

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

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 3

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 4

Using Splunk Web to modify config settings for a shared object, a revised config file with those changes is placed in which directory?

- A. \$SPLUNK_HOME/etc/apps/myApp/local
- B. \$SPLUNK_HOME/etc/system/default/
- C. \$SPLUNK_HOME/etc/system/local
- D. \$SPLUNK_HOME/etc/apps/myApp/default

Answer: A

NEW QUESTION 5

Which of the following is an example of a Splunk KV store use case? (Select all that apply.)

- A. Stores checkpoint data for modular inputs.
- B. Tracks workflow in an incident-review system.
- C. Indexes metrics data from remote HTTP sources.
- D. Stores application state as a user interacts with an app.

Answer: AB

NEW QUESTION 6

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 7

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 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

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 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 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 12

Which of the following are valid request arguments for the REST search endpoints? (Select all that apply.)

- A. latest_time=rt
- B. latest_time=now
- C. earliest_time=-5h@h
- D. earliest_time=rt_10m@m

Answer: BC

NEW QUESTION 17

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 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 22

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 25

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 29

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 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 37

Which of the following statements describe an HEC token? (Select all that apply.)

- A. Maps to a Splunk user.
- B. Can be used to download data.
- C. Is a GUID (globally unique identifier).
- D. Can be created in Splunk Web or using REST endpoints.

Answer: CD

NEW QUESTION 42

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 43

In order to successfully accelerate a report, which criteria must the search meet? (Select all that apply.)

- A. Cannot use event sampling.
- B. Use a transforming command.
- C. Use a standard Splunk visualization.
- D. Commands before the first transforming command must be streamable.

Answer: ABD

NEW QUESTION 47

Which of the following is a way to monitor app performance? (Select all that apply.)

- A. Using Splunk logs.
- B. Using the search job inspector.

- C. Using the Monitoring Console.
- D. Using the storage/collections/config REST endpoint.

Answer: AC

NEW QUESTION 48

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 53

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 56

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 58

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 62

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 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](#)