

Free Questions for SPLK-2001 by certscare

Shared by Harrell on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When output_mode is not used, which element of a feed is a human readable name for a returned entry?

Options:

A- Author

B- Title

C- Link

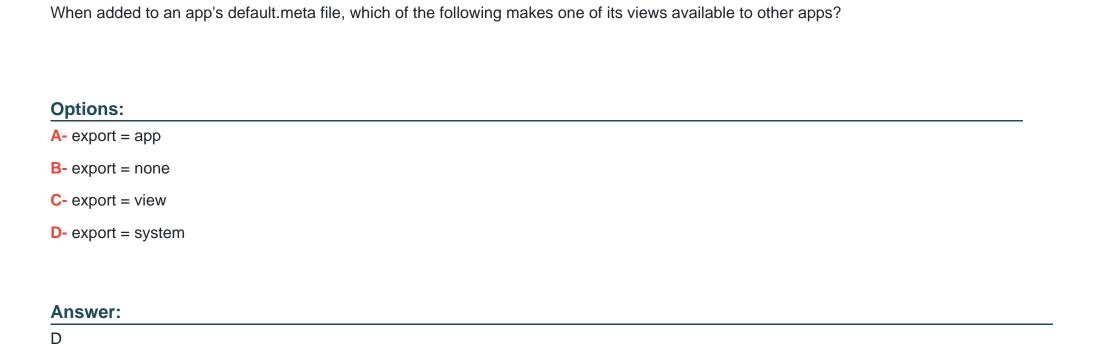
D- Id

Answer:

В

Question 2

Question Type: MultipleChoice



Question 3

Question Type: MultipleChoice

Which of the following are true of auto-refresh for dashboard panels? (Select all that apply.)

0	nt	io	n	S :
$\mathbf{\mathbf{\mathcal{C}}}$	νι			J .

- A- Applies to inline searches and saved searches.
- B- Enabling auto-refresh for a report requires editing XML.
- C- Post-processing searches are refreshed when their base searches are refreshed.
- D- Each post-processing search using the same base search can have a different refresh time.

Answer:

B, C

Question 4

Question Type: MultipleChoice

Which of the following is an example of a valid syntax for specifying an absolute time range modifier in a search?

Options:

A- earliest=01/01/2019:00:00:00

- B- earliest=01/01/2019T00:00:00
- C- earliest=2019-01-01 00:00:00
- **D-** earliest=2019-01-01T00:00:00

Answer:

Α

Question 5

Question Type: MultipleChoice

Given the following two files defining app navigation, which navigation options will be displayed to the end user? (Select all that apply.)

\$SPLUNK_HOME/etc/apps/app_name/default/data/ui/nav/default.xml

\$SPLUNK_HOME/etc/apps/app_name/local/data/ui/nav/default/xml

Options: A- Search

B- Reports

C- Datasets

D- Dashboards

Answer:

B, C

Question 6

Question Type: MultipleChoice

How can hiding or showing a panel by clicking on a chart or a table on the same form be performed?

Options:
A- By using vent drilldown.
B- By using workflow action.
C- By using contextual drilldown.
D- By using visualization drilldown.
Answer:
D
Question 7
Question Type: MultipleChoice
Which of the following is an example of a Splunk KV store use case? (Select all that apply.)
Options:
A- Stores checkpoint data for modular inputs.

B- Tracks workflow in an incident-review system.

- C- Indexes metrics data from remote HTTP sources.
- **D-** Stores application state as a user interacts with an app.

Answer:

A, B

Question 8

Question Type: MultipleChoice

Which type of command is tstats?

Options:

- A- Generating
- **B-** Transforming
- **C-** Centralized streaming
- **D-** Distributable streaming

-					
Λ	n	C	NA/		P =
М		J	VV	C	r:

Α

Question 9

Question Type: MultipleChoice

Which statements are true regarding HEC (HTTP Event Collector) tokens? (Select all that apply.)

Options:

- **A-** Multiple tokens can be created for use with different sourcetypes and indexes.
- B- The edit token http admin role capability is required to create a token.
- C- To create a token, send a POST request to services/collector endpoint.
- **D-** Tokens can be edited using the data/inputs/http/{tokenName} endpoint.

Answer:

A, C

To Get Premium Files for SPLK-2001 Visit

https://www.p2pexams.com/products/splk-2001

For More Free Questions Visit

https://www.p2pexams.com/splunk/pdf/splk-2001

