SPLK-2001 Dumps

Splunk Certified Developer Exam

https://www.certleader.com/SPLK-2001-dumps.html

NEW QUESTION 1
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

Answer: CD

NEW QUESTION 2
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.

Answer: A

NEW QUESTION 3
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

Answer: C

NEW QUESTION 4
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.

Answer: D

NEW QUESTION 5
Which of the following is an example of a Splunk KV store use case? (Select all that apply.)

A. Stores checkpoint data for modular inputs.
B. Tracks workflow in an incident-review system.
C. Indexes metrics data from remote HTTP sources.
D. Stores application state as a user interacts with an app.

Answer: AB

NEW QUESTION 6
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.

Answer: AC

NEW QUESTION 7
Which of the following statements describe oneshot searches? (Select all that apply.)

A. Are always executed asynchronously.
B. Can specify csv as an output format.
C. Stream all results upon search completion.
D. Can use auto_cancel to set a timeout limit.

Answer: BC

NEW QUESTION 8

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.

Answer: BD

NEW QUESTION 9
Which of the following search commands can be used to perform statistical queries on indexed fields in TSIDX files?

A. stats
B. tstats
C. tscollect
D. transaction

Answer: B

NEW QUESTION 10
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. $token_name|u$

Answer: D

NEW QUESTION 10
How can event logs be collected from a remote Windows machine using a standard Splunk installation and no customization? (Select all that apply.)

A. By configuring a WMI input.
B. By using HTTP event collector.
C. By using a Windows heavy forwarder.
D. By using a Windows universal forwarder.

Answer: AD

NEW QUESTION 14
Which of the following are types of event handlers? (Select all that apply.)

A. Search
B. Set token
C. Form input
D. Visualization

Answer: CD

NEW QUESTION 19
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

Answer: CD

NEW QUESTION 23
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

Answer: AB

NEW QUESTION 28
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.

Answer: CD

NEW QUESTION 32
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.

Answer: AB

NEW QUESTION 33
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.

Answer: AC

NEW QUESTION 38
Place content to set on page load inside which of the following Simple XML tags?

A.
B.
C.
D.

Answer: C

NEW QUESTION 41
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SPLK-2001 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-2001-dumps.html