

Splunk

Exam Questions SPLK-2001

Splunk Certified Developer Exam



NEW QUESTION 1

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 2

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 3

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 4

Which statements are true regarding HEC (HTTP Event Collector) tokens? (Select all that apply.)

- A. Multiple tokens can be created for use with different sourcetypes and indexes.
- B. The edit token http admin role capability is required to create a token.
- C. To create a token, send a POST request to services/collector endpoint.
- D. Tokens can be edited using the data/inputs/http/{tokenName} endpoint.

Answer: AC

NEW QUESTION 5

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 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

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 8

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

- A. <feed>
- B. <entry>
- C. <content>
- D. <namespace>

Answer: BC

NEW QUESTION 9

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 10

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

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 15

Which of the following log files contains logs that are most relevant to Splunk Web?

- A. audit.log
- B. metrics.log
- C. splunkd.log
- D. web_service.log

Answer: D

NEW QUESTION 18

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 23

Which of the following is a security best practice?

- A. Enable XSS.
- B. Eliminate all escape characters.
- C. Ensure the app passes App Certification.
- D. Ensure components have no Common Vulnerabilities and Exposures (CVE) vulnerabilities.

Answer: D

NEW QUESTION 25

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 28

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 30

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 33

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 38

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 39

Which type of command is tstats?

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

Answer: A

NEW QUESTION 40

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 45

Which of the following are reserved field names in a KV Store? (Select all that apply.)

- A. _key
- B. _time
- C. _user
- D. _source

Answer: BC

NEW QUESTION 49

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 54

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 59

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 61

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 62

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 65

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)