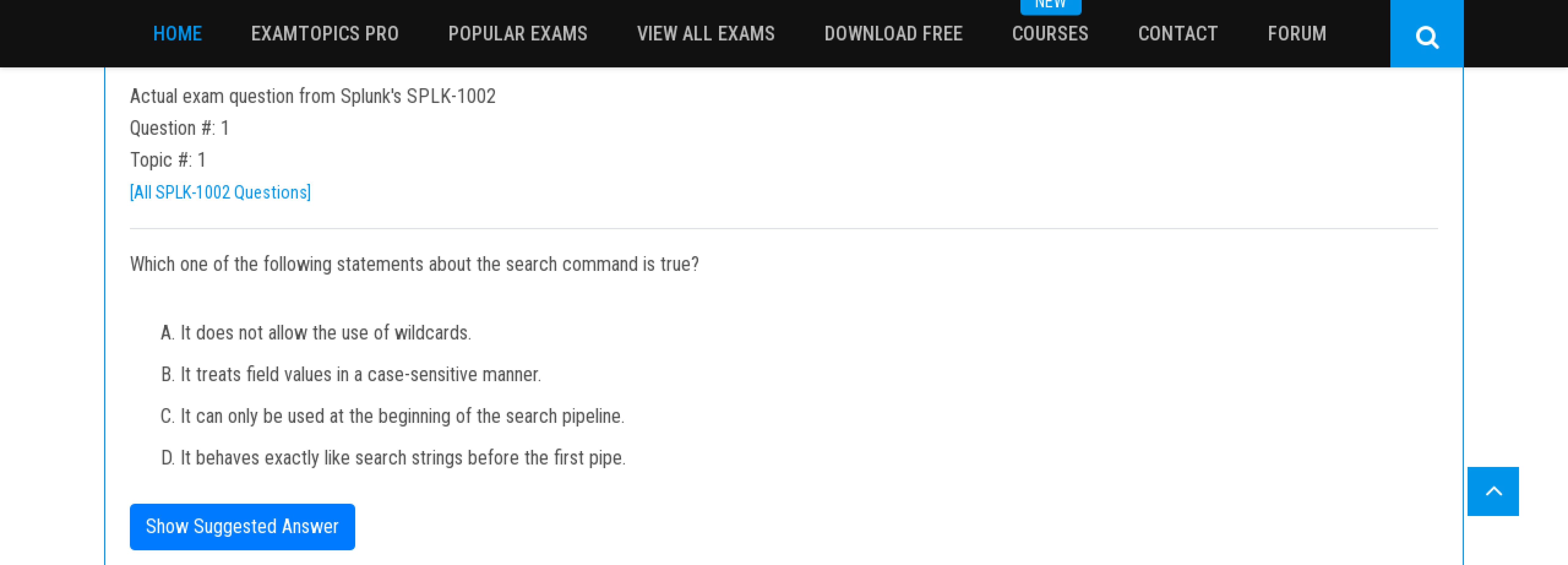


Actual exam question from Splunk's SPLK-1002

Question #: 1

Topic #: 1

[All SPLK-1002 Questions]

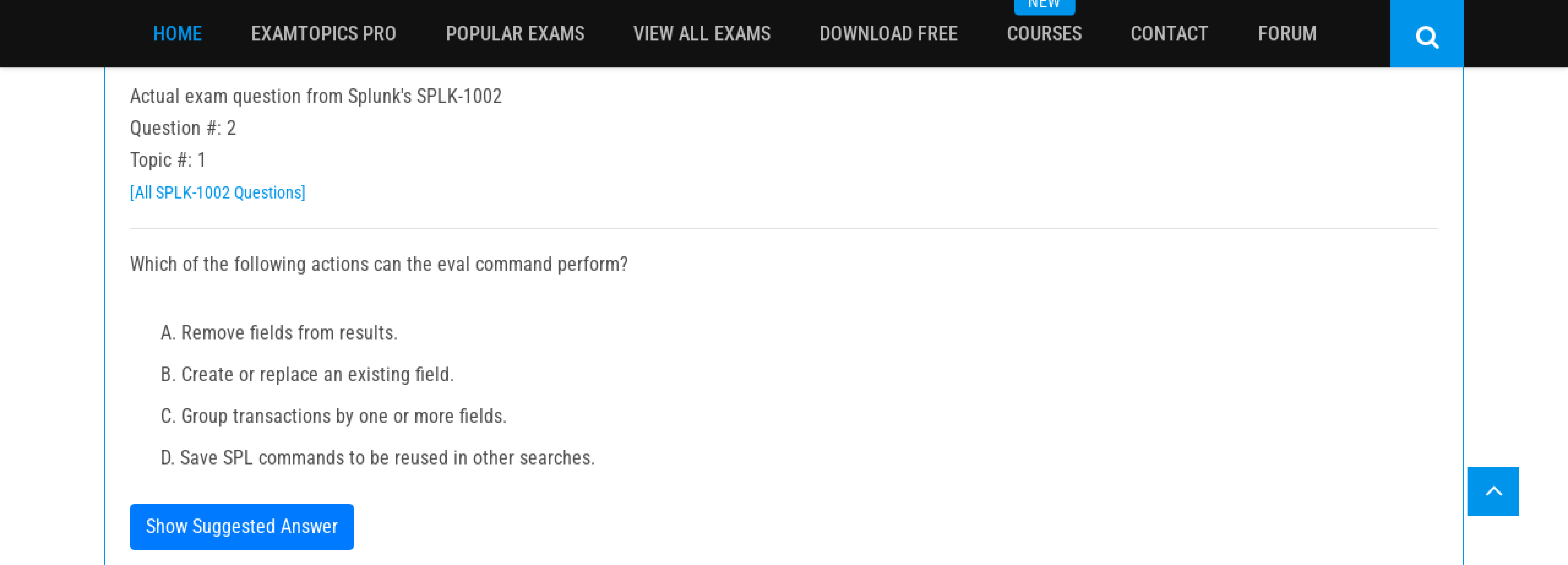
Which one of the following statements about the search command is true?

A. It does not allow the use of wildcards.

B. It treats field values in a case-sensitive manner.

C. It can only be used at the beginning of the search pipeline.

D. It behaves exactly like search strings before the first pipe.



Actual exam question from Splunk's SPLK-1002

Question #: 2

Topic #: 1

[All SPLK-1002 Questions]

Which of the following actions can the eval command perform?

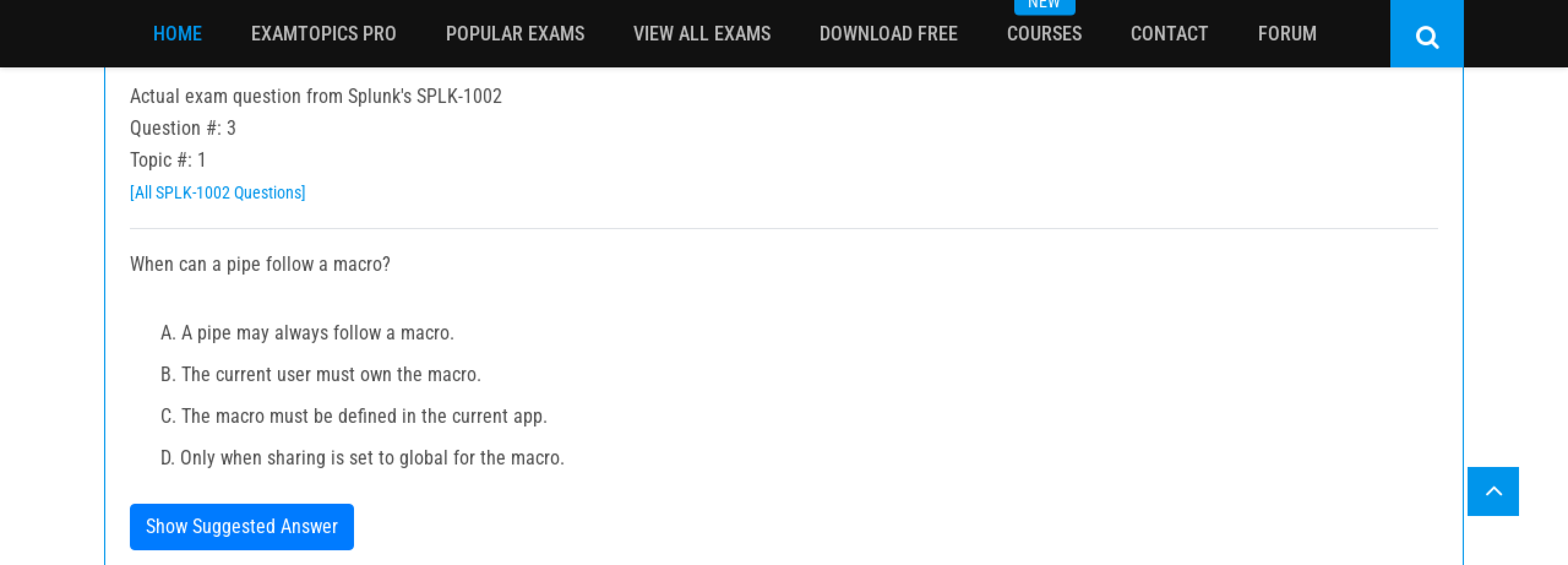
A. Remove fields from results.

B. Create or replace an existing field.

C. Group transactions by one or more fields.

D. Save SPL commands to be reused in other searches.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 3

Topic #: 1

[All SPLK-1002 Questions]

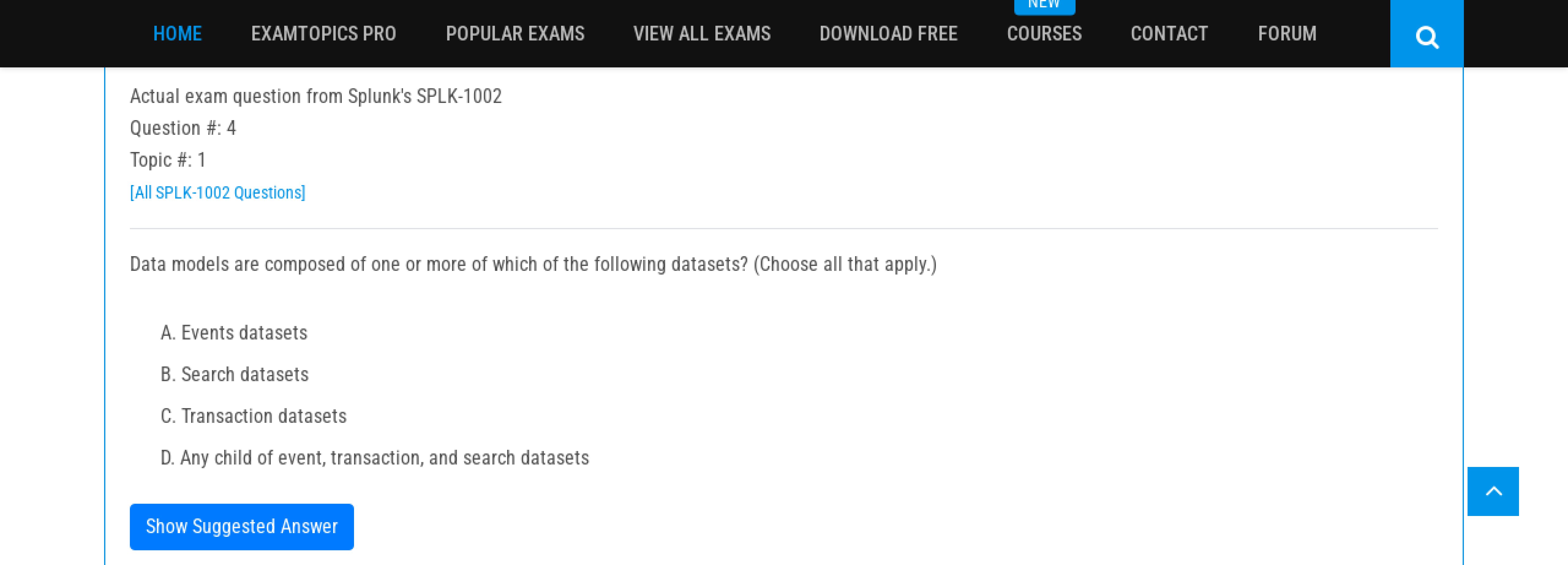
When can a pipe follow a macro?

A. A pipe may always follow a macro.

B. The current user must own the macro.

C. The macro must be defined in the current app.

D. Only when sharing is set to global for the macro.



Actual exam question from Splunk's SPLK-1002

Question #: 4

Topic #: 1

[All SPLK-1002 Questions]

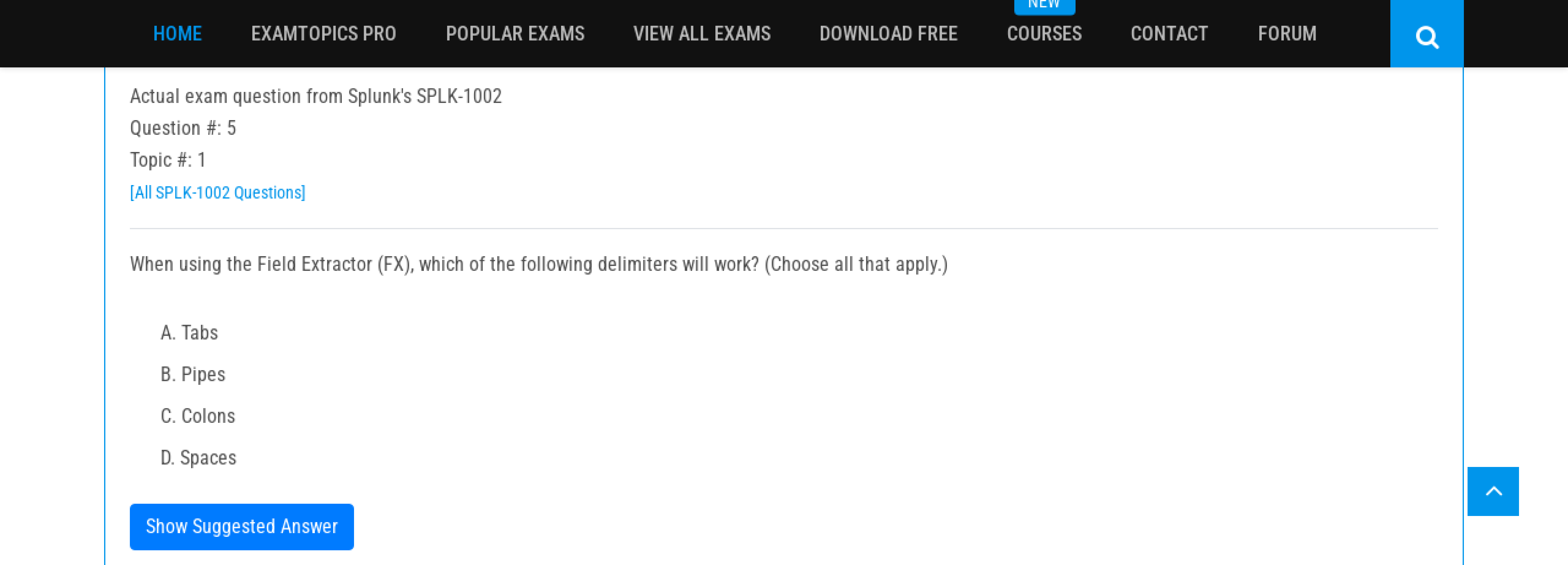
Data models are composed of one or more of which of the following datasets? (Choose all that apply.)

A. Events datasets

B. Search datasets

C. Transaction datasets

D. Any child of event, transaction, and search datasets



Actual exam question from Splunk's SPLK-1002

Question #: 5

Topic #: 1

[All SPLK-1002 Questions]

When using the Field Extractor (FX), which of the following delimiters will work? (Choose all that apply.)

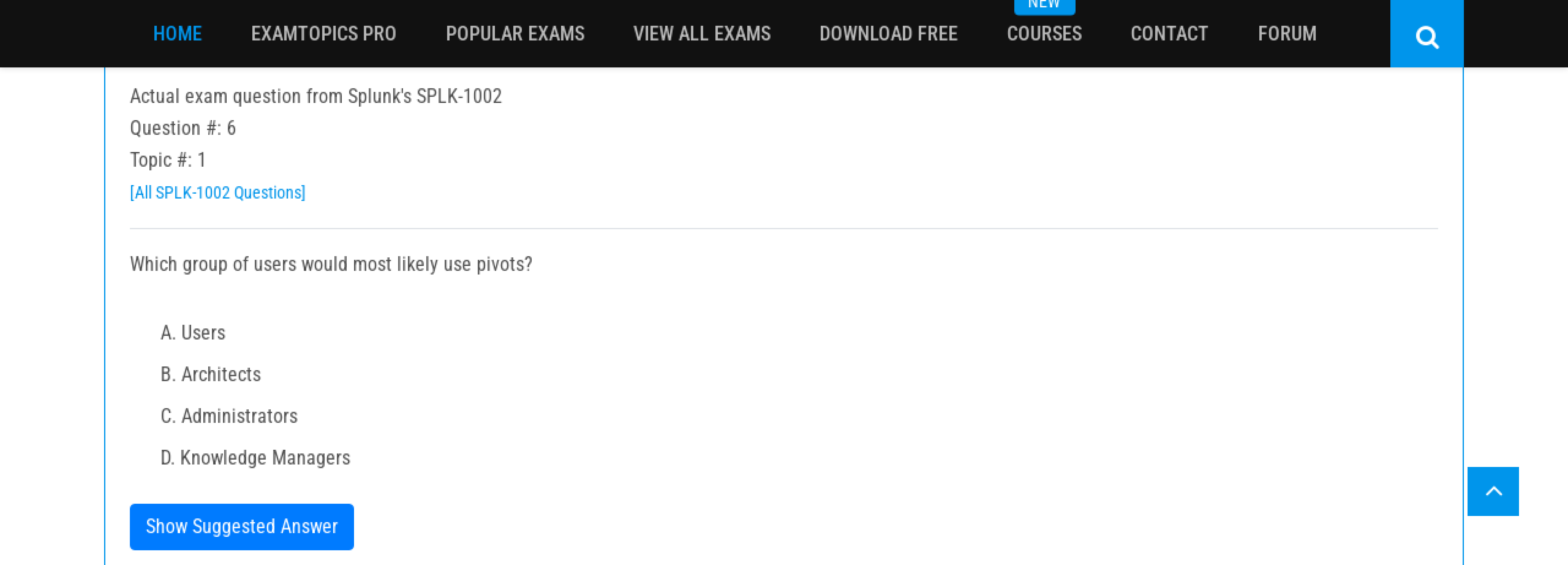
A. Tabs

B. Pipes

C. Colons

D. Spaces

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 6

Topic #: 1

[All SPLK-1002 Questions]

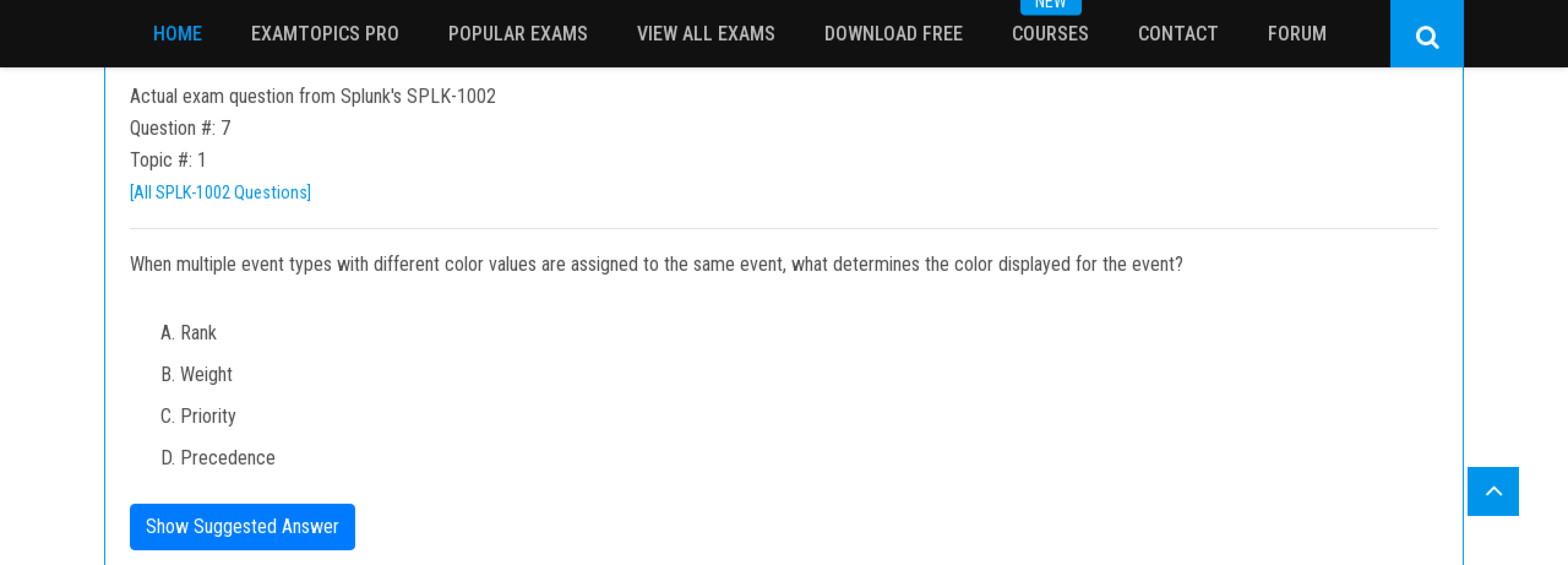
Which group of users would most likely use pivots?

A. Users

B. Architects

C. Administrators

D. Knowledge Managers



Actual exam question from Splunk's SPLK-1002

Question #: 7

Topic #: 1

[All SPLK-1002 Questions]

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?

A. Rank

B. Weight

C. Priority

D. Precedence

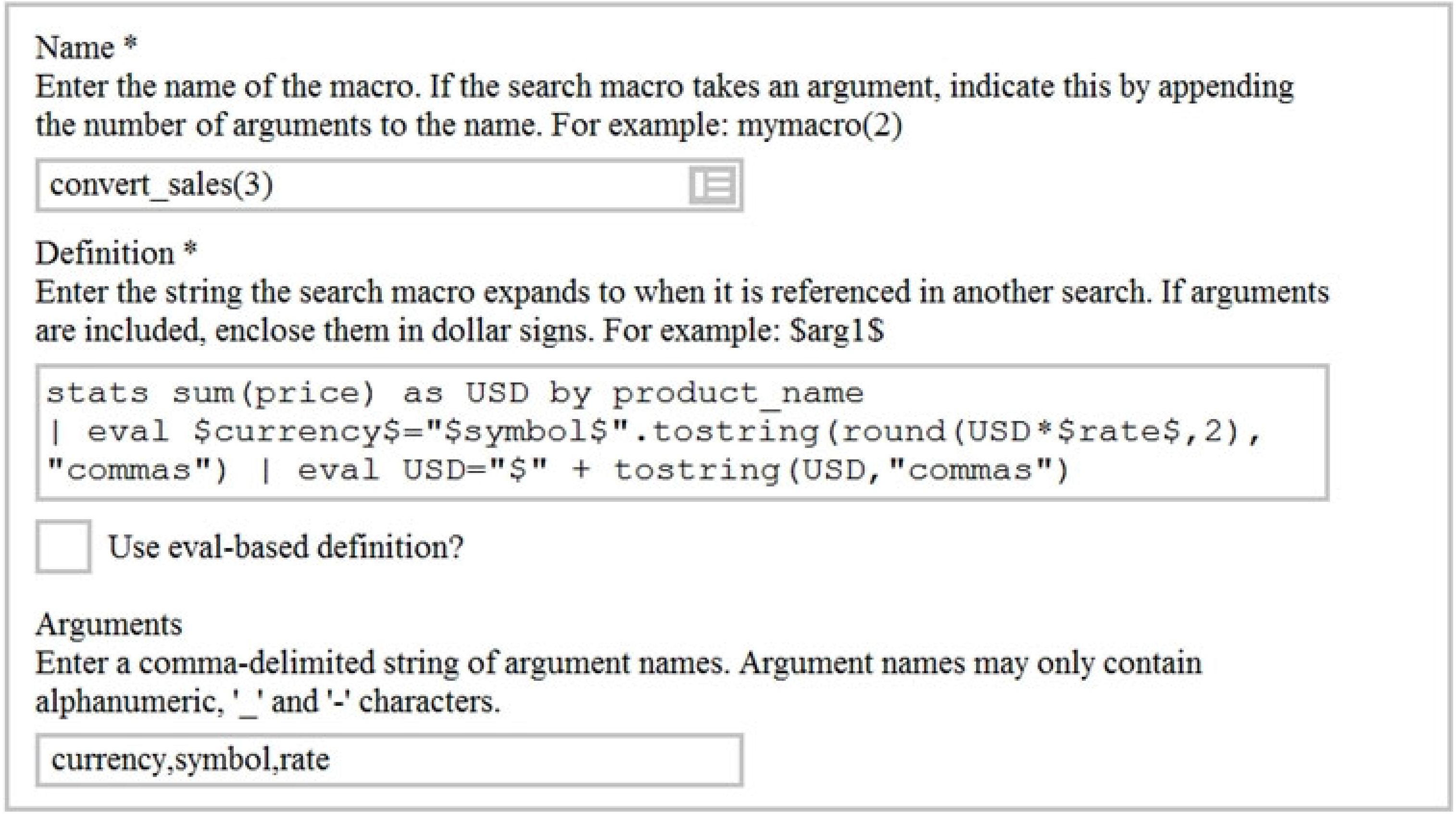
Actual exam question from Splunk's SPLK-1002

Question #: 8

Topic #: 1

[All SPLK-1002 Questions]

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



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

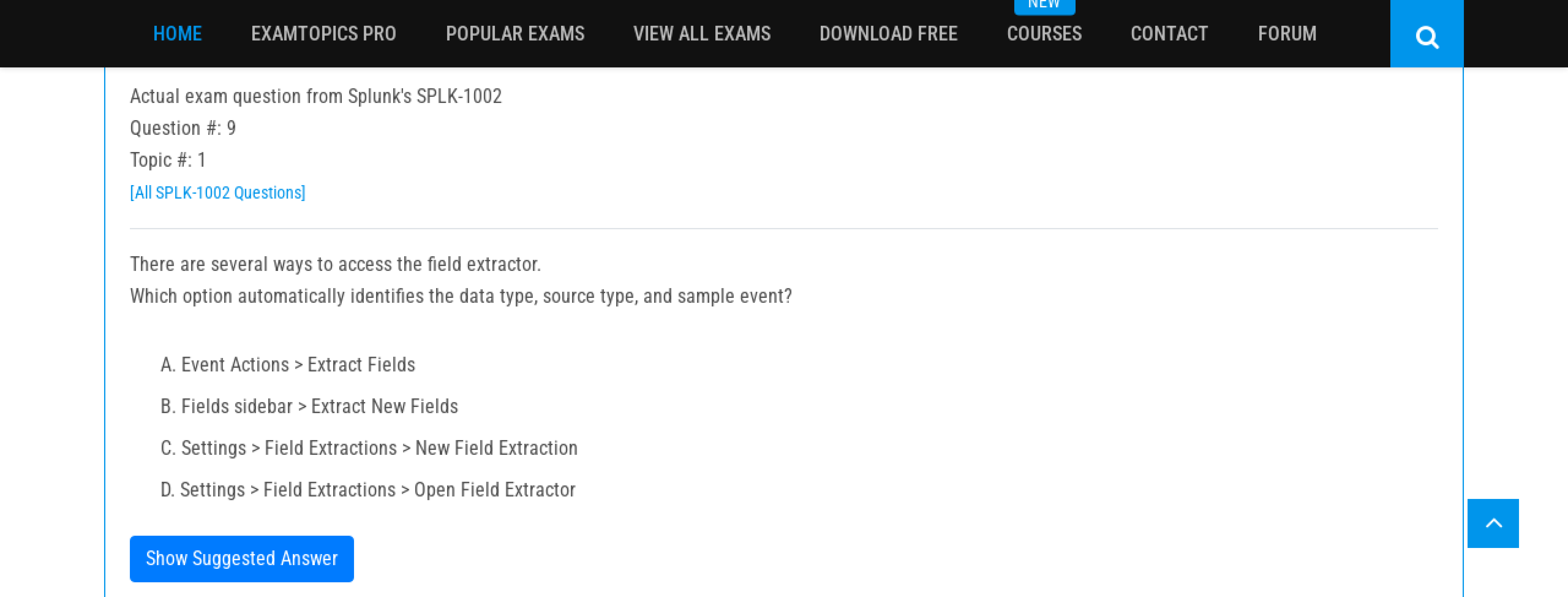
A. "convert_sales(euro,79.,¬,ג)"

B. 'convert_sales(euro,79.,¬,ג)'

C. "convert_sales($euro$,79.$,$¬,ג)"

D. 'convert_sales($euro$,79.$,$¬,ג)'

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 9

Topic #: 1

[All SPLK-1002 Questions]

There are several ways to access the field extractor.

Which option automatically identifies the data type, source type, and sample event?

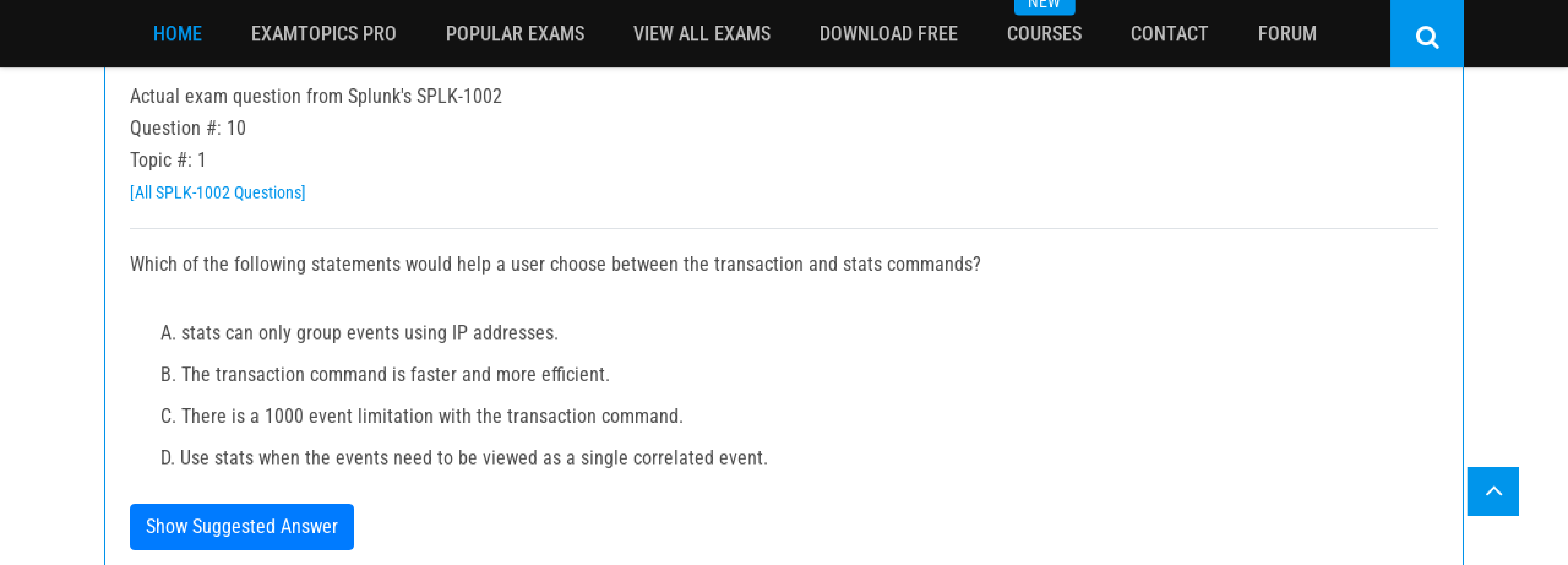
A. Event Actions > Extract Fields

B. Fields sidebar > Extract New Fields

C. Settings > Field Extractions > New Field Extraction

D. Settings > Field Extractions > Open Field Extractor

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 10

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements would help a user choose between the transaction and stats commands?

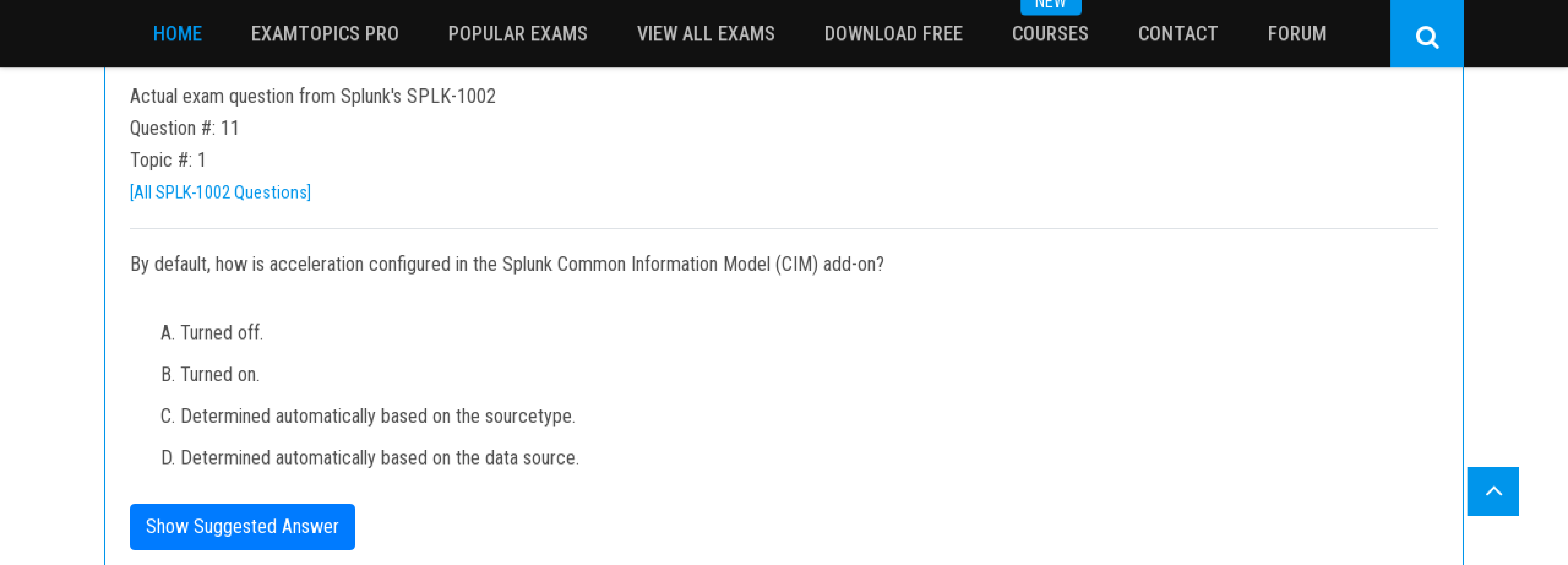
A. stats can only group events using IP addresses.

B. The transaction command is faster and more efficient.

C. There is a 1000 event limitation with the transaction command.

D. Use stats when the events need to be viewed as a single correlated event.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 11

Topic #: 1

[All SPLK-1002 Questions]

By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

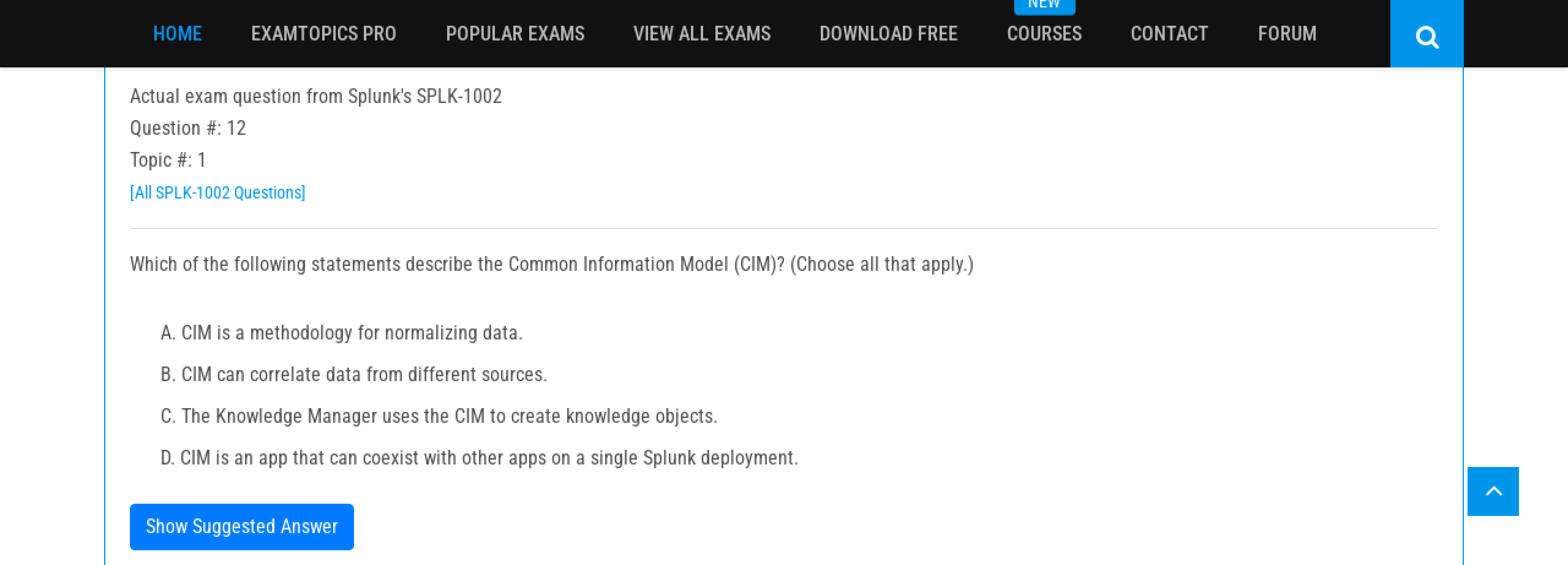
A. Turned off.

B. Turned on.

C. Determined automatically based on the sourcetype.

D. Determined automatically based on the data source.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 12

Topic #: 1

[All SPLK-1002 Questions]

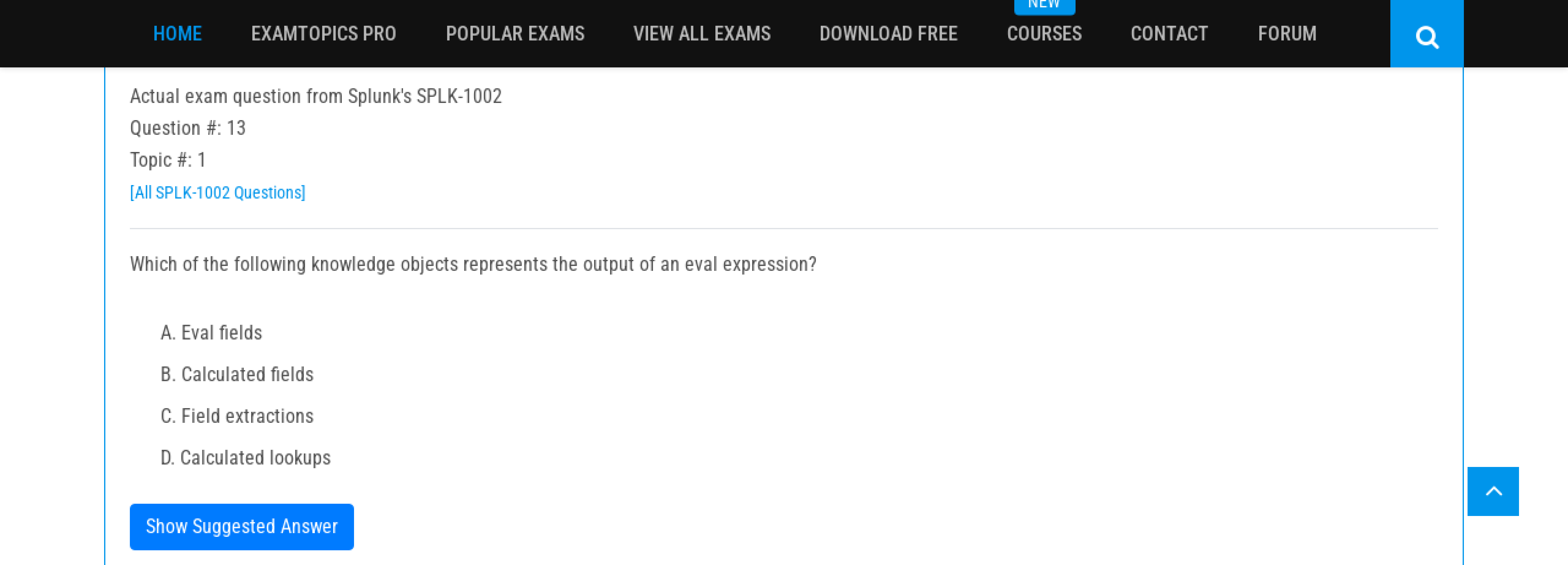
Which of the following statements describe the Common Information Model (CIM)? (Choose all that apply.)

A. CIM is a methodology for normalizing data.

B. CIM can correlate data from different sources.

C. The Knowledge Manager uses the CIM to create knowledge objects.

D. CIM is an app that can coexist with other apps on a single Splunk deployment.



Actual exam question from Splunk's SPLK-1002

Question #: 13

Topic #: 1

[All SPLK-1002 Questions]

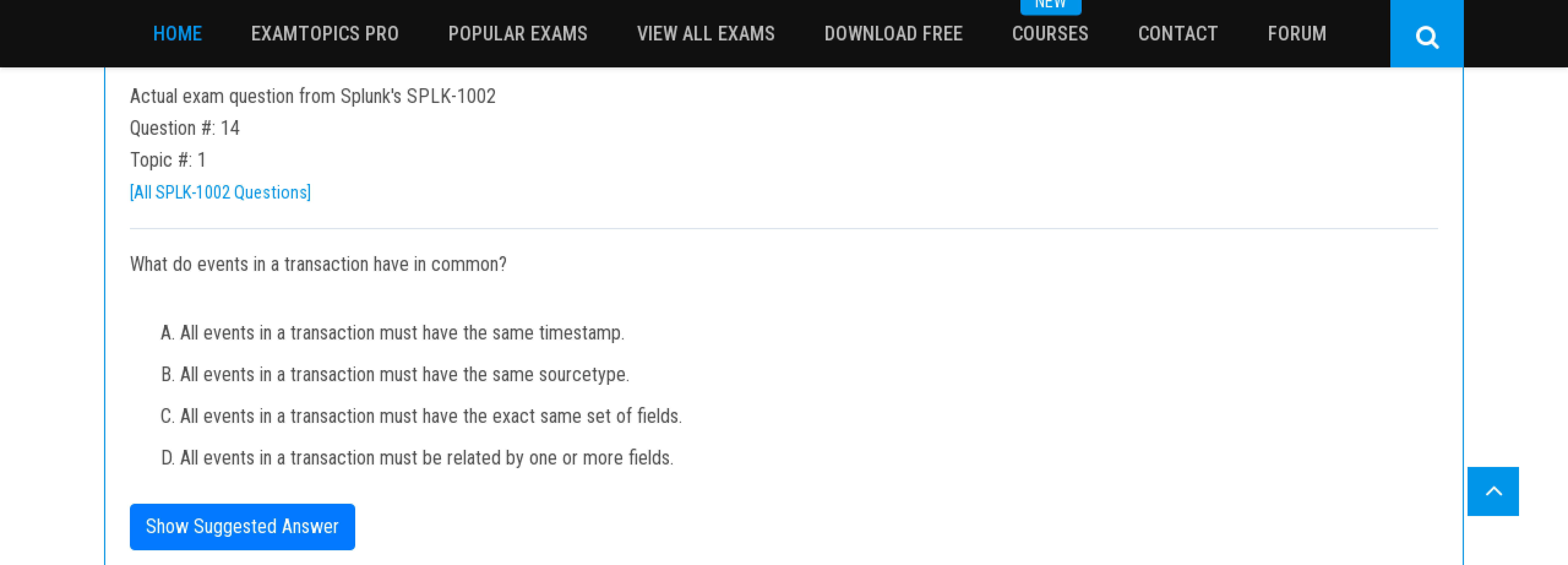
Which of the following knowledge objects represents the output of an eval expression?

A. Eval fields

B. Calculated fields

C. Field extractions

D. Calculated lookups



Actual exam question from Splunk's SPLK-1002

Question #: 14

Topic #: 1

[All SPLK-1002 Questions]

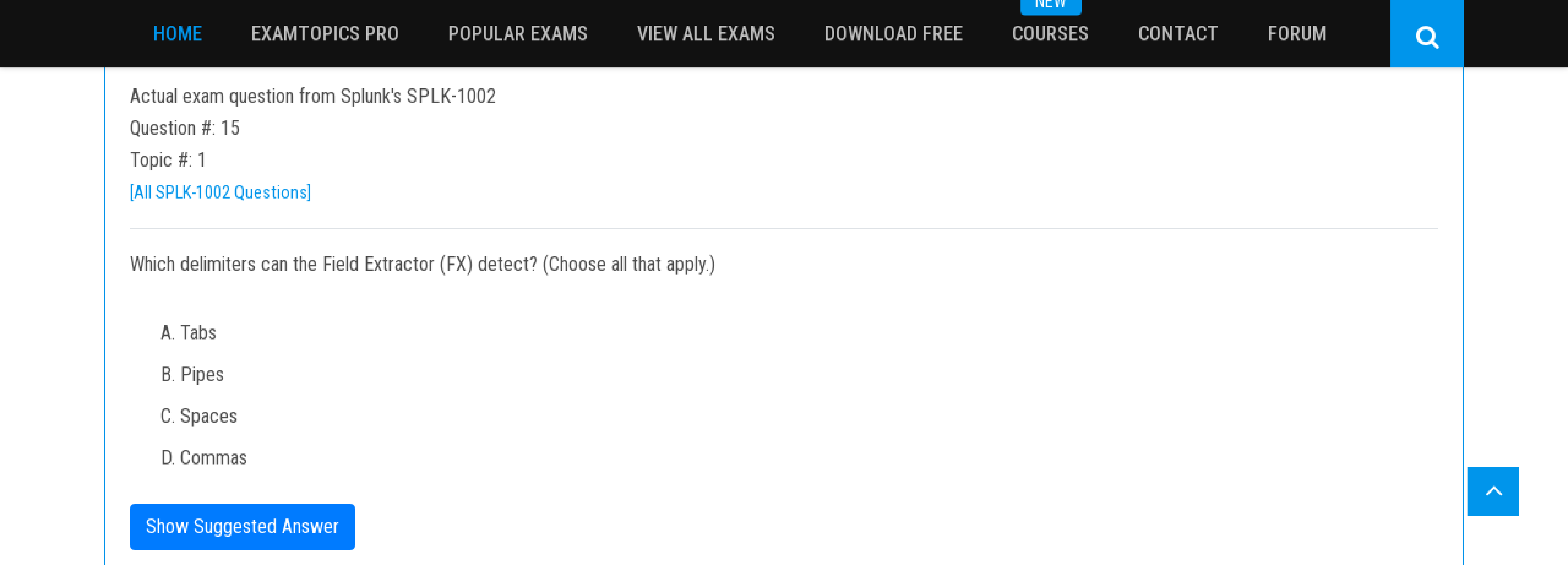
What do events in a transaction have in common?

A. All events in a transaction must have the same timestamp.

B. All events in a transaction must have the same sourcetype.

C. All events in a transaction must have the exact same set of fields.

D. All events in a transaction must be related by one or more fields.



Actual exam question from Splunk's SPLK-1002

Question #: 15

Topic #: 1

[All SPLK-1002 Questions]

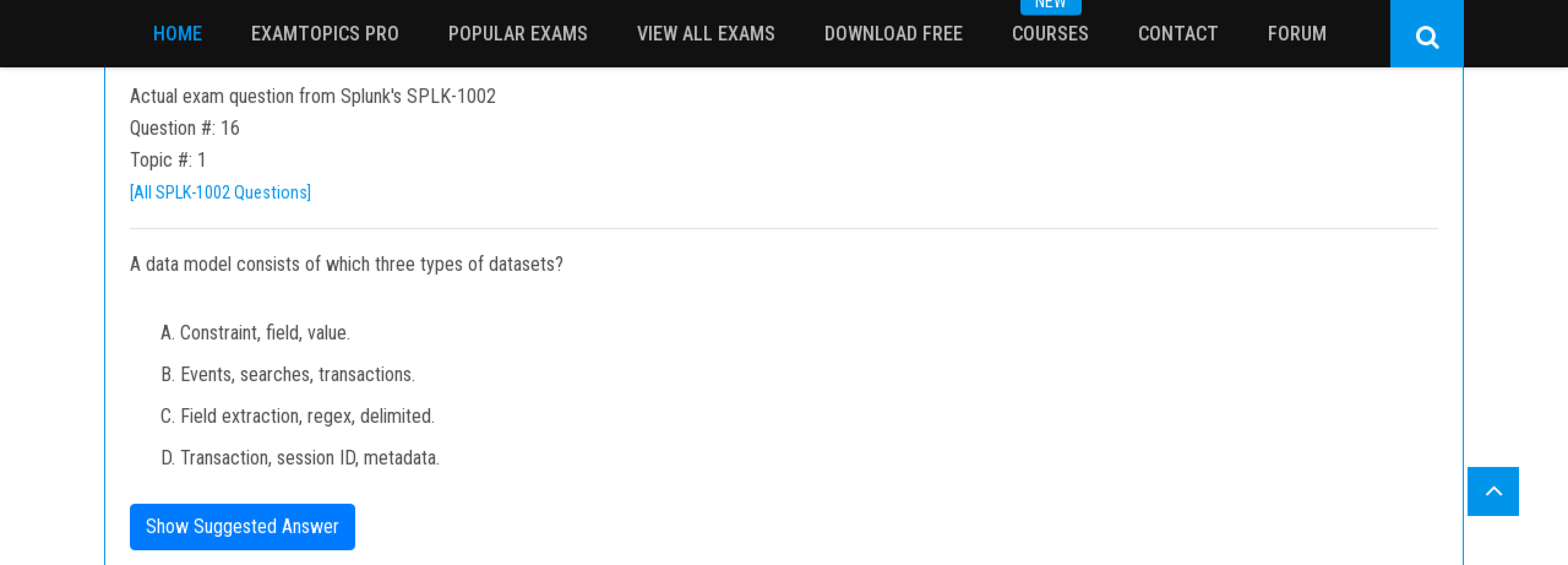
Which delimiters can the Field Extractor (FX) detect? (Choose all that apply.)

A. Tabs

B. Pipes

C. Spaces

D. Commas



Actual exam question from Splunk's SPLK-1002

Question #: 16

Topic #: 1

[All SPLK-1002 Questions]

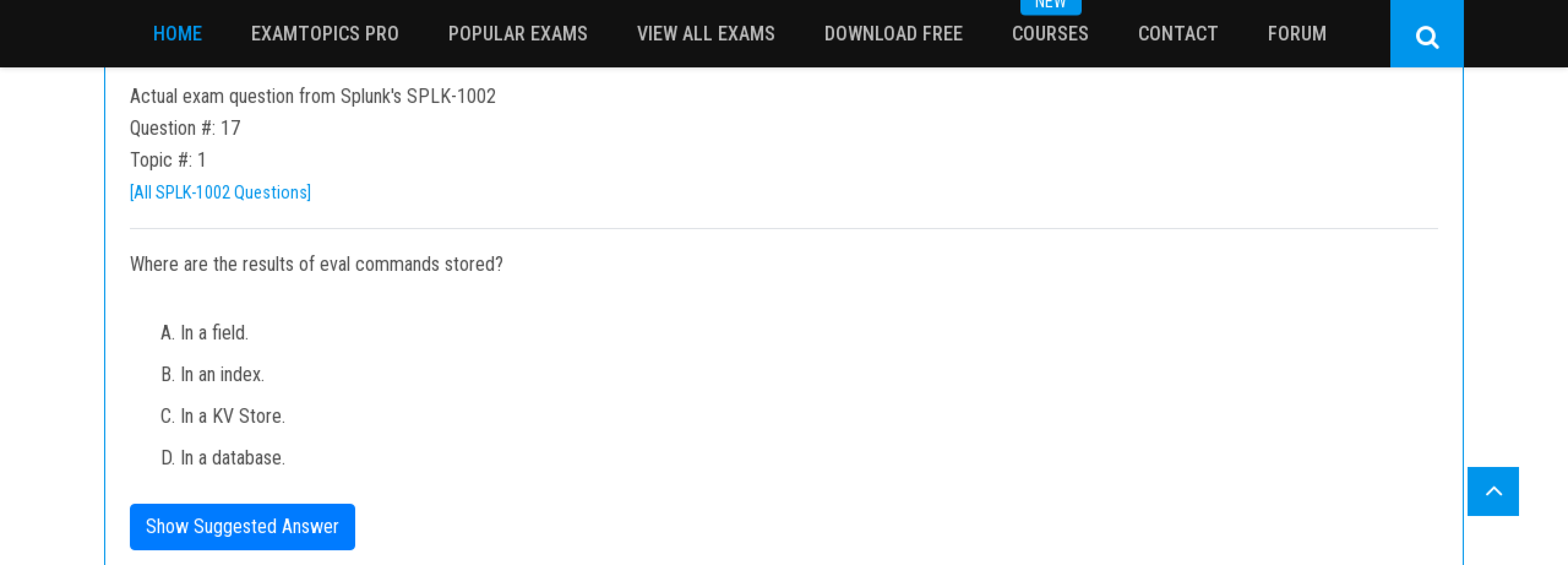
A data model consists of which three types of datasets?

A. Constraint, field, value.

B. Events, searches, transactions.

C. Field extraction, regex, delimited.

D. Transaction, session ID, metadata.



Actual exam question from Splunk's SPLK-1002

Question #: 17

Topic #: 1

[All SPLK-1002 Questions]

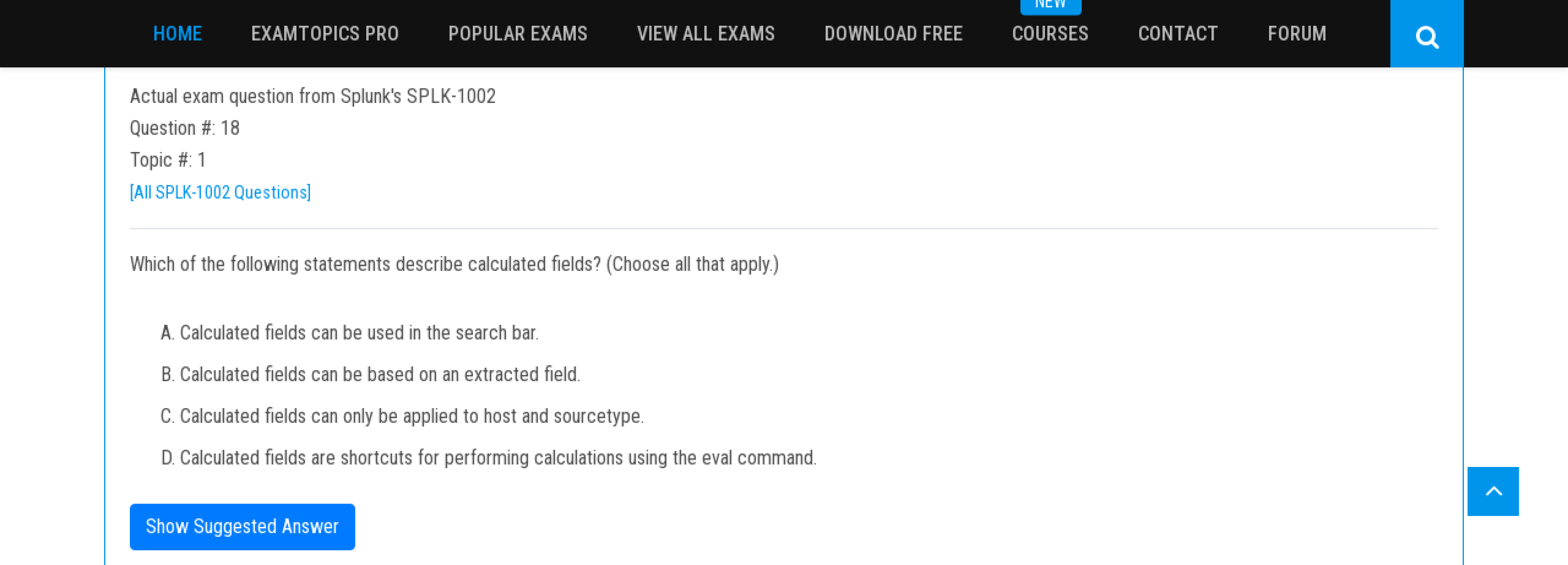
Where are the results of eval commands stored?

A. In a field.

B. In an index.

C. In a KV Store.

D. In a database.



Actual exam question from Splunk's SPLK-1002

Question #: 18

Topic #: 1

[All SPLK-1002 Questions]

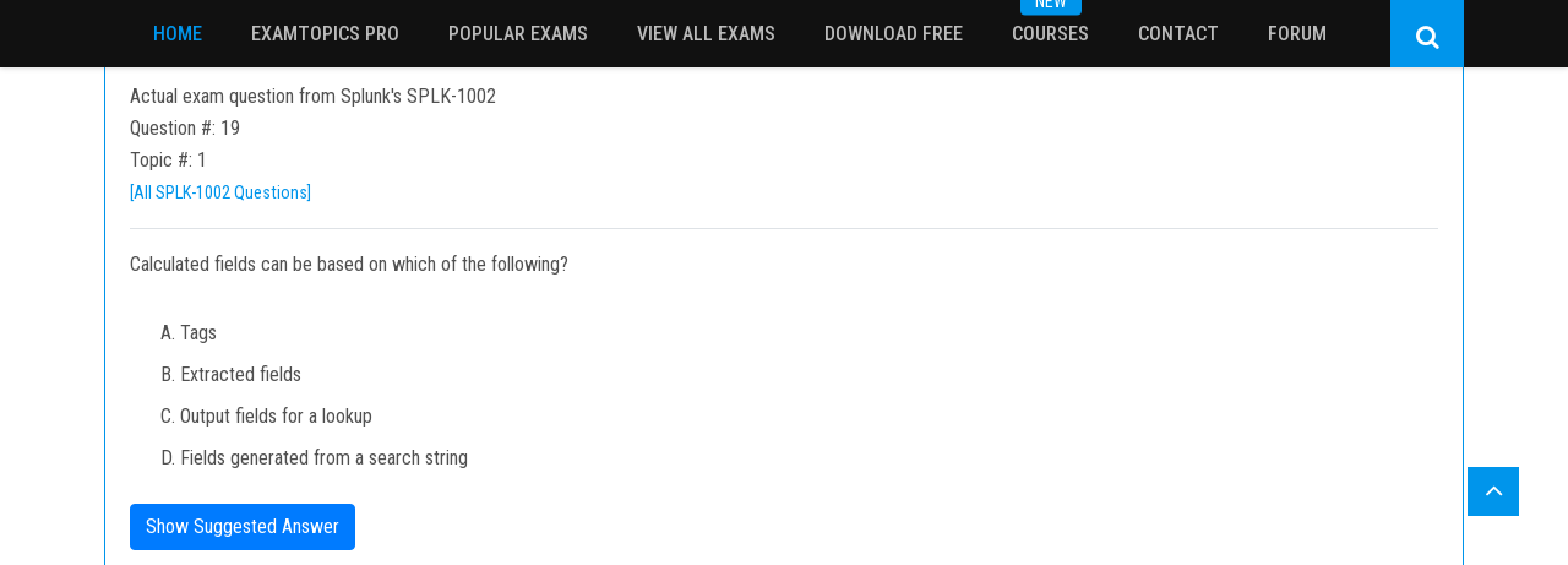
Which of the following statements describe calculated fields? (Choose all that apply.)

A. Calculated fields can be used in the search bar.

B. Calculated fields can be based on an extracted field.

C. Calculated fields can only be applied to host and sourcetype.

D. Calculated fields are shortcuts for performing calculations using the eval command.



Actual exam question from Splunk's SPLK-1002

Question #: 19

Topic #: 1

[All SPLK-1002 Questions]

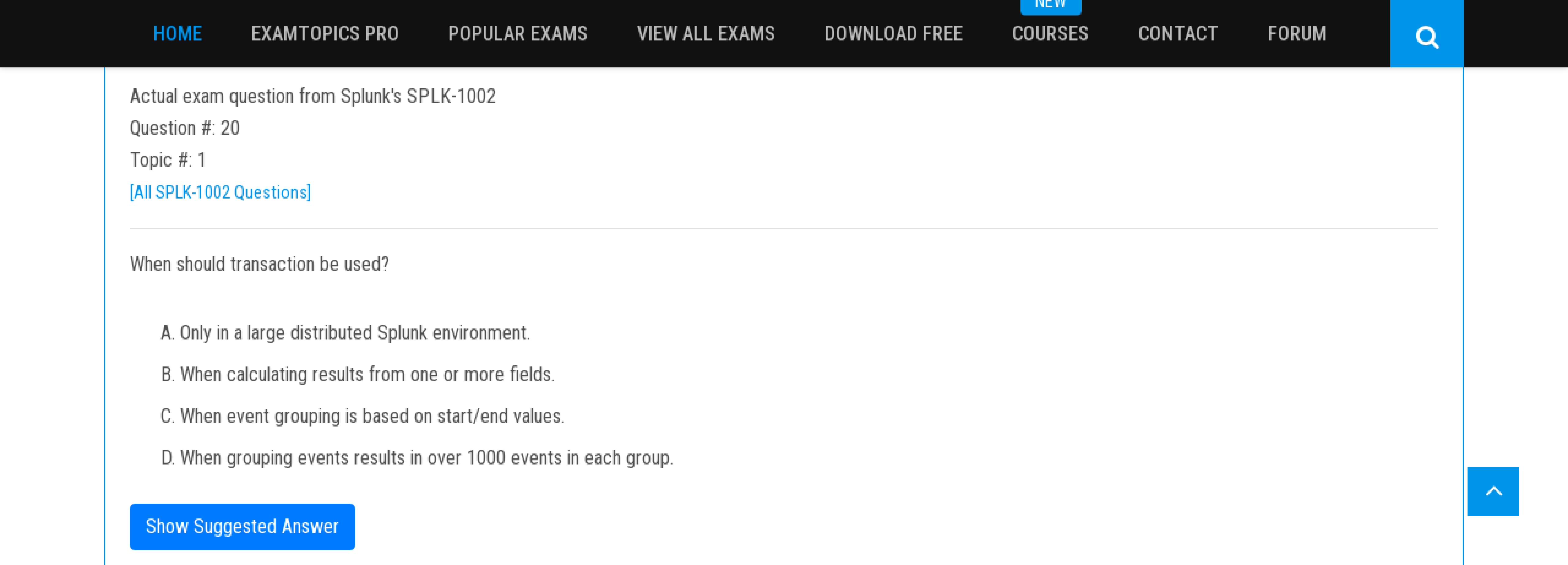
Calculated fields can be based on which of the following?

A. Tags

B. Extracted fields

C. Output fields for a lookup

D. Fields generated from a search string



Actual exam question from Splunk's SPLK-1002

Question #: 20

Topic #: 1

[All SPLK-1002 Questions]

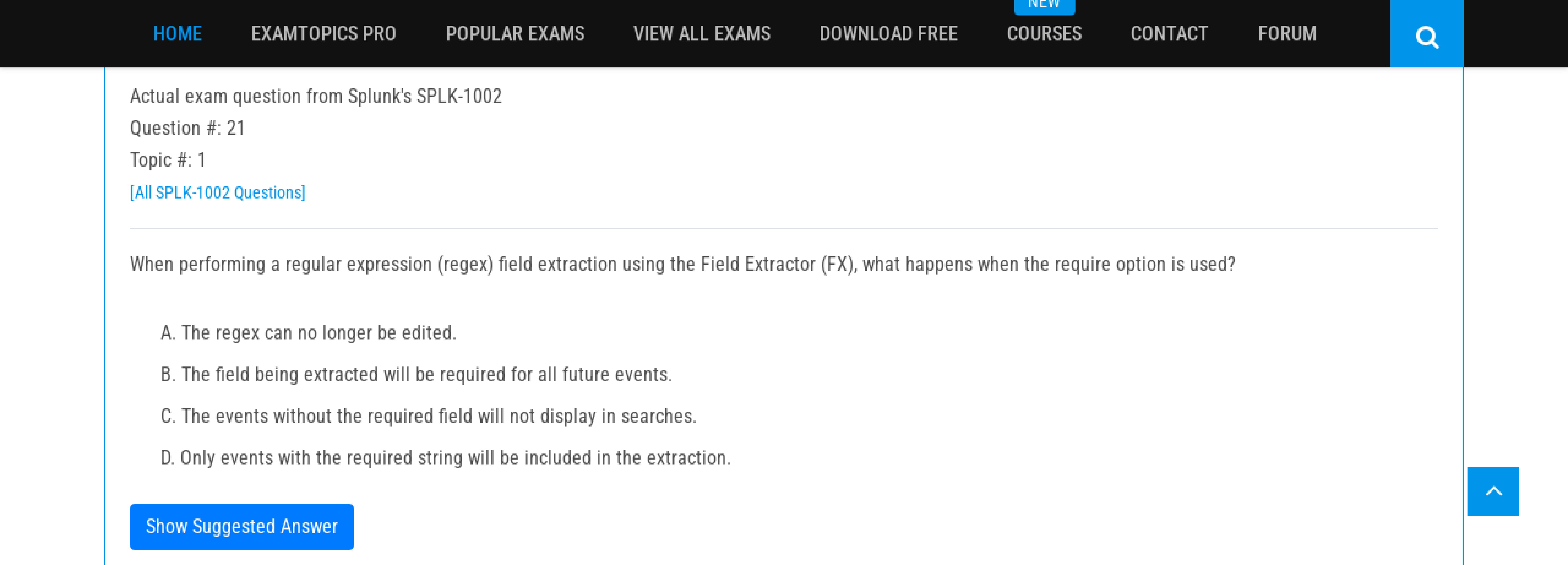
When should transaction be used?

A. Only in a large distributed Splunk environment.

B. When calculating results from one or more fields.

C. When event grouping is based on start/end values.

D. When grouping events results in over 1000 events in each group.



Actual exam question from Splunk's SPLK-1002

Question #: 21

Topic #: 1

[All SPLK-1002 Questions]

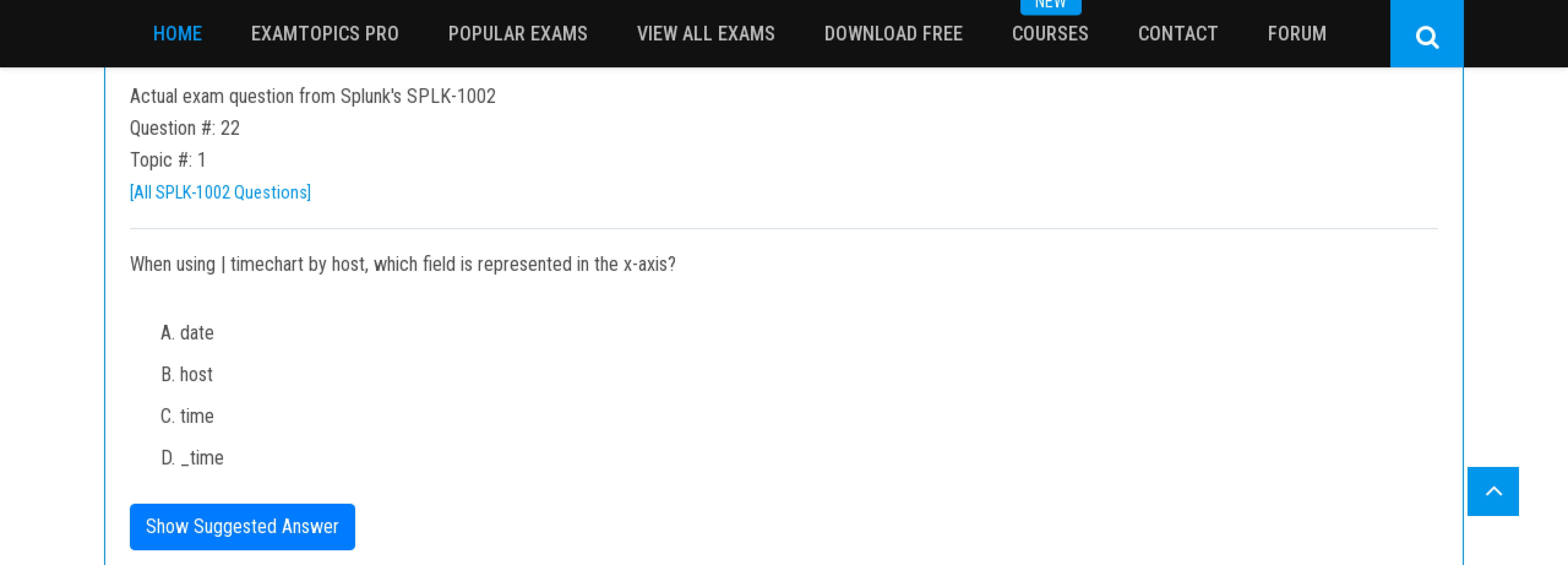
When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.

B. The field being extracted will be required for all future events.

C. The events without the required field will not display in searches.

D. Only events with the required string will be included in the extraction.



Actual exam question from Splunk's SPLK-1002

Question #: 22

Topic #: 1

[All SPLK-1002 Questions]

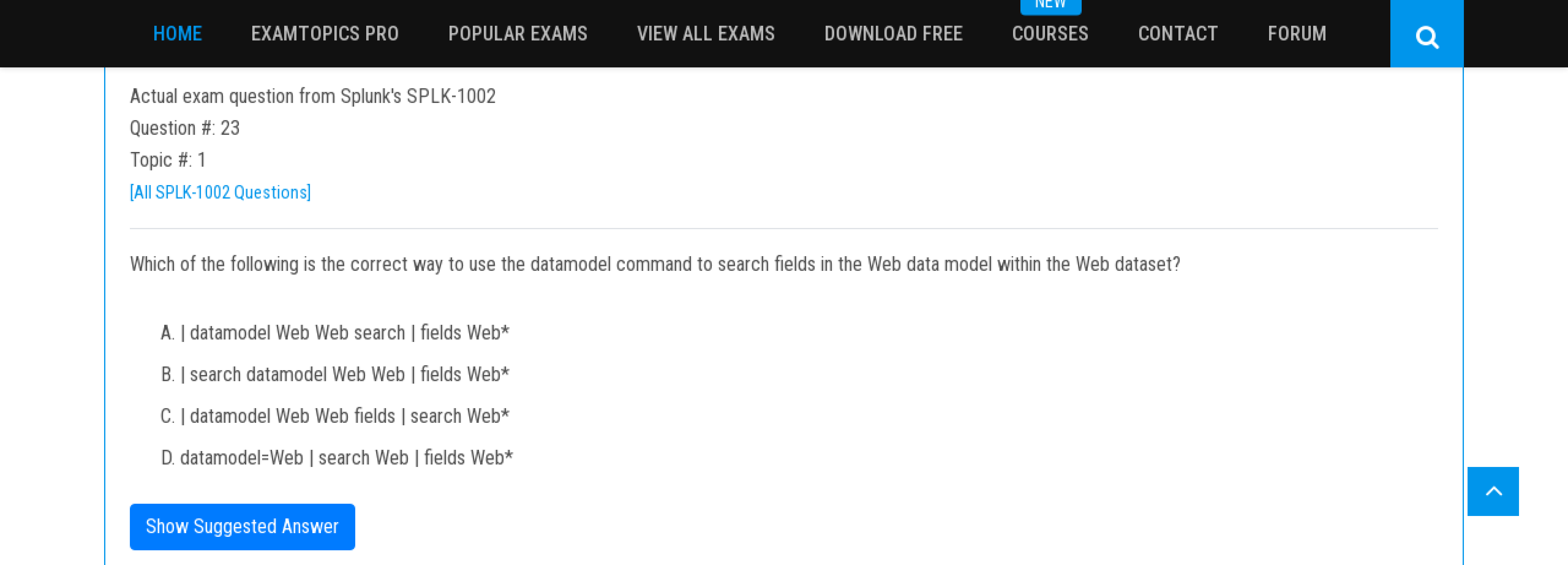
When using | timechart by host, which field is represented in the x-axis?

A. date

B. host

C. time

D. _time



Actual exam question from Splunk's SPLK-1002

Question #: 23

Topic #: 1

[All SPLK-1002 Questions]

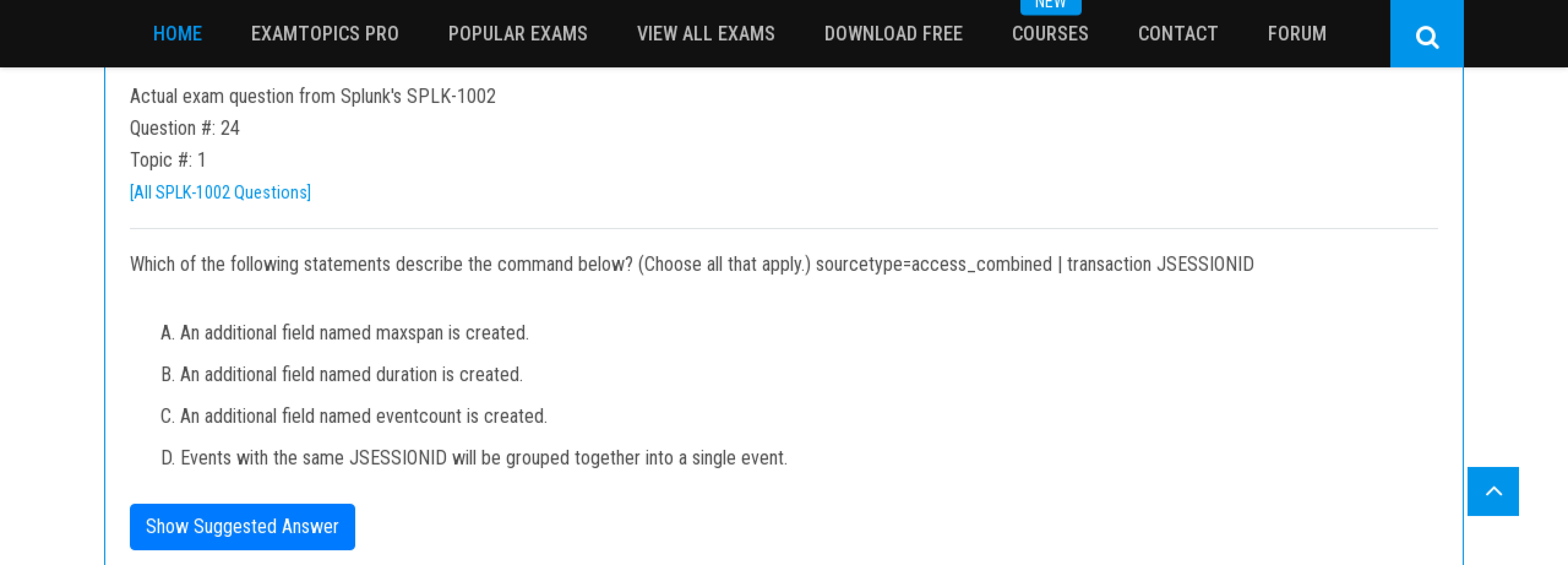
Which of the following is the correct way to use the datamodel command to search fields in the Web data model within the Web dataset?

A. | datamodel Web Web search | fields Web*

B. | search datamodel Web Web | fields Web*

C. | datamodel Web Web fields | search Web*

D. datamodel=Web | search Web | fields Web*



Actual exam question from Splunk's SPLK-1002

Question #: 24

Topic #: 1

[All SPLK-1002 Questions]

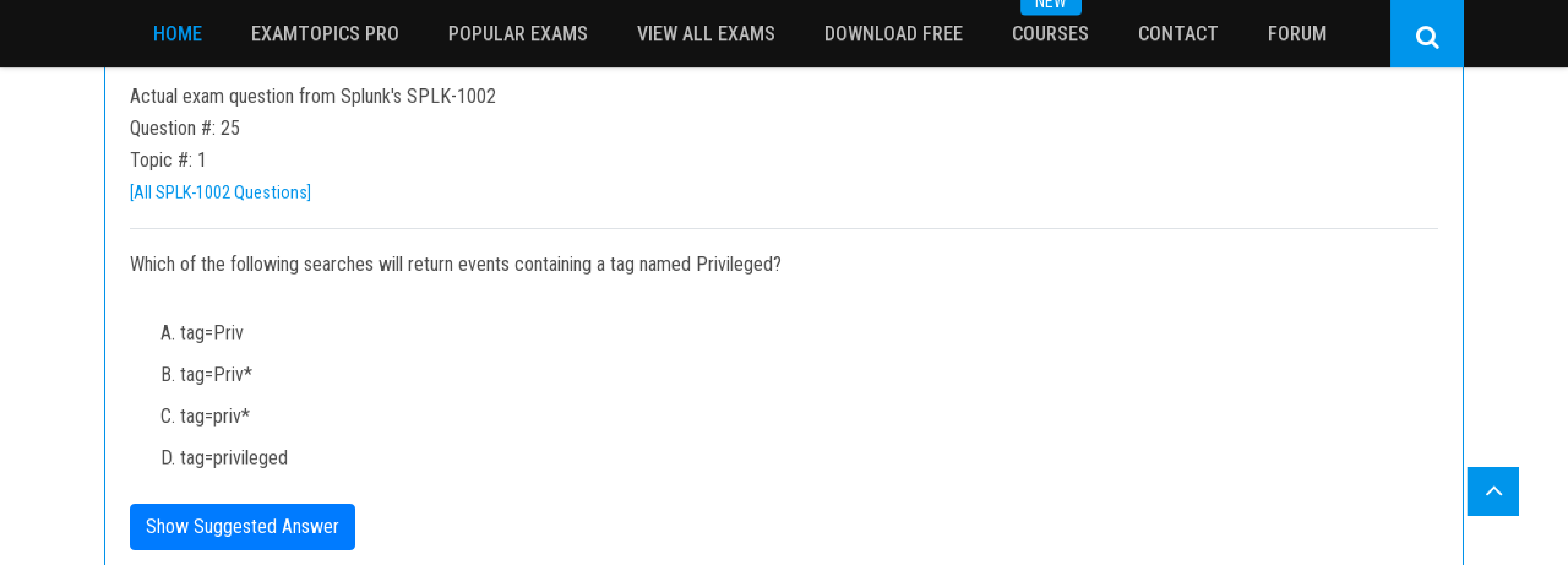
Which of the following statements describe the command below? (Choose all that apply.) sourcetype=access_combined | transaction JSESSIONID

A. An additional field named maxspan is created.

B. An additional field named duration is created.

C. An additional field named eventcount is created.

D. Events with the same JSESSIONID will be grouped together into a single event.



Actual exam question from Splunk's SPLK-1002

Question #: 25

Topic #: 1

[All SPLK-1002 Questions]

Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv

B. tag=Priv*

C. tag=priv*

D. tag=privileged

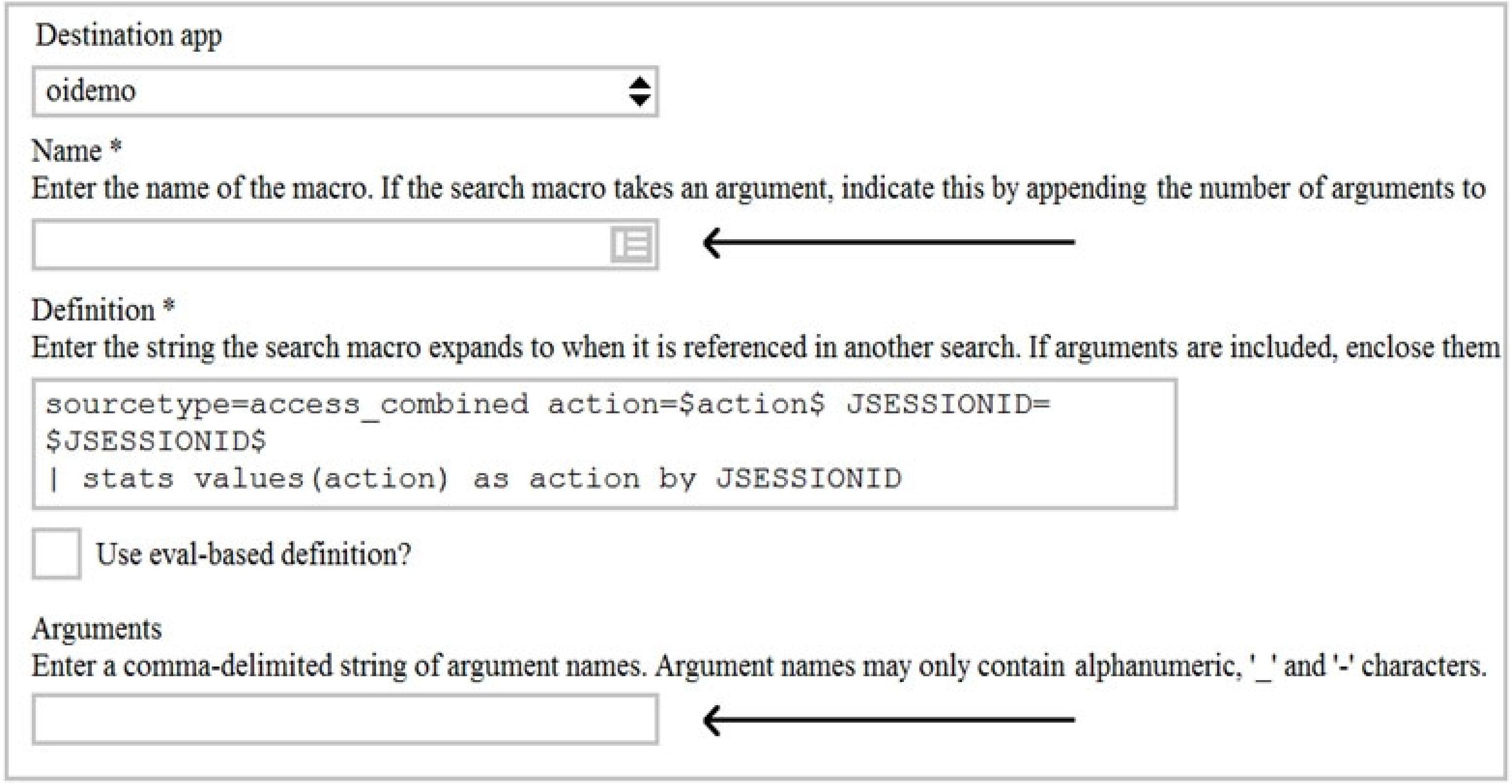
Actual exam question from Splunk's SPLK-1002

Question #: 26

Topic #: 1

[All SPLK-1002 Questions]

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configure the macro?



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.

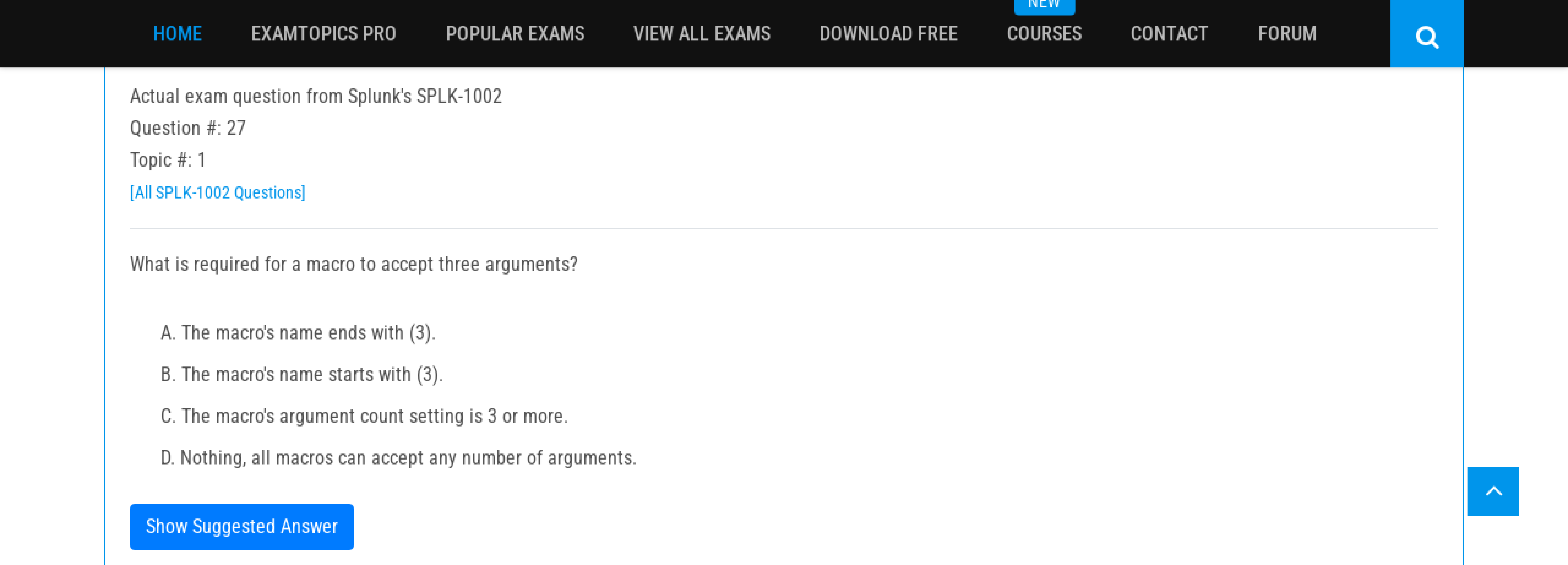
A. The macro name is sessiontracker and the arguments are action, JESSIONID.

B. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

C. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.

D. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 27

Topic #: 1

[All SPLK-1002 Questions]

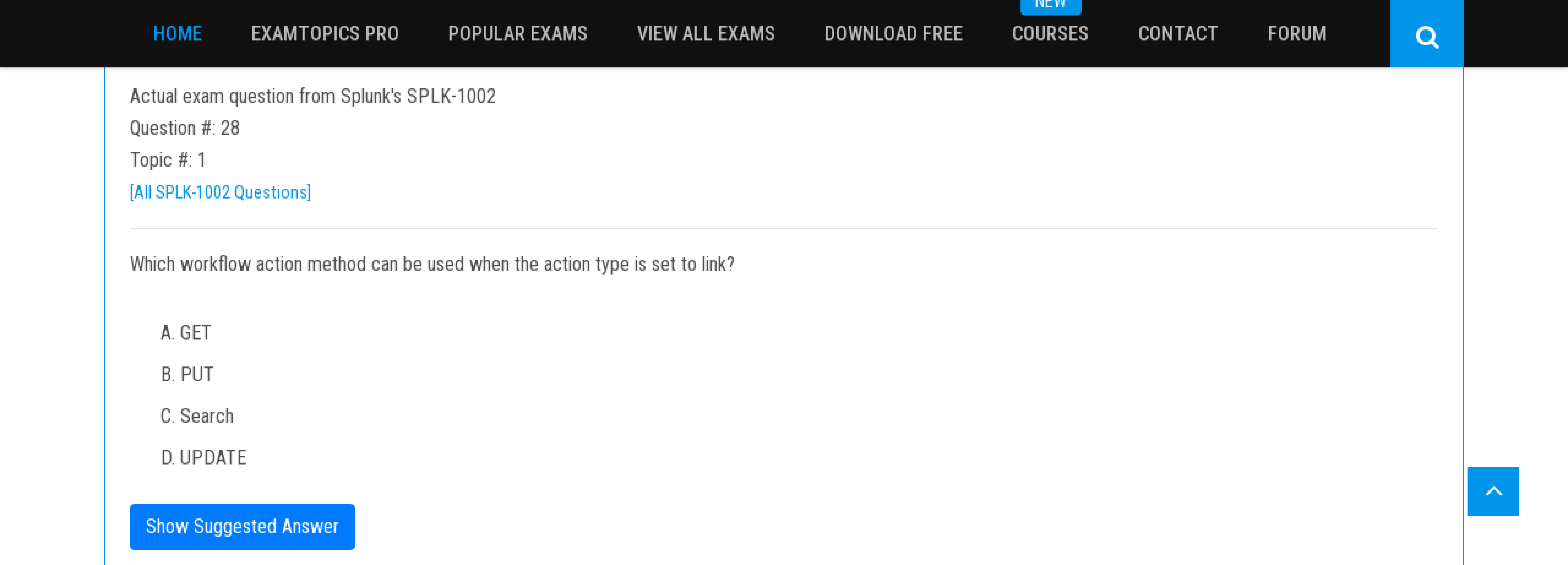
What is required for a macro to accept three arguments?

A. The macro's name ends with (3).

B. The macro's name starts with (3).

C. The macro's argument count setting is 3 or more.

D. Nothing, all macros can accept any number of arguments.



Actual exam question from Splunk's SPLK-1002

Question #: 28

Topic #: 1

[All SPLK-1002 Questions]

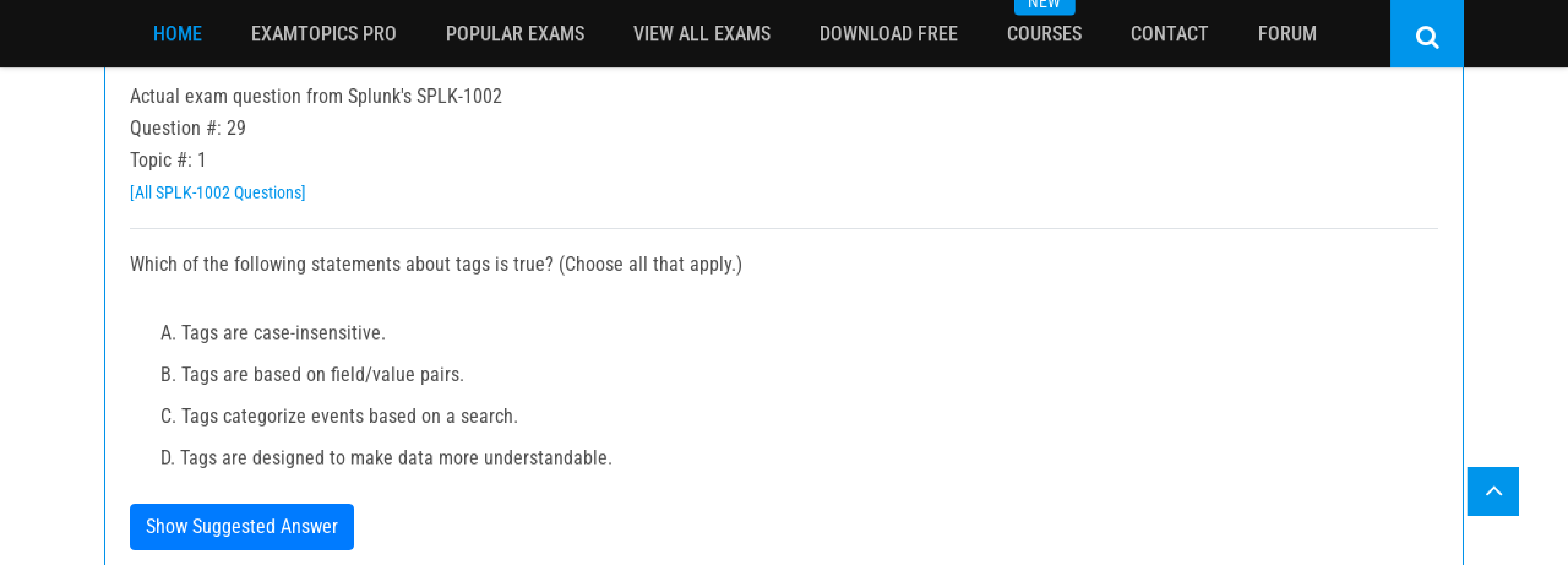
Which workflow action method can be used when the action type is set to link?

A. GET

B. PUT

C. Search

D. UPDATE



Actual exam question from Splunk's SPLK-1002

Question #: 29

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements about tags is true? (Choose all that apply.)

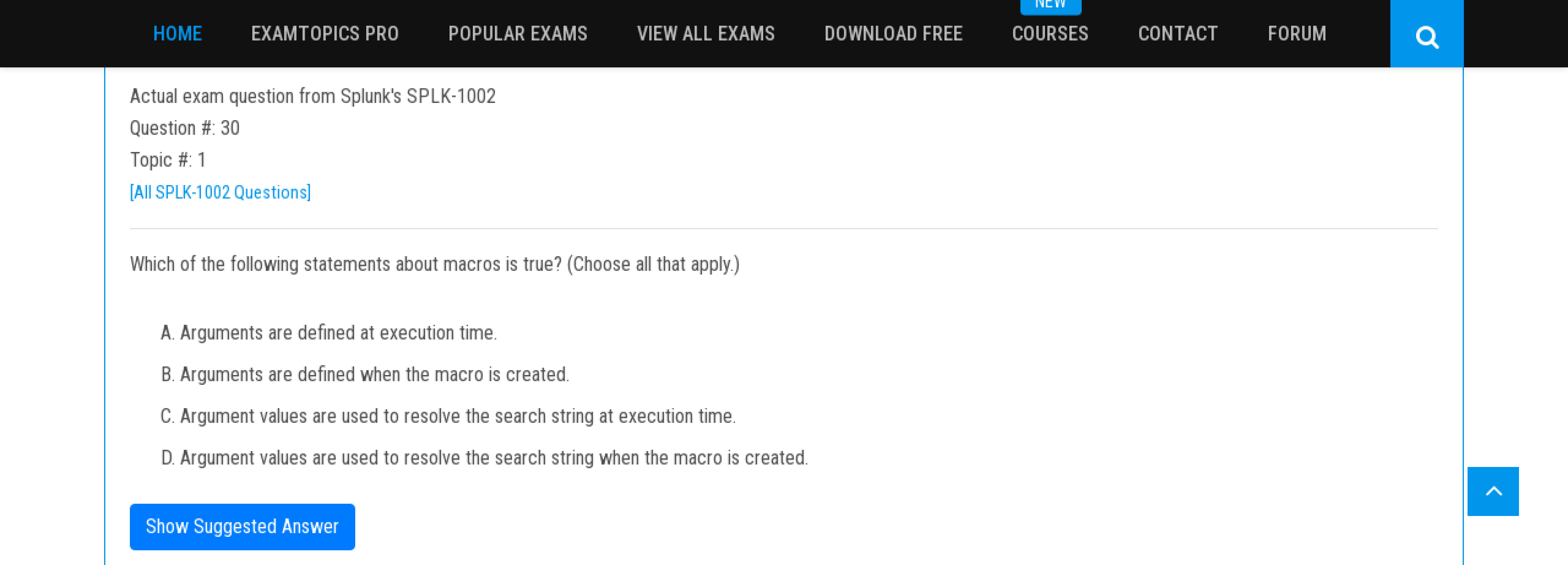
A. Tags are case-insensitive.

B. Tags are based on field/value pairs.

C. Tags categorize events based on a search.

D. Tags are designed to make data more understandable.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 30

Topic #: 1

[All SPLK-1002 Questions]

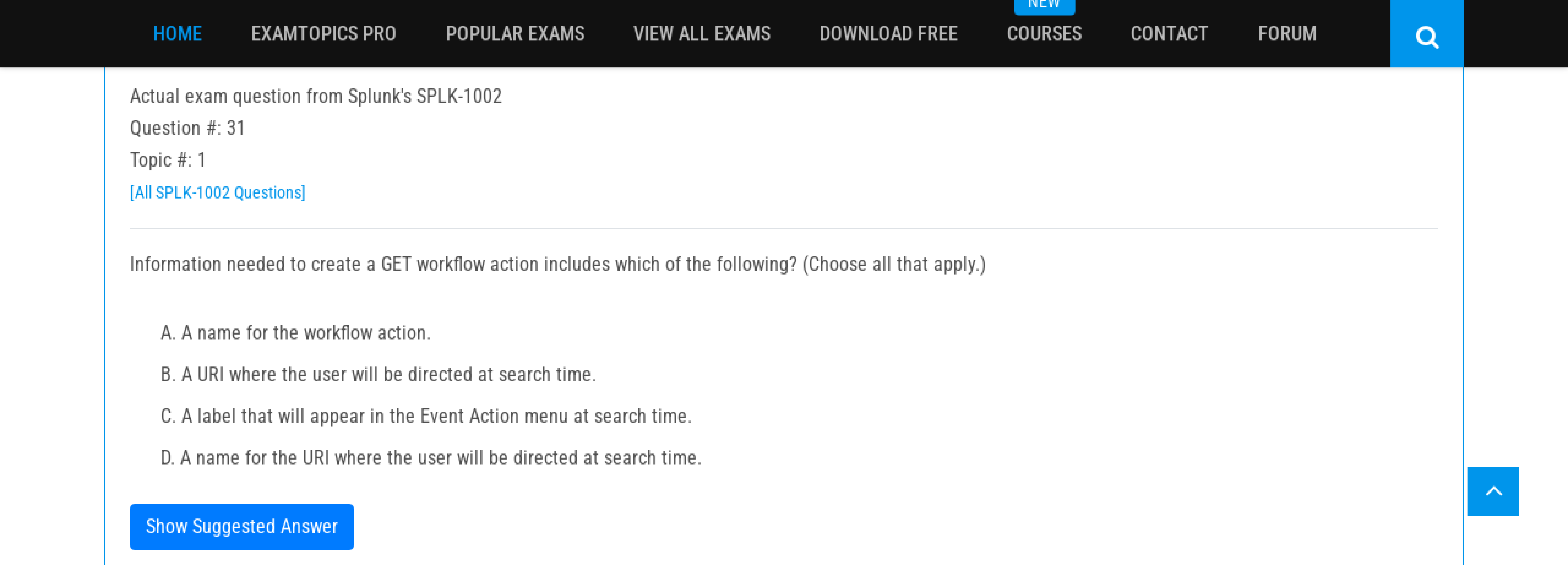
Which of the following statements about macros is true? (Choose all that apply.)

A. Arguments are defined at execution time.

B. Arguments are defined when the macro is created.

C. Argument values are used to resolve the search string at execution time.

D. Argument values are used to resolve the search string when the macro is created.



Actual exam question from Splunk's SPLK-1002

Question #: 31

Topic #: 1

[All SPLK-1002 Questions]

Information needed to create a GET workflow action includes which of the following? (Choose all that apply.)

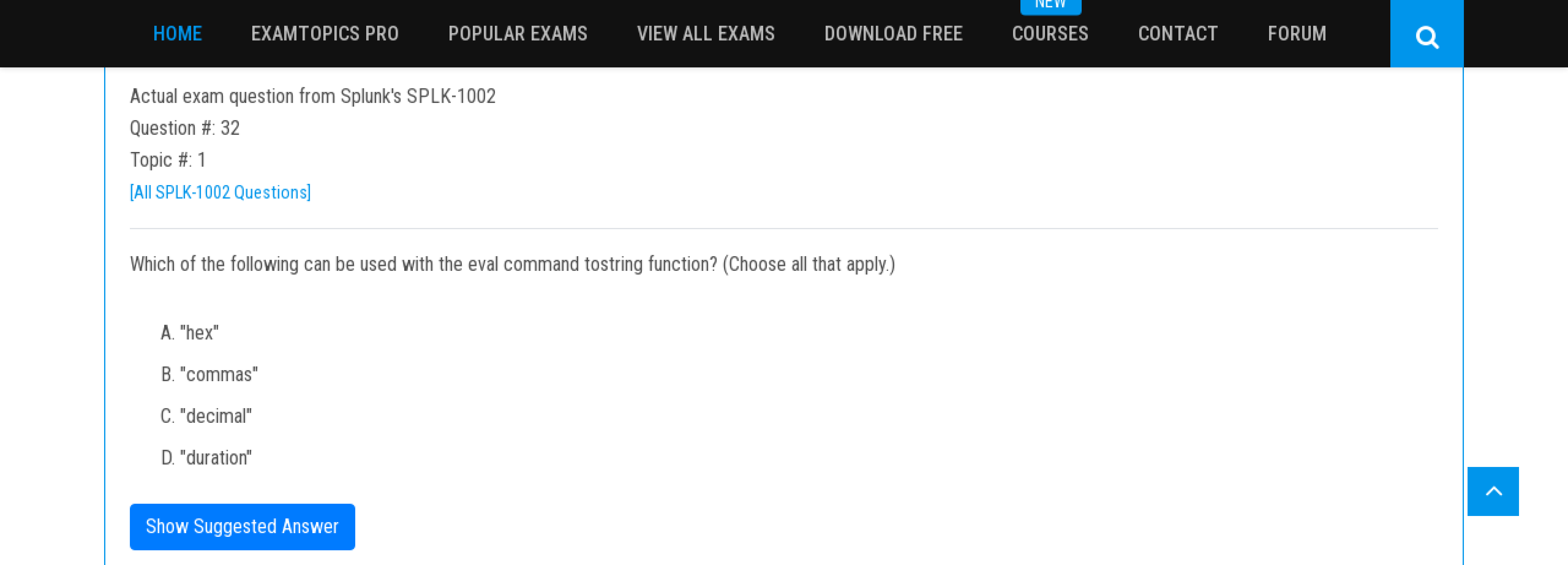
A. A name for the workflow action.

B. A URI where the user will be directed at search time.

C. A label that will appear in the Event Action menu at search time.

D. A name for the URI where the user will be directed at search time.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 32

Topic #: 1

[All SPLK-1002 Questions]

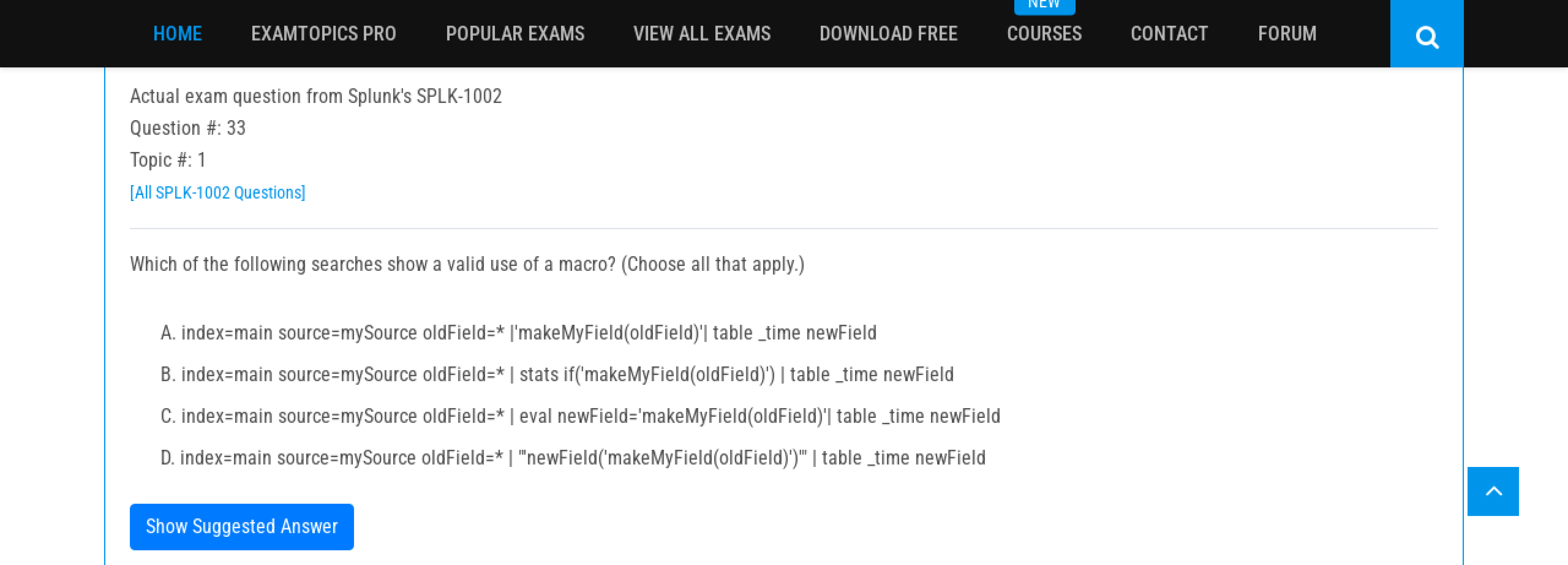
Which of the following can be used with the eval command tostring function? (Choose all that apply.)

A. "hex"

B. "commas"

C. "decimal"

D. "duration"



Actual exam question from Splunk's SPLK-1002

Question #: 33

Topic #: 1

[All SPLK-1002 Questions]

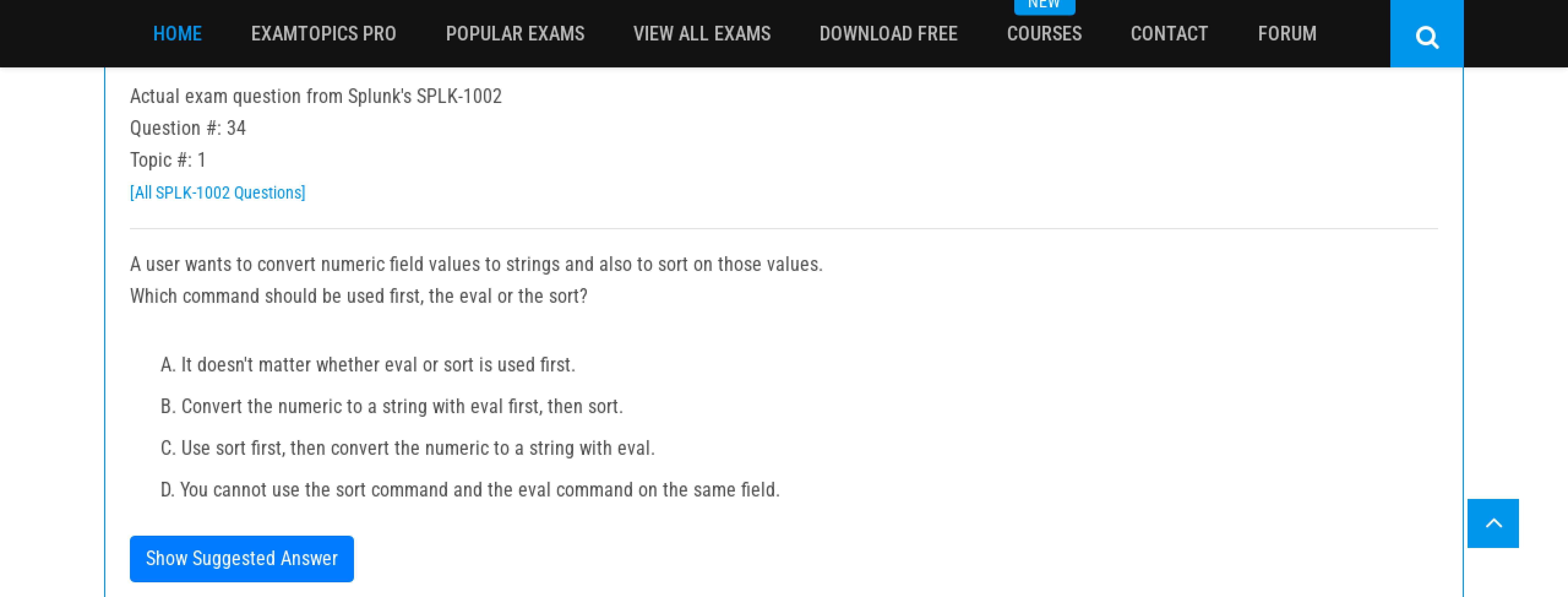
Which of the following searches show a valid use of a macro? (Choose all that apply.)

A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField

B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField

C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField

D. index=main source=mySource oldField=* | "newField('makeMyField(oldField)')'" | table _time newField



Actual exam question from Splunk's SPLK-1002

Question #: 34

Topic #: 1

[All SPLK-1002 Questions]

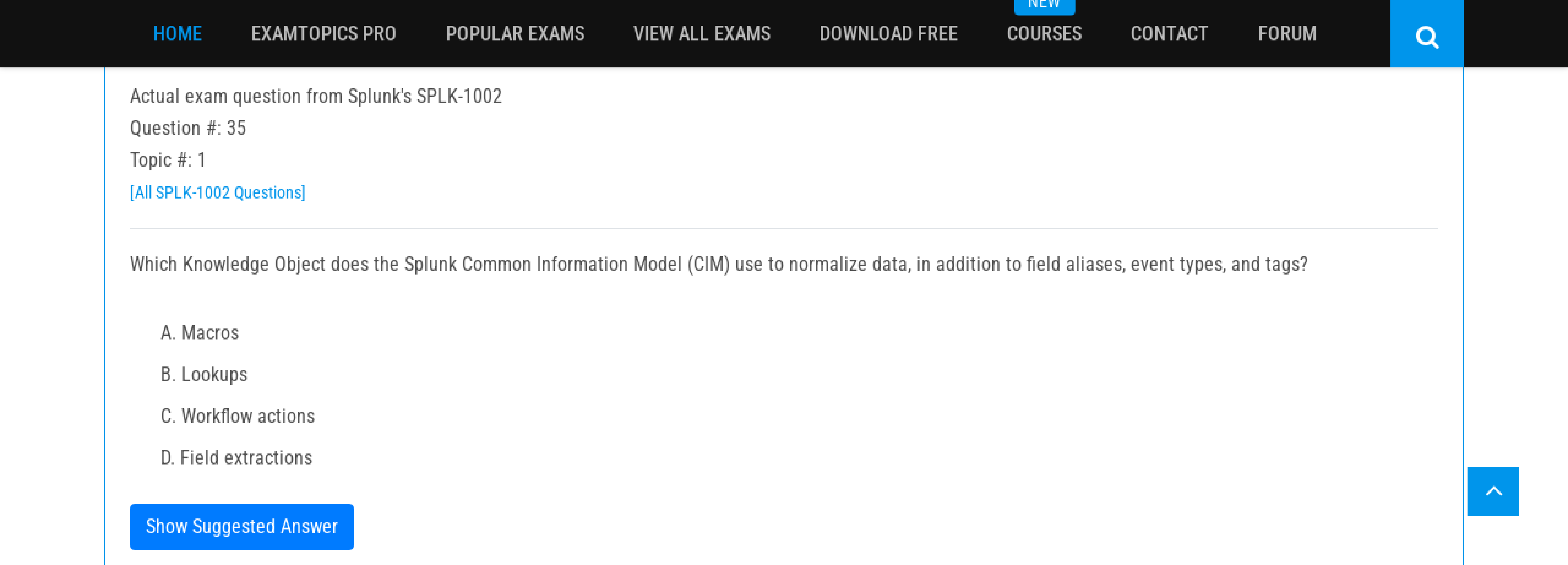
A user wants to convert numeric field values to strings and also to sort on those values.
Which command should be used first, the eval or the sort?

A. It doesn't matter whether eval or sort is used first.

B. Convert the numeric to a string with eval first, then sort.

C. Use sort first, then convert the numeric to a string with eval.

D. You cannot use the sort command and the eval command on the same field.



Actual exam question from Splunk's SPLK-1002

Question #: 35

Topic #: 1

[All SPLK-1002 Questions]

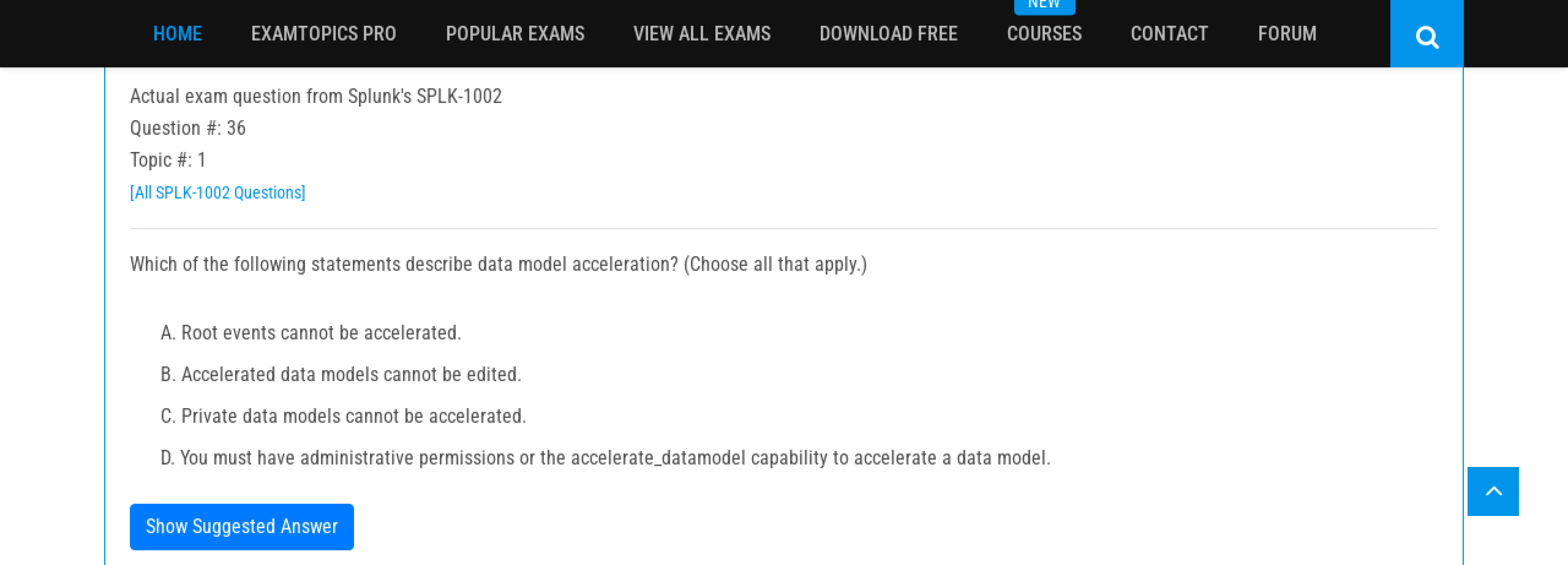
Which Knowledge Object does the Splunk Common Information Model (CIM) use to normalize data, in addition to field aliases, event types, and tags?

A. Macros

B. Lookups

C. Workflow actions

D. Field extractions



Actual exam question from Splunk's SPLK-1002

Question #: 36

Topic #: 1

[All SPLK-1002 Questions]

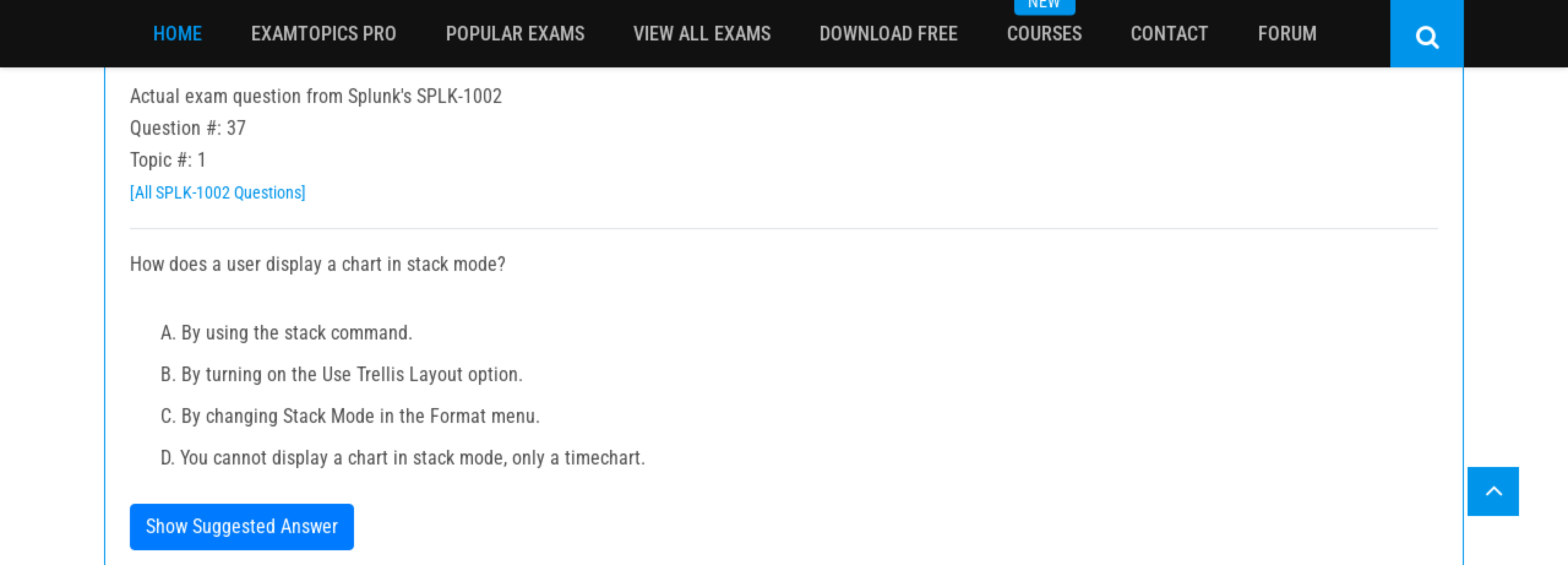
Which of the following statements describe data model acceleration? (Choose all that apply.)

A. Root events cannot be accelerated.

B. Accelerated data models cannot be edited.

C. Private data models cannot be accelerated.

D. You must have administrative permissions or the accelerate_datamodel capability to accelerate a data model.



Actual exam question from Splunk's SPLK-1002

Question #: 37

Topic #: 1

[All SPLK-1002 Questions]

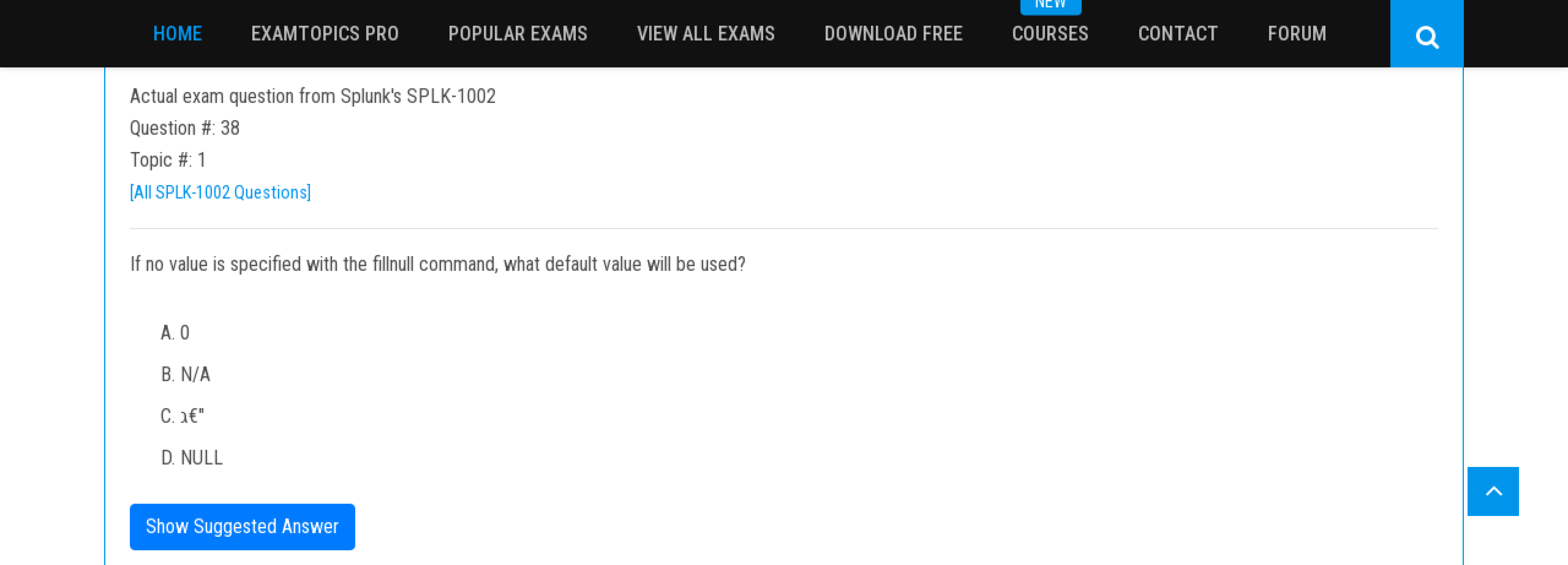
How does a user display a chart in stack mode?

A. By using the stack command.

B. By turning on the Use Trellis Layout option.

C. By changing Stack Mode in the Format menu.

D. You cannot display a chart in stack mode, only a timechart.



Actual exam question from Splunk's SPLK-1002

Question #: 38

Topic #: 1

[All SPLK-1002 Questions]

If no value is specified with the fillnull command, what default value will be used?

A. 0

B. N/A

C. ג€"

D. NULL

Show Suggested Answer

Actual exam question from Splunk's SPLK-1002

Question #: 39

Topic #: 1

[All SPLK-1002 Questions]

What other syntax will produce exactly the same results as | chart count over vendor_action by user?

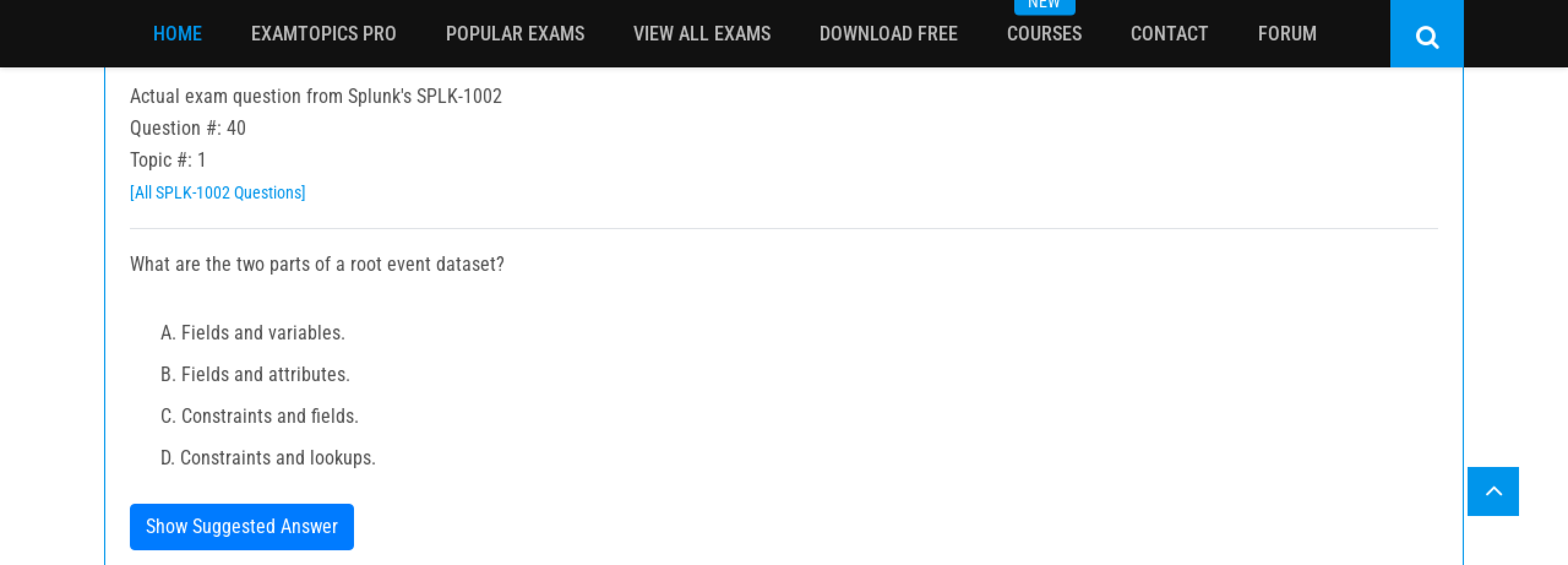
A. | chart count by vendor_action, user

B. | chart count over vendor_action, user

C. | chart count by vendor_action over user

D. | chart count over user by vendor_action

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 40

Topic #: 1

[All SPLK-1002 Questions]

What are the two parts of a root event dataset?

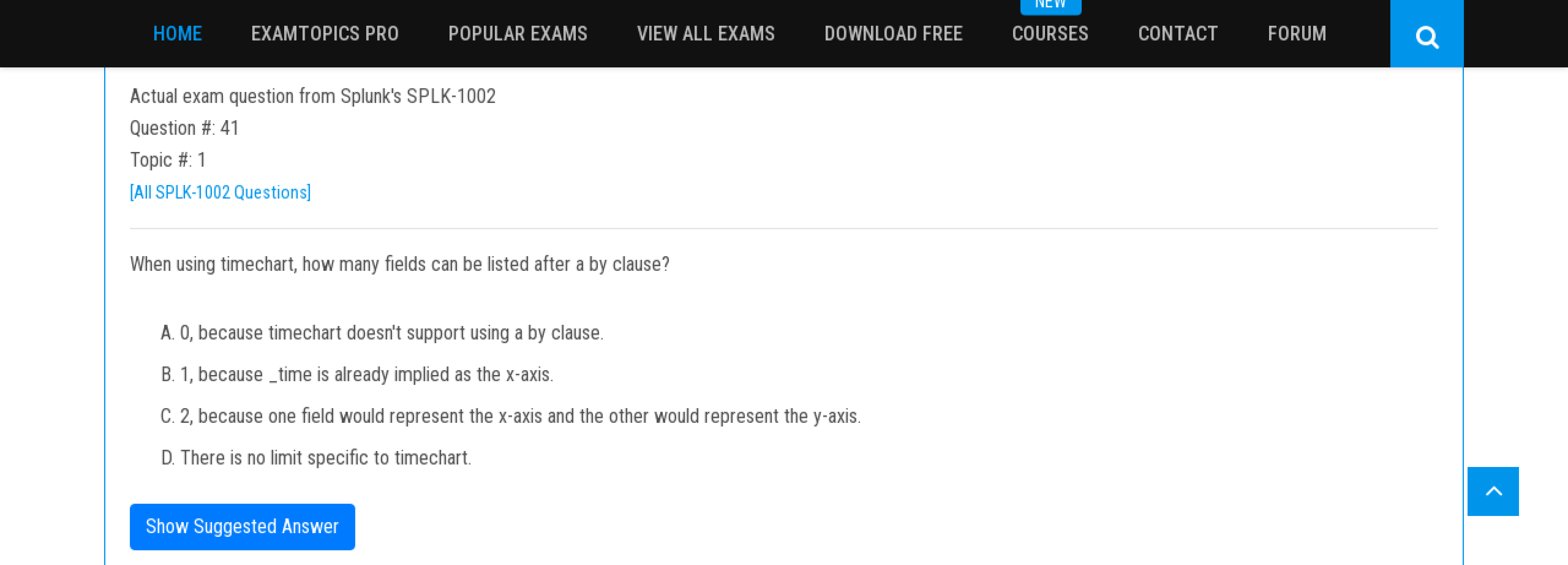
A. Fields and variables.

B. Fields and attributes.

C. Constraints and fields.

D. Constraints and lookups.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 41

Topic #: 1

[All SPLK-1002 Questions]

When using timechart, how many fields can be listed after a by clause?

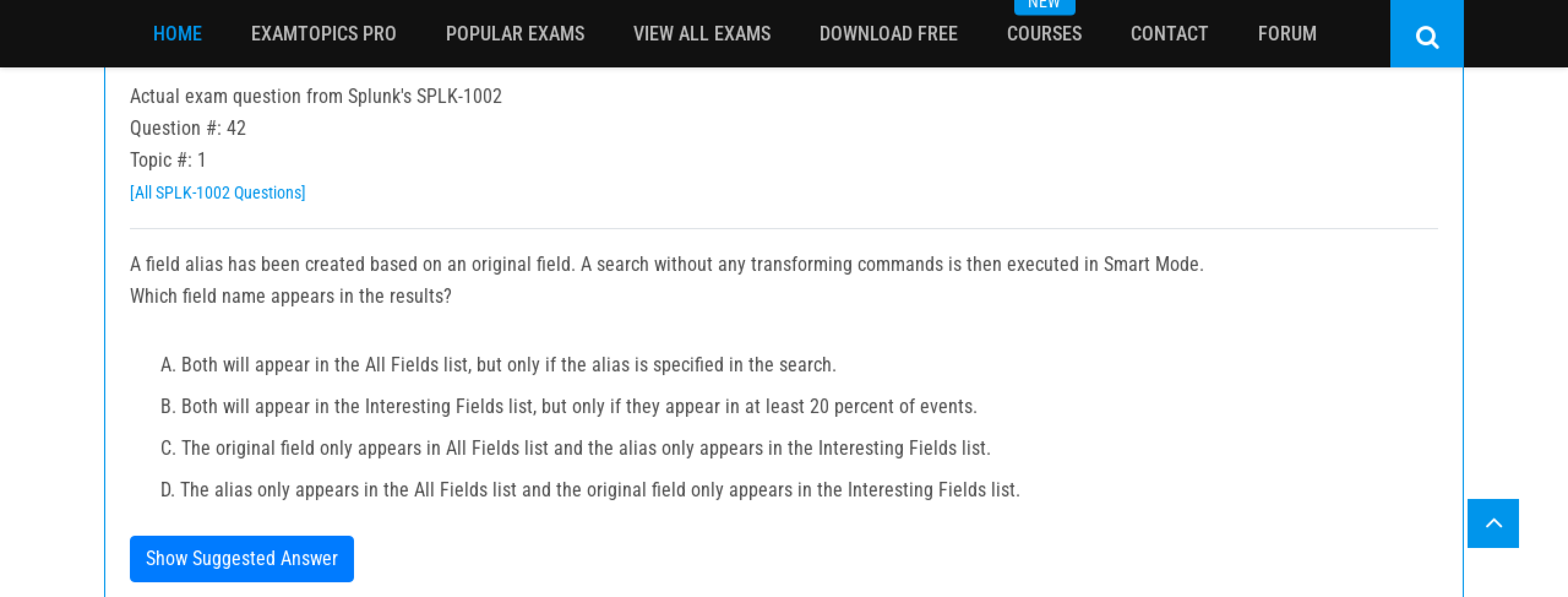
A. 0, because timechart doesn't support using a by clause.

B. 1, because _time is already implied as the x-axis.

C. 2, because one field would represent the x-axis and the other would represent the y-axis.

D. There is no limit specific to timechart.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 42

Topic #: 1

[All SPLK-1002 Questions]

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode.

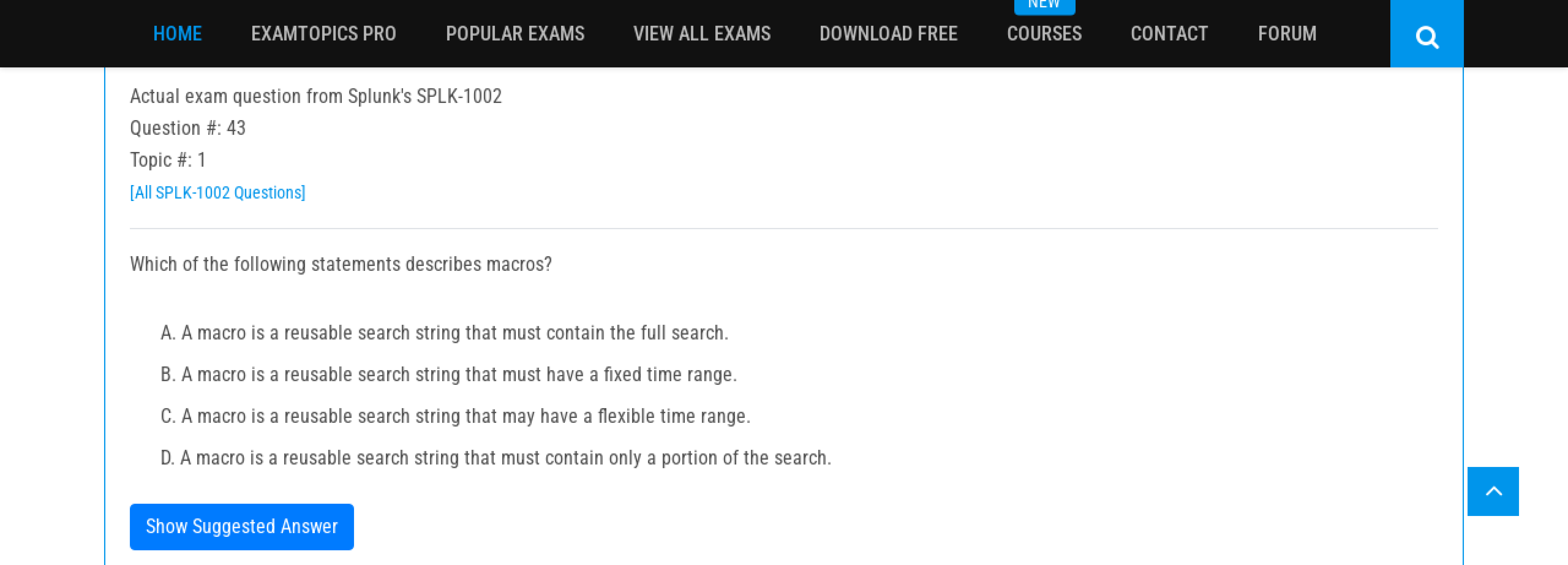
Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.

B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.

C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.

D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.



Actual exam question from Splunk's SPLK-1002

Question #: 43

Topic #: 1

[All SPLK-1002 Questions]

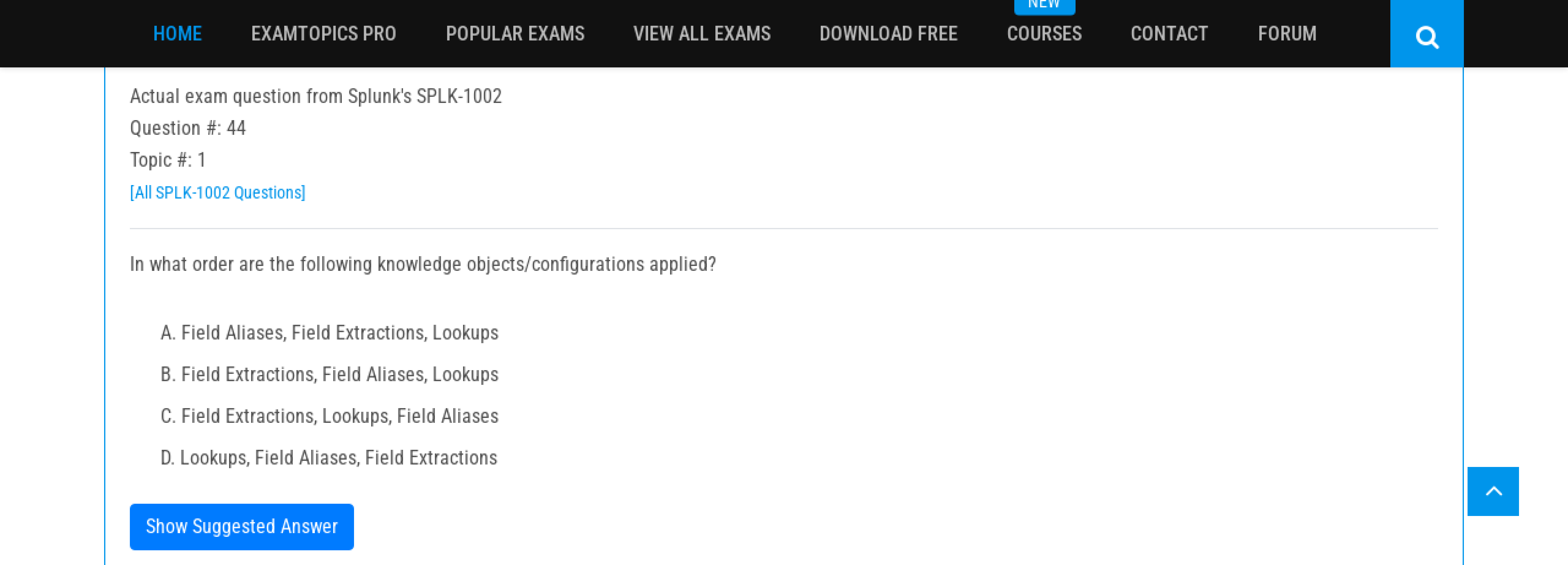
Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.

B. A macro is a reusable search string that must have a fixed time range.

C. A macro is a reusable search string that may have a flexible time range.

D. A macro is a reusable search string that must contain only a portion of the search.



Actual exam question from Splunk's SPLK-1002

Question #: 44

Topic #: 1

[All SPLK-1002 Questions]

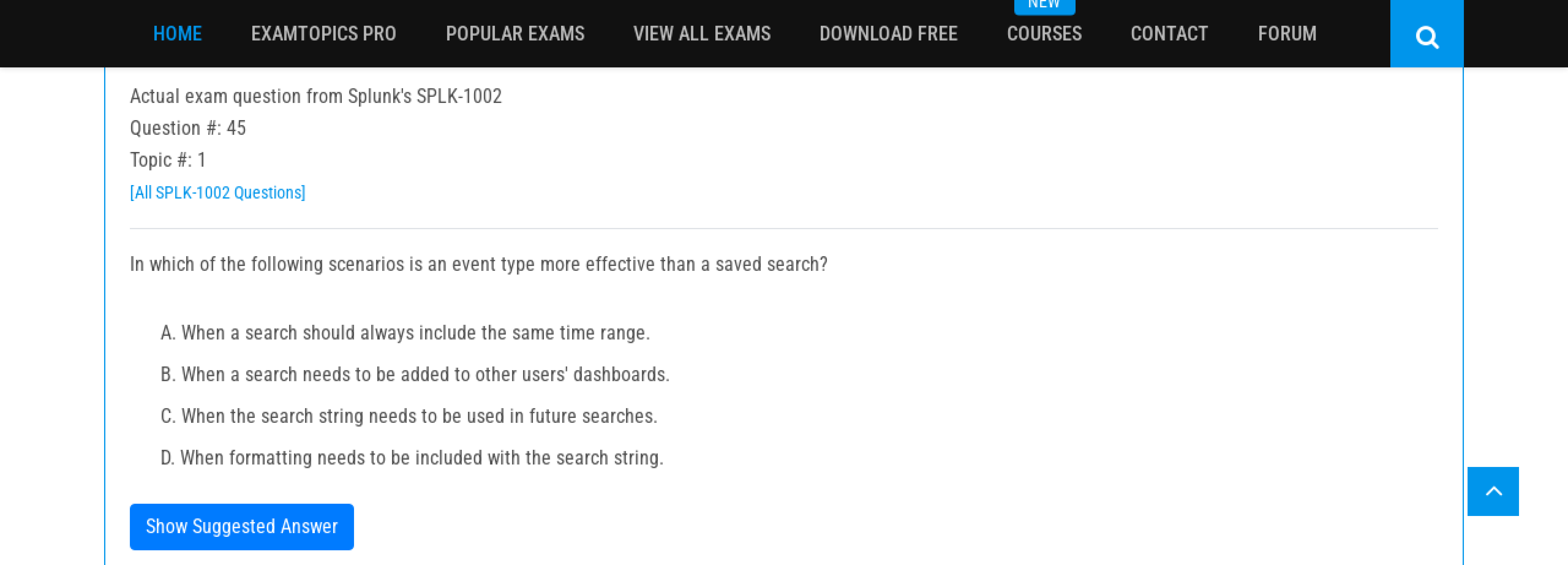
In what order are the following knowledge objects/configurations applied?

A. Field Aliases, Field Extractions, Lookups

B. Field Extractions, Field Aliases, Lookups

C. Field Extractions, Lookups, Field Aliases

D. Lookups, Field Aliases, Field Extractions



Actual exam question from Splunk's SPLK-1002

Question #: 45

Topic #: 1

[All SPLK-1002 Questions]

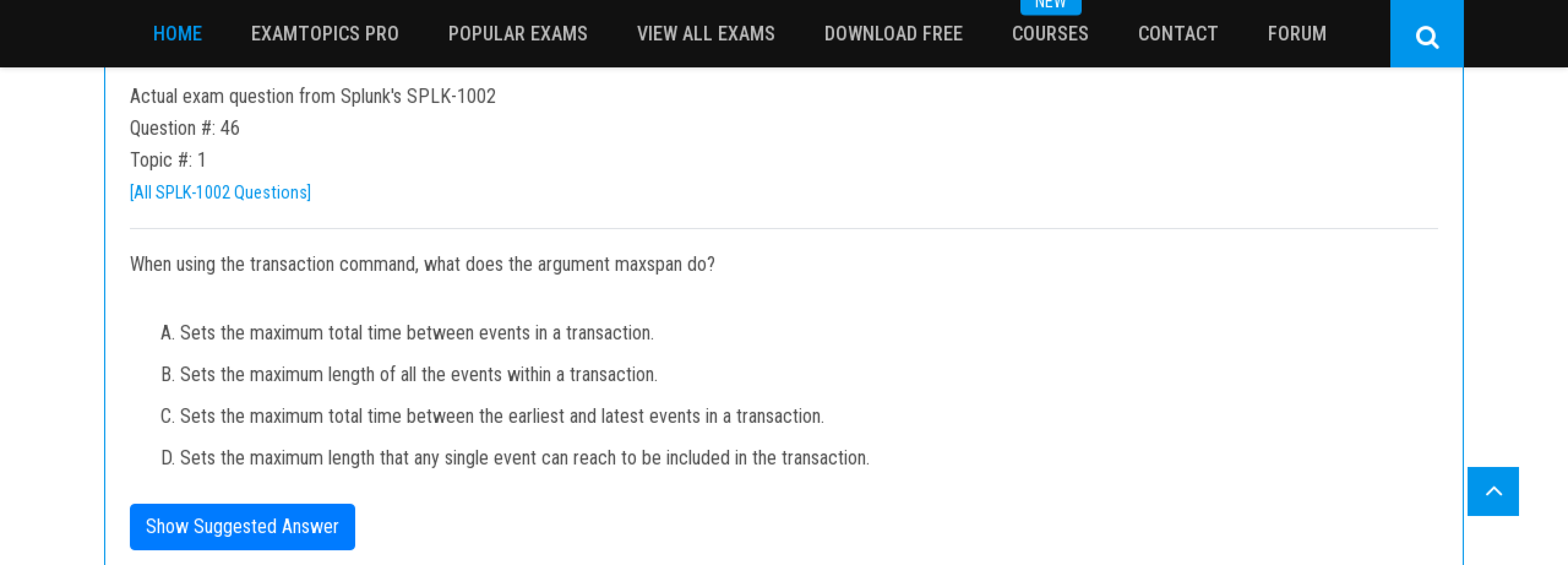
In which of the following scenarios is an event type more effective than a saved search?

A. When a search should always include the same time range.

B. When a search needs to be added to other users' dashboards.

C. When the search string needs to be used in future searches.

D. When formatting needs to be included with the search string.



Actual exam question from Splunk's SPLK-1002

Question #: 46

Topic #: 1

[All SPLK-1002 Questions]

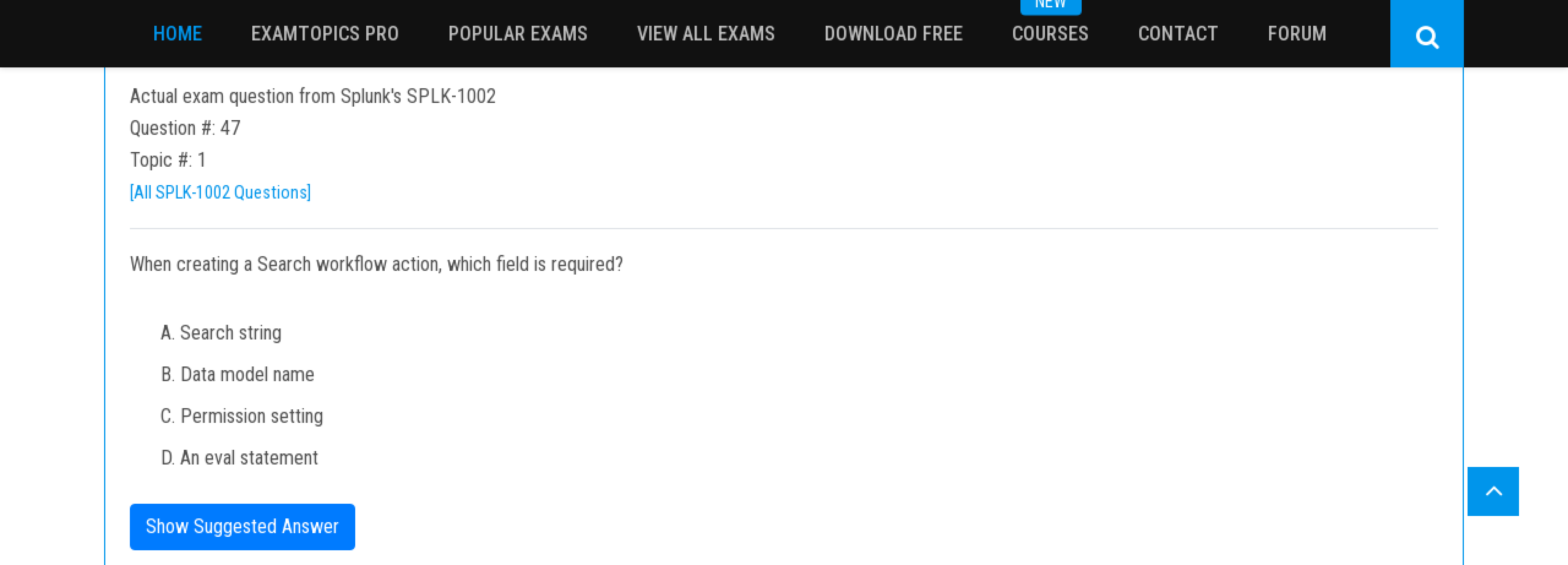
When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.

B. Sets the maximum length of all the events within a transaction.

C. Sets the maximum total time between the earliest and latest events in a transaction.

D. Sets the maximum length that any single event can reach to be included in the transaction.



Actual exam question from Splunk's SPLK-1002

Question #: 47

Topic #: 1

[All SPLK-1002 Questions]

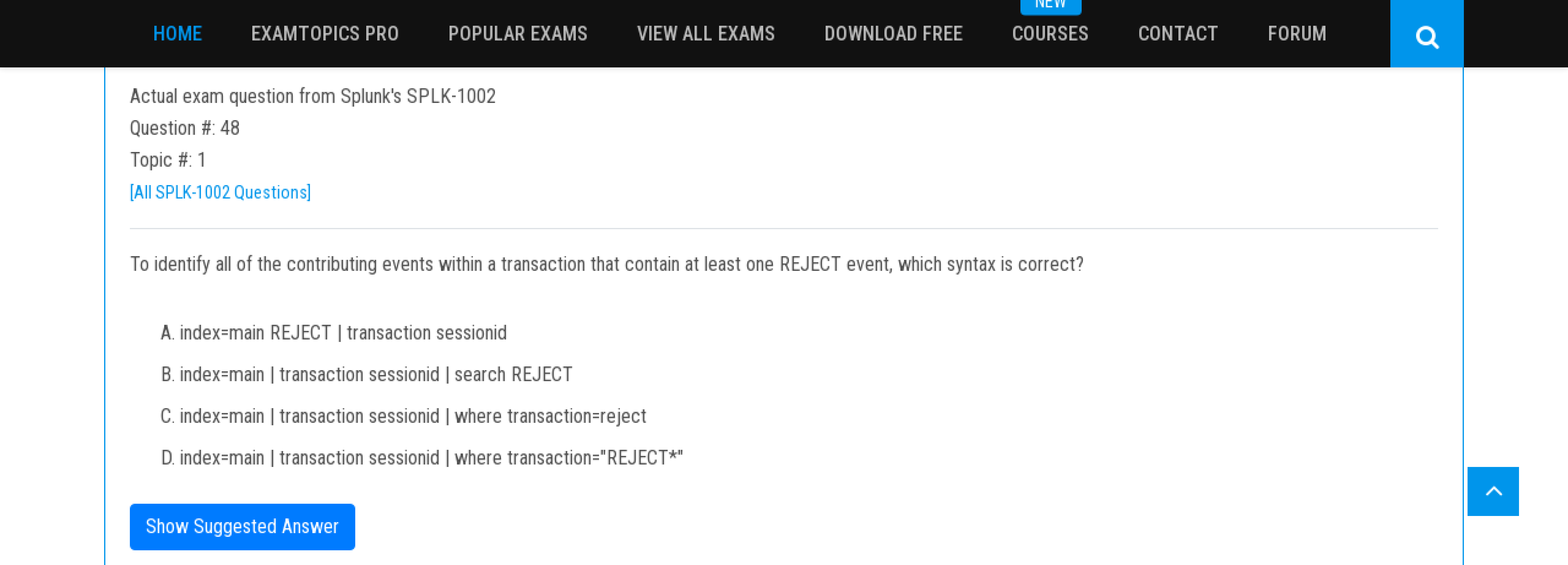
When creating a Search workflow action, which field is required?

A. Search string

B. Data model name

C. Permission setting

D. An eval statement



Actual exam question from Splunk's SPLK-1002

Question #: 48

Topic #: 1

[All SPLK-1002 Questions]

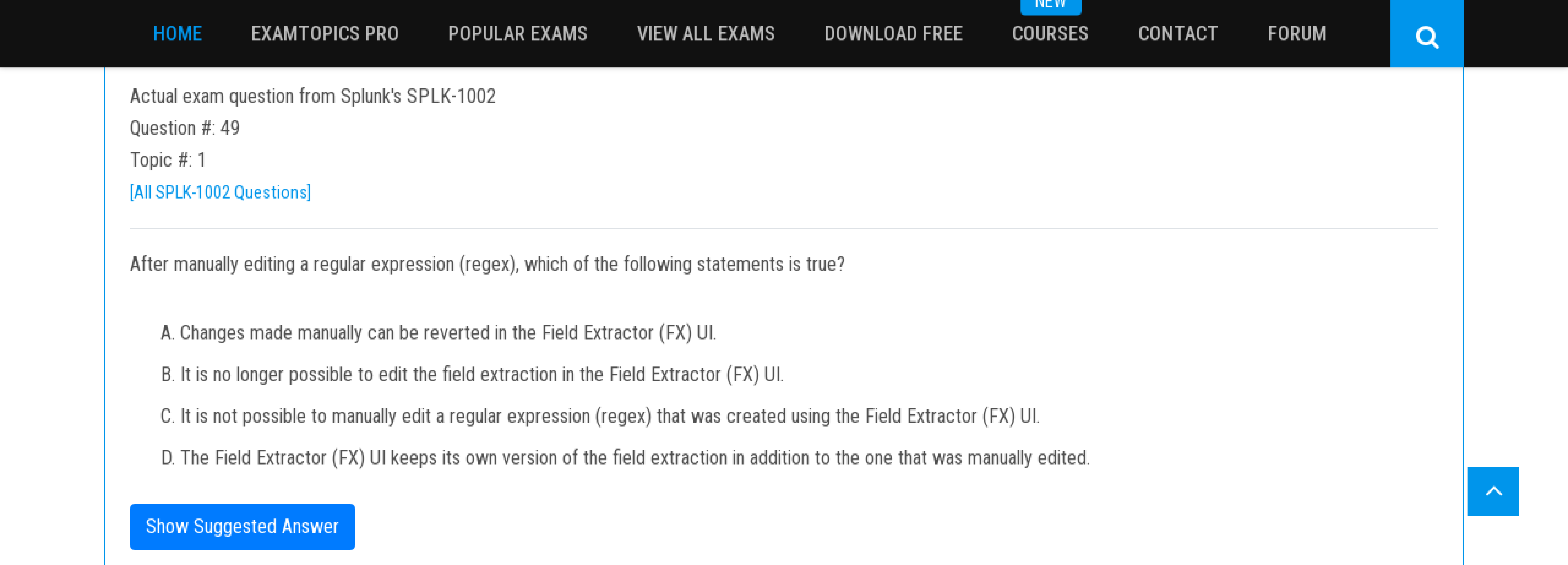
To identify all of the contributing events within a transaction that contain at least one REJECT event, which syntax is correct?

A. index=main REJECT | transaction sessionid

B. index=main | transaction sessionid | search REJECT

C. index=main | transaction sessionid | where transaction=reject

D. index=main | transaction sessionid | where transaction="REJECT*"



Actual exam question from Splunk's SPLK-1002

Question #: 49

Topic #: 1

[All SPLK-1002 Questions]

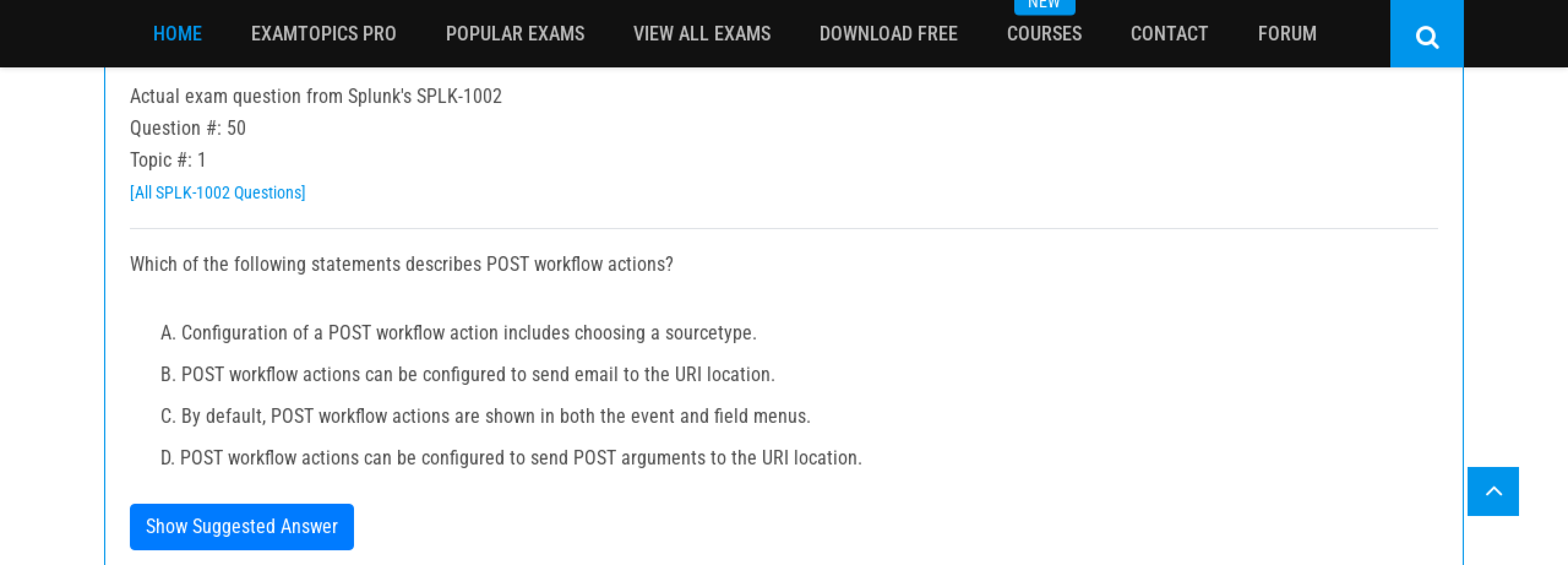
After manually editing a regular expression (regex), which of the following statements is true?

A. Changes made manually can be reverted in the Field Extractor (FX) UI.

B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.

C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.

D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.



Actual exam question from Splunk's SPLK-1002

Question #: 50

Topic #: 1

[All SPLK-1002 Questions]

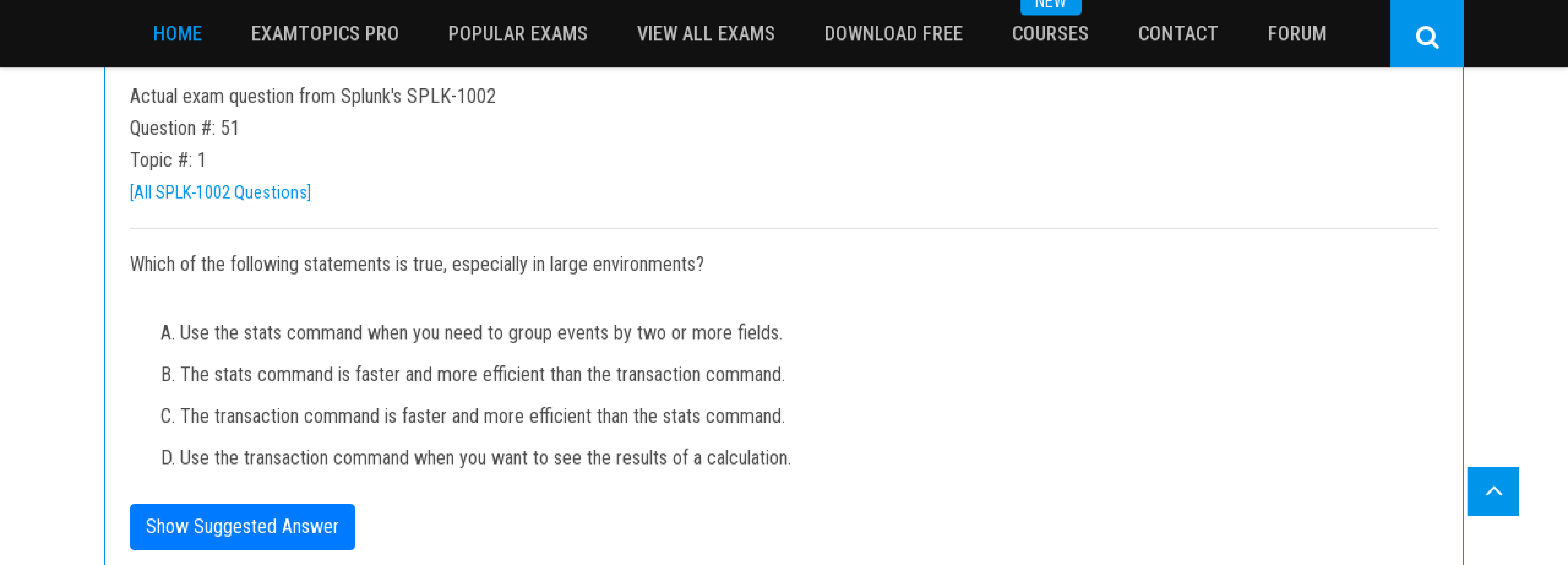
Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.

B. POST workflow actions can be configured to send email to the URI location.

C. By default, POST workflow actions are shown in both the event and field menus.

D. POST workflow actions can be configured to send POST arguments to the URI location.



Actual exam question from Splunk's SPLK-1002

Question #: 51

Topic #: 1

[All SPLK-1002 Questions]

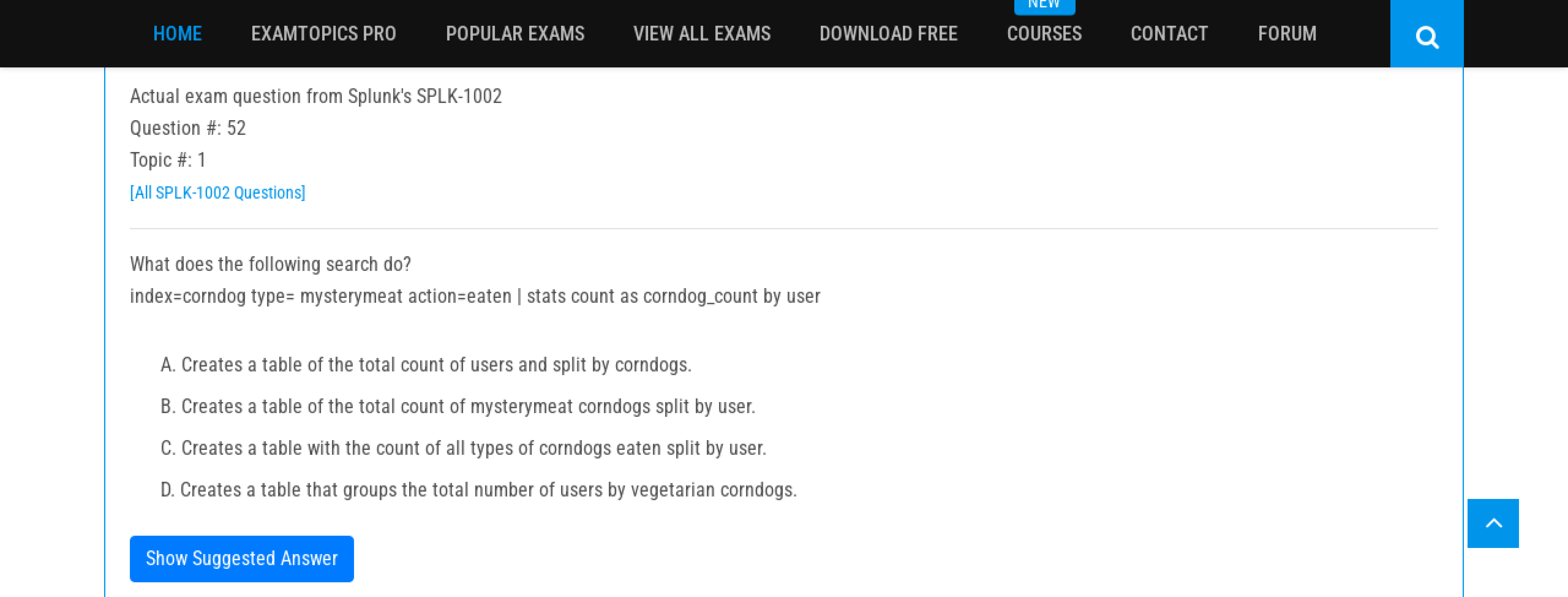
Which of the following statements is true, especially in large environments?

A. Use the stats command when you need to group events by two or more fields.

B. The stats command is faster and more efficient than the transaction command.

C. The transaction command is faster and more efficient than the stats command.

D. Use the transaction command when you want to see the results of a calculation.



Actual exam question from Splunk's SPLK-1002

Question #: 52

Topic #: 1

[All SPLK-1002 Questions]

What does the following search do?

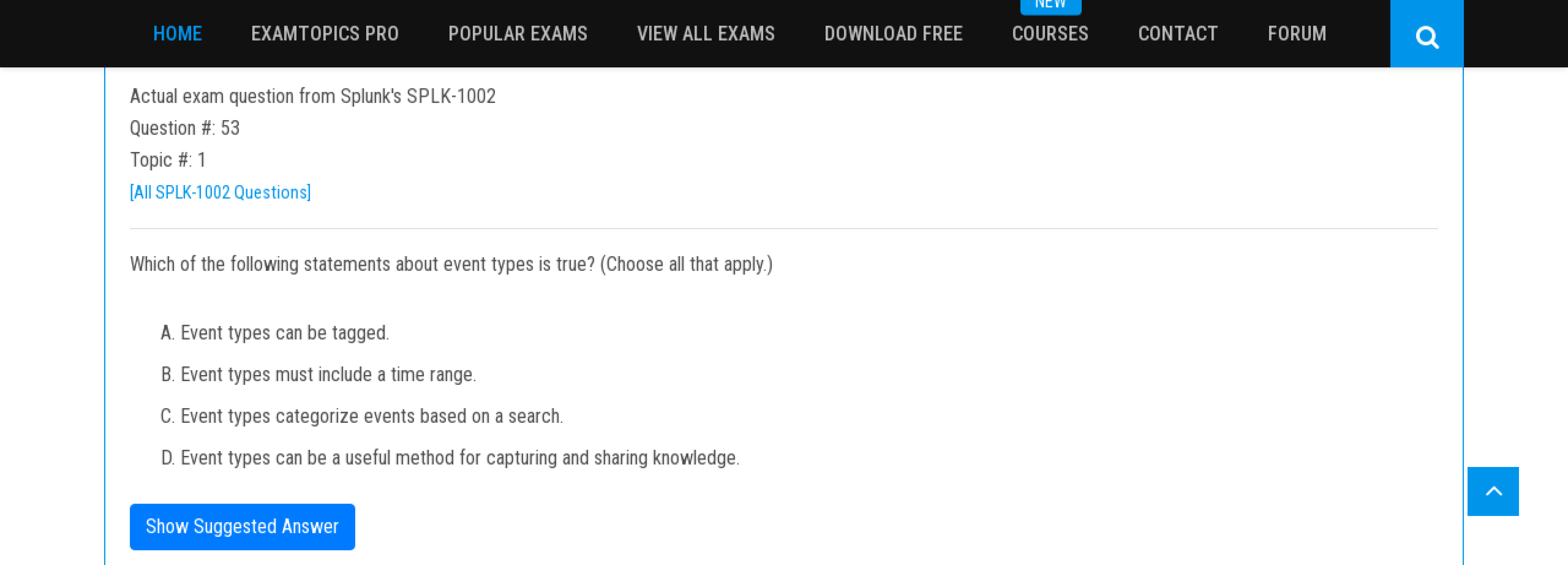
index=corndog type= mysterymeat action=eaten | stats count as corndog_count by user

A. Creates a table of the total count of users and split by corndogs.

B. Creates a table of the total count of mysterymeat corndogs split by user.

C. Creates a table with the count of all types of corndogs eaten split by user.

D. Creates a table that groups the total number of users by vegetarian corndogs.



Actual exam question from Splunk's SPLK-1002

Question #: 53

Topic #: 1

[All SPLK-1002 Questions]

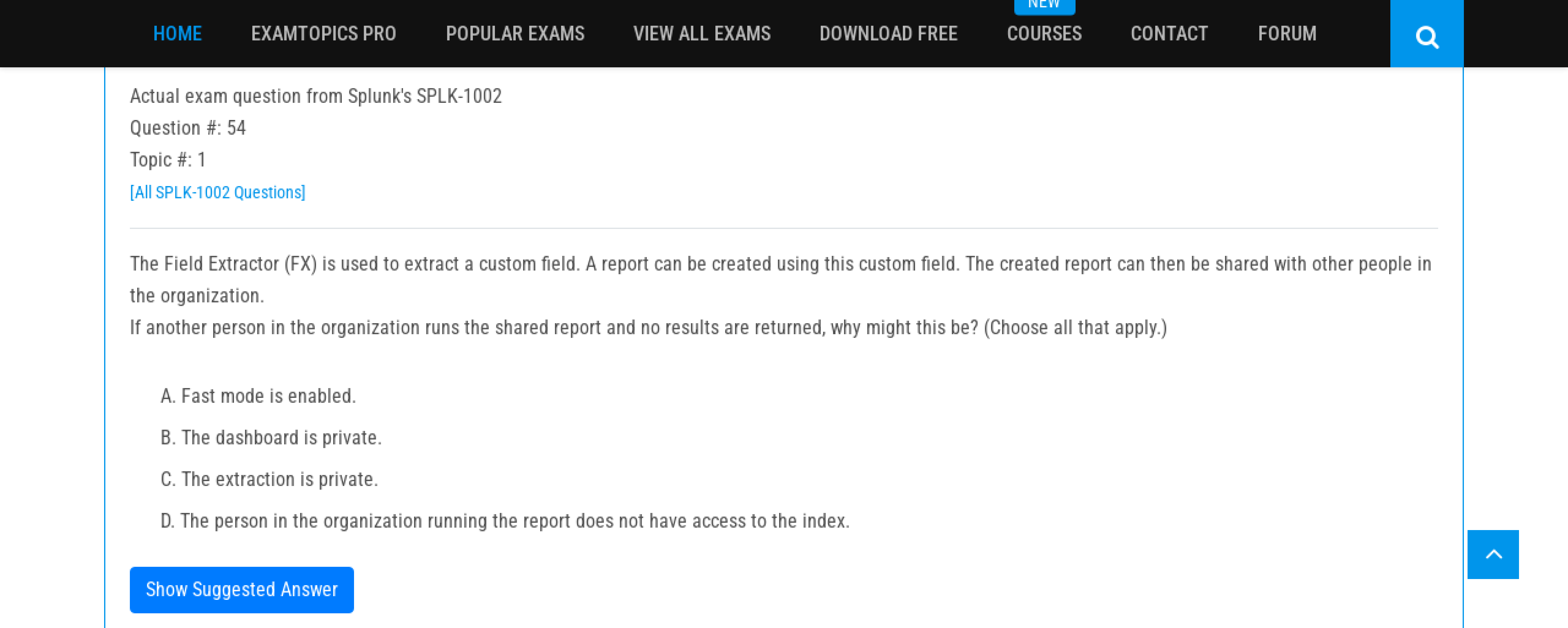
Which of the following statements about event types is true? (Choose all that apply.)

A. Event types can be tagged.

B. Event types must include a time range.

C. Event types categorize events based on a search.

D. Event types can be a useful method for capturing and sharing knowledge.



Actual exam question from Splunk's SPLK-1002

Question #: 54

Topic #: 1

[All SPLK-1002 Questions]

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization.

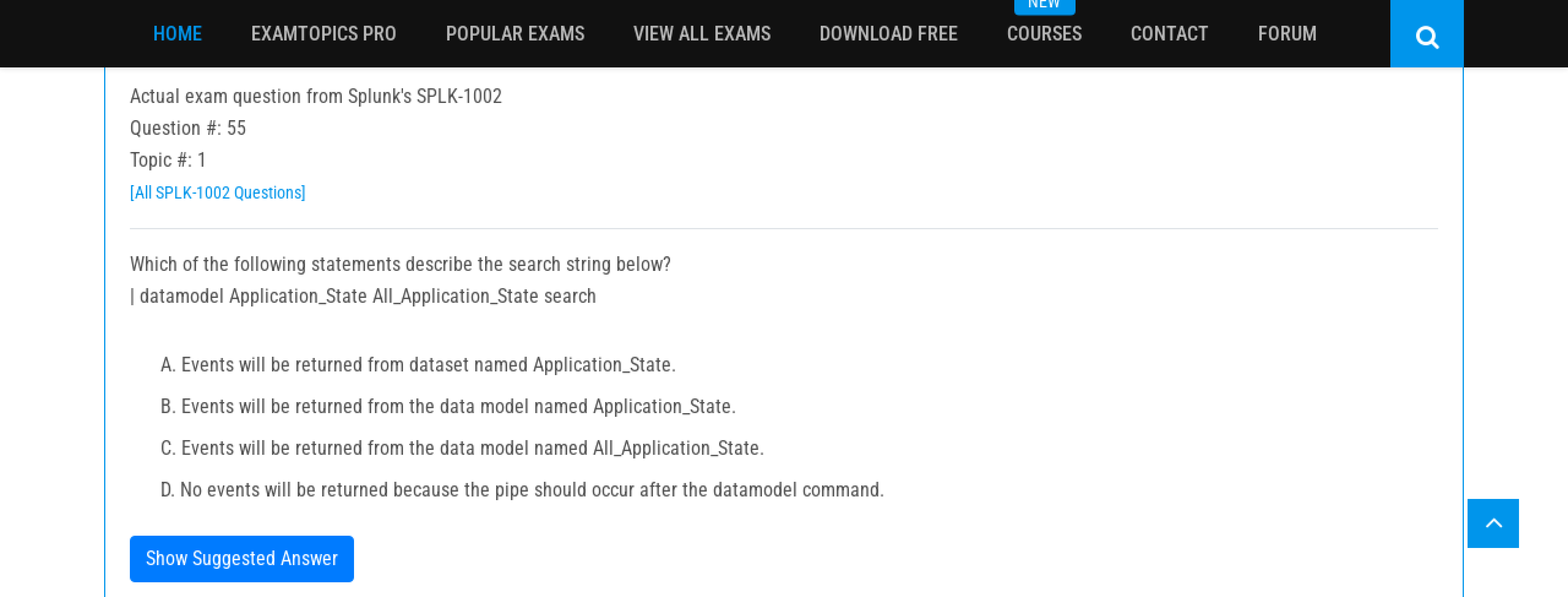
If another person in the organization runs the shared report and no results are returned, why might this be? (Choose all that apply.)

A. Fast mode is enabled.

B. The dashboard is private.

C. The extraction is private.

D. The person in the organization running the report does not have access to the index.



Actual exam question from Splunk's SPLK-1002

Question #: 55

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements describe the search string below?

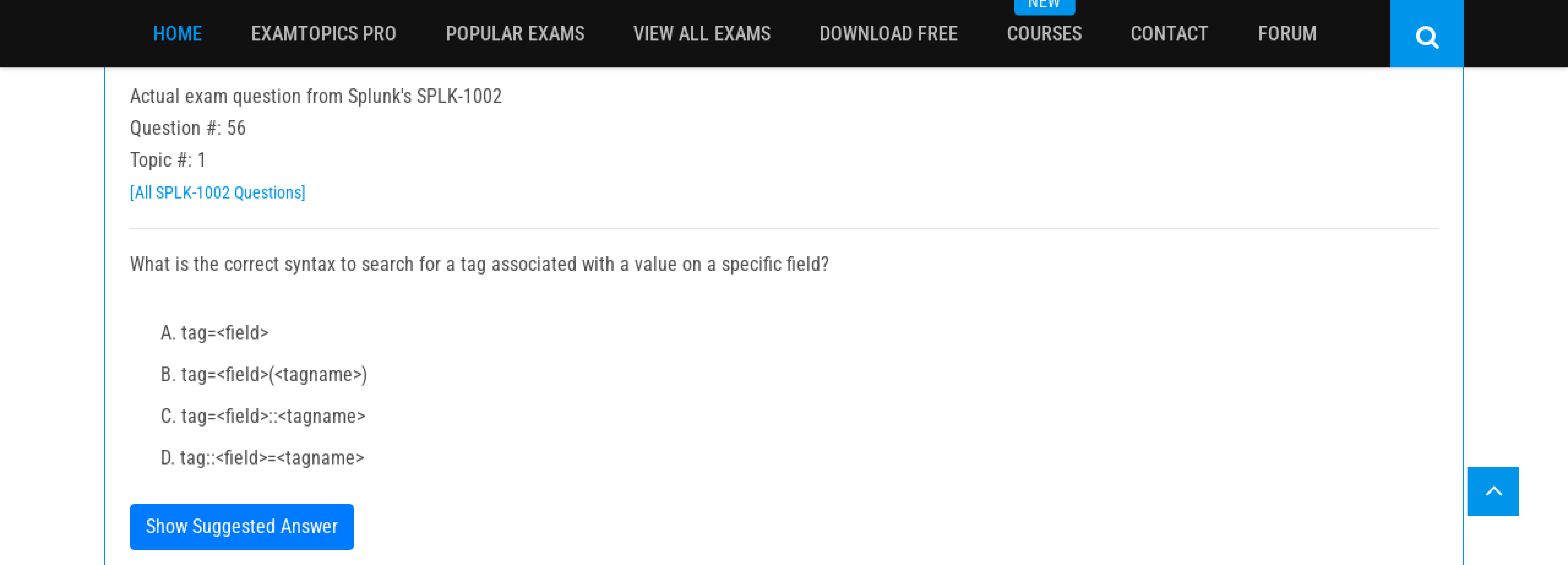
| datamodel Application_State All_Application_State search

A. Events will be returned from dataset named Application_State.

B. Events will be returned from the data model named Application_State.

C. Events will be returned from the data model named All_Application_State.

D. No events will be returned because the pipe should occur after the datamodel command.



Actual exam question from Splunk's SPLK-1002

Question #: 56

Topic #: 1

[All SPLK-1002 Questions]

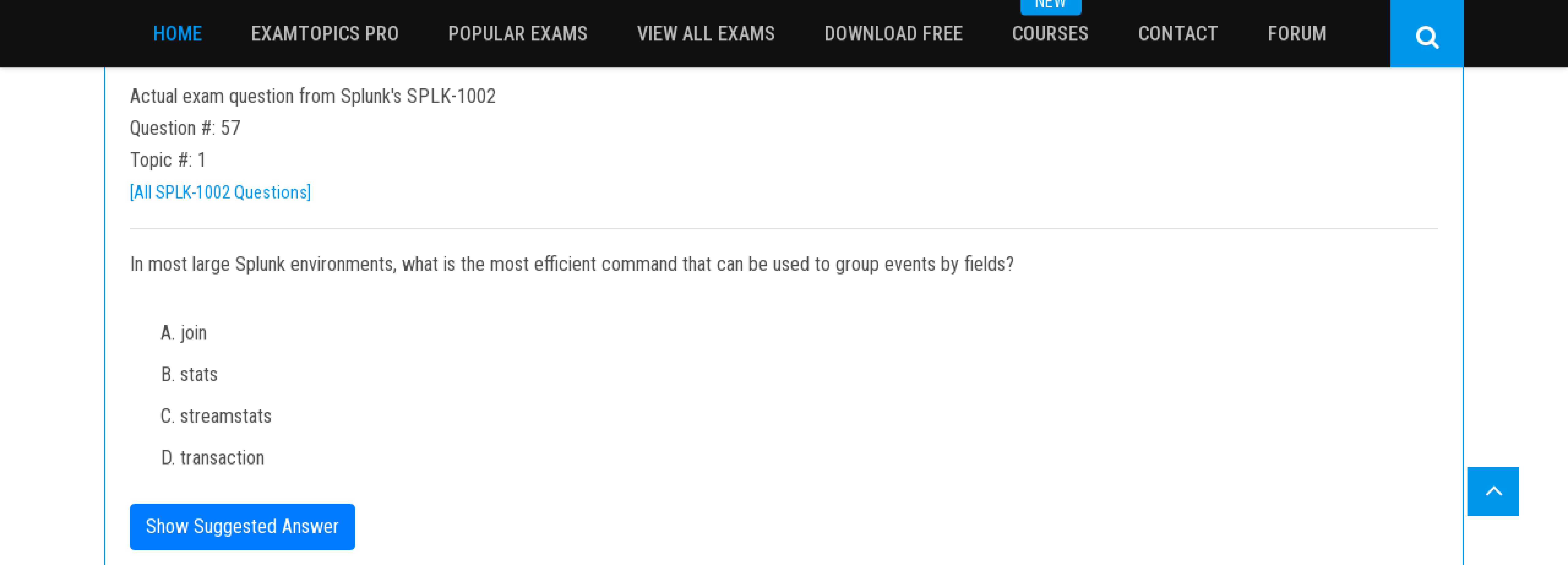
What is the correct syntax to search for a tag associated with a value on a specific field?

A. tag=<field>

B. tag=<field>(<tagname>)

C. tag=<field>::<tagname>

D. tag::<field>=<tagname>



Actual exam question from Splunk's SPLK-1002

Question #: 57

Topic #: 1

[All SPLK-1002 Questions]

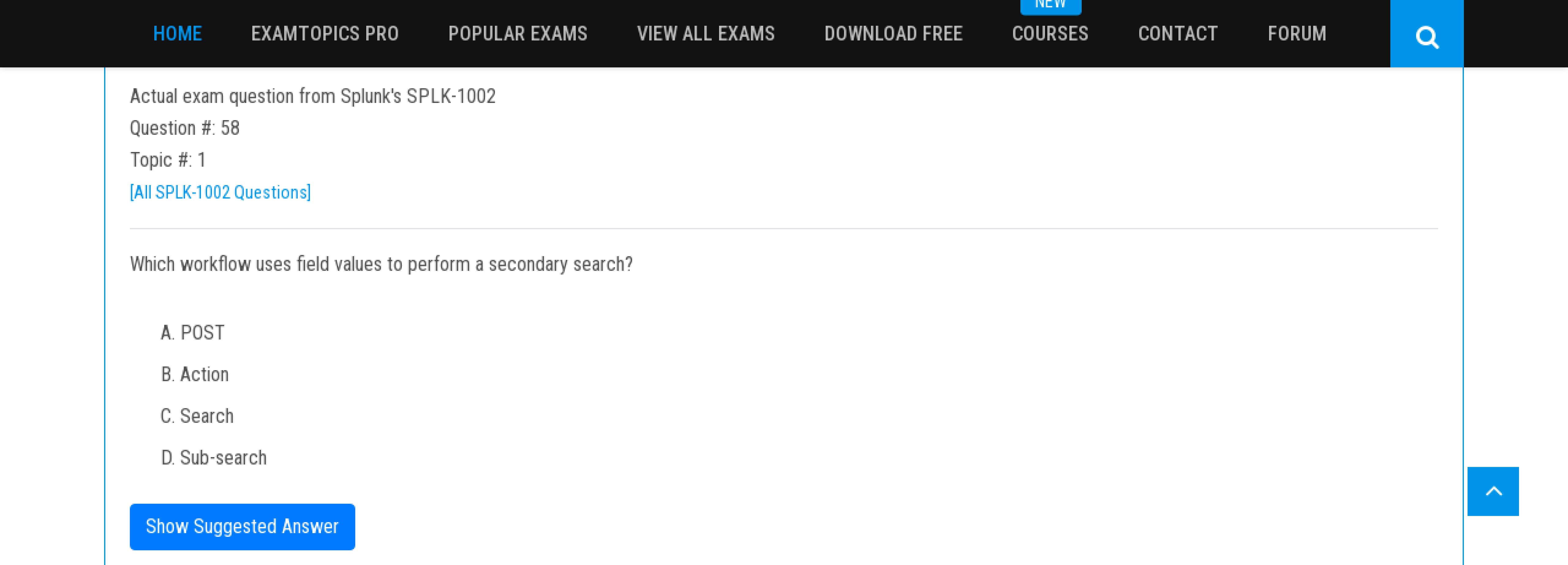
In most large Splunk environments, what is the most efficient command that can be used to group events by fields?

A. join

B. stats

C. streamstats

D. transaction



Actual exam question from Splunk's SPLK-1002

Question #: 58

Topic #: 1

[All SPLK-1002 Questions]

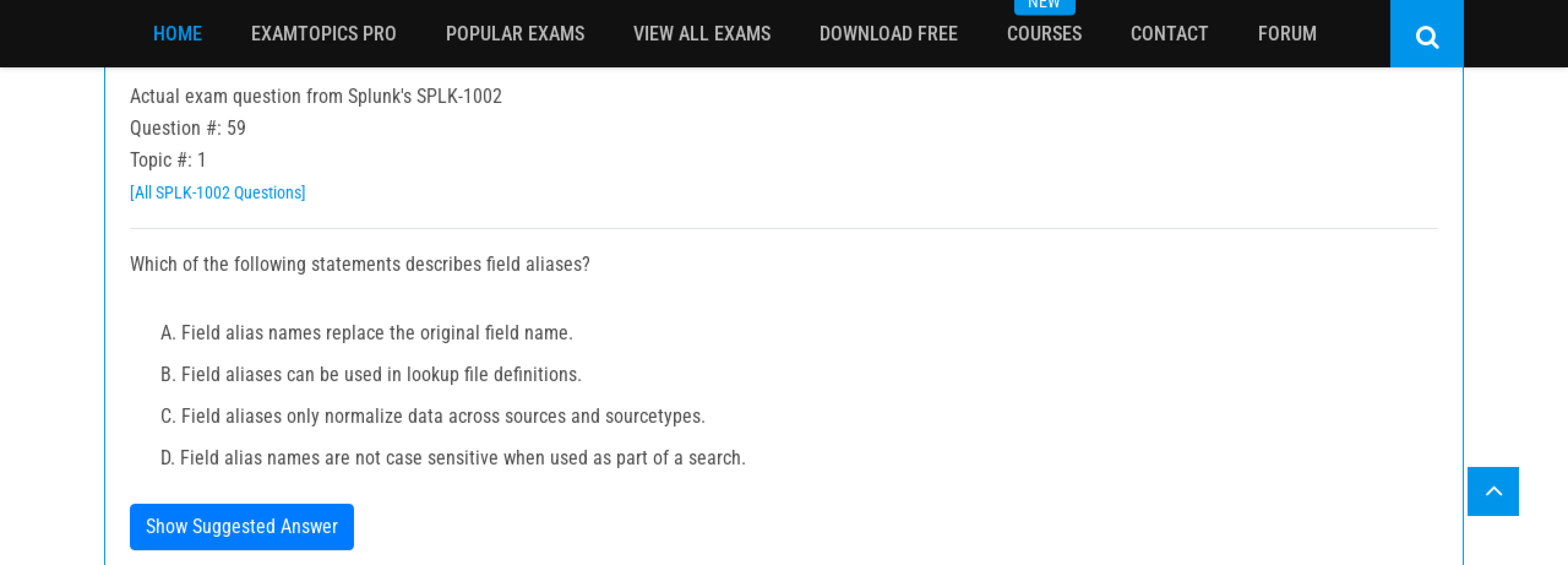
Which workflow uses field values to perform a secondary search?

A. POST

B. Action

C. Search

D. Sub-search



Actual exam question from Splunk's SPLK-1002

Question #: 59

Topic #: 1

[All SPLK-1002 Questions]

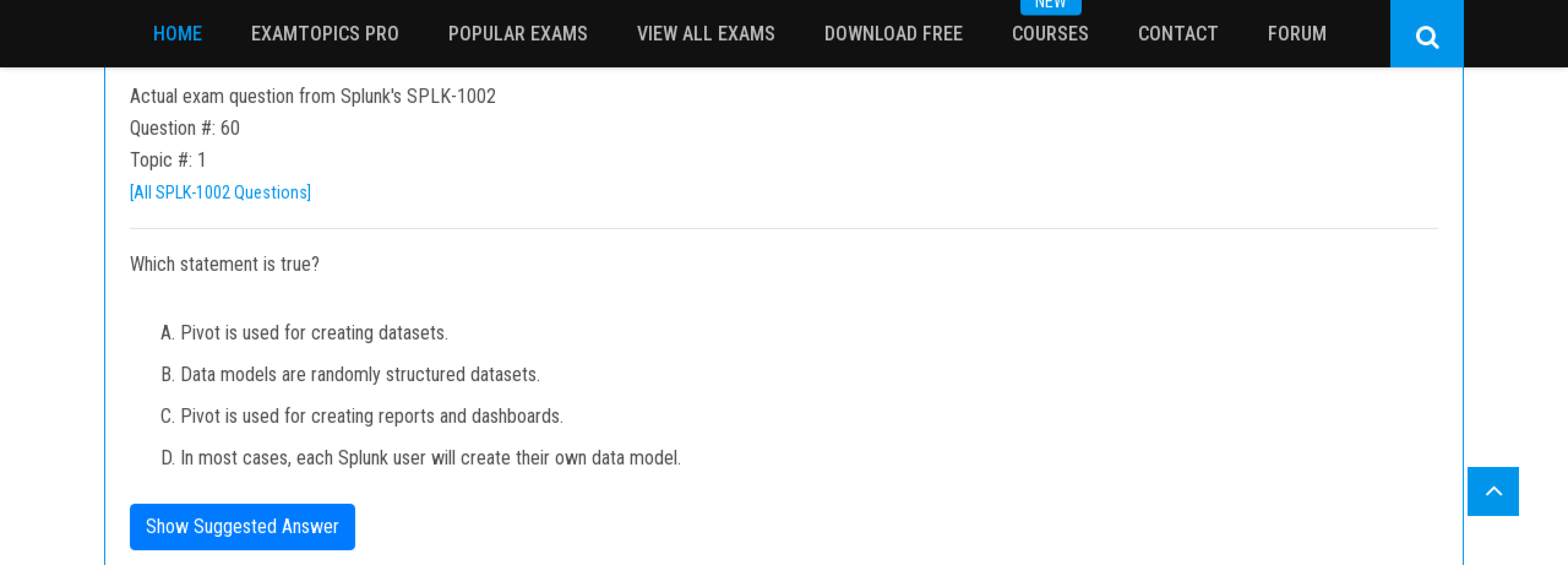
Which of the following statements describes field aliases?

A. Field alias names replace the original field name.

B. Field aliases can be used in lookup file definitions.

C. Field aliases only normalize data across sources and sourcetypes.

D. Field alias names are not case sensitive when used as part of a search.



Actual exam question from Splunk's SPLK-1002

Question #: 60

Topic #: 1

[All SPLK-1002 Questions]

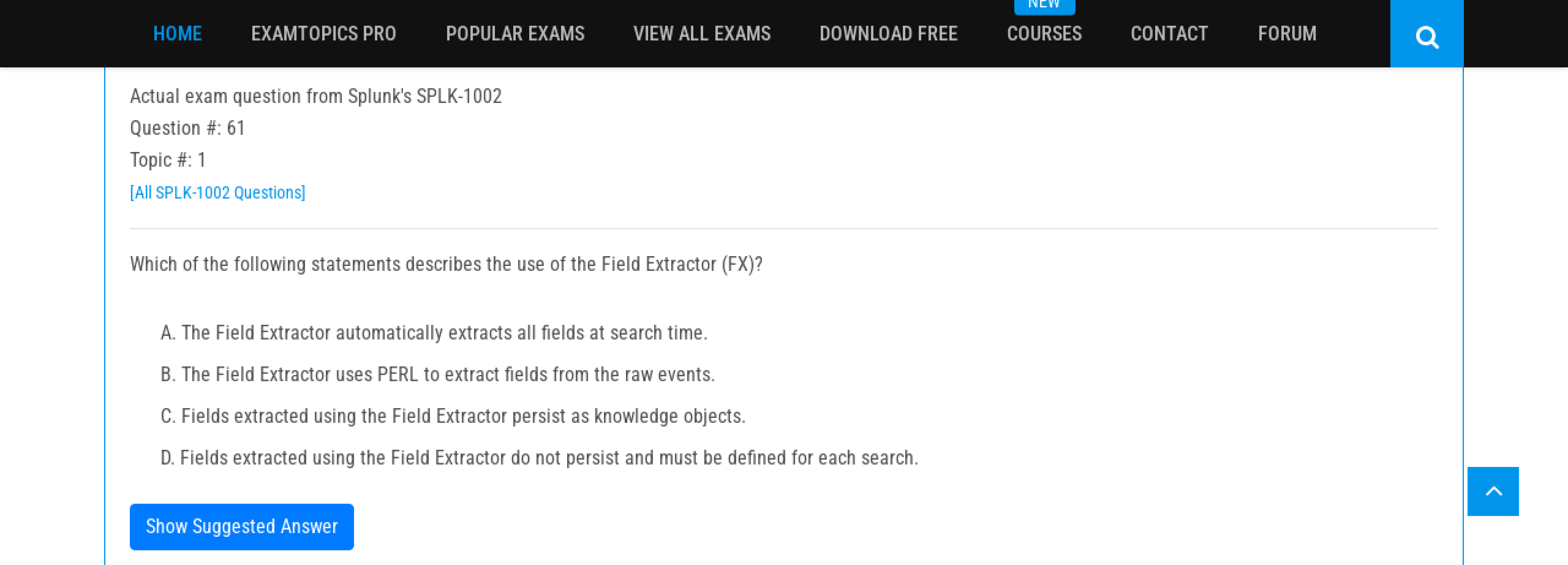
Which statement is true?

A. Pivot is used for creating datasets.

B. Data models are randomly structured datasets.

C. Pivot is used for creating reports and dashboards.

D. In most cases, each Splunk user will create their own data model.



Actual exam question from Splunk's SPLK-1002

Question #: 61

Topic #: 1

[All SPLK-1002 Questions]

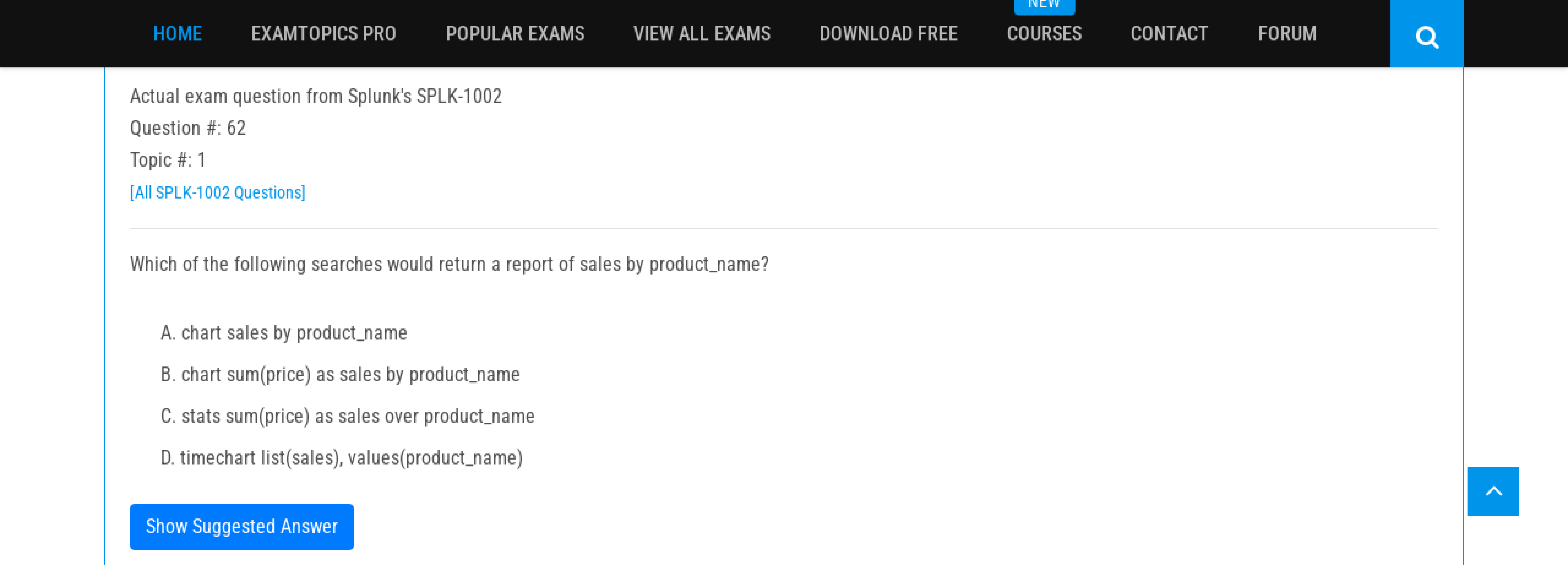
Which of the following statements describes the use of the Field Extractor (FX)?

A. The Field Extractor automatically extracts all fields at search time.

B. The Field Extractor uses PERL to extract fields from the raw events.

C. Fields extracted using the Field Extractor persist as knowledge objects.

D. Fields extracted using the Field Extractor do not persist and must be defined for each search.



Actual exam question from Splunk's SPLK-1002

Question #: 62

Topic #: 1

[All SPLK-1002 Questions]

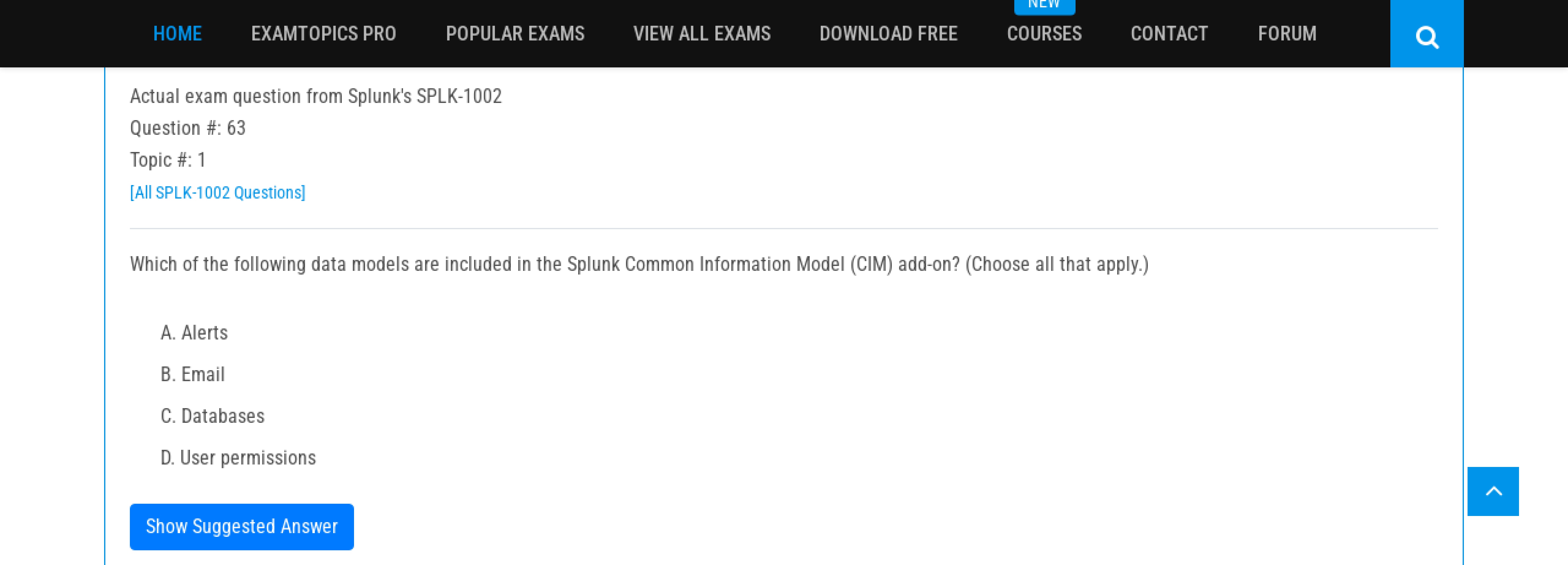
Which of the following searches would return a report of sales by product_name?

A. chart sales by product_name

B. chart sum(price) as sales by product_name

C. stats sum(price) as sales over product_name

D. timechart list(sales), values(product_name)



Actual exam question from Splunk's SPLK-1002

Question #: 63

Topic #: 1

[All SPLK-1002 Questions]

Which of the following data models are included in the Splunk Common Information Model (CIM) add-on? (Choose all that apply.)

A. Alerts

B. Email

C. Databases

D. User permissions

Actual exam question from Splunk's SPLK-1002

Question #: 64

Topic #: 1

[All SPLK-1002 Questions]

What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow actions cannot use macros.

B. Searches generated by workflow actions must be less than 256 characters long.

C. Searches generated by workflow actions must run in the same app as the workflow action.

D. Searches generated by workflow actions run with the same permissions as the user running them.

Show Suggested Answer

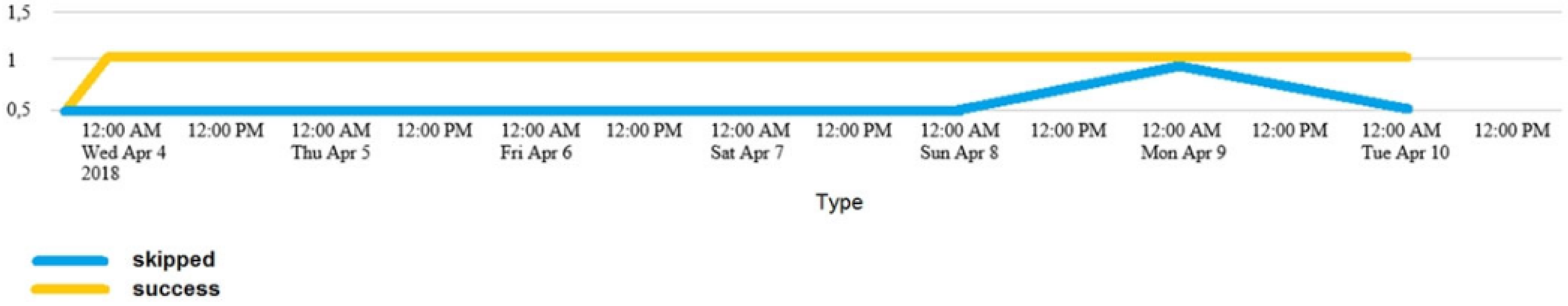
Actual exam question from Splunk's SPLK-1002

Question #: 65

Topic #: 1

[All SPLK-1002 Questions]

Which of the following searches would create a graph similar to the one below?



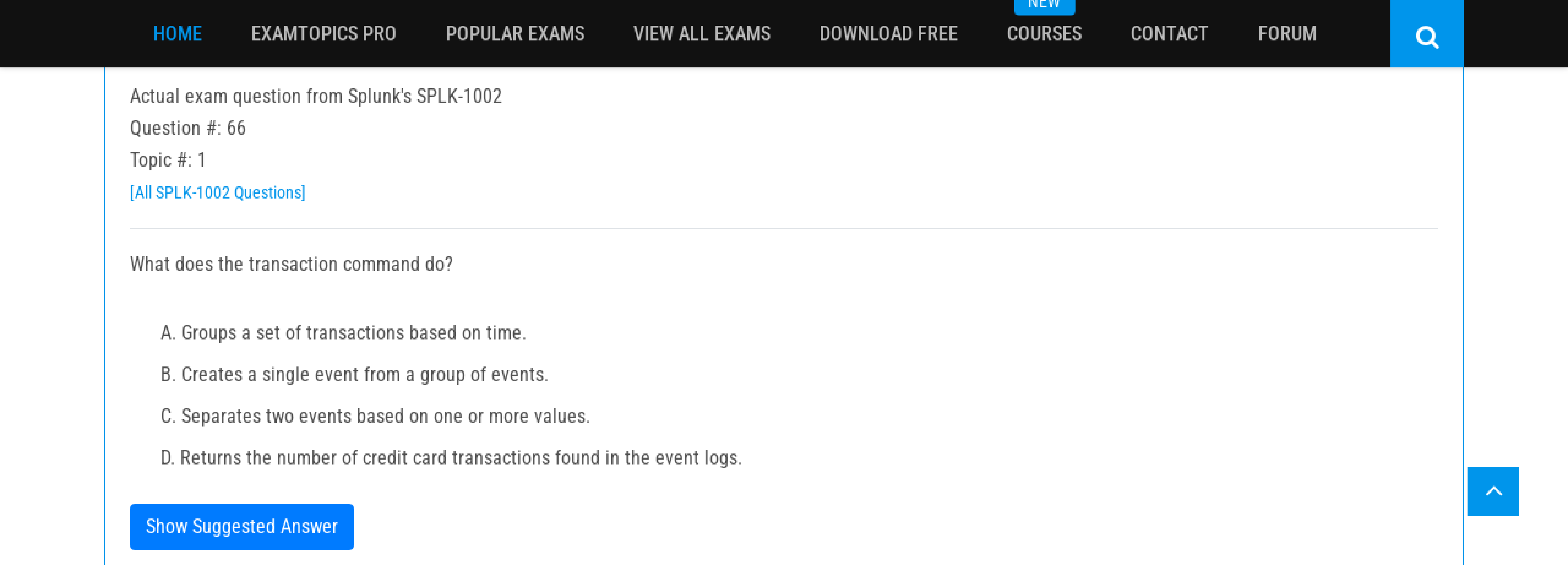
A. index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | stats count by status

B. index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | chart count OVER status by _time

C. index=_internal sourcetype=SavedSplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status

D. None of these searches would generate a similar graph.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 66

Topic #: 1

[All SPLK-1002 Questions]

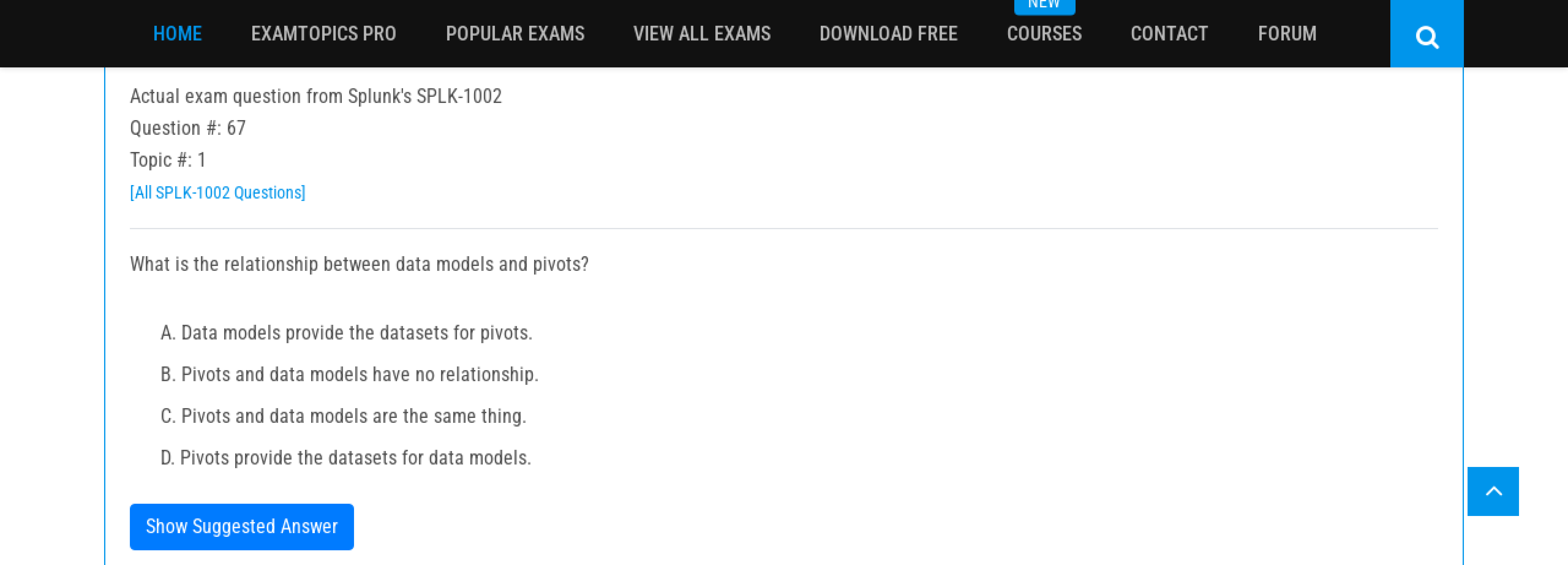
What does the transaction command do?

A. Groups a set of transactions based on time.

B. Creates a single event from a group of events.

C. Separates two events based on one or more values.

D. Returns the number of credit card transactions found in the event logs.



Actual exam question from Splunk's SPLK-1002

Question #: 67

Topic #: 1

[All SPLK-1002 Questions]

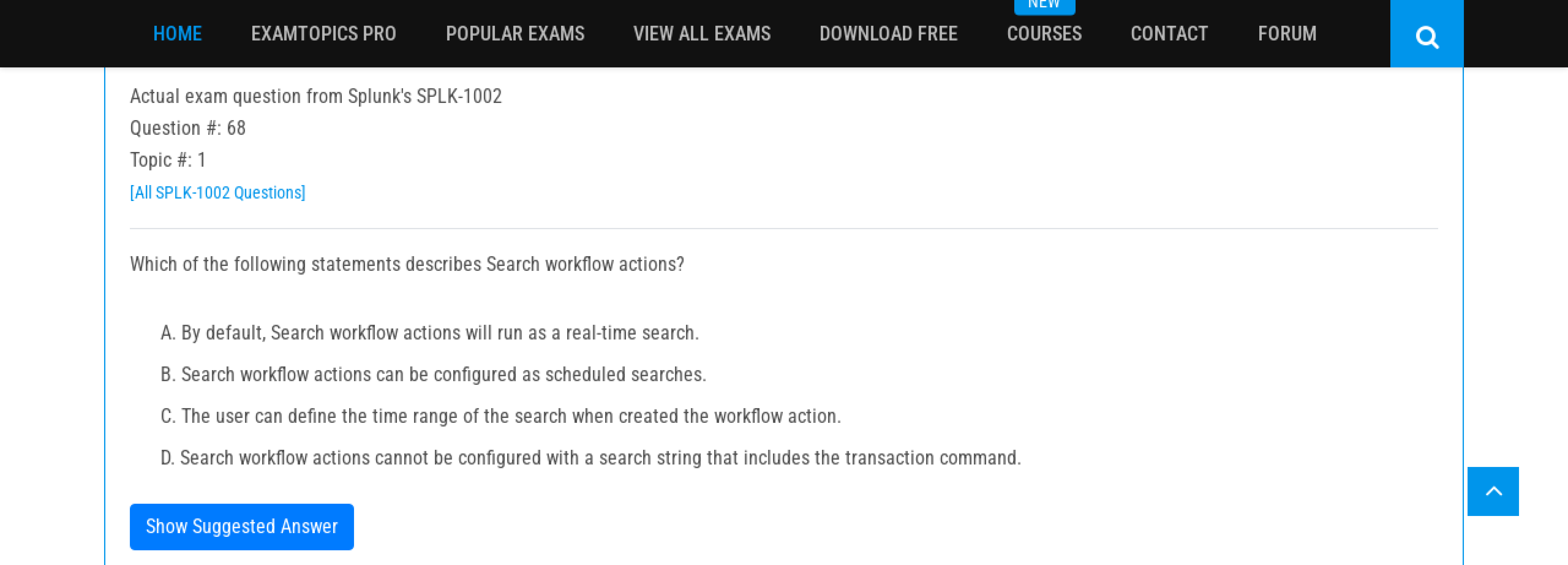
What is the relationship between data models and pivots?

A. Data models provide the datasets for pivots.

B. Pivots and data models have no relationship.

C. Pivots and data models are the same thing.

D. Pivots provide the datasets for data models.



Actual exam question from Splunk's SPLK-1002

Question #: 68

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements describes Search workflow actions?

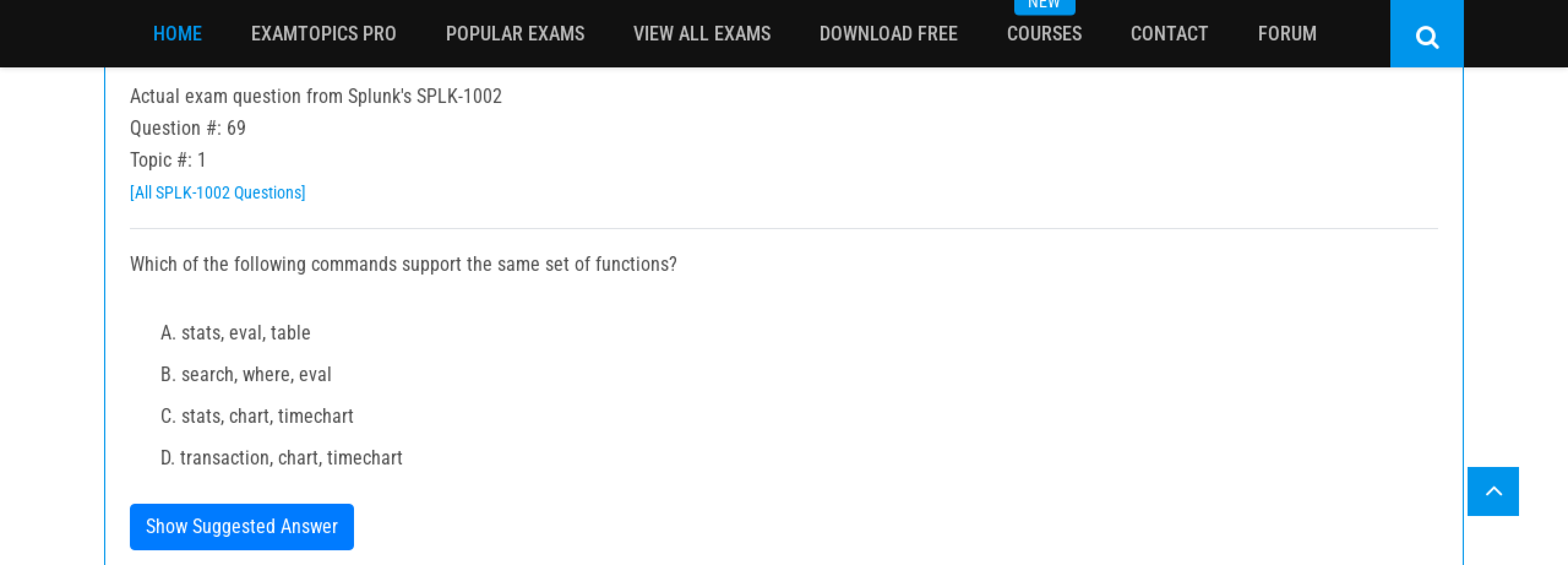
A. By default, Search workflow actions will run as a real-time search.

B. Search workflow actions can be configured as scheduled searches.

C. The user can define the time range of the search when created the workflow action.

D. Search workflow actions cannot be configured with a search string that includes the transaction command.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 69

Topic #: 1

[All SPLK-1002 Questions]

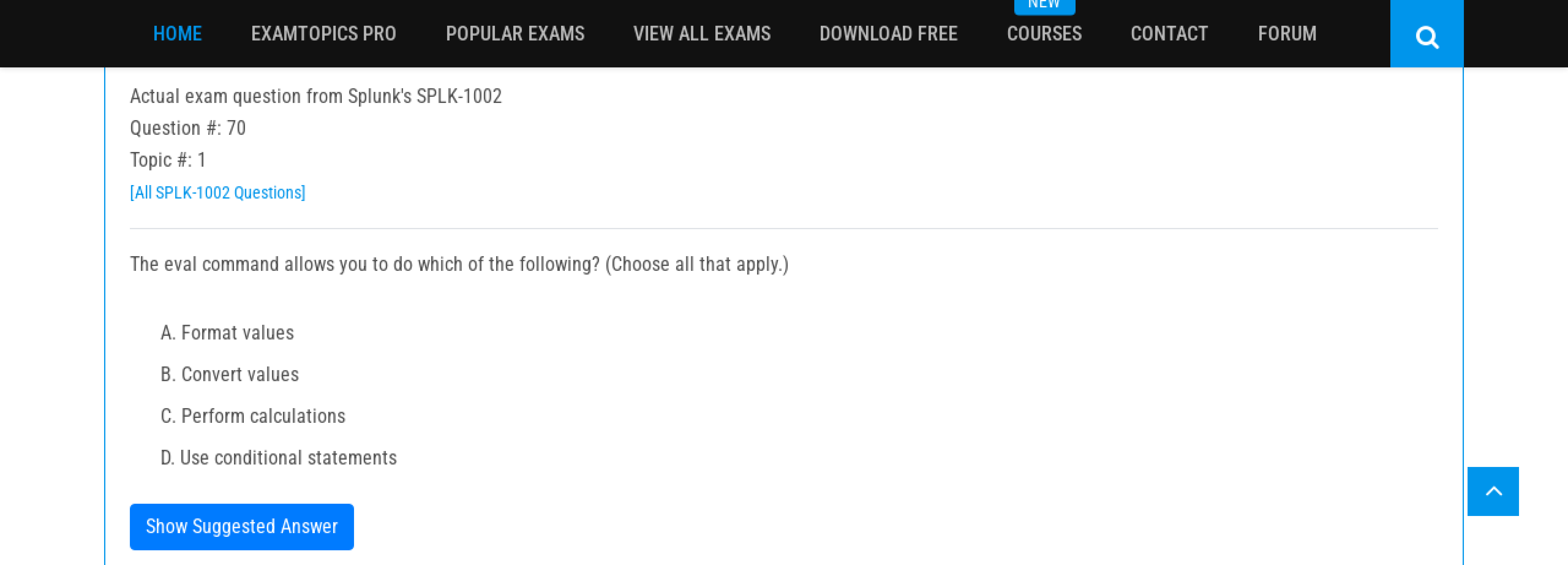
Which of the following commands support the same set of functions?

A. stats, eval, table

B. search, where, eval

C. stats, chart, timechart

D. transaction, chart, timechart



Actual exam question from Splunk's SPLK-1002

Question #: 70

Topic #: 1

[All SPLK-1002 Questions]

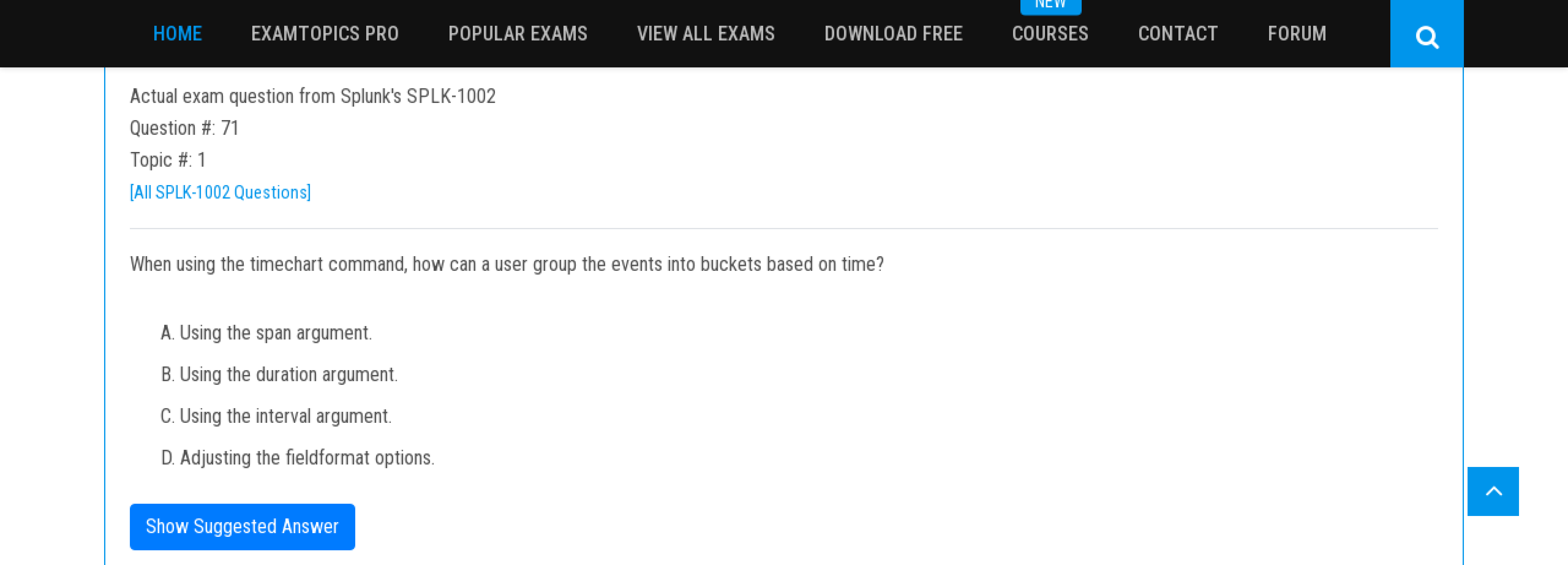
The eval command allows you to do which of the following? (Choose all that apply.)

A. Format values

B. Convert values

C. Perform calculations

D. Use conditional statements



Actual exam question from Splunk's SPLK-1002

Question #: 71

Topic #: 1

[All SPLK-1002 Questions]

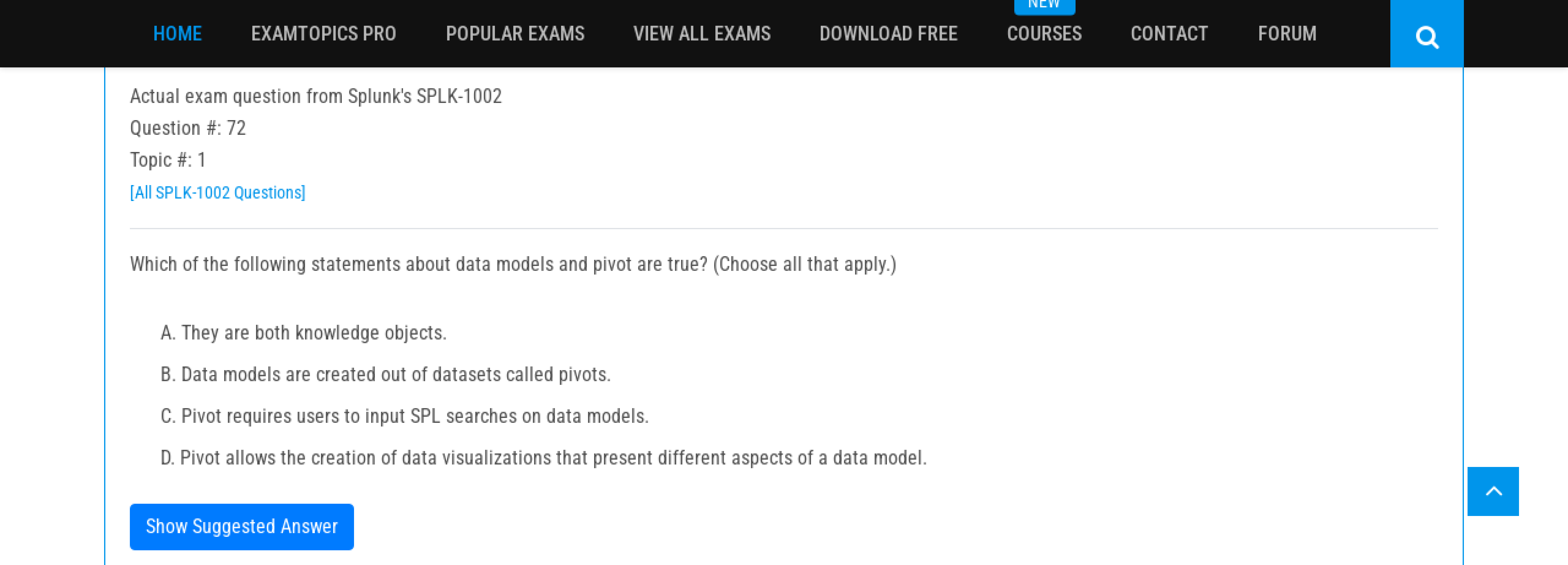
When using the timechart command, how can a user group the events into buckets based on time?

A. Using the span argument.

B. Using the duration argument.

C. Using the interval argument.

D. Adjusting the fieldformat options.



Actual exam question from Splunk's SPLK-1002

Question #: 72

Topic #: 1

[All SPLK-1002 Questions]

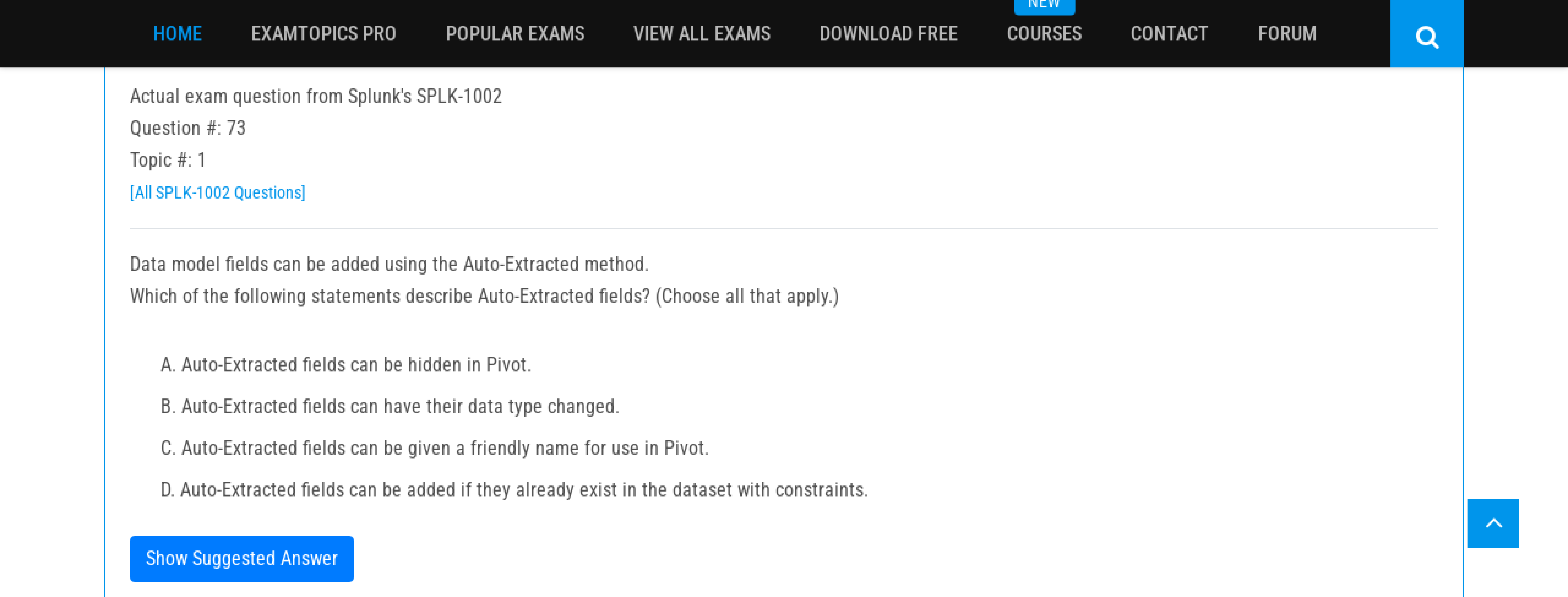
Which of the following statements about data models and pivot are true? (Choose all that apply.)

A. They are both knowledge objects.

B. Data models are created out of datasets called pivots.

C. Pivot requires users to input SPL searches on data models.

D. Pivot allows the creation of data visualizations that present different aspects of a data model.



Actual exam question from Splunk's SPLK-1002

Question #: 73

Topic #: 1

[All SPLK-1002 Questions]

Data model fields can be added using the Auto-Extracted method.

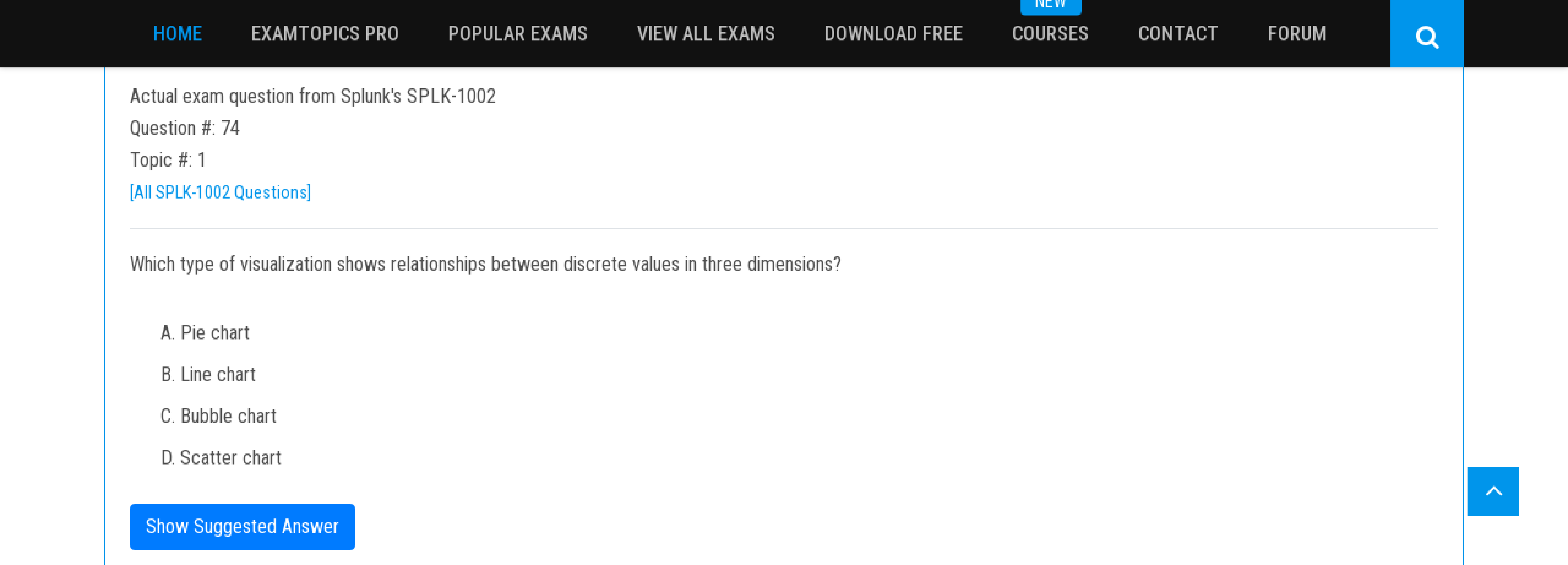
Which of the following statements describe Auto-Extracted fields? (Choose all that apply.)

A. Auto-Extracted fields can be hidden in Pivot.

B. Auto-Extracted fields can have their data type changed.

C. Auto-Extracted fields can be given a friendly name for use in Pivot.

D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.



Actual exam question from Splunk's SPLK-1002

Question #: 74

Topic #: 1

[All SPLK-1002 Questions]

Which type of visualization shows relationships between discrete values in three dimensions?

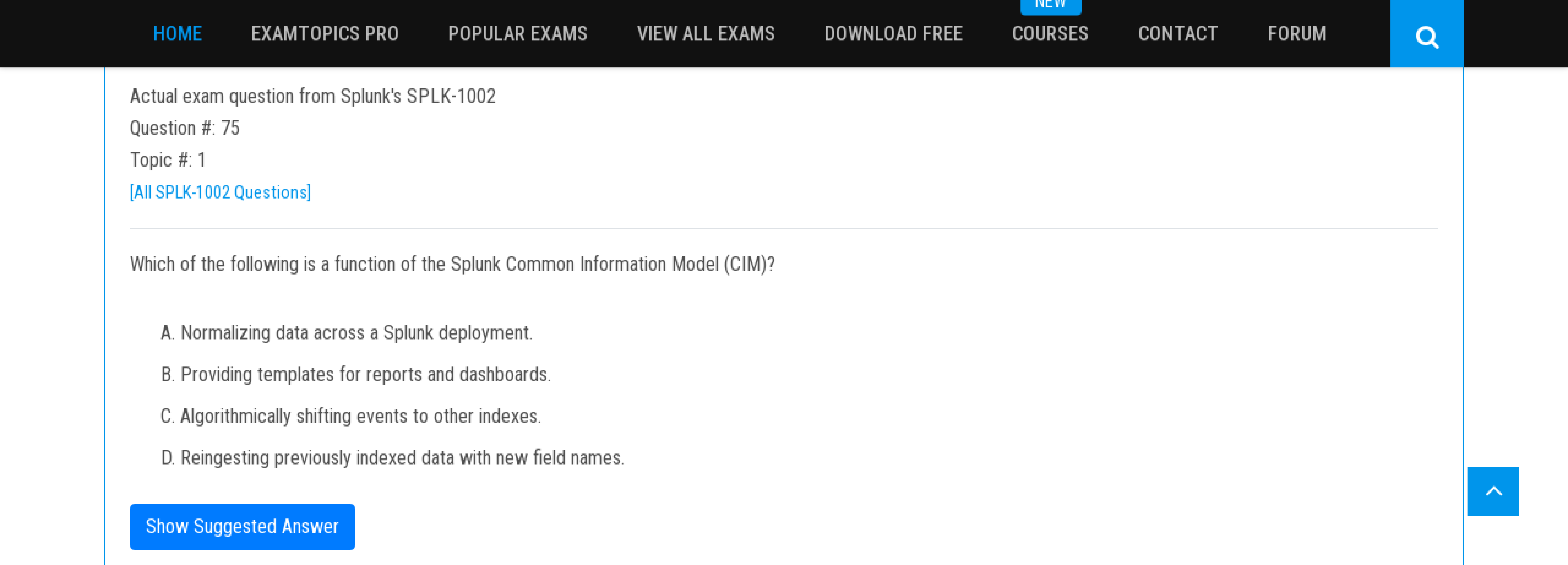
A. Pie chart

B. Line chart

C. Bubble chart

D. Scatter chart

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 75

Topic #: 1

[All SPLK-1002 Questions]

Which of the following is a function of the Splunk Common Information Model (CIM)?

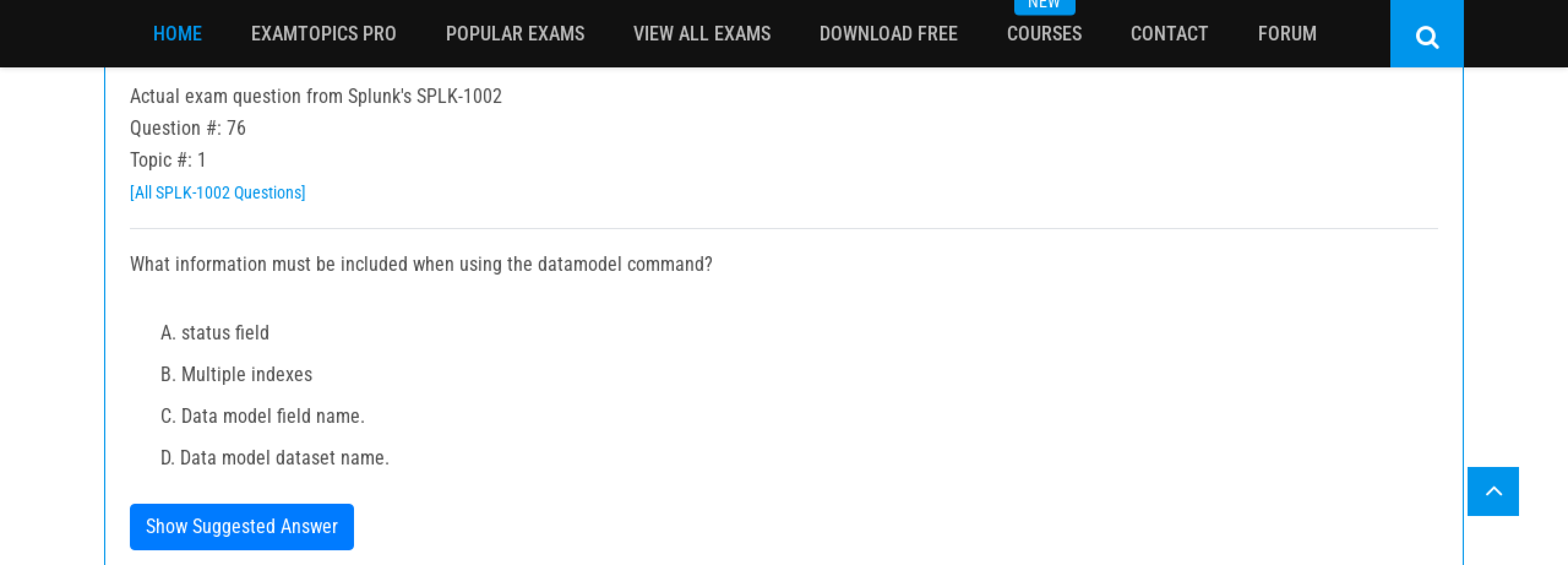
A. Normalizing data across a Splunk deployment.

B. Providing templates for reports and dashboards.

C. Algorithmically shifting events to other indexes.

D. Reingesting previously indexed data with new field names.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 76

Topic #: 1

[All SPLK-1002 Questions]

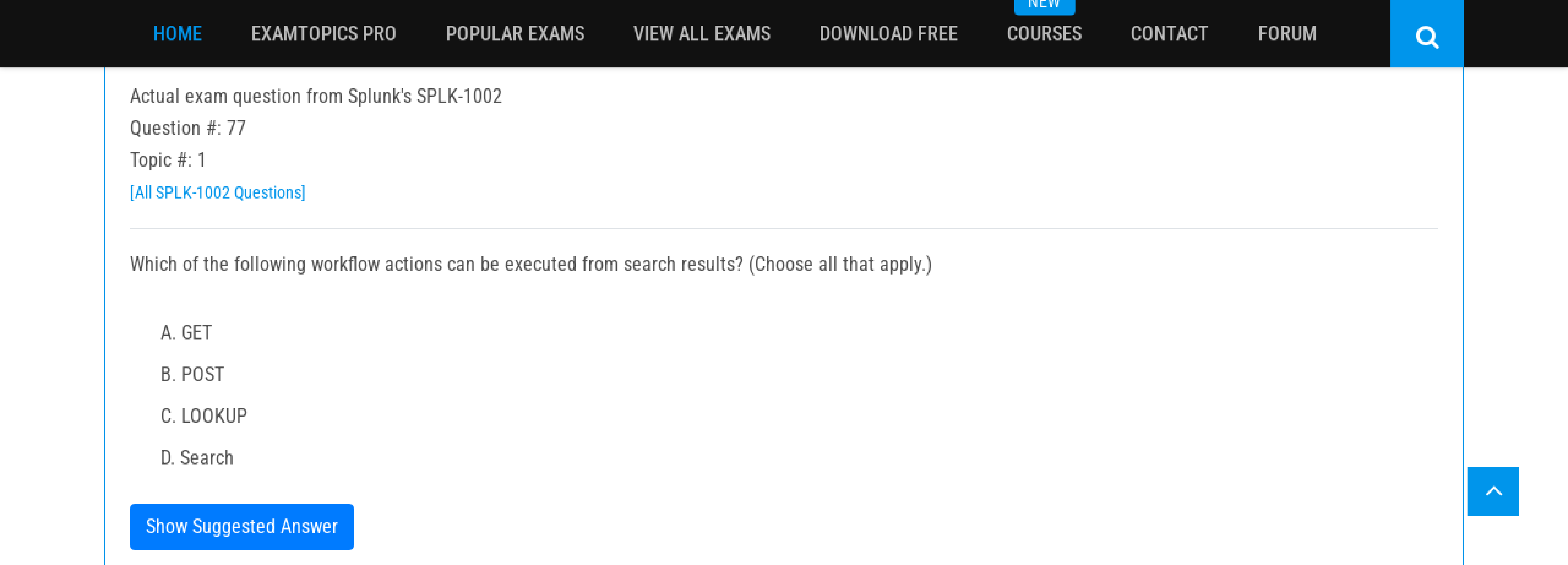
What information must be included when using the datamodel command?

A. status field

B. Multiple indexes

C. Data model field name.

D. Data model dataset name.



Actual exam question from Splunk's SPLK-1002

Question #: 77

Topic #: 1

[All SPLK-1002 Questions]

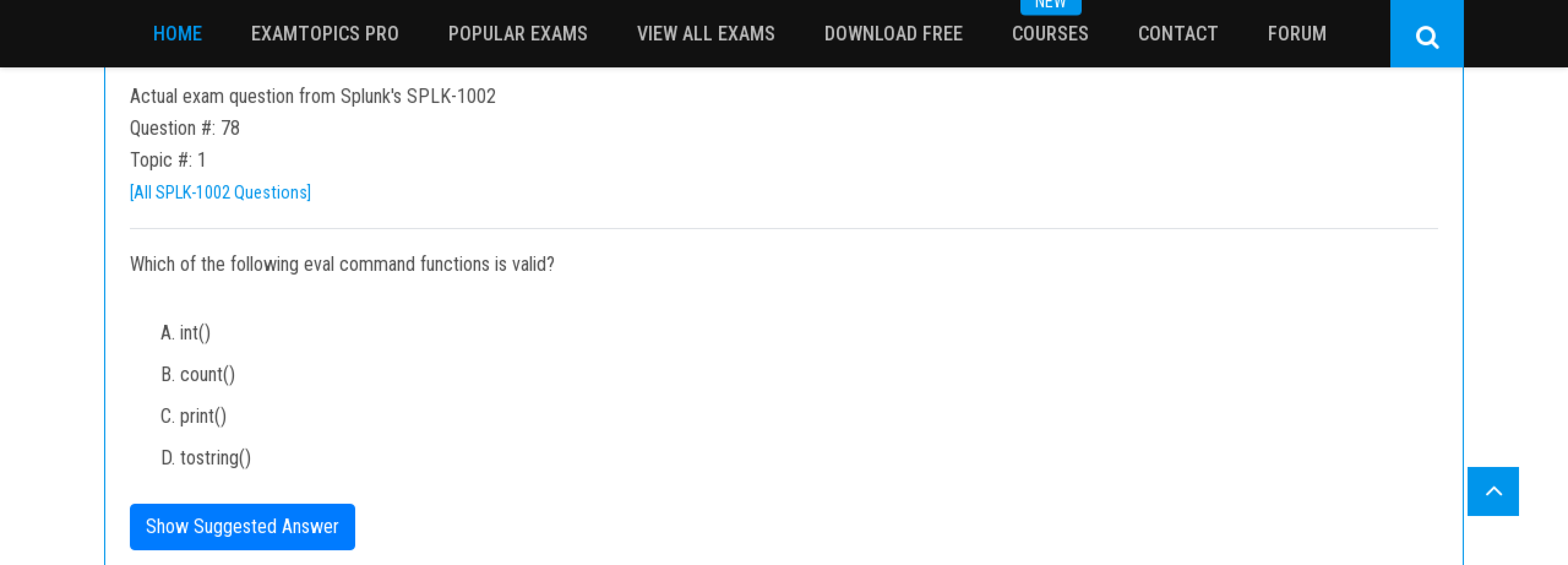
Which of the following workflow actions can be executed from search results? (Choose all that apply.)

A. GET

B. POST

C. LOOKUP

D. Search



Actual exam question from Splunk's SPLK-1002

Question #: 78

Topic #: 1

[All SPLK-1002 Questions]

Which of the following eval command functions is valid?

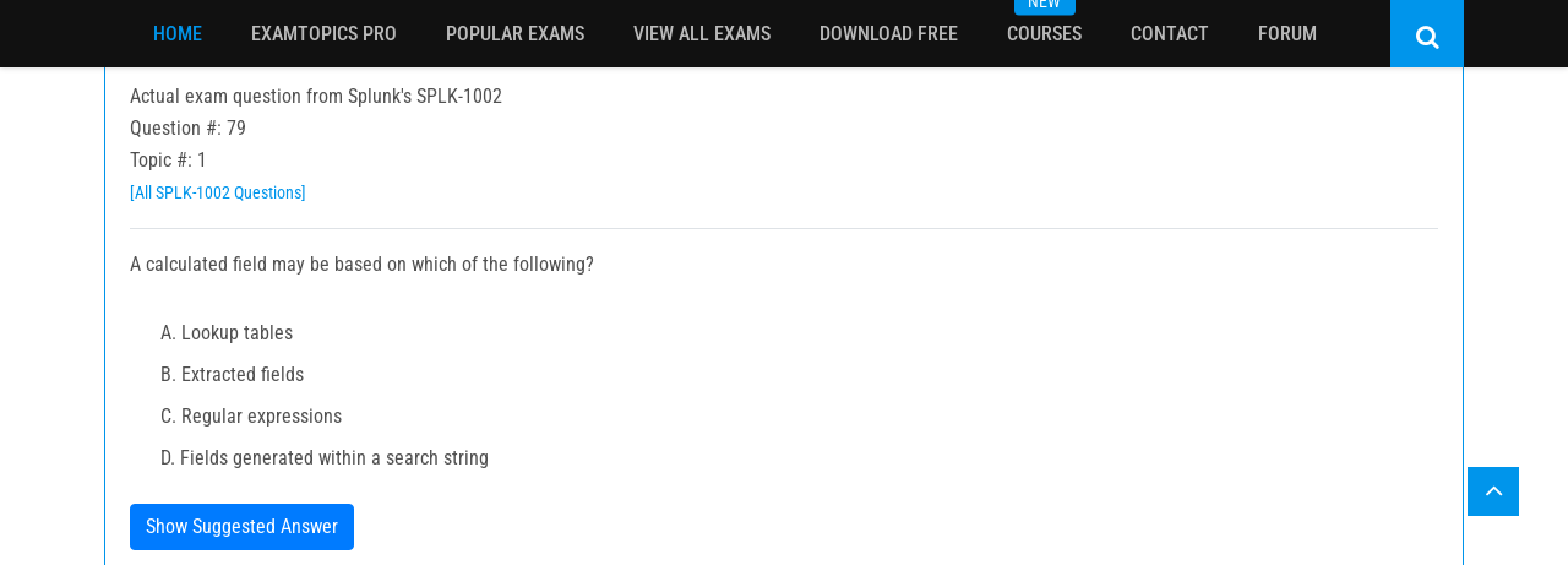
A. int()

B. count()

C. print()

D. tostring()

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 79

Topic #: 1

[All SPLK-1002 Questions]

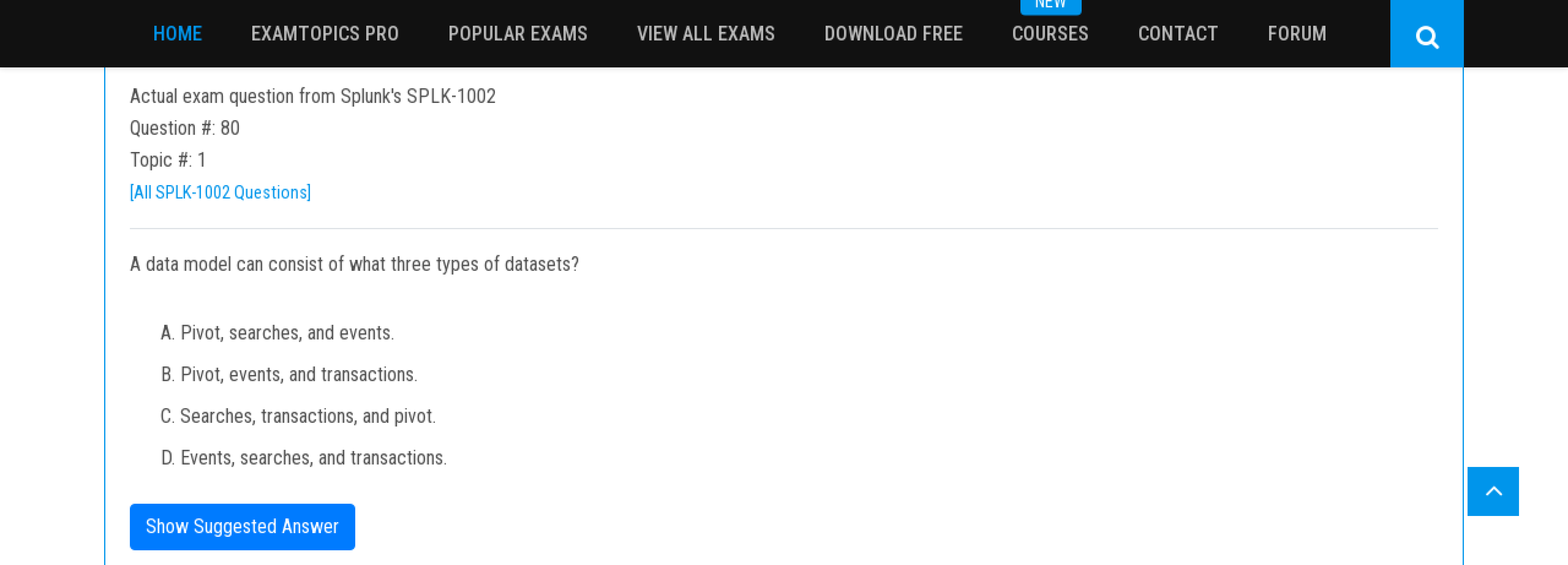
A calculated field may be based on which of the following?

A. Lookup tables

B. Extracted fields

C. Regular expressions

D. Fields generated within a search string



Actual exam question from Splunk's SPLK-1002

Question #: 80

Topic #: 1

[All SPLK-1002 Questions]

A data model can consist of what three types of datasets?

A. Pivot, searches, and events.

B. Pivot, events, and transactions.

C. Searches, transactions, and pivot.

D. Events, searches, and transactions.

Actual exam question from Splunk's SPLK-1002

Question #: 81

Topic #: 1

[All SPLK-1002 Questions]

When is a GET workflow action needed?

A. To send field values to an external resource.

B. To retrieve information from an external resource.

C. To use field values to perform a secondary search.

D. To define how events flow from forwarders to indexes.

Show Suggested Answer

Actual exam question from Splunk's SPLK-1002

Question #: 82

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements describe GET workflow actions?

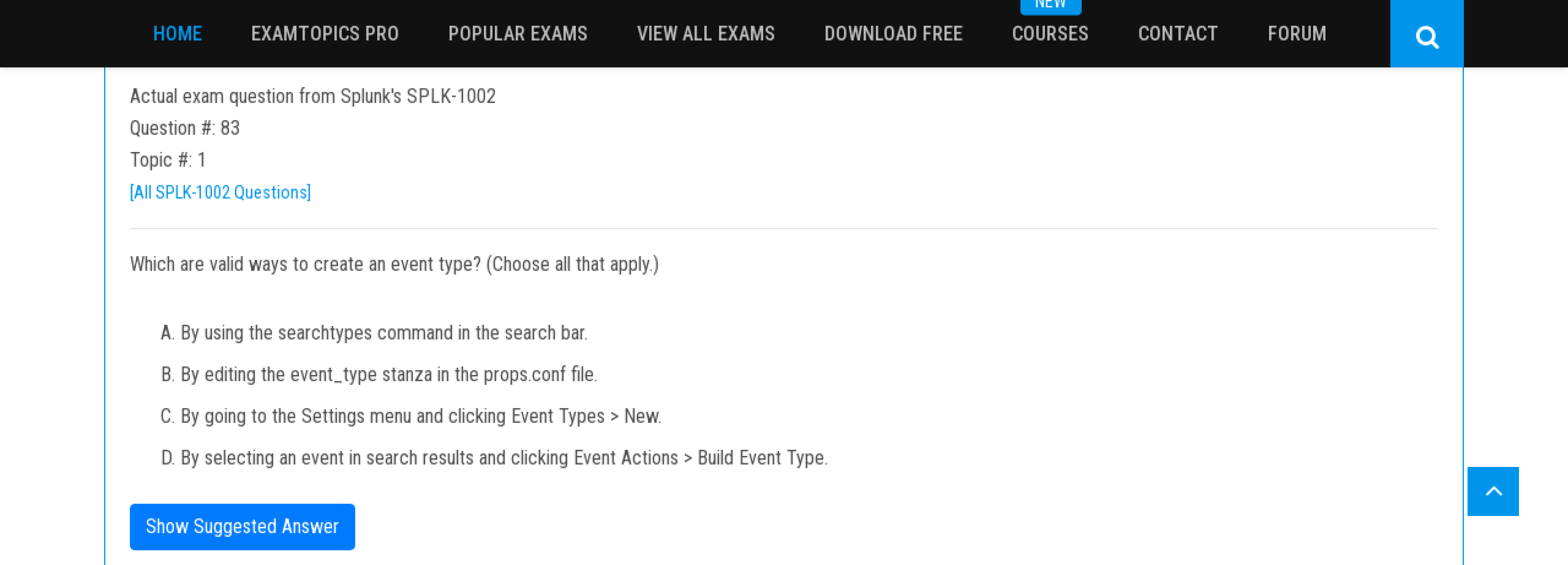
A. GET workflow actions must be configured with POST arguments.

B. Configuration of GET workflow actions includes choosing a sourcetype.

C. Label names for GET workflow actions must include a field name surrounded by dollar signs.

D. GET workflow actions can be configured to open the URI link in the current window or in a new window.

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 83

Topic #: 1

[All SPLK-1002 Questions]

Which are valid ways to create an event type? (Choose all that apply.)

A. By using the searchtypes command in the search bar.

B. By editing the event_type stanza in the props.conf file.

C. By going to the Settings menu and clicking Event Types > New.

D. By selecting an event in search results and clicking Event Actions > Build Event Type.

Actual exam question from Splunk's SPLK-1002

Question #: 84

Topic #: 1

[All SPLK-1002 Questions]

Which command can include both an over and a by clause to divide results into sub-groupings?

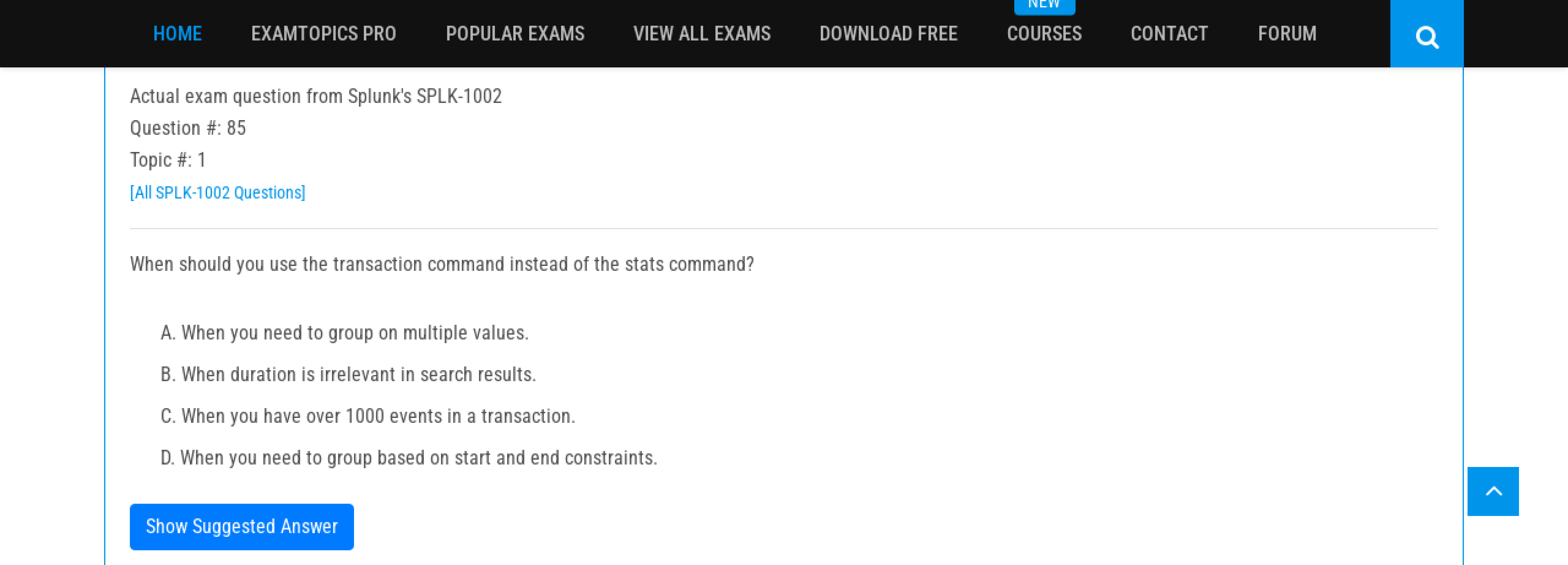
A. chart

B. stats

C. xyseries

D. transaction

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 85

Topic #: 1

[All SPLK-1002 Questions]

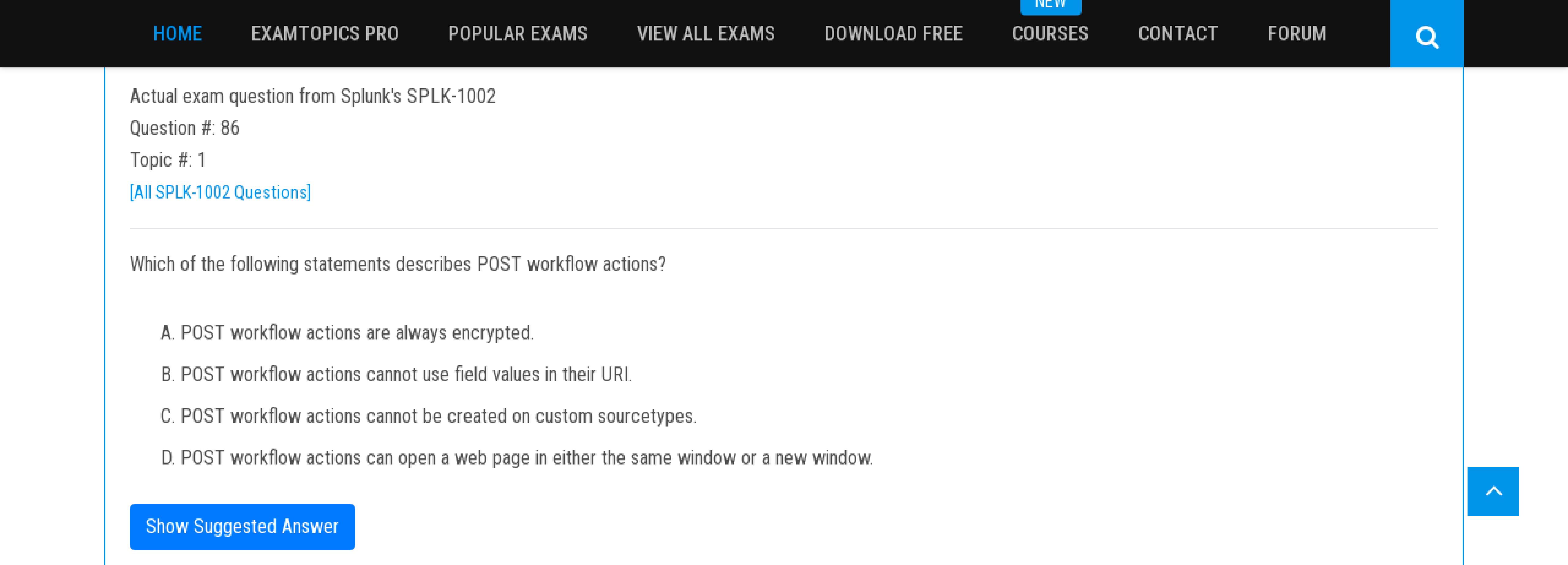
When should you use the transaction command instead of the stats command?

A. When you need to group on multiple values.

B. When duration is irrelevant in search results.

C. When you have over 1000 events in a transaction.

D. When you need to group based on start and end constraints.



Actual exam question from Splunk's SPLK-1002

Question #: 86

Topic #: 1

[All SPLK-1002 Questions]

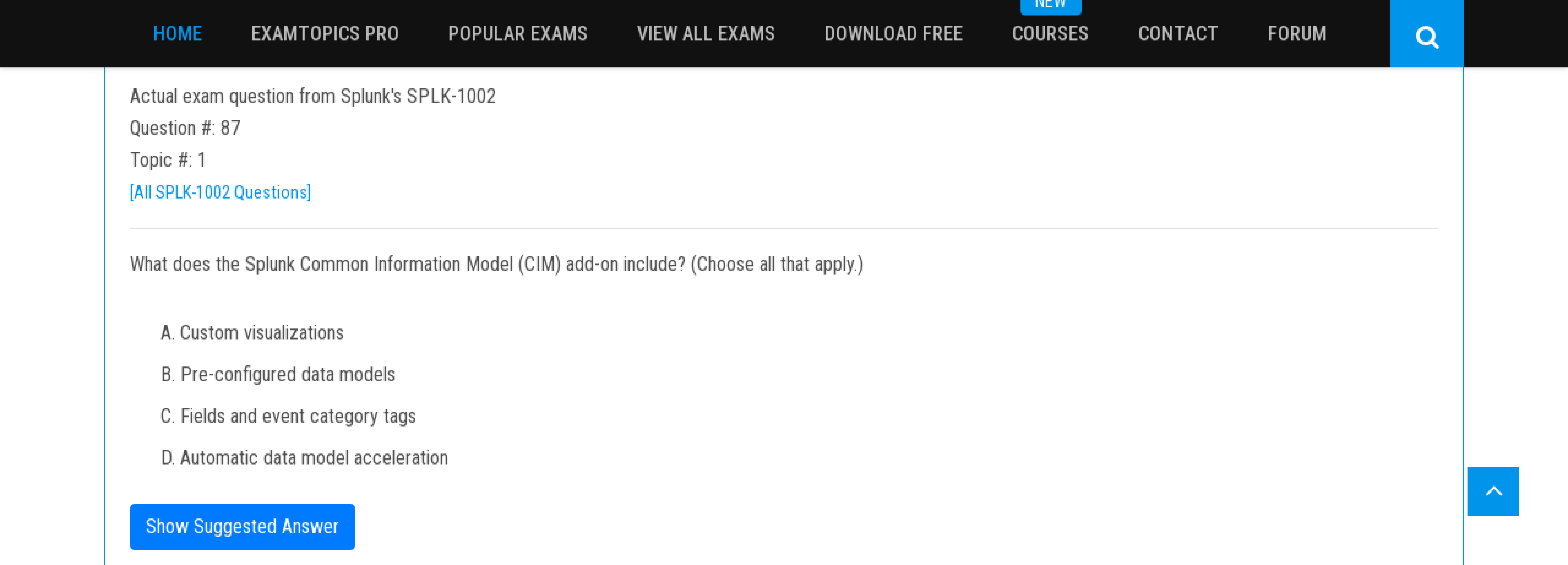
Which of the following statements describes POST workflow actions?

A. POST workflow actions are always encrypted.

B. POST workflow actions cannot use field values in their URI.

C. POST workflow actions cannot be created on custom sourcetypes.

D. POST workflow actions can open a web page in either the same window or a new window.



Actual exam question from Splunk's SPLK-1002

Question #: 87

Topic #: 1

[All SPLK-1002 Questions]

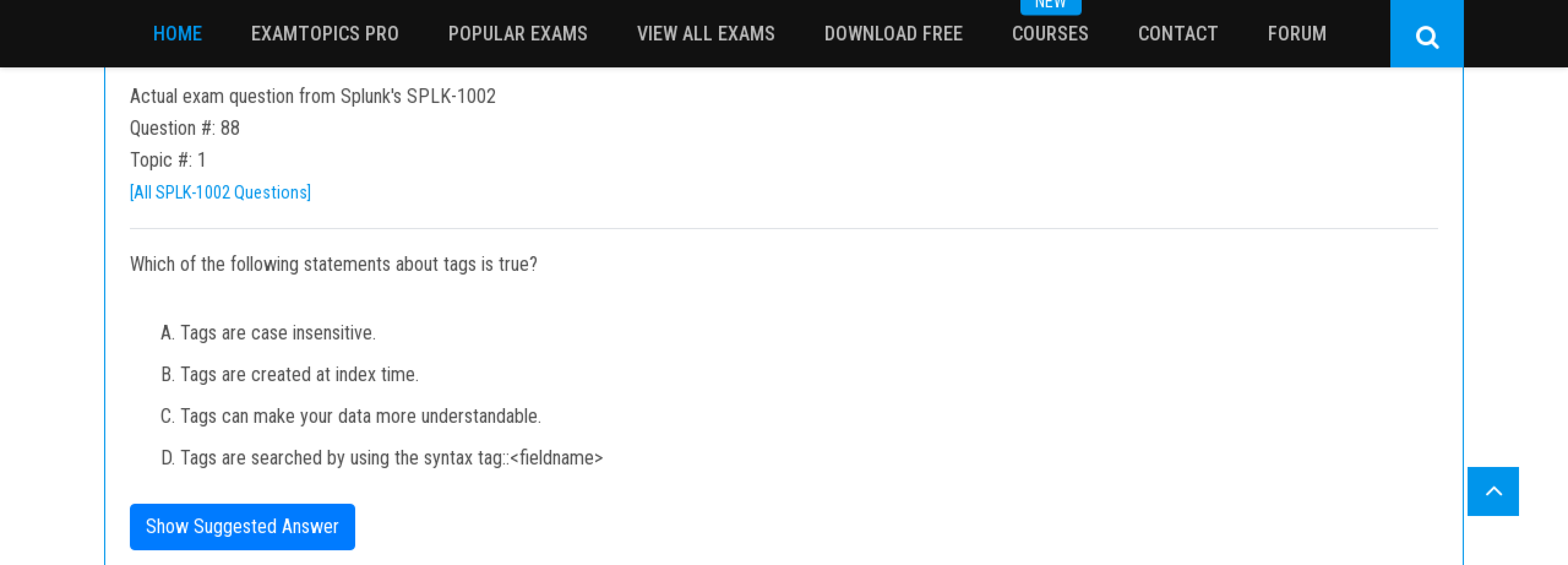
What does the Splunk Common Information Model (CIM) add-on include? (Choose all that apply.)

A. Custom visualizations

B. Pre-configured data models

C. Fields and event category tags

D. Automatic data model acceleration



Actual exam question from Splunk's SPLK-1002

Question #: 88

Topic #: 1

[All SPLK-1002 Questions]

Which of the following statements about tags is true?

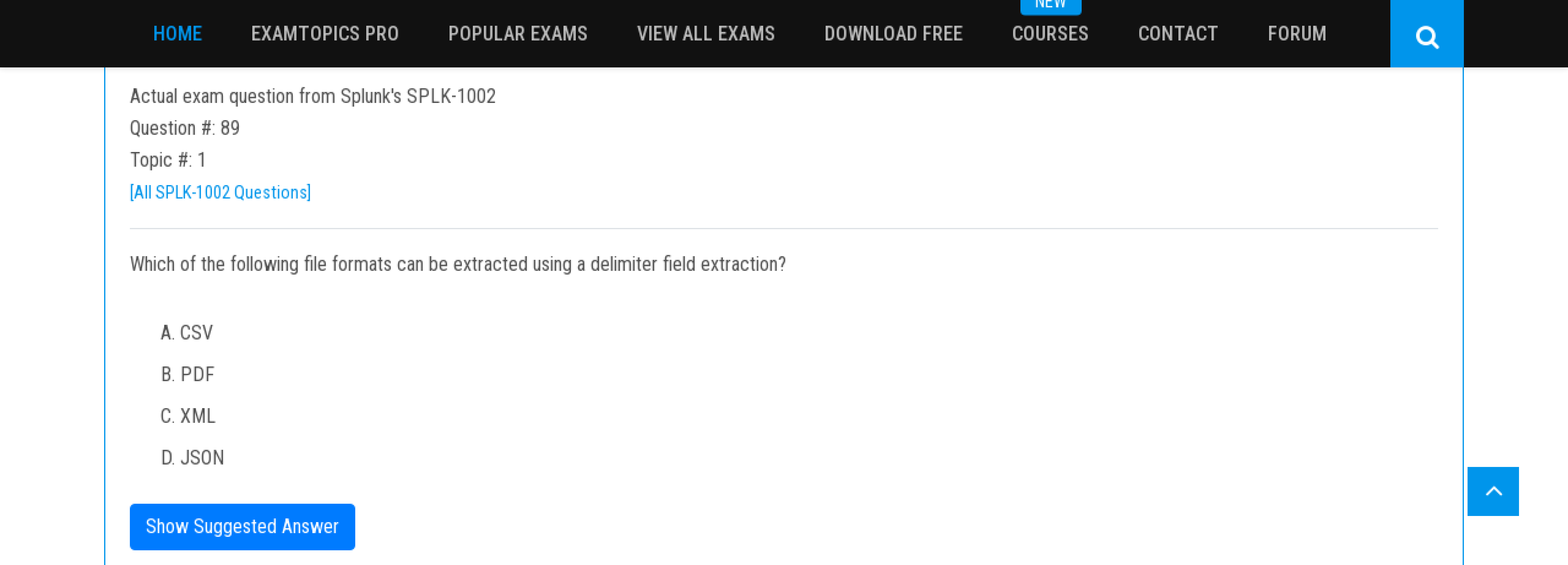
A. Tags are case insensitive.

B. Tags are created at index time.

C. Tags can make your data more understandable.

D. Tags are searched by using the syntax tag::<fieldname>

Show Suggested Answer



Actual exam question from Splunk's SPLK-1002

Question #: 89

Topic #: 1

[All SPLK-1002 Questions]

Which of the following file formats can be extracted using a delimiter field extraction?

A. CSV

B. PDF

C. XML

D. JSON