SPLK-2001 Q&As

Splunk Certified Developer

Pass Splunk SPLK-2001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-2001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

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.

Correct Answer: A

QUESTION 2

Which of the following are types of event handlers? (Select all that apply.)

A. Search

B. Set token

C. Form input

D. Visualization

Correct Answer: CD

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/EventHandlerReference

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

Correct Answer: D

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

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Admin/Howtoeditaconfigurationfile

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.

Correct Answer: AC

Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/

QUESTION 6

Place content to set on page load inside which of the following Simple XML tags?

A.

B.

C.

D.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens

QUESTION 7

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\\')

Correct Answer: C

Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/

QUESTION 8

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.

Correct Answer: ABD

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Knowledge/ Manageacceleratedsearchsummaries

QUESTION 9

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

A. _audit

B. _internal

C. _thefishbucket

D. _blocksignature

Correct Answer: AB

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Troubleshooting/Whatdatagetslogged

QUESTION 10

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

Correct Answer: AC

QUESTION 11

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

A. A dictionary of elements.

B. Metadata encapsulating the element.

C. A response code indicating success or failure.

D. An individual element in an collection.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 12

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

Correct Answer: CD

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/VisualizationTrellis

QUESTION 13

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.

Correct Answer: D

QUESTION 14

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.

Correct Answer: AB

QUESTION 15

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.

B.

C.

D.

Correct Answer: A

Reference: https://dev.splunk.com/enterprise/docs/developapps/visualizedata/usewebframework/ modifydashboards/