SPLK-1002 Q&As

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which is not a comparison operator in Splunk

A.

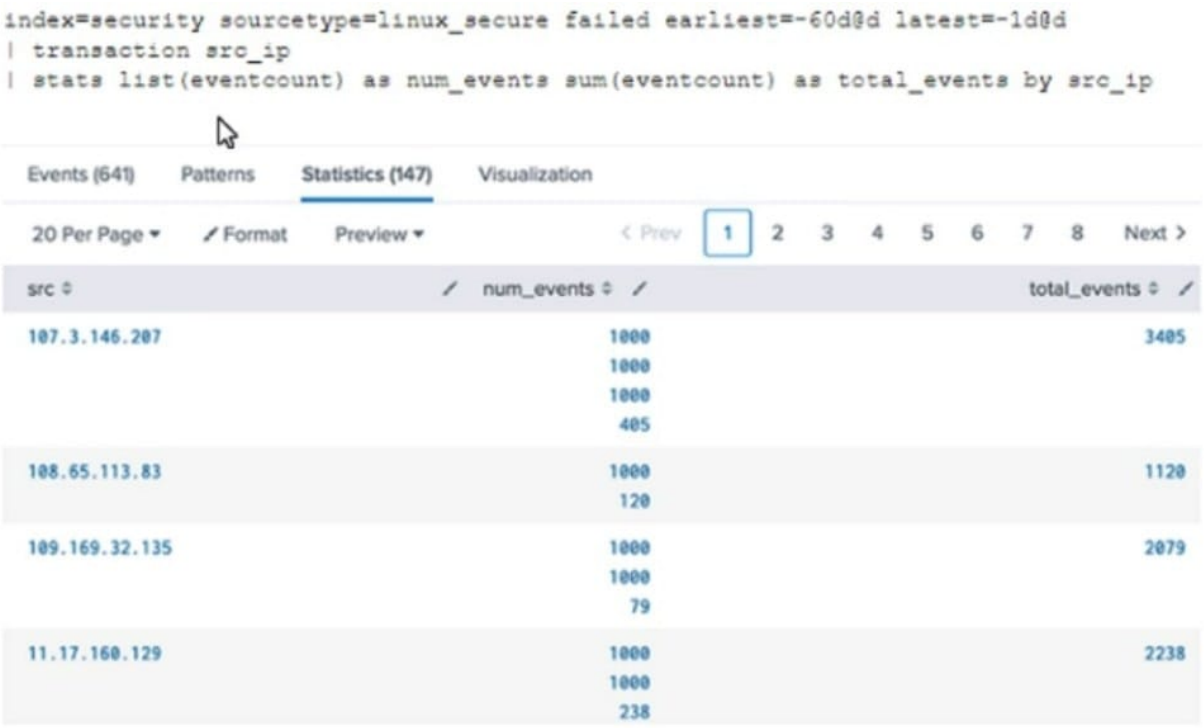
E. ?=

Correct Answer: E

Explanation: A comparison operator is a symbol that compares two values and returns a Boolean result (true or false)2. Splunk supports various comparison operators such as , =, !=, =, IN and LIKE2. However, ?= is not a valid comparison operator in Splunk and will cause a syntax error if used in a search string2. Therefore, option E is correct, while options A, B, C and D are incorrect because they are valid comparison operators in Splunk

QUESTION 2

Why would the following search produce multiple transactions instead of one?



A. The maxspan option is not included.

B. The transaction command has a limit of 1000 events per transaction.

C. The transaction and commands cannot be used together.

D. The stats list () function is used.

Correct Answer: A

Explanation: The correct answer is A. The maxspan option is not included1. In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command

groups all matching events into a single transaction1.

However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.

Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.

Here is an example of how you can use the maxspan option in a search:

index=main sourcetype=access_combined | transaction someuniqefield maxspan=1h In this search, the transaction command groups events that share the same someuniqefield value into a single transaction, but only if the time span

between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

QUESTION 3

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 action are shown in both the event and field menus.

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

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaPOSTworkflowacti on

QUESTION 4

Which search would limit an "alert" tag to the "host" field?

A. tag=alert

B. host::tag::alert

C. tag==alert

D. tag::host=alert

Correct Answer: D

Explanation: The search below would limit an "alert" tag to the "host" field.

tag::host=alert

The search does the following:

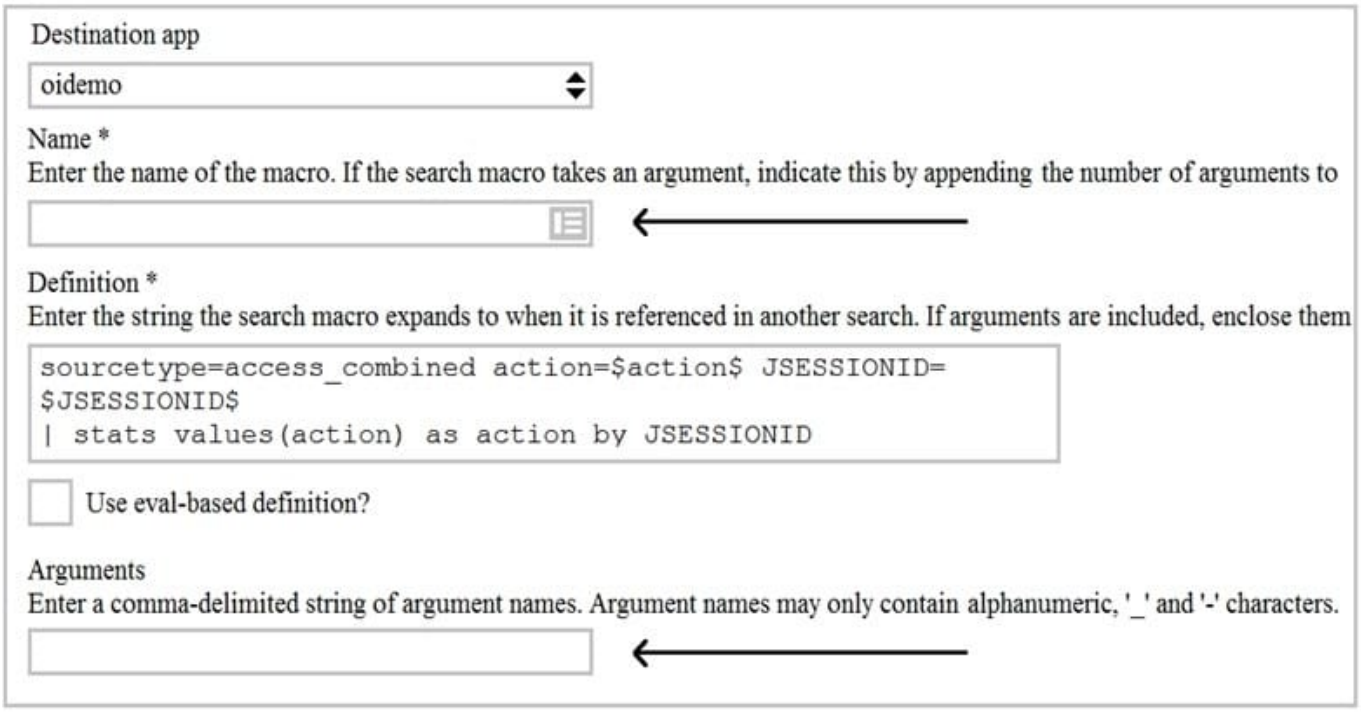
It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data.

It specifies tag::host=alert as the tag filter. This means that it will only return events that have an "alert" tag applied to their host field or host field value. It uses an equal sign (=) to indicate an exact match between the tag and the field or field

value.

QUESTION 5

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



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 $action$, $JESSIONID$.

Correct Answer: B

Reference:

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

The macro definition below shows a macro that tracks user sessions based on two arguments: action and

JSESSIONID.

sessiontracker(2)

The macro definition does the following:

It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string.

It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when it is executed.

It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed.

The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are

variables for the arguments that will be replaced by their values when the macro is executed.

Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.