



# SPLK-2001<sup>Q&As</sup>

Splunk Certified Developer

## Pass Splunk SPLK-2001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/splk-2001.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Which type of command is tstats?

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

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats>

---

### QUESTION 2

When using the Splunk REST API, which of the following containers is/are included in the Atom Feed response? (Select all that apply.)

- A.
- B.
- C.
- D.

Correct Answer: BC

Reference: <https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing>

---

### QUESTION 3

When the search/jobs REST endpoint is called to execute a search, what can be done to reduce the results size in the results? (Select all that apply.)

- A. Use a generating search.
- B. Remove unneeded fields.
- C. Truncate the data, using selective functions.
- D. Summarize data, using analytic commands.

Correct Answer: AB

---

### QUESTION 4



How can indexer acknowledgement be enabled for HTTP Event Collector (HEC)? (Select all that apply.)

- A. No need to do anything, it is turned on by default.
- B. When a REST request is sent to create a token, the property for indexer acknowledgement must be set to 1.
- C. When a new HEC token is created in Splunk Web, select the checkbox labeled "Enable indexer acknowledgement".
- D. When the Global Settings for HEC are updated in Splunk Web, select the checkbox labeled "Enable indexer acknowledgement".

Correct Answer: CD

Reference: <https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/UsetheHTTPEventCollector>

---

### QUESTION 5

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.)

- A. \_raw
- B. name
- C. sourcetype
- D. instantaneous\_kbps

Correct Answer: AC

[SPLK-2001 PDF Dumps](#)

[SPLK-2001 VCE Dumps](#)

[SPLK-2001 Study Guide](#)