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.certbus.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

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 2

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 3

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 4

When using the Splunk REST API, which of the following containers is/are included in the Atom Feed response? (Select all that apply.)

A.

B.

C.

D.

Correct Answer: BC

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

QUESTION 5

Which of the following describes a Splunk custom visualization?

A. A visualization with custom colors.

B. Any visualization available in Splunk.

C. A visualization in Splunk modified by the user.

D. A visualization that uses the Splunk Custom Visualization API.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/AdvancedDev/CustomVizTutorial

QUESTION 6

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

Correct Answer: C

QUESTION 7

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 8

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.

Correct Answer: CD

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

QUESTION 9

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 10

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 11

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 12

Which statements are true regarding HEC (HTTP Event Collector) tokens? (Select all that apply.)

A. Multiple tokens can be created for use with different sourcetypes and indexes.

B. The edit token http admin role capability is required to create a token.

C. To create a token, send a POST request to services/collector endpoint.

D. Tokens can be edited using the data/inputs/http/{tokenName} endpoint.

Correct Answer: AC

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.

Correct Answer: AD

QUESTION 14

What must be done when calling the serviceNS endpoint?

A. Authenticate with an admin user.

B. Specify the user and app context in the URI.

C. Authenticate with the user of the required context.

D. Pass the user and app context in the request payload.

Correct Answer: B

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

QUESTION 15

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. $token_name|u$

Correct Answer: D

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

[SPLK-2001 Study Guide](#)   [SPLK-2001 Exam Questions](#)   [SPLK-2001 Braindumps](#)