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 output_mode is not used, which element of a feed is a human readable name for a returned entry?

A. Author

B. Title

C. Link

D. Id

Correct Answer: B

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

QUESTION 2

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

Correct Answer: D

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

QUESTION 3

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 4

Which of the following are benefits from using Simple XML Extensions? (Select all that apply.)

A. Add custom layouts.

B. Add custom graphics.

C. Add custom behaviors.

D. Limit Splunk license consumption based on host.

Correct Answer: AC

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

QUESTION 5

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.

Correct Answer: AD

QUESTION 6

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.

Correct Answer: D

QUESTION 7

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

Correct Answer: A

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

QUESTION 8

Which type of command is tstats?

A. Generating

B. Transforming

C. Centralized streaming

D. Distributable streaming

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats

QUESTION 9

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".

Correct Answer: C

QUESTION 10

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

Correct Answer: CD

Reference: https://dev.splunk.com/enterprise/docs/devtools/customsearchcommands/ manageaccesstocustom/

QUESTION 11

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 12

Which event handler uses the element to support pan and zoom functionality?

A. Visualization event handler

B. Form input event handler

C. Condition event handler

D. Search event handler

Correct Answer: A

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

QUESTION 13

A dashboard is taking too long to load. Several searches start with the same SPL. How can the searches be optimized in this dashboard? (Select all that apply.)

A. Convert searches to include NOT expressions.

B. Restrict the time range of the search as much as possible.

C. Replace | stats command with | transaction command wherever possible.

D. Convert the common SPL into a Global Search and convert the other searches to post-processing searches.

Correct Answer: CD

QUESTION 14

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

Correct Answer: A

Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/ usetherestapitomanagekv/

QUESTION 15

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

SPLK-2001 PDF Dumps SPLK-2001 VCE Dumps SPLK-2001 Braindumps