

Exam Questions SPLK-2001

Splunk Certified Developer Exam

<https://www.2passeasy.com/dumps/SPLK-2001/>



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

What application security best practices should be adhered to while developing an app for Splunk? (Select all that apply.)

- A. Review the OWASP Top Ten List.
- B. Store passwords in clear text in .conf files.
- C. Review the OWASP Secure Coding Practices Quick Reference Guide.
- D. Ensure that third-party libraries that the app depends on have no outstanding CVE vulnerabilities.

Answer: AC

NEW QUESTION 6

When updating a knowledge object via REST, which of the following are valid values for the sharing Access Control List property?

- A. App
- B. User
- C. Global
- D. Nobody

Answer: A

NEW QUESTION 7

Which of the following search commands can be used to perform statistical queries on indexed fields in TSIDX files?

- A. stats
- B. tstats
- C. tscollect
- D. transaction

Answer: B

NEW QUESTION 8

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
<nav search_view=??search?? color=??#65A637??>
<view name=??search?? default=??true?? />
<view name=??datasets?? />
<view name=??reports?? />
<view name=??dashboards?? />
</nav>

$SPLUNK_HOME/etc/apps/app_name/local/data/ui/nav/default.xml
<nav search_view=??search?? color=??#65A637??>
<view name=??search?? default=??true?? />
<view name=??datasets?? />
<view name=??dashboards?? />
</nav>
```

- A. Search
- B. Reports
- C. Datasets
- D. Dashboards

Answer: BC

NEW QUESTION 9

A KV store collection can be associated with a namespace for which of the following users?

- A. Nobody
- B. Users in the admin role.
- C. Users in the admin and power roles.
- D. Users in the admin, power, and splunk-system-user roles.

Answer: B

NEW QUESTION 10

Suppose the following query in a Simple XML dashboard returns a table including hyperlinks:

```
<search>
<query>index news sourcetype web_proxy | table sourcetype title link
</query>
</search>
```

Which of the following is a valid dynamic drilldown element to allow a user of the dashboard to visit the hyperlinks contained in the link field?

- A. <option name ??link.openSearch.viewTarget">\$row.link\$</option>
- B. <drilldown><link target=?? blank">\$\$row.link\$\$</link></drilldown>
- C. <drilldown><link target="_blank">\$row.link|n\$</link></drilldown>
- D. <drilldown><link target ??_blank">http://localhost:8000/debug/refresh</link></drilldown>

Answer: A

NEW QUESTION 10

Which of the following will unset a token named my_token?

- A. <unset>\$my_token\$</unset>
- B. <unset token=??my_token??></unset>
- C. <set token=??my_token??>>false</token>
- D. <set token=??my_token??>disabled</set>

Answer: B

NEW QUESTION 11

Which of the following are ways to get a list of search jobs? (Select all that apply.)

- A. Access Activity > Jobs with Splunk Web.
- B. Use Splunk REST to query the /services/search/jobs endpoint.
- C. Use Splunk REST to query the /services/saved/searches endpoint.
- D. Use Splunk REST to query the /services/search/sid/results endpoint.

Answer: AB

NEW QUESTION 15

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 18

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 21

Which files within an app contain permissions information? (Select all that apply.)

- A. local/metadata.conf
- B. metadata/local.meta
- C. default/metadata.conf
- D. metadata/default.meta

Answer: CD

NEW QUESTION 24

Which of the following are characteristics of an add-on? (Select all that apply.)

- A. Requires navigation file.
- B. Occupies a unique namespace within Splunk.
- C. Can depend on add-ons for correct operation.
- D. Contains technology or components not intended for reuse by other apps.

Answer: AD

NEW QUESTION 26

In a DELETE request, what would omitting the value of _key from the REST endpoint do?

- A. Clean the KV store, deleting all content.
- B. Produce the syntax error ??Key value missing??.
- C. Cause all records in a collection to be deleted.
- D. Mean that the _key value must be passed as an argument.

Answer: C

NEW QUESTION 27

Log files related to Splunk REST calls can be found in which indexes? (Select all that apply.)

- A. _audit
- B. _internal
- C. _thefishbucket
- D. _blockssignature

Answer: AB

NEW QUESTION 31

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.

Answer: AB

NEW QUESTION 33

Which of the following are security best practices for Splunk app development? (Select all that apply.)

- A. Store passwords in clear text in .conf files.
- B. Implement security in software development lifecycle.
- C. Manually test application with the controls listed in the OWASP Security Testing Guide.
- D. Use a dynamic scanner such as OWASP ZAP to scan web application components for vulnerabilities.

Answer: CD

NEW QUESTION 37

A fellow Splunk administrator is reviewing an app that has been downloaded from splunkbase and deployed in an organization. The admin has e-mailed the following configuration snippet with a brief note that says ??fix the permissions??.

In what configuration file should the snippet be placed? []

access = read : [*], write : [admin] export - system

(Assume that \$APP_HOME refers to the path that the app is installed, e.g. \$SPLUNK_HOME/etc/apps/<app name>)

- A. \$APP_HOME/default/app.conf
- B. \$APP_HOME/local/default.meta
- C. \$APP_HOME/metadata/local.meta
- D. \$SPLUNK_HOME/etc/system/local/server.conf

Answer: D

NEW QUESTION 40

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 42

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 43

A dashboard is taking too long to load. Several searches start with the same SPL. How can the searches be optimized in this dashboard? (Select all that apply.)

- A. Convert searches to include NOT expressions.
- B. Restrict the time range of the search as much as possible.
- C. Replace | stats command with | transaction command wherever possible.
- D. Convert the common SPL into a Global Search and convert the other searches to post-processing searches.

Answer: CD

NEW QUESTION 48

Which of the following describes a Splunk custom visualization?

- A. A visualization with custom colors.
- B. Any visualization available in Splunk.
- C. A visualization in Splunk modified by the user.
- D. A visualization that uses the Splunk Custom Visualization API.

Answer: D

NEW QUESTION 51

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-2001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-2001 Product From:

<https://www.2passeasy.com/dumps/SPLK-2001/>

Money Back Guarantee

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