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 syntax is used to represent an argument in a macro definition?

A. "argument"

B. %argument%

C. `argument\\'

D. $argument$

Correct Answer: D

The correct answer is D.

A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain

another search macro within it, which is called a nested macro1.

To represent an argument in a macro definition, you need to use the dollar sign ($) character to enclose the argument name. For example, if you want to create a search macro that takes one argument named "object", you can use the

following syntax:

[my_macro(object)] search sourcetype= object

This will create a search macro named my_macro that takes one argument named object. When you call the macro in a search, you need to provide a value for the object argument, such as:

my_macro(web)

This will replace the object argument with the value web and run the following SPL code:

search sourcetype=web

The other options are not correct because they use quotation marks (\\' or '') or percentage signs (%) to represent arguments, which are not valid syntax for macro arguments. These characters will be interpreted as literal values instead of

variables.

References:

Use search macros in searches

QUESTION 2

What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.

B. The CIM provides a methodology to normalize data from different sources and source types.

C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.

D. The CIM is a data exchange initiative between software vendors.

Correct Answer: B

Explanation: The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

QUESTION 3

Which of the following examples would use a POST workflow action?

A. Perform an external IP lookup based on a domain value found in events.

B. Use the field values in an HTTP error event to create a new ticket in an external system.

C. Launch secondary Splunk searches that use one or more field values from selected events.

D. Open a web browser to look up an HTTP status code.

Correct Answer: B

The correct answer is B. Use the field values in an HTTP error event to create a new ticket in an external system.

A workflow action is a knowledge object that enables a variety of interactions between fields in events and other web resources. Workflow actions can create HTML links, generate HTTP POST requests, or launch secondary searches based

on field values1. There are three types of workflow actions that can be set up using Splunk Web: GET, POST, and Search2.

GET workflow actions create typical HTML links to do things like perform Google searches on specific values or run domain name queries against external WHOIS databases2.

POST workflow actions generate an HTTP POST request to a specified URI. This action type enables you to do things like creating entries in external issue management systems using a set of relevant field values2. Search workflow actions

launch secondary searches that use specific field values from an event, such as a search that looks for the occurrence of specific combinations of ipaddress and http_status field values in your index over a specific time range2.

Therefore, the example that would use a POST workflow action is B. Use the field values in an HTTP error event to create a new ticket in an external system. This example requires sending an HTTP POST request to the URI of the external

system with the field values from the event as arguments.

The other examples would use different types of workflow actions. These examples are:

A. Perform an external IP lookup based on a domain value found in events: This example would use a GET workflow action to create a link to an external IP lookup service with the domain value as a parameter.

C. Launch secondary Splunk searches that use one or more field values from selected events: This example would use a Search workflow action to run another Splunk search with the field values from the event as search terms. D. Open a web browser to look up an HTTP status code: This example would also use a GET workflow action to create a link to a web page that explains the meaning of the HTTP status code. References: Splexicon:Workflowaction About workflow actions in Splunk Web

QUESTION 4

Field aliases are used to _____ data

A. clean

B. transform

C. calculate

D. normalize

Correct Answer: D

QUESTION 5

_____ datasets can be added to root dataset to narrow down the search

A. parent

B. extracted

C. event

D. child

Correct Answer: D

Explanation: Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.