



Splunk

Exam Questions SPLK-2001

Splunk Certified Developer Exam

NEW QUESTION 1

What predefined drilldown tokens are available specifically for trellis layouts? (Select all that apply.)

- A. trellis.Xaxis
- B. trellis.Yaxis
- C. trellis.name
- D. trellis.value

Answer: CD

NEW QUESTION 2

When using the Splunk Web Framework to create a global search, which is the correct post-process syntax for the base search shown below?

```
var searchmain = new SearchManager({ id: ??base-search??, search: ??index= internal | head 10 | fields ??*??, preview: true, cache: true
});
```

- A. var mypostproc1 = new PostProcessManager {{ id: ??post1??, managerid: ??base-search??,search: ??| stats count by sourcetype??}};
- B. var mypostproc1 = new PostProcessManager({ id: ??post1??, managerid: ??base??,search: ??| stats count by sourcetype??});
- C. var mypostproc1 = new PostProcess({ id: ??post1??, managerid: ??base-search??,search: ??| search stats count by sourcetype??});
- D. You cannot create global searches in the Splunk Web Framework.

Answer: A

NEW QUESTION 3

Which of the following endpoints is used to authenticate with the Splunk REST API?

- A. /services/auth/login
- B. /services/session/login
- C. /services/auth/session/login
- D. /servicesNS/authentication/login

Answer: A

NEW QUESTION 4

Consider the following Python code snippet used in a Splunk add-on:

```
if not os.path.exists(full_path): self.doAction(full_path, header) else: f = open (full_path) oldORnew = f.readline().split(??,??) f.close()
```

An attacker could create a denial of service by causing an error in either the open() or readline() commands. What type of vulnerability is this?

- A. CWE-693: Protection Mechanism Failure
- B. CWE-562: Return of Stack Variable Address
- C. CWE-404: Improper Resource Shutdown or Release
- D. CWE-636: Not Failing Securely (??Failing Open??)

Answer: C

NEW QUESTION 5

Given a dashboard with a Simple XML extension in myApp, what is the XML reference for the file myJS.js located in myOtherApp in the location shown below?

\$SPLUNK_HOME/etc/apps/myOtherApp/appserver/static/javascript/

- A. <dashboard script=??myJs.js??>
- B. <dashboard script=??myOtherApp/myJS.js??>
- C. <dashboard script=??myOtherApp:javascript/myJS.js??>
- D. <dashboard script=??myOtherApp:appserver/static/javascript/myJS.js??>

Answer: A

NEW QUESTION 6

Which of the following statements describe oneshot searches? (Select all that apply.)

- A. Are always executed asynchronously.
- B. Can specify csv as an output format.
- C. Stream all results upon search completion.
- D. Can use auto_cancel to set a timeout limit.

Answer: BC

NEW QUESTION 7

Which of the following are benefits from using Simple XML Extensions? (Select all that apply.)

- A. Add custom layouts.
- B. Add custom graphics.
- C. Add custom behaviors.
- D. Limit Splunk license consumption based on host.

Answer: AC

NEW QUESTION 8

A user wants to add the token \$token_name\$ to a dashboard for use in a drilldown. Which token filter encodes URL values?

- A. \$\$token_name\$\$
- B. \$token_name|h\$
- C. \$token_name|n\$
- D. \$token_name|u\$

Answer: D

NEW QUESTION 9

Which of the following is an intended use of HTTP Event Collector tokens?

- A. A cookie.
- B. An HTTP header field.
- C. A JSON field in the HTTP request.
- D. A password in conjunction with login.

Answer: B

NEW QUESTION 10

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

- 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: BC

NEW QUESTION 10

How can event logs be collected from a remote Windows machine using a standard Splunk installation and no customization? (Select all that apply.)

- A. By configuring a WMI input.
- B. By using HTTP event collector.
- C. By using a Windows heavy forwarder.
- D. By using a Windows universal forwarder.

Answer: AD

NEW QUESTION 12

Which Splunk REST endpoint is used to create a KV store collection?

- A. /storage/collections
- B. /storage/kvstore/create
- C. /storage/collections/config
- D. /storage/kvstore/collections

Answer: A

NEW QUESTION 13

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

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

- A. data/inputs/http/{name}
- B. services/collector/raw
- C. services/collector
- D. data/inputs/http

Answer: B

NEW QUESTION 16

Which of the following options would be the best way to identify processor bottlenecks of a search?

- A. Using the REST API.
- B. Using the search job inspector.
- C. Using the Splunk Monitoring Console.
- D. Searching the Splunk logs using index=?? internal??.

Answer: C

NEW QUESTION 19

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

- 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: A

NEW QUESTION 23

Data can be added to a KV store collection in which of the following format(s)?

- A. JSON
- B. JSON, XML
- C. JSON, XML, CSV
- D. JSON, XML, CSV, TXT

Answer: A

NEW QUESTION 24

Which type of command is tstats?

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

Answer: A

NEW QUESTION 26

Which of the following ensures that quotation marks surround the value referenced by the token?

- A. \$token_name|s\$
- B. ??\$token_name\$??
- C. (\$token_name\$)
- D. \??\$token_name\$\??

Answer: A

NEW QUESTION 28

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

```
<search id=??global_search??>
<query>
index-_internal source=*splunkd.log | stats count by component, log_level
</query>
</search>
```

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

- 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: CD

NEW QUESTION 29

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

Answer: AC

NEW QUESTION 33

After updating a dashboard in myApp, a Splunk admin moves myApp to a different Splunk instance. After logging in to the new instance, the dashboard is not seen. What could have happened? (Select all that apply.)

- A. The dashboard??s permissions were set to private.
- B. User role permissions are different on the new instance.

- C. The admin deleted the myApp/local directory before packaging.
- D. Changes were placed in: \$SPLUNK_HOME/etc/apps/search/default/data/ui/nav

Answer: AB

NEW QUESTION 36

Which of these URLs could be used to construct a REST request to search the employee KV store collection to find records with a rating greater than or equal to 2 and less than 5?

- A. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={\$and:[{rating:{\$gte:2}}, {rating:{\$lt:5}}]}&output_mode=json??
- B. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={\$and:[{rating:{\$gte:2}}, {rating:{\$lt:5}}]}&output_mode=json??
- C. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={%22rating%22:{%22\$gte%22:2}},{%22\$and%22},{%22rating%22:{%22\$lt%22:5}}}&output_mode=json??
- D. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={%22\$and%22:[{%22rating%22:{%22\$gte%22:2}}, {%22rating%22:{%22\$lt%22:5}}]}&output_mode=json??

Answer: C

NEW QUESTION 39

Which of the following Simple XML elements configure panel link buttons? (Select all that apply.)

- A. <title>Open In Search</title>
- B. <option name=??link.visible??>true</option>
- C. <option name=??trellis.enabled??>false</option>
- D. <option name=??refresh.link.visible??>false</option>

Answer: AB

NEW QUESTION 43

Place content to set on page load inside which of the following Simple XML tags?

- A. <set></set>
- B. <eval></eval>
- C. <init></init>
- D. <value></value>

Answer: C

NEW QUESTION 48

Which of the following are valid parent elements for the event action shown below? (Select all that apply.)

<set token=??Token Name??>sourcetype=\$click.value|s\$</set>

- A. <eval>
- B. <change>
- C. <change><condition>
- D. <drilldown><condition>

Answer: AC

NEW QUESTION 52

Assuming permissions are set appropriately, which REST endpoint path can be used by someone with a power user role to access information about mySearch, a saved search owned by someone with a user role?

- A. /servicesNS/-/data/saved/searches/mySearch
- B. /servicesNS/object/saved/searches/mySearch
- C. /servicesNS/search/saved/searches/mySearch
- D. /servicesNS/-/search/saved/searches/mySearch

Answer: D

NEW QUESTION 55

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-2001 Practice Exam Features:

- * SPLK-2001 Questions and Answers Updated Frequently
- * SPLK-2001 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-2001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-2001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-2001 Practice Test Here](#)