DUMPS ARENA

Splunk Certified Developer Exam

Splunk SPLK-2001

Version Demo

Total Demo Questions: 10

Total Premium Questions: 72

Buy Premium PDF

QUESTION NO: 1

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

QUESTION NO: 2

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: A D

QUESTION NO: 3

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

QUESTION NO: 4

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: C D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/UsetheHTTPEventCollector

QUESTION NO: 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.

ANSWER: A D

QUESTION NO: 6

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: C D

Explanation:

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

QUESTION NO: 7

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: B C

Explanation:

Reference: https://community.splunk.com/t5/Getting-Data-In/How-to-create-Search-via-REST-api-in-verbose-mode/td-p/406400

QUESTION NO: 8

Which type of command is tstats?

A. Generating

B. Transforming

C. Centralized streaming

D. Distributable streaming

ANSWER: A

Explanation:

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

QUESTION NO: 9

Which of the following will unset a token named my_token?

A. `<unset>$my_token$</unset>`

B. `<unset token="my_token"></unset>`

C. `<set token="my_token">false</token>`

D. `<set token="my_token">disabled</set>`

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

Explanation:

Reference: https://community.splunk.com/t5/Dashboards-Visualizations/Unset-a-token-if-it-is-equal-to-a-value/m-p/353512

QUESTION NO: 10

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/FormateventsforHTTPEventCollector