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.pass4itsure.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

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

Correct Answer: BC

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

QUESTION 2

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.

Correct Answer: AC

QUESTION 3

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.

Correct Answer: BD

QUESTION 4

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 5

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 6

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.

Correct Answer: CD

QUESTION 7

Which of the following is an example of a valid syntax for specifying an absolute time range modifier in a search?

A. earliest=01/01/2019:00:00:00

B. earliest=01/01/2019T00:00:00

C. earliest=2019-01-01 00:00:00

D. earliest=2019-01-01T00:00:00

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Search/Specifytimemodifiersinyoursearch

QUESTION 8

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 9

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

QUESTION 10

In a DELETE request, what would omitting the value of _key from the REST endpoint do?

A. Clean the KV store, deleting all content.

B. Produce the syntax error "Key value missing".

C. Cause all records in a collection to be deleted.

D. Mean that the _key value must be passed as an argument.

Correct Answer: C

QUESTION 11

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 12

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 13

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 14

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.

Correct Answer: B

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

QUESTION 15

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