Splunk SPLK-1002 Practice Questions

Shared by Dawson on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is true about Pivot?

Options:

A- Users can save reports from Pivot.
B- Users cannot share visualizations created with Pivot.
C- Users must use SPL to find events in a Pivot.
D- Users cannot create visualizations with Pivot.

Answer:

A

Explanation:

In Splunk, Pivot is a tool that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL)1.You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations12.

One of the features of Pivot is that it allows you to save your reports1.This can be useful when you want to reuse a report or share it with others1.Therefore, it's not true that users cannot share visualizations created with Pivot or that they must use SPL to find events in a Pivot12.It's also not true that users cannot create visualizations with Pivot, as creating visualizations is one of the main functions of Pivot12.

Question 2

Question Type: MultipleChoice

How is an event type created from the search window? (select all that apply)

Options:

A- In the top right corner, click Save As > Event Type.
B- In an event's detail dropdown, click Event Actions > Build Event Type.

C- Edit eventtypes.conf and add a new stanza.
D- Add | eventtype to the SPL and execute the search.

Answer:

A, C

Explanation:

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clickingSave Asand selectingEvent Type1.This opens theSave as Event Typedialog, where you can provide the event type name and optionally apply tags to it1.

You can also create an event type by editing theeventtypes.conffile and adding a new stanza1.Each stanza in theeventtypes.conffile represents an event type1.The stanza name is the name of the event type, and thesearchattribute specifies the search string that defines the event type1.

It's important to note that while you can use theeventtypecommand in a search to find events associated with a specific event type, adding| eventtypeto the SPL and executing the search does not create a new event type1.Similarly, clickingEvent Actions > Build Event Typein an event's detail dropdown does not create a new event type1.

Question 3

Question Type: MultipleChoice

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

Options:

A- Sets the maximum total time between events in a transaction.
B- Sets the maximum length of all 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.

Answer:

C

Question 4

Question Type: MultipleChoice

Which option best data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

Options:

A- Alerts
B- Email
C- Database
D- User permissions

Answer:

A, B, C

Explanation:

The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3.The CIM add-on includes several data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, options A, B and C are correct because they are names of some of the data models included in the CIM add-on. Option D is incorrect because User permissions is not a name of a data model in the CIM add-on.

Question 5

Question Type: MultipleChoice

What is a limitation of searches generated by workflow actions?

Options:

A- Searches generated by workflow action cannot use macros.
B- Searches generated by workflow actions must be less than 256 characters long.
C- Searches generated by workflow action must run in the same app as the workflow action.
D- Searches generated by workflow action run with the same permissions as the user running

them.

Answer:

D

Question 6

Question Type: MultipleChoice

For the following search, which command would further filter for only IP addresses present more than five times?

Options:

A- index=games I stats count as IP_count by IP B. | where IP_count > 5
B- index=games | search IP_Count > 5
C- index=games | where IP > 5
D- index=games I search IP > 5

Answer:

A

Explanation:

To filter for only IP addresses that appear more than five times in the search results for index=games, you can use a combination of the stats and where commands. The stats command counts the occurrences of each IP address and assigns the count to IP_count. The where command then filters the results to include only those IP addresses with a count greater than five.

Here is how the complete search would look:

index=games | stats count as IP_count by IP | where IP_count > 5

Splunk Docs: stats command

Splunk Docs: where command

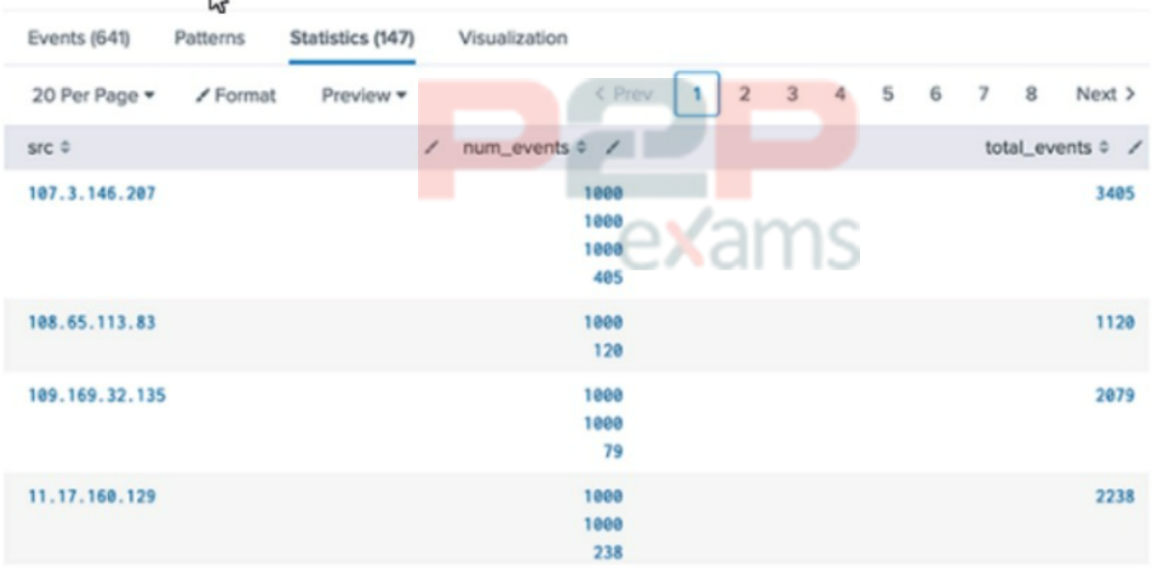
Splunk Answers: Filtering results using stats and where commands

Question 7

Question Type: MultipleChoice

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

```
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
```



Options:

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.

Answer:

A

Explanation:

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.