DUMPSARENA

Splunk Core Certified Power User Exam

Splunk SPLK-1002

Version Demo

Total Demo Questions: 10

Total Premium Questions: 96

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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.

ANSWER: A B C

Explanation:

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

QUESTION NO: 2

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

ANSWER: B

Explanation:

Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

QUESTION NO: 3

In which Settings section are macros defined?

A. Fields

B. Tokens

C. Advanced Search

D. Searches, Reports, Alerts

ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/Definesearchmacros

QUESTION NO: 4

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

ANSWER: A B C

Explanation:

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

QUESTION NO: 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: B

QUESTION NO: 6

Which of the following statements describe the search below? (Choose all that apply.)

index=main | transaction clientip host maxspan=30s maxpause=5s

A. Events in the transaction occurred within 5 seconds.

B. It groups events that share the same clientip and host.

C. The first and last events are no more than 5 seconds apart.

D. The first and last events are no more than 30 seconds apart

ANSWER: A D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/Transaction

QUESTION NO: 7

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

ANSWER: B D

Explanation:

Reference: https://docs.splunk.com/Documentation/CIM/4.18.0/User/Overview

QUESTION NO: 8

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

A. 0

B. N/A

C. –

D. NULL

ANSWER: A

Explanation:

Reference: https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html

QUESTION NO: 9

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.

ANSWER: A C

QUESTION NO: 10

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.

ANSWER: A