□□ □□□ □ □□□□.
□□□ □□□□□□ □□□□□ regex2□ □□□□ □□□□ FX□ □□□□ □□□ □□□ □□□ □
□□□ □□ require □□□ □□□□ □□□□ □□□□ □□ □□□□ □□□ □ □□□□.
□□□ □□□2. □□□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□□□ □□□ □□ □ □□□□.
□□□ □□□ □□□□ □□ 2. □□□ □□ D□ □□ □□ A, B □ C□ □□□□.
□□□□□.

NEW QUESTION: 94

timechart□ □□□ □ by □ □□ □ □□ □□□ □□□ □ □□□?

- A. timechart□ by □□ □□□□ □□ □□□□ □□ □□□□□.
- B. _time□ □□ x□□□ □□□□ □□ □□□□□.
- C. □ □□□ x□□ □□□□ □□ □□□ y□□ □□□□ □□□□□.
- D. □□□□□ □□□ □□□ □□□□□.

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

timechart □□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □ □□□□□. timechart □□□ by □□
□□□□ □□□ □□ □□□ □□□ □□□□ chart2□ □□ □□ □□□□ □□ □ □□□□. □□□ timechart
□□□ □□□ □□ by □ □□ □□□ □□□ □□□ □ □□□□. chart2□ x□□□ _time□ □□ □□□□ □□
□□□□□. □□□ □□ B□ □□ □□ A, C, D□ □□□□.

NEW QUESTION: 95

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

□□ □□□ □□ □□□ □□ □□□ _____ .-----□□□□□ □□□ □□□□□.

- A. □□□□□ □□□ □□□□□ □□□□ □□□ □
- B. □□ □□ □□□ □□□□ □□□□□ □□□ □□□ □

Answer: ([SHOW ANSWER](#))

`timechart` □□□ □□□ □□ □□ □□□□ □□□□ □□□□□□.

- Answer: A (LEAVE A REPLY)**

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

- Answer: D (LEAVE A REPLY)**

██████, Bing████. Splunk Core Power User Technologies █████ █████ ██████████.
████ D████. █████ █████ █████ █████ ████████████████████.
████ █████ ████████.

* □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□□ □□ □□ □□□□
□.1 □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□ □ □□□□.12

* □□□ □□□□ □□ □□□□ □□□ □□□, □□□ □□ □ □□□□ □□□ □ □□□□.3. □□□ □□□□
□□□□ □□□ □ □□□, □□□ □□□ □□ □□□ □□□□□.34. □□□

* □□□□ □□ □□□□ □□□□ □□□□□ □□□ □ □□□□.

* □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□
□ □□ □□□ □□□□□ □□□□.14 □, □□□ □□□ □□ □□□ □□□□ □□□□ □ □□ □□, □□□
□□□□ □□ □□ □□ □ □□□ □□ □□□ □□□□□.14

□□ □ GET □□□□ □□□ □□□□ □□ □□□□□?

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

[illegible]

Splunk 的 搜索 语言 支持 正则 表达式 的 使用。GET 请求 的 格式 为：
搜索 语言 的 格式 为：
URL 的 格式 为：
。

NEW QUESTION: 100

在 Splunk 中，web_errors 事件 的 搜索 语言 为：

- A. tag=web_errors
- B. eventtype=web_errors
- C. eventtype "web_errors"
- D. eventtype(web_errors)

Answer: (SHOW ANSWER)

在 Splunk 中，B. eventtype=web_errors 是正确的。

在 Splunk 中，搜索语言 的 格式 为：
URL 的 格式 为：
。

在 Splunk 中，搜索语言 的 格式 为：
。

在 Splunk 中，搜索语言 的 格式 为：

在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

在 Splunk 中，搜索语言 的 格式 为：

在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

A) tag=web_errors: 在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

C) eventtype "web_errors": 在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

D) eventtype(web_errors): 在 Splunk 中，搜索语言 的 格式 为 web_errors 的 搜索 语言 为：

在 Splunk 中：

在 Splunk 中：

在 Splunk 中：

在 Splunk 中：

NEW QUESTION: 101

transaction 命令 的 搜索 语言 为，maxspan 命令 的 搜索 语言 为？

- A. transaction 命令 的 搜索 语言 为，maxspan 命令 的 搜索 语言 为。
- B. transaction 命令 的 搜索 语言 为，maxspan 命令 的 搜索 语言 为。
- C. transaction 命令 的 搜索 语言 为，maxspan 命令 的 搜索 语言 为。

C. □□□ □□□ □□ □□□ □□□□□.

D. `□□□ JSESSIONID□ □□ □□□□ □□ □□□□ □□□□□□.`

Answer: ([SHOW ANSWER](#))

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
 □ **SPLK-1002** □□ □□□ □□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
 □□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount:

KrDump)

NEW QUESTION: 107

□□ □□ □ □□ □□□ Privileged□ □□□ □□□□ □□□□ □□ □□□□□?

A. $\square\square = \text{Pri}^*$

B. $\square\square = \text{Priv}^*$

C. $\square\square = \square\square \square\square$

D. $\square\square = \square\square$

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 108

□ □ □ □ □ □ □ □ □ □ □ □ ?

A. ☐☐☐ ☐☐ Splunk ☐☐☐☐☐☐ ☐☐☐☐.

B. □□ □□□ □□□□ □□□ □□□ □.

C. □□□ □□□□ □□/□□ □□ □□□□ □□ □□.

D. □□□□ □□□□□ □ □□□ 1000□□ □□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 109

☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐

☐☐☐?

A. $\square\square\square\square\square\square=\square \mid \square\square\square \mid \square\square\square^*$

B. | | *

C. | | *

D. | | *

Answer: (SHOW ANSWER)

NEW QUESTION: 110

scats transaction

A. □□ □□ □□□□ □□□□□ □ □.

B. □□ □□□□ □□□ □□□□ □□ □□.

C. □□□ 1000□□ □□ □□□□ □□ □□.

[illegible]

Answer: D (LEAVE A REPLY)

```
transaction 000 00, 00 00 0 00 00 0 00 0000 0000 0000 000000 00
000 0 000000. transaction 000 000000 00 00 000 0000 00 00 00 000000 0
0 0 00 00 000 0000 00 00000. stats 000 00, 00, 00 00 00 0000 00 0000 00
00 0 000000. stats 000 00 0 00 00 0000 0000 0000 0000 0 0000, 00 00 0
0 000 000000 0000 0 00000. 0000 00 0 00 00 000 0000 0000 000000 0
0 00000 stats 00 00 transaction 000 00000 0000.
```

NEW QUESTION: 111

□□□ □□□□ □□□ □□□ □□□ □□□ □ □□□?

A. □□□□ □□□ □□□ .tsidx □□□ □□□□ □□□ □ □□□□.

B. □□□□ □□□ □□□ □□ □□□□ □□□ □ □□□□.

C. □□□ □□□ □□□ □□□□□ □□ □□□ □□□□ □□□.

D. □□□ □ □□□□. □ □□□ □□□ □□□□ □□□.

Answer: ([SHOW ANSWER](#))

□□ □□ □□□ □□□ □□□ □ □□□, □□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□□ □□□
(□□ C). □□ □□□□□□ □□□ □□ □□ □ □□□ □□□□, □□□ □□□ □□□ □□□□ □□ □□□
□□□□ □□□□□□ □□□ □ □□ □□□□□.

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

NEW QUESTION: 112

□□ □□□□ □□ □□ □□□□ 2□ □□□ □□□□□?

A. ☐ ☐

B. □□

C. ☐ ☐

D. □□ □□

Answer: C (LEAVE A REPLY)

11

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

NEW QUESTION: 113

timechart □□□ □□ □□ □□ □ □□ □□ □□□□?

A. □□□□□□□

B. ☐ ☐

C. ☐ ☐

D. ☐ ☐ ☐

Answer: (SHOW ANSWER)

11

□□□ □□□ □□□□.

□□ □□□ □□□□ □□□□ □□□□ □□□□□.3

timechart

□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

- Answer: ([SHOW ANSWER](#))**

□□ □□□ □□ □□□□ □□□ □□ □□ □□□□ □□ □□□ □□□□□. □□□ □□, □□ □□ □□□ □
□□□ □□□□ □□□□□ □□□ □□□□. □□□ □□ □□□, □□ □□□, □□□□, □□□, □□ □ □□
□ □□□ □□ □ □□□□. □□ □□ □□, □□ □□, □□□ □ □□□ □□□ □□ □ □□□□. □□ □□□
□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □ □□□□ □□ □□□ □□ □□ □□□□□.

□□ □□□(FX)□ □□□ □ □□ □□ □□ □□ □□ □□□□□? (□□□□ □□ □□□ □□□□□)

- Answer: A,B,D (LEAVE A REPLY)**

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep>

□□ □□□□ □□ □□□ 2□ □□□ □□□□□?

- Answer: (SHOW ANSWER)**

☐ ☐ ☐ D. ☐ ☐ ☐ ☐ ☐.

□□□□ □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□□□. □□□ □ □□□ HTML □□□ □□□□□, HTTP POST □□□ □□□□□, □□ □□ □□□□ □□ □□□ □□□ □ □□□□.

Splunk Web□ □□□□ □□□ □ □□ □□□□ □□□□ GET, POST, Search2□ □ □□ □□□ □□□□.

* GET □□□□ □□□ □□ □□ □□ Google □□□ □□□□□ □□ WHOIS □□□□□□□□ □□ □□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ HTML □□□ □□□□□.

* POST □□□□ □□□ □□□ URI□ □□ HTTP POST □□□ □□□□□. □ □□ □□□ □□□□ □□ □□ □ □□□ □□□□ □□ □□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□.

* □□ □□□□ □□□ □□□□ □□ □□ □□ □□□□ 2□ □□□ □□□□□. □□ □□, □□ □□ □□ □ □□□□□ ipaddress□ http_status □□ □□ □□ □□□ □□□□□ □□ □□□ □□□□.

□□□ 2□ □□□ □□□□ □□□□ □□ □□□ □□□□□.

□□□□:

* Splxicon:□□□□ □□

* Splunk Web□ □□□□ □□□ □□□

NEW QUESTION: 117

□□□□ □□□ Splunk □□□□ □□□□ □□□□□ □ □□□ □ □□ □□ □□□□ □□□ □□□□□? □□/

A. □□

B. □□

C. □□□ □□

D. □□

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

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Search/Abouttransactions>

□□ □□□□ □□ □ □□□□□ □□□□ stats □□□ □□□□ □□ □□□□□ □ □□□□.

□□ □□□□□ □□□□ □□ ID□ □□ □□□ □□□, □□□ □□□ □ □□□□.

NEW QUESTION: 118

□□ □□□ □□□□□ □□ □□ □:

□□ □□□□□.

A. □□ □□□ □□□ □ □□□□.

B. □□□□ □□□□ □□□ □□□ □ □□□□.

C. □□□□□ □□□ □□□□ □□ □□ □□□ □ □□□□.

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

NEW QUESTION: 119

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

A. □□, □□

B. □□, □□

C. □□, □□

`□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ . □ □ □ □ □ □ □ □ □ □ □ □ maxspan=ld`

`□ □ □ □ □ □ □ □ .`

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
 □ **SPLK-1002** □□ □□□ □□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
 □□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 122

☐☐ ☐ ☐☐ ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐

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

Answer: C (LEAVE A REPLY)

[illegible]

NEW QUESTION: 123

□□ □□ □, □□ □□□ □□□□ □□□ □□ □□□□□?

- A. □□ □□□ □□ □□ □ transaction □□□ □□□□□.
- B. scats □□□ transaction □□□□ □□□ □□□□□□.
- C. □ □ □□□ □□□ □□□□ □□□□□□ scats □□□ □□□□□.
- D. transaction □□□ stats □□□□ □□□ □□□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 124

☐☐☐ ☐☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐☐☐

- A.** \$arg\$
- B.** '□□'
- C.** %□□%
- D.** "□□"

Answer: A (LEAVE A REPLY)

```

□□□□ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□□□□(□: arg1 □□
fragment).
□□
```

□□□ □□ □□
□□□□ □□ □□□ □□
□□□□ □□ □□□ □□

NEW QUESTION: 125

□□□□ □□ □□□□ □□□ □□□ □□□□□?

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

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

NEW QUESTION: 126

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

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: Sarg1\$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

- A. □□ □□ □□(□□, €, 79)"
- B. □□ □□ □□(□□, €, .79)
- C. □□_□□ (\$euro,\$€\$,s79\$
- D. □□_□□ (\$euro, \$€\$,S,79\$)

Answer: ([SHOW ANSWER](#))

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros> □□ □□□□□ □□

□□ □□□□ □□□ □□□ macro_name(\$arg1\$, \$arg2\$, □□□ □□□□ □□□□).

...) `$arg1$, $arg2$` `convert_sales`, `$euro$, $€$, .79`.

NEW QUESTION: 127

36. `convert_sales` `$euro$, $€$, .79`.

A. `$euro$, $€$, .79`.

B. `$euro$, $€$, .79`.

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

NEW QUESTION: 128

`convert_sales` `$euro$, $€$, .79`. `1: $euro$, $€$, .79` `2: action=$euro$, $€$, .79`.

A. `$euro$, $€$, .79`.

B. `$euro$, $€$, .79`.

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

NEW QUESTION: 129

`convert_sales` `$euro$, $€$, .79`. `1: $euro$, $€$, .79` `2: action=$euro$, $€$, .79`.

`eval` `sort` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`?

A. `eval` `sort` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`.

B. `$euro$, $€$, .79` `sort` `$euro$, $€$, .79` `eval` `$euro$, $€$, .79` `$euro$, $€$, .79`.

C. `$euro$, $€$, .79` `$euro$, $€$, .79`, `eval` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`.

D. `$euro$, $€$, .79` `eval` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`.

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

NEW QUESTION: 130

`convert_sales` `$euro$, $€$, .79`.

`$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`.

A. `$euro$, $€$, .79`.

B. `$euro$, $€$, .79`.

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

NEW QUESTION: 131

`convert_sales` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79` `$euro$, $€$, .79`?

index=security sourcetype=linux_secure@failed earliest=-60d@d latest=-1d@d
 | transaction src_ip
 | stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip

Events (641) Patterns Statistics (147) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

- A. maxspan □□□ □□□□ □□□□□.
- B. □□□□ □□□ □□□□□ □□ 1000□□ □□□□ □□□□□.
- C. □□□□□ □□□ □□ □□□ □ □□□□.
- D. □□ □□() □□□ □□□□□.

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

□□

□□□ B□□□. □□ □□□ □□□ □□ 1000□□ □□□□ □□□□□.

transaction □□□ □□ □□ □□□□ □□□□ □□□□□□□□ □□ □□□□ □□□□□ □ □□□□□□. □□ □□□ □□ □□□□ □□ □□□ □□ □□ □ □□□, □□ □□□ □□□ □□□□□ □□ □□□□□ □□ □□□□ □ □□□ □ □□□□.

□□□ □□□□ □□□□ □ □□ □□ □□□ □□□, □□ □□□ □□□□□ □□ 1000□□ □□□□ □□□ □ □ □□□ □□□□. □, □□□□ □□□ □□ □□□□ 1000□□ □□□□ □□ □□□□□□ □□□□□. □ □ □□ □□□□□ □□□□□□ □□□□□ □ □□□□.

□□□ □□□ □□□□ transaction □□ □□ stats □□□ □□□ □ □□□□. stats □□□ □□ □□ □□□□ □□□□ □□□□ □□ □□□, □□□ □□□ □□□ □□□ □□□□. □□ stats □□□ transaction □□□□ □□□ □□□ □□□ □□□□ □□□□.

□□□□ stats list() □□□ □□□□ src_ip□ dest_ip□ □□□□ □□□□□ □□□□. □ □□□ □ □□□ □ □ □□□ □□□ □□ □□ □□□□ □□□ □□□ □□□□□. □□□ □ □□□ transaction □□□□ □□ □ □ □□□□ □□□□ □□□□. □□, □□□□ □ □, □□□□ □ □□ □□□ □□ □□□□ □□□□□.

□□□ □□□□□ □□□ □□ 1000□□ □□□ transaction □□□ □□□□, □□ □□ □□□□ □□□□ □□ stats list() □□□ □□□□ □□□ □□ □□□□ □□□ □□ □□ □□□□□ □□□□□.

□□□□:

stats □□ □□

□□□□ □□ □□

Splunk □□□□ □□: □□ □ □□ □□

NEW QUESTION: 132

0000 00 0000 000 000 00000?

- A. 00 000 00000.
- B. 00 0000 00 000 000.
- C. 00 0000 00 000 00000.
- D. 00 00000 000 000 0 00, 00000 000 0 0000.

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

00

000 0 0 000 00 00 000 0000 00 000 000 00000.2. 00 0000 00 00 00
0 0000 000 00 000 000 0 0000.2. 00 000 0000 0000 00 000 00 000
0 000 00 00 000 0 0000.2. 000 00 C0 00000, 00 A, B, D0 00 000 000 00
00 000 0000 000 0000.

NEW QUESTION: 133

00 0 eval 00 tostring 000 00 000 0 00 00 00000? (0000 00 000 00000)

- A. "1600"
- B. "00"
- C. "1000"
- D. "00"

Answer: ([SHOW ANSWER](#))

00: <https://splunkonbigdata.com/2018/10/27/usage-of-splunk-eval-function-tostring/>

NEW QUESTION: 134

00 000 000 000 00 00 000 0000 0000?

- A. 000
- B. 000
- C. 000
- D. 00 000

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

00: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot> 000 SPL 0000 000
0 000 000 000 0000 0000 00000 00 0 00 00000.2 000 0000 000 00
0000 00 0000 00, 000, 00 0 0000 0 0000.2 000 SPL 0000 0000 00 00
0 000 000 0000 0000 00000 0000 00 00000000.2 000 00 A0 00000,
00 B, C, D0 000 0000 0000 000 000 0000 000 0000.

NEW QUESTION: 135

000 000 0000 000 000 00000? (0000 00 000 00000)

- A. 00000 searchtypes 000 00000.

props.conf □□□□ □□□ □ □□□□. □□ □□□ □□□ □□□□□ □□, □□□, □□□□ □ □□□ □□ □□ □□□ □ □□□□.

□□□ □□□ eval □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□ □□□□□□. eval □□□ □ □□□ □□□□ □□□ □□□□□ □□□□ □ □□□□□. eval □□□ □□□ □□ □□ □□, □□□, □□ □□, □□, □□ □ □□ □□□ □□□ □ □□□□.

□□ □□, price□ tax□□ □ □□□ □□□ total□□□ □ □□□ □□□□ □□□ □□ eval □□□ □□□□ □ □□.

| □□ □□=□□+□□

□□□ □ □ □□□ □□ □□, □□□ □□ □□□□□□ □□□□□ □□ eval □□□ □□□□ □□ □□ □□ □ □□ □ □□□□. Splunk Web□□ □□ □□□ □□□□ □□ > □□ > □□ □□□ □□□□ □ □□ □□ (total), sourcetype □□(sales), □□□ □□□(price+tax)□ □□□□ □□□. □□□ □□ total□□□ □□□ □□ □□□ □□□□ □□ □□□ sourcetype□ sales□ □□ □□□□ □□□□□. □□□ eval □□□□ □□□□ □ □□ □□ □□□ □□□□ total □□□ □□□ □ □□□□.

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

* A. □□□□: □ □□□ □□ □□ □□□□ □□□□ □□□□□□□ □□ □□□□ □□□□□ □ □□□□□. □□□□□ □□ □□□□ □□ □□□ □□ □□ □ □□□, □□ □□□ □□□ □□□□□ □□ □□□□□ □ □□□□ □ □□□□ □ □□□□.

* B. lookup: □ □□□ CSV □□□□ □□□□□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □ □□ □□□. lookup□ □□□, □□, □□ □□ □□ □□ □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□ □ □□ □□□ □ □□□□.

* C. stats: □ □□□□ □□ □□□ □□□ □□ □□ □□(count, sum, average □)□ □□□□ □ □□□□□. □ □□□ □□□ □□□□ □□□□□ □□□□ □ □□□ □ □□□□.

□□□□:

* □□□ □□□ □□□

* eval □□ □□

* □□□□ □□ □□

* [□□ □□ □□]

* [□□ □□ □□]

NEW QUESTION: 138

□□□ □□□ □□ □ □□ □□ □□□□ □ □ □□□□?

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

Answer: D (LEAVE A REPLY)

Splunk□□ □□□ □□□ □□□□ □□ □□□ □□ □□□□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□ □ □□□□. □□□ □□ □□□ □□□ □□ □ □□□, □□□ □□□ □□ □ □□□□ □□□ □□□ □ □□ □□ □□□□□ □□□ □□□□□.

Destination app
oidemo

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$
| stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

- A. sessiontracker action, JSESSIONID.
- B. sessiontracker(2) action, JSESSIONID.
- C. sessiontracker \$action\$, \$JSESSIONID\$.
- D. sessiontracker(2) \$action\$, \$JSESSIONID\$.

Answer: (SHOW ANSWER)

: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros action JSESSIONID

(2)

sessiontracker.

sessiontracker. session tracker session tracker.

session tracker(2) session tracker session tracker.

session tracker index=main sourcetype=access_combined_wcookie action=\$action\$ JSESSIONID=

\$JSESSIONID\$ | stats count by JSESSIONID. session tracker session tracker.

. session tracker, session tracker session tracker session tracker.

session tracker.

session tracker JSESSIONID session tracker session tracker.

session tracker session tracker session tracker session tracker, session tracker JSESSIONID session tracker

. session tracker(2) session tracker session tracker.

NEW QUESTION: 143

session tracker session tracker?

A. session tracker session tracker.

B. session tracker session tracker session tracker session tracker.

C. session tracker session tracker session tracker session tracker session tracker.

D. session tracker session tracker session tracker session tracker.

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

NEW QUESTION: 144

| □□□□ □□□□ □□□□ □□□□ □□□ □□□□□? (□□□ A=B)

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

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

□□□ C□□□. □□ A□ □□ □□ B□ □□ □□ □□□□□□.

where □□□ □ □□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□□□ □ □□□□□.

where □□□ □ □□, □ □, □□ □□□ □□ □□□ □ □□□□. where □□□ □□, □□□, □□□□□□ □ □□□ □□□ □□□□ □□ □□ □□□□.

where □□□ □□□ □□□ □□□□.

| □□□ <□□□>

□□□□ □□, □□, □□ □□ □□ □□□ □□□ □ □□□□. □□□□ □ □□□□ □□ □ □□ □□□□ □ □□□□ □□□.

where □□□□ □ □□□ □□□□□ □□□ □□ □□ □□□ □□□□ □□□. □□ □□, □□ A□ □□ □□ B□ □□ □□□□ □□□□ □□□□ □□ □□□ □□□ □ □□□□.

| □□□ A=B

□□□ □□ □ □□□ □□ □□ □□□□ □□□□□.

□□ □□□ where □□□ □□ □□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□. □□□ □□□ □□□ □□□□.

A: □□□ □ where A=B□ □□□□ □□□: □ □□□ □□□ □ where A=B□ □□□□ □□□□□, □□ where □□□ □□□ □□□ □□□□. □ □□□ □□□ □□□□ □□ □□□□ □□□□□.

"□□□ A=B"□□□.

B: □□□ □ A=B□ □□□□ □□□: □ □□□ □□□ □ A=B□ □□□□ □□□□□, □□ where □□□ □□ □ □□ □□□□□. □ □□□ □□□ □ "A=B"□ □□□□ □□□□ □□□□□.

D: □□ A□ □□□ □ B□ □□□ □□□: □ □□□ □ B□ □□□□ □□□□. □□ where □□□□ □□□ □ □□□ □ □□□ □ □□ □□□□□. □□□□ □□□□ □□□□ □□□ □□ □□□ □□ □ □□□□□. □ □ □□ □□ A□ □□□ □ "B"□ □□□ □□□□ □□□□□.

□□□□:

where □□□ □□□

□□ □□ □□□□

NEW QUESTION: 145

Splunk Common Information Model(CIM)□ □□ □□ □□□ □□ □□□ □□□□□ □□ □□ □□□ □□□□ □?

- A. □□ □□.
- B. □□□.

- C. CIM□ □□□ □□□ □□ □□ □□ □□□ □ □□□□.
- D. □□ □□□ □□.

Answer: (SHOW ANSWER)

NEW QUESTION: 146

| □□□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□ □□ □□□ □□□□□?

- A. | vendor_action, user□ □□ □
- B. | vendor_action, user□ □□ □□ □
- C. | □□□□ □□□□ □□□ □□ □
- D. | vendor_action□ □□□ □□ □□ □

Answer: (SHOW ANSWER)

NEW QUESTION: 147

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

□□ □□□□□.

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

Answer: B (LEAVE A REPLY)

□□ □□ □□□□(FX)□ □□□ □□□□□□ □□□□□ □□ □□□□ □□ □□□□ □□□□□ □□□ □□□□ □ □□□ □□ □□□□□.2 FX□□ □□□ □□□ □□□□ □□ □□□□ □□□□ "□□□□ □□" □□ □□□□.2 "□□□□ □□" □□□ □□ □□□ □□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□.2 □□ □□ □□ □□□ □□□□ □□□□ □□□ □ □□□□.2 □□□□ □□ B□ □□□, □□ A, C, D□ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□□.

NEW QUESTION: 148

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

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

Answer: (SHOW ANSWER)

□□:

□□ □□□□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□□.2. □□ □□□ □□□ □□□ □ □□□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□.2. □□ □□ A□ □□□□. □□□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□.2. □□□ □□ C□ □□□□. □□ □ □□□ □□□ □□□□ □□□□ □ □□□ □□□ □ □ □□□□. □, □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□ □□□□ □□□ □ □□□□.2. □□□ □□ D□ □□□□. □□□ □□□□

□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□ □ □□□
□.2. □□□ □□ B□ □□□□□.

NEW QUESTION: 149

- □□ □□□ □□□□ □□□ □□□□□?
- A. □□ □□ □□ □□□□ □□□□ □□□□□□.
- B. □□ □□□ □□□□□.
- C. □ □□□ □□□□ □□□ □□.
- D. □□/□□ □□ □□□□ □□□□ □□□□□□.

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

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

□□/□□ □, □□ □□ □□ □□ □□□ □□ □□□ □□□□□. stats □□□ □□□ □□□ □□ □□□ □□
□□ □ □□□□□.

□□ □□ □□□.

□□□□

Splunk □□□□

Splunk □□□□ - □□□ □□□ □□ □□

NEW QUESTION: 150

- datamodel □□□ □□□ □ □□ □□□ □□□□ □□□?
- A. □□□ □□ □□□ □□ □□.
- B. □□ □□
- C. □□□ □□ □□ □□.
- D. □□ □□□

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

NEW QUESTION: 151

- □□□□ □□□ □□□□□?
- A. macroname □□□ □□□□□.
- B. □□□ □□□ □□□□□.
- C. □□□ □□□ □□ □□(')□ □□□□.
- D. □□□ □□□ □□□□□(')□ □□□□.

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

□□□ C□□□. □□□ □□□ □□ □□(')□ □□□□.

□□□□ SPL □□□ □□ □□□□ □□□□□ □□□□□. □□□□ □□□ □□ □ □□□, □□□ □□□□
□□□ □ □□ □□□ □□□ □ □□ □□□□□. □□□□ □□□ □□ □□□□ □□□ □□ □□□, □□ □□
□□□□□ □□□.

□□□□ □□□□ □□□□□ □□□ □□□ □□ □□(')□ □□□ □□□. □□ □□, □□□ □□□ □□
my_macro□□ □□□□ □□ □□, □□ □□□ □□□□ □□□□ □□ □□□□ □□□ □ □□□□.

... | my_macro(□□) | ...

Splunk SPL 1002. 1002, 1002 1002 1002
 1002 1002:
 [my_macro(argument)] sourcetype=\$argument\$
 1002 1002 1002 1002.
 index=main | my_macro() | 1002 1002 1002
 1002 1002 1002 1002 1002 SPL 1002 1002 1002.
 index=main | search sourcetype=web | 1002 1002 1002
 1002:
 1002 1002 1002 1002

SPLK-1002 1002 1002 1002 1002 DumpTop 1002 1002 1002 SPLK-1002 1002! DumpTop 1002 1002
SPLK-1002 1002 1002 1002 1002, DumpTop SPLK-1002 1002 1002 1002 1002 1002 1002 1002
 1002 1002. 1002 1002 1002 1002 DumpTop SPLK-1002 1002 1002 1002.
<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 152

1002 1002 1002 1002 1002 1002 1002 1002?

- A. 1002 1002
- B. 1002 1002 1002 1002 1002
- C. 1002 1002
- D. 1002 1002

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

1002
 1002 1002 1002 1002 1002 1002() 1002 1002 1002 1002 1002.2 1002 1002 1002 1002
 1002 1002 1002 1002, 1002 1002 1002 1002, 1002 1002 1002 1002 1002 1002 1002 1002
 1002 1002 1002 1002 1002.2 1002 B 1002 1002 1002, A, C, D 1002 1002 1002. 1002 1002
 1002 1002 1002 1002 1002 1002 1002 1002 1002 1002 1002.

NEW QUESTION: 153

1002 1002 1002 1002 1002 1002 1002 1002?

- A. 1002=1002_48 1002 1002=BETA_881 1002=220
- B. index=server_48 sourcetype=BETA_881 code=220 | 1002 1002 1002
- C. index=server_48 sourcetype=BETA_881 code=220 | inputlookup append=t servercode.csv
- D. index=server_48 sourcetype=BETA_881 code=220 | code > 220 1002 1002 1002

Answer: ([SHOW ANSWER](#))

1002 1002 1002 1002 1002 1002 1002 1002, 1002 1002 1002 1002 1002 1002. 1002 1002
 1002 A(index=server_48 sourcetype=BETA_881 code=220) 1002(: stats, inputlookup) 1002 1002 1002
 1002 1002 1002. 1002 1002 stats 1002 lookup 1002 1002 1002 1002 1002 1002.

□□:

Splunk □□ - □□□□ □□

NEW QUESTION: 154

timechart □□□ □□□ □, _time□ □□□ □□□□ □ □□□□ □□□ □□□ □□□□□?

A. □

B. □ □□

C. □□

D. □

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

□□□□□ □□□ □□□ □□

Splunk□ timechart □□□ □□□□ □□□ □□□□ □□□□ □ □□□□□.

span □□□ _time □□□ □□(□□ □ □□)□ □□□□ □ □□□□□.

□□ □:

CSS

□□□□

index=_internal | timechart span=1h count

□ □□□ _time□ 1□□ □□□□ □□□□ □□□□□ □□□□□.

bin□ bin □□□□ □□ □□ □□ □□ □□□□□ □ □□□□□ timechart□□ □□□□□ □□□□.

by□ □□ □□□ □□ □□□ □□□□ □ □□□□□ □□□ □□□□□ □□□□.

over□ timechart□ □□ □□□ □□□ □□□□.

□□: Splunk Docs - timechart □□

NEW QUESTION: 155

1 □□□ □□ Renewal-MonthYear□ □□ □□□□ □□□□ □□ □ □□ □□□ □□□□□?

□□?

A. | □□□ 10yearAnnerversary=□□ □□

B. | □□□ '10yearAnnerversary=□□ □□'

C. | □□□ 10yearAnnerversary='□□ □ □'

D. | □□□ '10yearAnnerversary'='□□ □□'

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

□□□ A. |□□□. □□□ 10yearAnnerversary=Renewal-MonthYear□□□.

where □□□ □ □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□ □ □□□□□.

where □□□ □ □□ □□, □ □□ □ □□ □□□ □□ □□□ □ □□□□. where □□□ □□ □□□ □□□ □ □□□□.

□□, □□□, □□□□□□ □□□□ □□□ □□□□ □□□□.

where □□□ □□□ □□□ □□□□.

| □□□ <□□□>

□□□□ □□, □□, □□ □□ □□ □□□ □□□ □ □□□□.

□□□□ □ □□□□ □□ □ □□ □□□□ □□□□□ □□□.

where □□□ □□□□ □ □□□ □□□□□ □□□ □□ □□ □□□ □□□□ □□□.

□□. □□ □□, 10yearAnniversary □□ □□ □□□□ □□□□ □□□□

Renewal-MonthYear □□□ □□ □□□□□ □□ □□□ □□□ □ □□□□.

| 10yearAnniversary=-

☐☐☐ ☐☐ ☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐☐☐☐

☐☐ ☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

[illegible]| `□□□ '10yearAnniversary'='□□ □ □'`

□□□ □ '10yearAnniversary'□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□.

□□□ □ '□□-□□'.

□ □ □ □ :

where $\square\square\square\square\square\square$

NEW QUESTION: 156

Splunk ☐☐ ☐(☐) ☐☐☐☐ ☐☐☐☐ ☐ ☐☐☐☐☐. (☐☐☐☐ ☐☐ ☐☐☐☐☐.)

A. ☐ ☐ ☐ ☐ ☐

B. ☐ ☐ ☐ ☐ ☐

C. □□□□ □□□□ □□□□.

Answer: A,B (LEAVE A REPLY)

Splunk □□□ □□□ □□ □□□□ □□□ □□ □□□□ □□□ □□□□ □ □ □□□□.3 □□□ □□□□
 □□□□□□ □□ □□□ □□□ □ □□□ □□ □□□□□.3 □□□ □□□ □□□ □□□□ □□□ □□□ □
 □□□□.3 □□ □□ □□□ □□ □□ □□□ □□□ □ □□□□.3 □□ □□□ □□□□□ □□□ □ □□□
 □. □, Splunk3□ □□□□□□ □□□□ □□□□□ □□□□□□□. □□ □□□□ □□□ □□ □□ □□□
 □□□ □ □□□□. □, □□□ □□ □□□ □□ □□□ □□□□ □□□□□.3 □□□ □□ A□ B□ □□□, □
 □ C□ □□ □□□ □□□□ □□□ □□□□ □□□□.

NEW QUESTION: 157

Splunk ☐ ☐ ☐ (CIM) ☐ ☐ ☐ ☐ ?

A. CIM □ □ □ □ □ Splunk □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ .

B. CIM

C. CIM □ Splunk □□ □□□□ □□□ □ □□ □ □□□□ □□□□□.

D. CIM □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ .

Answer: B (LEAVE A REPLY)

Splunk Common Information Model(CIM) □ □□□ □□□□ □□□□□ □□□□ □□□□□.

□□ □ □□ □□.CIM□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□ □ □□ □□□ □□□□□.

[illegible]

□ □ .

NEW QUESTION: 158

□□ □□□□ x□□ □□ □□□□ □□□□□?

☐☐ ☐ ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐☐☐

□□ □□□ □□□□ □□□ □□□□ □□ □□ □□ □□ □□□□□ □□ □□□ □□□□ □□□□.
□□ □□□ □□ □□□ □□ □□□□ □□□□ □□ □ □□ □□ □□ □□□ □□ □□□□□.
□□.
□□□ field1-field2□ □□ □□□ □□□ □□ □ □□□□ □□□ □□□□
□□□□ field1□ □□ □□ □□□□ □□ □□, field2□ □□ field1□ □□□ □□□□□.
□□□□:
□□□ □□□ □□□
□□ □□□ □□□
Splunk Web□□ □□ □□ □□□

NEW QUESTION: 160

eval □□ 'if' □□□□ □□ □ □□ □□□ □□□□□(□□□□).

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

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

eval □□ 'if' □□□□ □□ □ □□ □□□ □□□□□(□□□□): □□ □□□, □□ if
true□□ □□□ false□□□. eval □□□ □ □□□ □□□□ □□□ □ □□ □□ □□□□□.
□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□. eval □□□ □□□
□□□ □□ □□□ □□□ □□□□ □□□□□. 'if' □□□ □□□ □ □□ □□ □ □□□□□.
eval □□□ □□□□ □□□ □□ □□□ □□□ □□□□□. 'if' □□□ □ □□ □□□ □□□□□.
□ □□ □□□□ □□□□ □□ □□□, □□ □□□□ □□ □□ □□□□ □□
□□□ □□ □□□□ □□□□ □□□□ □□□□□. 'if' □□□ □ □□ □ □□□ □□□□□.
□□ □□□□ □□□ □□ □□□□□.

NEW QUESTION: 161

□□ □□ □ □□ □□ □□□ □ □□ □□□□ □□□□□?

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

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

□□□ □□□ □□□□.
* transaction □□□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□□□.
* □□□ □ □□□ □□ □□□(_raw □□), □□ □□ □□□ □□ □ □□ □□, □□□ □ □□□ □□ □□ □
□□ □□□□□ □□□□□.1
* startswith □□□ □□□□ □□□□ □□□□ □□□□ □□□□□ □ □□ □□□□ □□□□ □ □
□□□□.

```
* 00 00, | transaction clientip JSESSIONID startswith="view" clientip JSESSIONID 000 0000 0
0000 0000, 0 000000 0 00 00000 _raw 000 "view"00 0000 000000.2.
```

NEW QUESTION: 162

□□ □□□ □□□ □□□ □ □□□ □□□□□?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 163

□□ □□□(FX)□ □□□□ □□ □□□ □□□ □ □□ □□ □□□ □□□ □ □□□□?

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

Answer: D (LEAVE A REPLY)

[illegible]

□ □ □ □ :

* Splunk ☐: ☐ ☐

* Splunk Answers: ☐ ☐ ☐ ☐

NEW QUESTION: 164

```
raw  time  fields
```

- A. ☐
- B. ☐ ☐

Answer: B (LEAVE A REPLY)

NEW QUESTION: 165

□□□ □□□ □□□ □□□ □, □□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□□ □□□?

oidemo

Name *

Downloaded from <http://ajph.org/> at University of California, San Diego on June 11, 2015

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in curly braces.

```
sourcetype=access_combined action=$action$ JSESSIONID=$JSESSIONID$
| stats values(action) as action by JSESSIONID
```

☐ Use eval-based definition?

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters

--	--

- A.** `sessiontracker` `action`, `JSESSIONID`.
- B.** `sessiontracker(2)` `action`, `JSESSIONID`.
- C.** `sessiontracker` `$action$`, `$JSESSIONID$`.
- D.** `sessiontracker(2)` `$action$`, `$JSESSIONID$`.

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/DefineSearchMacros> □□ □□□ □□□

action□ JSESSIONID□□ □ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□□.

□□□□□(2)

□ □ □ □ □ □ □ □ □ □ □ □ □ □ .

```

000 000 sessiontracker 0 00000. 0 000 00 000000 0000 00000 0 000000.

```

□□□□ □□ □□□ 2□ □□□□□. □□ □□□□ □□□ □ □ □□ □□□ □□□□ □□ □□□□□.

☐ ☐ ☐ ☐ index=main sourcetype=access combined wcookie action=\$action\$ JSESSIONID=

```
$JSESSIONID$ | stats count by JSESSIONID
```

□. □□ □□□□ □□□, □□, □□ □ □□□ □□ □□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□

☐ ☐☐ ☐☐☐ ☐☐ ☐☐☐☐.

☐ ☐ action ☐ JSESSIONID ☐ ☐☐☐ ☐☐ ☐ ☐☐ ☐☐ ☐☐ ☐☐☐.

```
00. 00 0000 sessiontracker(2) 0000 0000 0 0000.
```

dedup ☐☐☐ ☐☐☐☐ .

- A.** □□□□ □□ □□ □□□
- B.** □□ □□□ □□□ □ □□ □□□ □□ □□ □□□ □□□□□.
- C.** □□ □ □□

Answer: C (LEAVE A REPLY)

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

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

- Answer: A,B,C (LEAVE A REPLY)**

<https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels>

□□ □□□□ □□□□□?

- Answer: B (LEAVE A REPLY)**

□□□ B□□□. □□□ □□□ □□ □□ □□□□□.

□□ □□□□ SPL □□□ □□ □□□ □□□ □ □□ □□ □□□□□.

eval

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

□□ □□□□ □□□□ SPL □□□ □ □□ □□□□ □□ □□ □ □□□□.

□□ □□□□ □□ □□□□ □□□□ □□□ □□^[1]□□ □□□ □□ □□()□ □□□ □□□. □:

mymacro`.

`transactioncommand` □ □□ □, `maxspando` □□□ □□□□□?

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

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

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction>

NEW QUESTION: 170

□□ □ POST □□□□ □□□ □□□□ □□ □□□□□?

- A. POST □□□□□ □□□ □□□□□ URI □□□ □□□□ □□ □ □□□□.
- B. □□□□□ POST □□□□ □□□ □□□□ □□ □□□ □□ □□□□□.
- C. POST □□□□ □□□ URI □□□ POST □□□ □□□□ □□□ □ □□□□.
- D. POST □□□□ □□ □□□□ □□ □□ □□□ □□□□□.

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

NEW QUESTION: 171

□□ □□□ _____□□ □□□ □□□□ □ □ □□□□.

- A. □□□ □□
- B. □□
- C. □□□ □

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

NEW QUESTION: 172

□□□ □□ □□ □□ □ □□ □□ □□□□□?

- A. □□□ □□□□□ □□□□ □□□□.
- B. □□□ □□□ □□□ □□□□□.
- C. □□□ □□□□ □□□□ □ □□□□ □□ □□ □ □□□□.
- D. □□□ □□ □□□ □□□□ □□□□□: <fieldname>

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

□□□ Splunk□□ □□ □□ □□ □□ □□ □□□□□. □□□ □□□□□ □□□□ □□ □□ □□□□□□
□□□□ □□□ □□□□ □□□□ □ □□ □□□ □ □□□ □□□. □□ □□, "200"□ □□ □□ □□ "OK" □
□ "success" □□□ □□□□ □□ □□□ □□ HTTP □□ □□□□ □□□ □ □□□□. □□□ □□□□□ □
□□□□ "OK"□ "ok"□ □□ □□ □□□□□. □□□ □□ □ □□□□□ □□□ □□□ □□□ □ □□□□□.
□□□ tag::<tagname> □□□ □□□□ □□□□□. □□□ <tagname>□ □□□ □□□ □□□□□.

NEW QUESTION: 173

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

```
index=main source=mySource oldField=* | `makeMyField(oldField)` | table _time newField
index=main source=mySource oldField=* | stats if(`makeMyField(oldField)`) | table _time
newField
index=main source=mySource oldField=* | eval newField=`makeMyField(oldField)` | table _time
newField
index=main source=mySource oldField=* | `newField`(`makeMyField(oldField)`) | table _time
newField
```

- A. □□ B
- B. □□ D

D. □□ C

NEW QUESTION: 174

A. ☐ ☐ ☐ ☐

C. ☐☐ ☐☐

D. ☐☐☐ ☐☐

□ □ :

NEW QUESTION: 175

| 10yearAnniversary= - | '10yearAnniversary= -

| 10yearAnniversary='--'

| □□□ '10yearAnniversary'='□□ □ □'

Answer:

□□□ 10yearAnniversary=□□-□□.

[illegible]

where $\square\square\square\square\square\square\square\square\square\square$.

| ☐ ☐ ☐ < ☐ ☐ ☐ >

□□□□ □□, □□, □□ □□ □□□ □□□ □ □□□□. □□□□ □ □□□□ □□ □ □□ □□□□ □
□□□□ □□□.

where $\square\square\square\square$ $\square$ $\square\square\square\square$ $\square\square\square\square\square$ $\square\square\square$ $\square\square$ $\square\square\square\square$ $\square\square\square\square$ $\square\square\square$. $\square\square$ $\square\square$, 10yearAnniversary
 $\square\square$ $\square\square$ Renewal-MonthYear $\square\square$ $\square\square$ $\square\square\square\square$ $\square\square\square\square$ $\square\square\square\square$ $\square\square$ $\square\square\square\square$ $\square\square\square\square$.

| □□□ 10yearAnniversary=□□-□□

☐☐☐ ☐☐ ☐ ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐☐

□□ □□□ □□ □□□ □□□□ □□□ where □□□ □□ □□ □□ □□□ □□□ □□□□ □□□ □□□□
 □□□□. □□ □□. □□□ □□□□ □□:

| □□□ '10yearAnniversary'='□□ □ □'

□□ □ □□□□ □□□ URI: □□ □□ □ □□□□ □□ URL□□□.
GET □□□ □□□ □□□□□□□□□□. URI□□ □□□ □□ □ □□□ □□□ □ □□□□.
□□ □□□ □□ □□ □□ □□ □□□□. □□ □□, □□ □ □□ ip□ □□ □□ □□□ □□ □□□ □ □□□
□.
http://example.com/ip=\$ip□ IP □□□ □□□□□ □□ □ □□□□ □□□□□□□□ □□□□□.
□□ □ □□□ □□ □□□ □□□□ □□□: □□□□□ □□ □□□□□.
□□ □□□□ □□ □□ □□□□ □□□ □□ □□□ □□□□ □□□□□.
□□□□ □□□□□ □□□ □□□ □□□ □ □□□ □□□ □□□□ □□□□ □□□□.
□□□ □□ A, B, C□ □□□□□.

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
□ **SPLK-1002** □□ □□□ □□□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
□□□□□. □□□□ □□□ □□□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.
<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 182

□□□ □□□□ □□□ □□□□ □ □□□□ □□□ □□□□□?

- A. "□□"
- B. %□□%
- C. '□□'
- D. \$□□\$

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

□□□ D□□□□.
□□ □□□□ SPL □□□ □□ □□□□ □□□□□ □□□□□. □□ □□□□ □□□ □□ □ □□□, □□□
□□□□ □□□ □ □□ □□□ □□□ □ □□ □□□□□. □□ □□□□ □□□ □ □□ □□ □□□□ □□□
□ □□□, □□ □□ □□□1□□ □□□.
□□□ □□□□ □□□ □□□□□ □□ □□(\$)
□ □□□□ □□ □□□ □□□ □□□ □□□. □□ □□, "object"□□
□□□ □□ □□□ □□ □□ □□□□ □□□□ □□ □□□ □□□ □ □□□□.
[my_macro(□□)] □□ □□ □□ = □□
□□□ □□ object□□ □□ □□□ □□ my_macro□□ □□ □□□□ □□□□□. □□□□ □ □□□□ □□
□ □□ □□□ □□ object □□□ □□ □□□□ □□□.
my_macro(□)
□□□ □□ □□ □□□ web □□□ □□□ □□ SPL □□□ □□□□□.
□□ sourcetype=web
□□ □□□ □□□ □□□□ □ □□□(' □□ ")□ □□□ □□(%)□ □□□□□ □□□□ □□□□. □□ □□□
□□□ □□□ □□□ □□□□. □□□ □□□ □□□ □□ □□□ □□□ □□□□□.
□□□□:
* □□□□ □□ □□□□ □□□□□

NEW QUESTION: 183

□□ □ POST □□□□ □□□ □□□□ □□ □□□□□?

- A.** □□□□□ □□□ □□□ □□ □□□□ □□ IP □□□ □□□□□.
- B.** HTTP □□ □□□□ □□ □□ □□□□ □□ □□□□ □□ □□□ □□□□.
- C.** □□□ □□□□□ □□ □□□ □□ □□ □□□□ □□ Splunk □□□ □□□□□.
- D.** □ □□□□□ □□ HTTP □□ □□□ □□□□.

Answer: B (LEAVE A REPLY)

□□□ B□□□. HTTP □□ □□□□ □□ □□ □□□□ □□ □□□□ □ □□□ □□□□.

□□□□ □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□□□. □□□
□ □□□ HTML □□□ □□□□□, HTTP POST □□□ □□□□□, □□ □□ □□□□ □□ □□□ □□□ □
□□□□.

Splunk Web ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ GET, POST, Search2 ☐ ☐ ☐ ☐ ☐.

GET / HTTP/1.1 200 OK Googlebot [62.152.160.100] WHOIS: 192.168.1.1
192.168.1.1 192.168.1.1 192.168.1.1 HTML 192.168.1.1.

POST □□□□ □□□ □□□ URI□ □□ HTTP POST □□□ □□□□□. □ □□ □□□ □□□□ □□ □□
□ □□□ □□□□ □□ □□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.

```

00 0000 000 0000 00 00 00 0000 20 0000 000000. 00 00, 00 00 00 00
00000 ipaddress0 http_status 00 00 00 0000 000000 00 0000 00000.

```

□□□ POST □□□□ □□□ □□□□ □□ B□□□. HTTP □□ □□□□ □□ □□ □□□□ □□ □□□□
 □ □□□ □□□□□. □ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□□□ URI□ HTTP POST □□
 □ □□□□ □□□.

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

- A) □□□□□ □□ □□□ □□ □□□□ □□ IP □□□ □□□□□. □ □□□□ GET □□□□ □□□ □□□
□ □□□ □□ □□□□□ □□□□ □□ IP □□ □□□□ □□ □□□ □□□□.
- C) □□□ □□□□ □□ □□□ □□ □□ □□□□ □□ Splunk □□ □□: □ □□□□ □□ □□□□ □□□
□□□□ □□□□ □□ □□ □□□□ □□□□ □□ Splunk □□□ □□□□□.
- D) □ □□□□□ □□ HTTP □□ □□□ □□□□□. □ □□□□□ GET □□□□ □□□ □□□□ HTTP □□
□□□ □□□ □□□□ □ □□□□ □□ □□□ □□□□.

□ □ :

Splexicon: ☐☐☐☐ ☐☐

Splunk Web

NEW QUESTION: 184

☐ REJECT

- A.** Index-main | REJECT trans sessionid
B. Index=main | □□□□ □□ ID | □□ □□□□ □□□
C. Index=main | □□□□ □□ ID | □□□ □□□□=□□"
D. Index-main | □□□□ □□ ID | □□ REJECT

Answer: B (LEAVE A REPLY)

NEW QUESTION: 185

□□ □□□ □□□ □□□ □ □□□ □□□□□?

A. .

B. ☐☐☐ ☐☐.

C. ☐☐ ☐☐ ☐ ☐☐.

D. ☐☐ ☐☐ ☐ ☐☐.

Answer: C (LEAVE A REPLY)

□□: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects>

☐☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

□□□□ □□□□ □□ □□ □ □□1. □□ □□□ □□□ □□□□ □□ □□□

```
fields1. □□ □□□ □□□□ □□ □□□, □□, □□ □□, □□□ □□ □□□□ □□□□ □□□□□.
```

□□□1. □□□ □□□□ □□□□ □□□□, □□, □□ □□ □□□ □□□□□.

□□□ □□ C□ □□, □□ A, B, D□ □□□□□.

NEW QUESTION: 186

☐☐ ☐ CIM(Common Information Model) ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐☐?

A. ☐☐☐ ☐☐

B. ☐☐☐ ☐☐☐☐ ☐☐

C. ☐☐☐☐☐ ☐☐

D. tsidx ☐ ☐

Answer: ([SHOW ANSWER](#))

□□□ B. □□□ □□ □□□□□. □□ CIM □□ □□□ □□ □ □□□□ □□□ □ □□ □□ □□□ □□□

□□ □□□ □□□□ □□ □□□□□. CIM□ □ □□□ □□□ □□ □□□□ □□□□□□ □□□□□ □□ □□

[illegible]

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

□. Splunk □□□12□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□. □□ □□□ CIM □□ □□□ □□

[illegible]

□□. □□ Splunk □□ □□ □□ □□□□ □□□ □ □□□ CIM □□ □□□□ □□□□□ □□□□. □□□□

[illegible]

CIM □□□□□ □□□□□ □□□, □□ Splunk □□ □□ □□□□ □□□ □□□ □ □□□□. tsidx □□□

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

□□□ □□□□ CIM □□□□□ □□□□ □□□□ □□□□.

NEW QUESTION: 187

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

- A. macroname □□□ □□□□□.
- B. □□□ □□□ □□□□□.
- C. □□□ □□□ □□ □□(')□ □□□□.
- D. □□□ □□□ □□□□□(')□ □□□□.

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

□□□ C□□□. □□□ □□□ □□ □□(')□ □□□□.

□□□□ SPL □□□ □□ □□□□ □□□□□ □□□□□. □□□□ □□□ □□ □□□ □□□ □ □□□□.

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

□ □□ □□□□ □□□, □□ □□ □□□1□□ □□□.

□□□□ □□□□ □□□□□ □□□ □□□ □□ □□(')□ □□□ □□□. □□ □□,

□□□ □□□ □□□ my_macro`□□ □□□□ □□ □□ □□□□ □□□ □□□□ □□□ □ □□□□.

□□ □□:

|my_macro(□□)| ...

□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□ SPL □□□ □□□□□.

□□ □□, □□□ □□□ □□□ □□ □□:

[my_macro(argument)] □□ sourcetype=\$argument\$

□□□ □□□□ □□□ □□□□□.

index=main |my_macro(web)| □□□□ □□ □

□□□ □□ □□□□ □□□□ □□ SPL □□□ □□□□□.

index=main | search sourcetype=web | □□□□ □□ □

□□□□:

□□□□ □□ □□□ □□

NEW QUESTION: 190

- □ eval □□□ □□ □□□ □□□ □ □□□?
- A. □□□□ □□□ □□□□□.
 - B. □□ □□□ □□□□ □□□□.
 - C. □□ □□□ □□□ □□□ □□□□□□.
 - D. □□ □□□□ □□□□ □ □□□ SPL □□□ □□□□□.

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

eval □□□ □□□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□ □ □□□□□.

□□□ □□, □□, □□□ □□ □ □□□ □□□ □□□ □ □□□□.

eval □□□ □□□ □ □□ □□ □ □□□ □□ □□□ □ □□□ □□□□ □□□ □□□□.

□□□2□ □□□□ □□□. □□ □□, | eval status=if(status="200","OK","ERROR")□ □□□ □□□□□ □□ □□□.

status2□ □□ □□ □□ OK □□ ERROR□ □□ □□ □□□□□. □□□ □□ B□

□□□ □□ □□ A, C □ D□ eval □□□□ □□□ □ □□ □□□ □□□ □□□ □□□□ □□□□.

□□□□.

NEW QUESTION: 191

NEW QUESTION: 197

POST □□□□ □□□ □□□□ □ □□□ □□ □□□□□?

- A. □□, URI, □□ □□□.
- B. XMI □□, URI, □□.
- C. □□, URI, □□ □□.
- D. URI, □□ □□□, □□ □□ □□□.

Answer: (SHOW ANSWER)

POST □□□□ □□□ □□□ □□□□ □ □□□ POST □□□ □□□ □□□ □□ □□□□□.
□□ □□□□ □□ □□□□□. POST □□□□ □□□ □□□□ □□ □□□ □□□□ □□□ □ □□□□.
□□, □□ URL, URI □□□□, □□ □□, □ □□□□ □. □□□ □□ □ □□
POST □□□□ □□□ □□□□ □□ □□□ □□□□□. □□□ □□□ □□□ □□□□ □-□ □□□□.
□ □□□ □□ □□□ □□□□ □□ POST □□□ □□. Post □□□□ □□□ □□□ □ □□□□.
□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□ □□□□□.

NEW QUESTION: 198

□□ □□ □□/□□□ □□ □□□ □□□□□?

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

Answer: B (LEAVE A REPLY)

□□:

□□ □□□ □□□□ □□□ □□□□ □□ □ □□□ □ □□ □□□ □□ □□□ □□□□□.2 □□ □□□
□ □□ □□□ □□ □□, □□ □□ □ □□□ □□□□.2 □□ □□□ □□ □□□, □□ □□ □□ □-□ □□ □
□ □□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□□.2 □□ □□□ □□ □□ □□□□ □□
□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□.2 □□□ CSV □□□□ □□□□□□□ □□ □□
□□□□ □□ □□□ □□□□ □□□□ □□ □□□□□.2 □□□ □□ □□/□□□ □□□□ □□□ □□□ □
□□□. □□ □□, □□ □□, □□2. □, Splunk□ □□ □□ □□□□□ □□□ □□□ □□ □□□ □□□ □□
□ □□□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.2 □□□ □□ B□ □□ □□ A, C □ D□ □□□□
□.

NEW QUESTION: 199

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

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

Answer: A,C,D (LEAVE A REPLY)

`geom`, `geostats`, `iplocation`. `geom` is, `geostats` is, `iplocation` is
`geom` is, `geostats` is, `iplocation` is, `geom` is, `geostats` is, `iplocation` is.
`geom` is, `geostats` is, `iplocation` is, `geom` is, `geostats` is, `iplocation` is.
`geom` is, `geostats` is, `iplocation` is, `geom` is, `geostats` is, `iplocation` is.

geom: □ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□□□□ □□□ □ □□□
 □□. geom □□□ □□□ □□□ □□□ □□□□ KMZ □□□ □□□ □□□□□. □□, geom □□□ □□ □
 □□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□□.

```
geostats: 0 000 00 000 0000 000 000 000 000 0000 0000 00 0000
0 00000. geostats 000 0000 000 0000 000 00 000 000 00000. 00, 000
00 00 0 00 000 000 0000 0000 00 000 000 00000.
```

```

iplocation: 1 1111 IP 1111 11 1111 1111 11 11111 11111 11 11 11111 11111 1 11
1111. iplocation 1111 IP 11 1111 1111 11111 11, 11, 11, 11 11 1111 11111 11111
1. iplocation 1111 geom 11 geostats 1 11 11 1111 11 11111 IP 11 11 1111 1111 1 11
11.

```

NEW QUESTION: 200

☐☐ ☐ ☐☐ ☐☐☐ ☐☐☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐ ☐ ☐☐☐☐

- A.** □□□ IP □□□ □□□□□ □□□□ □□□□ □ □□□□.
- B.** □□ □□□ □ □□□ □□□□□□.
- C.** □□□□ □□□□ 1000□□ □□□ □□□□ □□□□.
- D.** □□□□ □□ □□□□ □□□□ □□ □□ state□ □□□□□□.

Answer: C (LEAVE A REPLY)

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction>

NEW QUESTION: 201

value □□□ □□□□ □□ □□ fillnull □□□ null □□ □□□□ □□□□?

- A.** 0
B. □□ □□
C. NaN
D. NULL

Answer: A (LEAVE A REPLY)

□ □ :

```
fillnull 000 null 00 000 000 0000, 00 0000 00 00 000 000 00 00000. null 0
0 Splunk00 000000 00 000 0000 00 0000. fillnull 000 00 00 00 00 000 null
00 00 0 0000. fillnull 000 null 00 00 00 0000 value00 000 000 000 0 0000.
value 000 0000 000 fillnull 000 00000 null 00 000 0000.
```

NEW QUESTION: 202

□□ □□□(FX)□ □□□ □ □□ □□ □□ □□ □□ □□□□□? (□□□□ □□ □□□ □□□□□)

- Answer: A,B,D (LEAVE A REPLY)**

<https://community.splunk.com/t5/Splunk-Search/Field-Extraction-Separate-on-Colon/mp/29751> □□ □□□(FX)

□: □□ □□□□ □□□□ □□ □□□□□.

□□: □□□ □□□ □□□□ □ □□.

□□□ □□ □□ A, B, D□ FX□□ □□□□□.

□□ □ □□□ □□ □ □□□ □□ □□□□□?

- Answer: C (LEAVE A REPLY)**

□□□□ SPL □□□ □□ □□□□ □□□□□ □□□□□. □□□□ eval □□□ □□□□ □□ □□□ □□ □
□□□ □ □ □□□, □□□ □□□ □□□ □□□□. □□□□ □□□ □□ □□ □□□, □□□ □□□□ □□□
□ □□ □□□ □□□ □ □□ □□□□□. □□□□ □□□ □□ □□□□ □□□ □□ □□□, □□ □□ □□□
1□□ □□□.

□□, □□, □□ □ □□□ □□□□ □□□. □□□□ □□□□ □□□□□ □□□ □□□ □□ □□() □ □□ □
□□ □□ □□ □□ □□□□ □□ □□ □□□□ □□□.

- sourcetype= object

```
my macro(□)
```

☐ ☐ sourcetype=web

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

C. □□□□ □□□□ 1000□□ □□□ □□□ □□□□.

D. state .

Answer: C (LEAVE A REPLY)

□ □ :

<https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction>

NEW QUESTION: 206

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

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

stats sum(price) as USD by product_name
| eval \$currency\$="\$symbol\$".toString(round(USD*\$rate\$,2),
"commas") | eval USD="\$" + toString(USD,"commas")

☐

Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. □□ □□ □□(□□, €, 79)"

B. □□ □□ □□(□□, €, .79)

C. (\$euro,\$€\$,s79\$

D. ☐☐ ☐☐ (\$euro, \$€\$, S, 79\$)

Answer: B (LEAVE A REPLY)

□ □ :

□□ □□□□ □□□□ □□□ □□□ macro name(\$arg1\$, \$arg2\$, ...) □□□ □□□□ □□□□.

`$arg1$, $arg2$` `convert sales`, , , ,

[illegible]

```
□ convert sales($euro$, $€$, .79)□□□.
```

NEW QUESTION: 207

□□□□ □ □□ □□□ □□□□□ □□□ □□□□□?

A. □□□□ □□□ (3)□□ □□□□.

B. (3) .

C. 3 .

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

Answer: (SHOW ANSWER)

11

Which of the following are valid macro arguments? (Select all that apply.)
my_macro(3) is a valid macro argument. Which of the following are valid macro arguments?
1. my_macro A B C D

NEW QUESTION: 208

GET workflowaction is a valid macro argument? (Select all that apply.)
A. workflowaction is a valid macro argument.
B. workflowaction is a valid macro argument.
C. workflowaction is a valid macro argument.
D. workflowaction is a valid macro argument.

Answer: B,C (LEAVE A REPLY)

URL: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction

NEW QUESTION: 209

Splunk Common Information Model (CIM) is a standard for data ingestion and storage. Which of the following are valid CIM data types? (Select all that apply.)
A. CIM is a standard for data ingestion and storage.
B. CIM is a standard for data ingestion and storage.
C. CIM is a standard for data ingestion and storage.
D. CIM is a standard for data ingestion and storage.

Answer: B (LEAVE A REPLY)

Splunk CIM (Common Information Model) is a standard for data ingestion and storage. Which of the following are valid CIM data types? (Select all that apply.)
1. CIM is a standard for data ingestion and storage.
2. CIM is a standard for data ingestion and storage.
3. CIM is a standard for data ingestion and storage.
4. CIM is a standard for data ingestion and storage.

NEW QUESTION: 210

Which of the following are valid macro arguments? (Select all that apply.)
A. my_macro(3) is a valid macro argument.
B. my_macro(3) is a valid macro argument.
C. my_macro(3) is a valid macro argument.
D. my_macro(3) is a valid macro argument.

Answer: C (LEAVE A REPLY)

Which of the following are valid macro arguments? (Select all that apply.)
1. my_macro(3) is a valid macro argument.
2. my_macro(3) is a valid macro argument.
3. my_macro(3) is a valid macro argument.
4. my_macro(3) is a valid macro argument.

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

Q2. Which of the following is a valid Splunk search syntax? (Select all that apply.)

NEW QUESTION: 211

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

- A. CIM `search` `index=main` `type=*`
- B. CIM `search` `index=main` `type=*` `OR` `type=*`
- C. `search` `index=main` `type=*` `OR` `type=*`
- D. CIM `search` `index=main` `type=*` `OR` `type=*`

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

Q2:

<https://docs.splunk.com/Documentation/CIM/4.15.0/User/Quickstart>

SPLK-1002 is a collection of Splunk dumps. DumpTop is a tool that can be used to extract Splunk-1002 dumps! DumpTop is a tool that can be used to extract Splunk-1002 dumps. DumpTop is a tool that can be used to extract Splunk-1002 dumps. DumpTop is a tool that can be used to extract Splunk-1002 dumps.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 212

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

- A. `search` `index=main` `type=*`
- B. `search` `index=main` `type=*` `OR` `type=*`
- C. `search` `index=main` `type=*` `OR` `type=*`
- D. `search` `index=main` `type=*` `OR` `type=*`

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 213

GET is a valid Splunk search syntax. (Select all that apply.)

- A. `search` `index=main` `type=*`
- B. `search` `index=main` `type=*` `OR` `type=*`
- C. `search` `index=main` `type=*` `OR` `type=*`
- D. `search` `index=main` `type=*` `OR` `type=*`

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

Q2: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction>

NEW QUESTION: 214

□□□ □□□ □□□ □□□ □, □□□□ □□□□ □□□□□ □□□ □□ □□□ □□□ □□□□ □□□?

Destination app
oidemo

Name *
Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *
Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

sourcetype=access_combined action=\$action\$ JSESSIONID=\$JSESSIONID\$
| stats values(action) as action by JSESSIONID

☐ Use eval-based definition?

Arguments
Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

- A. □□□ □□□ sessiontracker□□ □□□ action, JSESSIONID□□□.
- B. □□□ □□□ sessiontracker(2)□□ □□□ action, JSESSIONID□□□.
- C. □□□ □□□ sessiontracker□□ □□□ \$action\$, \$JSESSIONID\$□ □□.
- D. □□□ □□□ sessiontracker(2)□□ □□□ \$action\$, \$JSESSIONID\$□ □□.

Answer: B (LEAVE A REPLY)

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros> □□ □□□ □□□
action□ JSESSIONID□□ □ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□□.

□□□□□(2)

□□□ □□□ □□□ □□□□□.

□□□ □□□ sessiontracker□ □□□□□. □ □□□ □□ □□□□□ □□□□ □□□□ □ □□□□□.

□□□□ □□ □□□ 2□ □□□□□. □□ □□□□ □□□ □ □ □□ □□□ □□□□ □□ □□□□□.

□□□ □□□ index=main sourcetype=access_combined_wcookie action=\$action\$ JSESSIONID=\$JSESSIONID\$ | stats count by JSESSIONID□ □□□□□. □□ □□□□ □□□ □ □□□□ □□ □□□□□□
□. □□ □□□□□ □□□, □□, □□ □ □□□ □□ □□□ □□□ □ □□□□□. □□□ □□ □□□ □□ □□
□ □□ □□□ □□ □□□□.

□ □□ action□ JSESSIONID□ □□□□ □□□ □ □□□ □□□ □□□ □□ □□□□□.

□□□ □□□□ □□□□ □□□□□ □□□□ sessiontracker□, □□□ action□, JSESSIONID□ □□□□ □
□□. □□ □□□□ sessiontracker(2)□ □□□□ □□□ □□□ □ □□□□.

NEW QUESTION: 215

□□□ □□□ REJECT□□□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□□ □□ □□□ □□□□
□?

- A. index=main REJECT | □□□□ □□ ID
- B. index=main | □□□□ □□ ID | □□ REJECT
- C. index=main | transaction sessionid | □□□ transaction=reject
- D. index=main | □□□□ □□ ID | □□□ transaction="REJECT*"

Answer: B (LEAVE A REPLY)

□□/□□:

NEW QUESTION: 216

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

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

- A. □□ □□ □□(□□, €, 79)"
- B. □□ □□ □□(□□, €, .79)
- C. □□_□□ (\$euro,\$€\$,s79\$
- D. □□_□□ (\$euro, \$€\$,S,79\$)

Answer: (SHOW ANSWER)

□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros> □□ □□□□□ □□
□□ □□□□ □□□ □□□ macro_name(\$arg1\$, \$arg2\$, □□□ □□□□ □□□□.
...) □□□ \$arg1\$, \$arg2\$ □□ □□□□ □□□□□. □ □□ □□□ □□□ convert_sales□□, □□, □□, □□
□ □□□ □□□ □□□□. □□□ □□ □□□ □□□ □□□ □□□□□. □□□ □□□□ □□□□ □□□ □
□□ convert_sales(\$euro\$, \$€\$,
.79).

NEW QUESTION: 217

value □□□ □□□□ □□ □□ fillnull □□□ null □□ □□□□ □□□□?

- A. 0
- B. □□ □□
- C. NaN
- D. NULL

Answer: (SHOW ANSWER)

□□□ □□□ □□ □□□ eval □□□□ □□□□ □□□□ □□□□ □□□□□. □□□ □□□ □□□□ □□
□□□□ □ □ □□□ □□ □□ □□□□ □□□ □□□ □ □□□□. □□□ □□□ □□□□ □□ □□□ □□
□□ □□ □□□ □□□□ □□□ □ □□□□.

□□ □□□ CSV □□□□ □□□□□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□□. □□
□□□ □□□, □□, □□ □□ □□ □□ □□□ □□□ □□ □□ □□□ □□ □□□□ □□□□ □□□ □□□
□ □□□□.2 □□ □□□ □□□ □□□ □□□□ □□ □□□□□, □□□ □□ □□□ □□□ □□□ □□□
□□□ □□□ □ □□□□.3

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

□□□□:

- * □□□ □□□ □□□
- * □□□ □□□
- * □□ □□ □□

NEW QUESTION: 222

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

- A. GET
- B. □□
- C. □□
- D. □□□□

Answer: ([SHOW ANSWER](#))

□□

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction> GET □□□□ □□
□□ □□

- * □□ > □□ > □□□□ □□□□ □□□□□.
 - * □□ □□□□ □□□□ □ □□□□ □□ □□□ □□□□.
 - * □□□ □□ □□□□ □□□□□.
- □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □ □□□□.
- □□□ □□ □□ □□ □□□ □□ □□□ □□ □□□□.
- * □□□□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□□ □□□ □□□□□.
- □□□ □□□ □□□□□ "□□ □□□□ □□"□ □□□□□. □□□ □□□□ □□ □□□ □□ □□□(□
□□ □□ □□ □□ □□)□□ □□□□ □□□ □□□□□. □ □□□ □□ □□□ □□□ □□□□ □□ □□□
□□□ □□□ □□□□□.
- □□□ □□□ □□□ □□□□□ [□□ □□□ □□□□ □□]□ □□□□□. □□□ □□□ □□□□ □□
□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□.
- * □□ □□□□ □□□ □□□ □□, □□ □□ □□ □ □□ □□□□ □□□ □□□□□.
 - * □□ □□□ □□□ □□□□□.
 - * URI□□ □□ □□ □□ □□ □□□□ □□□ □□ URI□ □□□□□.
- □□□ □□□□□ □□ □□ □□□ □□ □□ □□□ □□ □□ □□□ □□□□□.
- URI□ □□ GET □□□□ □□□ □□□ □□ □□ □□□□ URL □□□□□□. □, □□□ □□□ □□□ □□
□ □□ □□ □□□ □ □□□□□.

* □□ □□□□ □□□□ □□□ □□ □□ □□□□□ □□□ □ □□□ □□□ □□ □□□ □□□□□.

* Link □□□□ □□□□ □□□□□.

* □□□ □□□□ □□□□ □□ □□□□ □□□□□.

NEW QUESTION: 223

□□ □□ □□□ □ □□□□ □□ □□ □□□□□?

A. index=□ □□=50* | □□□, □□ □□ □□ □

B. index=□ □□=50* | □□□ □□□□ □□ □□ □

C. index=□ □□=50* | □□□, □□□ □□ □

Answer: A (LEAVE A REPLY)

22

[illegible]

NEW QUESTION: 224

□□ □□□□ □□ □□ □□□□ 2□ □□□ □□□□□?

A. ☐☐

B. ☐ ☐

C. ☐ ☐

D. ☐ ☐ ☐ ☐

Answer: ([SHOW ANSWER](#))

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

NEW QUESTION: 225

Splunk □□ □□ □□(CIM)□□ □□□□□?

A. CIM □ Splunk □□ □□□□ □□□ □ □□ □ □□□□ □□□□.

B. CIM□ □□□□ □□□□ □□ □□□ □□ □□□□□□□□.

C. CIM □ □ □ □ □ Splunk □ .

D. CIM□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□□ □□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 226

□ □ □ □ □ □ □ □ □ ?

A. □□□ □□□ □□□ □□□ □ □□□□□.

B. □□□ □□□ □□□□ □□□□ □□□ □□□□□.

C. □□□ □□□□ □□□□□ □□□ □ □□□□□.

D. ☐☐☐☐ ☐☐ Splunk ☐☐☐☐ ☐☐☐ ☐☐☐☐.

Answer: C (LEAVE A REPLY)

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot>

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
□ **SPLK-1002** □□ □□□ □□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.

<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 227

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

- A. □
- B. □□□
- C. □□
- D. □□

Answer: B,D (LEAVE A REPLY)

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep>

NEW QUESTION: 228

□□ □□ □□ □ □□ □□ □□□□□ □□ □□□ □ □□□?

□□, □□□□, □□, □□□ □□
□□, □□□□, □□, □□
□□, □□□□, □□□ □□, □□
□□, □□□, □□, □□

Answer:

□□, □□□□, □□, □□□ □□.
□□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□□. □□ □□, □□□ □□ □□ □□□ □□□□
□□□ □□□ □□□ □ □□□□.
□□□□□ □ □□ □□ □□ □□□□ □□ □□□□□ □□□ □□□ □□□□□. □□□□□ transaction □□
□ □□□□□ transactiontypes.conf □□□ □□□□ □□□ □□□□ □□□ □ □□□□.
□□ □□ □□□ □□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □ □□□□. □□□ □□□□ □
□□ □□□□□.

□□: □ □□□ □ □ □□□ □□ □□ □□□ □□□□ □ □□ □□□ □□□□. □□ □□□□□, □□ □□□
□□□, □□□ □□□□ □ □□□ □ □□□□.

timechart: □ □□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□. □□, □□ □□ □□□□
□□□□ □ □□□ □ □□□□.

stats: □ □□□ □□ □□□ □□□ □□ □□ □□(count, sum, average □)□ □□□□□. □□ □□□ □□□□□
□□□□ □□□□□ □□□□ □ □□□ □ □□□□.

eventstats: □ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□□. stats □□□□ □□□□□, □ □□□
□ □□ □□□ □ □□□ □□□□□. □□□□ □□ □□□ □□□□ □ □□□ □ □□□□.

1. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

2. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

3. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

4. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

5. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

6. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

7. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

8. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

9. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

10. Which of the following is a valid Splunk search command? (Select all that apply.)
 A. search "login" | stats sum(eventcount) as total_events by user
 B. search "login" | timechart span=1h avg(duration) by user
 C. search "login" | eventstats avg(duration) as avg_duration
 D. search "login" | diff

NEW QUESTION: 229

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

- A. search "login" | stats sum(eventcount) as total_events by user
- B. search "login" | timechart span=1h avg(duration) by user
- C. search "login" | eventstats avg(duration) as avg_duration
- D. search "login" | diff

Answer: (SHOW ANSWER)

The correct answers are A, B, C, and D. All four commands are valid Splunk search commands.

□ □□□ □□□□ □□ □□ □□□□ □□ □□□□ □□ □□ □□□ □□ □□□□.2 □□
□□□ □□□□ □□□ □□ □□ □□ □□□ □□ □□ □□□ CIM □□□ □□□□ □□ □□ □□□ □□□
□ □□□□.3 □□□ □□ B□ □□ □□ A, C, D□ □□□□.

NEW QUESTION: 236

□□□□ □□□□□ □□□□□ □□□□□.

A. □□□

B. □□□□

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

NEW QUESTION: 237

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

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: Sarg1\$

```
stats sum(price) as USD by product_name  
| eval $currency$="$symbol$",tostring(round(USD*$rate$,2),  
"commas") | eval USD="$" + tostring(USD,"commas")
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. "□□_□□(□□,€,79)"

B. '□□_□□(□□,€,79)'

C. "□□_□□(\$euro\$,€€\$,\$.79\$)"

D. '□□_□□ (\$□□\$,€€\$,\$.79\$)'

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

□□/□□: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros>

NEW QUESTION: 238

timechart □□□ □□□ □□ □□ □□□□ □□□□ □□□□□□.

A. □□□ □□□ □

B. □□□ □□ □□

C. □□□ □□□ □□

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

timechart □□□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□□. timechart

□□□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □□□□□□.
_time □□2. □□ □□□ □□□ □□□ □□ □□□ □□ □□□□□.
□□ □□, □□ □□□ □□ 24□□□ □□□□ Splunk□ 30□ □□□ □□□□□.
timechart. □□ □□□ '□□ 7□'□ □□□□ Splunk□ timechart2□ 4□□ □□□ □□□ □□□□□.
□□□ □□ B□ □□□ □□ A□ C□ □□□ □□□ □□□ □□□ □□□□□.
□□ □□□ □□.

SPLK-1002 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SPLK-1002 □□! DumpTop □ □
□ **SPLK-1002** □□ □□□ □□□□□□, DumpTop SPLK-1002 □□ □□□ □□□□□□□□ □□□ □□
□□□□□. □□□□ □□□ □□□□ □□ DumpTop SPLK-1002 □□□ □□□□□.
<https://www.dumptop.com/Splunk/SPLK-1002-dump.html> (308 Q&As Dumps, **30%OFF** Special Discount:
KrDump)