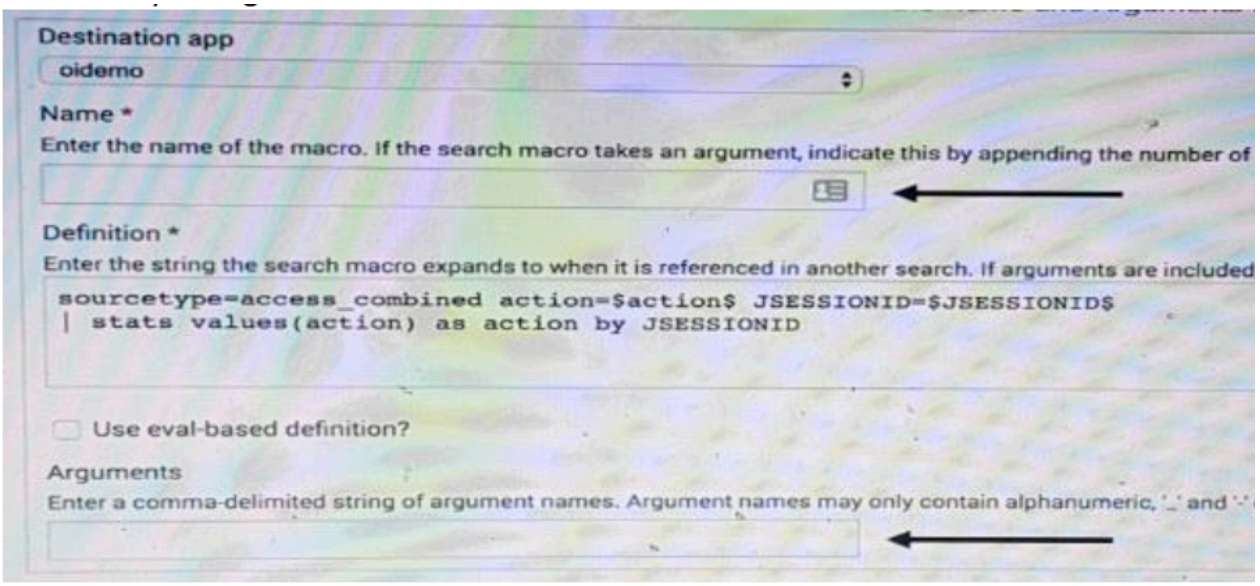
Splunk Core Certified Power User

1. 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 argument are action, JESSION.

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

C. The macro name is sessiontracker and the argument are sectional ,$ JESSIONIDS.

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

Answer(s): B

---

2. Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv

B. Tag= Priv*

C. Tag= Priv*

D. Tag= Privileged

Answer(s): D

---

3. Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *

B. | Search datamodel web web | filed web*

C. | datamodel web web field | search web*

D. Datamodel=web | search web | filed web*

Answer(s): A

---

4. Data model are composed of one or more of which of the fo-owing datasets? (select all that apply.)

- ☐ A. Events datasets
- ☐ B. Search datasets
- ☐ C. Transaction datasets
- ☐ D. Any child of event, transaction, and search datasets

Answer(s): A B C

---

5. 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.

Answer(s): D

---

6. 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.

Answer(s): D

---

7. Which of the following eval command function is valid?

A. Int ()

B. Count ( )

C. Print ()

D. Tostring ()

Answer(s): D

8. Which of the following statements describe the search string below?
dacamodel 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

Answer(s): C

---

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

A. Tag-

B. Tag

C. Tag=::

D. Tag::=

Answer(s): D

---

10. 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.

Answer(s): C

---

11. 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

Answer(s): B

---

12. 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.

Answer(s): A

---

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

- [ ] A. Tabs
- [ ] B. Pipes
- [ ] C. Spaces
- [ ] D. Commas

Answer(s): B C D

---

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

- [ ] A. index=main source=mySource oldField=* | 'makeMyField(oldField)' | table _time newField
- [ ] B. index=main source=mySource oldField=* | state if ('makeMyField(oldField ') | table _time
- [ ] C. index=main source=mySource oldField=* | eval newField= 'makeMyField(oldField) ' | table _time
- [ ] D. index=main source=mySource oldField=* | '"newField('makeMyField(oldField) ") ' " | table _time

Answer(s): A C

---

15. 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 URT link in the current window or in a new window

Answer(s): D

---

16. 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.

Answer(s): B

---

17. 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.

Answer(s): D

---

18. Which of the following statements describe calculated fields? (select 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.

Answer(s): A B D

---

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

A. Search string

B. Data model name

C. Permission setting

D. An eval statement

Answer(s): A

---

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

- [ ] A. `"hex"
- [ ] B. `"commas"
- [ ] C. `"Decimal"

- [ ] D. ``duration''

Answer(s): A B D
