Splunk

Exam Questions SPLK-2001

Splunk Certified Developer Exam

NEW QUESTION 1
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 2
To delete the record with a _key value of smith from the sales collection, a DELETE request should be sent to which REST endpoint?

A. /storage/collections/sales/smith
B. /storage/kvstore/data/sales/smith
C. /storage/collections/data/sales/smith
D. /storage/kvstore/collections/sales/smith

Answer: C

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
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 6
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 7
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 8
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 9
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 10
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 10
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 11
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 13
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 16
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 19
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 21
Which type of command is tstats?

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

Answer: A

NEW QUESTION 25
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 28
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 32
Which of the following statements define a namespace?

A. The namespace is a combination of the user and the app.
B. The namespace is a combination of the user, the app, and the role.
C. The namespace is a combination of the user, the app, the role, and the sharing level.
D. The namespace is a combination of the user, the app, the role, the sharing level, and the permissions.

Answer: A

NEW QUESTION 37
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 38
......

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