Free Questions for SPLK-2001 by actualtestdumps

Shared by Perkins on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which HTTP Event Collector (HEC) endpoint should be used to collect data in the following format?

{"message":"Hello World", "foo":"bar", "pony":"buttercup"}

Options:

A) data/inputs/http/{name}

B) services/collector/raw

C) services/collector

D) data/inputs/http

Answer:

B

Question 2

Question Type: MultipleChoice

Searching "index=_internal metrics | head 3" from Splunk Web returned the following events:

04-12-2018 18:39:43.514 +0200 INFO Metrics -- group=thruput, name=thruput, instantaneous_kbps=0.9651774014563425, instantaneous_eps=5.645638802094809, average_kbps=1.198995639527069, total_k_processed=2676, kb=29.91796875, ev=175, load_average=3.85888671875

04-12-2018 18:39:43.514 +0200 INFO Metrics -- group_thruput, name_syslog_output, instantaneous_kbps=0, instantaneous_eps_0, average_kbps=0, total_k_processed=0, kb=0, ev=0

04-12-2018 18:39:43.513 +0200 INFO Metrics -- group_thruput, name_index_thruput, instantaneous_kbps=0.9651773703189551, instantaneous_eps=4.87137960922438, average_kbps=1.1985932324065556, total_k_processed=2675, kb=29.91796875, ev=151

When the same search is required from a REST API call, which fields will be given? (Select all that apply.)

Options:

A) _raw

B) name

C) sourcetype

D) instantaneous_kbps

Answer:

A, C

Question 3

Question Type: MultipleChoice

There is a global search named "global_search" defined on a form as shown below:

index-_internal source-*splunkd.log | stats count by component, log_level

Which of the following would be a valid post-processing search? (Select all that apply.)

Options:

A) | tstats count

B) sourcetype=mysourcetype

C) stats sum(count) AS count by log level

D) search log_level=error | stats sum(count) AS count by component

Answer:

C, D

Question 4

Question Type: MultipleChoice

Searching "index=_internal metrics | head 3" from Splunk Web returned the following events:

04-12-2018 18:39:43.514 +0200 INFO Metrics -- group=thruput, name=thruput, instantaneous_kbps=0.9651774014563425, instantaneous_eps=5.645638802094809, average_kbps=1.198995639527069, total_k_processed=2676, kb=29.91796875, ev=175, load_average=3.85888671875

04-12-2018 18:39:43.514 +0200 INFO Metrics -- group_thruput, name_syslog_output, instantaneous_kbps=0, instantaneous_eps_0, average_kbps=0, total_k_processed=0, kb=0, ev=0

04-12-2018 18:39:43.513 +0200 INFO Metrics -- group_thruput, name_index_thruput, instantaneous_kbps=0.9651773703189551, instantaneous_eps=4.87137960922438, average_kbps=1.1985932324065556, total_k_processed=2675, kb=29.91796875, ev=151

When the same search is required from a REST API call, which fields will be given? (Select all that apply.)

Options:

A) _raw

B) name

C) sourcetype

D) instantaneous_kbps

Answer:

A, C

Question 5

Question Type: **MultipleChoice**

Which HTTP Event Collector (HEC) endpoint should be used to collect data in the following format?

{"message":"Hello World", "foo":"bar", "pony":"buttercup"}

Options:

A) data/inputs/http/{name}

B) services/collector/raw

C) services/collector

D) data/inputs/http

Answer:

B

Question 6

Question Type: **MultipleChoice**

There is a global search named "global_search" defined on a form as shown below:

index-_internal source-*splunkd.log | stats count by component, log_level

Which of the following would be a valid post-processing search? (Select all that apply.)

Options:

A) | tstats count

B) sourcetype=mysourcetype

C) stats sum(count) AS count by log level

D) search log_level=error | stats sum(count) AS count by component

Answer:

C, D