

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

Which of the following is true of a namespace?

- A. The namespace is a type of token filter.
- B. The namespace includes an app attribute which cannot be a wildcard.
- C. The namespace filters the knowledge objects returned by the REST API.
- D. The namespace does not filter knowledge objects returned by the REST API.

Answer: D

NEW QUESTION 3

Which of the following formats are valid for a Splunk REST URI?

- A. host:port/endpoint
- B. scheme://host/servicesNS/*
- C. \$SPLUNK_HOME/services/endpoint
- D. scheme://host:port/services/endpoint

Answer: D

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

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 is a customization option for the Open in Search panel link button?

- A. Display the refresh time.
- B. Show the Export Results button.
- C. Show link buttons at the bottom of a panel.
- D. Define an alternative search or target view to use.

Answer: D

NEW QUESTION 8

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 9

Which of the following are requirements for arguments sent to the data/indexes endpoint? (Select all that apply.)

- A. Be url-encoded.
- B. Specify the datatype.
- C. Include the bucket path.
- D. Include the name argument.

Answer: BD

NEW QUESTION 10

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??.

Answer: CD

NEW QUESTION 10

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 14

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 15

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 20

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 24

Which items below are configured in inputs.conf? (Select all that apply.)

- A. A modular input written in Python.
- B. A file input monitoring a JSON file.
- C. A custom search command written in Python.
- D. An HTTP Event Collector as receiver of data from an app.

Answer: AD

NEW QUESTION 26

How can hiding or showing a panel by clicking on a chart or a table on the same form be performed?

- A. By using vent drilldown.
- B. By using workflow action.
- C. By using contextual drilldown.
- D. By using visualization drilldown.

Answer: D

NEW QUESTION 28

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 30

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 31

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 36

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 41

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 44

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 48

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 52

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 57

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 61

Which event handler uses the `<selection>` element to support pan and zoom functionality?

- A. Visualization event handler
- B. Form input event handler
- C. Condition event handler
- D. Search event handler

Answer: A

NEW QUESTION 63

The response message from a successful Splunk REST call includes an `<entry>` element. What is contained in an `<entry>` element?

- A. A dictionary of `<eai:acl>` elements.
- B. Metadata encapsulating the `<content>` element.
- C. A response code indicating success or failure.
- D. An individual element in an `<entries>` collection.

Answer: B

NEW QUESTION 66

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 68

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 71

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 73

For a KV store, a lookup stanza in the transforms.conf file must contain which of the following? (Select all that apply.)

- A. collection
- B. fields_list
- C. external_type
- D. internal_type

Answer: AB

NEW QUESTION 74

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 78

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 81

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 85

.....

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