Splunk

Exam Questions SPLK-2001

Splunk Certified Developer Exam

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
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 3
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.

Answer: AC

NEW QUESTION 4
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 5
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 6
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 7
Given the following two files defining app navigation, which navigation options will be displayed to the end user? (Select all that apply.)

```
$SPLUNK_HOME/etc/apps/app_name/default/data/ui/nav/default.xml
<nav search_view=??search?? color=??#65A637??>
<view name=??search?? default=??true?? />
<view name=??datasets?? />
<view name=??reports?? />
<view name=??dashboards?? />
</nav>
$SPLUNK_HOME/etc/apps/app_name/local/data/ui/nav/default/xml
<nav search_view=??search?? color=??#65A637??>
<view name=??search?? default=??true?? />
<view name=??datasets?? />
<view name=??dashboards?? />
</nav>
```

A. Search
B. Reports
C. Datasets
D. Dashboards

Answer: BC

NEW QUESTION 8
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

NEW QUESTION 9
Suppose the following query in a Simple XML dashboard returns a table including hyperlinks:
<search>
<query>index news sourcetype web_proxy | table sourcetype title link
</query>
</search>
Which of the following is a valid dynamic drilldown element to allow a user of the dashboard to visit the hyperlinks contained in the link field?

A. <option name ??link.openSearch.viewTarget">$row.link$</option>
B. <drilldown><link target=?? blank">$$row.link$$</link></drilldown>
C. <drilldown><link target="_blank">$row.link|n$</link></drilldown>
D. <drilldown><link target ??_blank">http://localhost:8000/debug/refresh</link></drilldown>

Answer: A

NEW QUESTION 10
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: AD

NEW QUESTION 10
How can hiding or showing a panel by clicking on a chart or a table on the same form be performed?

A. By using vent drilldown.
B. By using workflow action.
C. By using contextual drilldown.
D. By using visualization drilldown.

Answer: D

NEW QUESTION 11
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>

Answer: B

NEW QUESTION 14
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

Answer: D

NEW QUESTION 17
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

NEW QUESTION 19
Which of the following are true of auto-refresh for dashboard panels? (Select all that apply.)

A. Applies to inline searches and saved searches.
B. Enabling auto-refresh for a report requires editing XML.
C. Post-processing searches are refreshed when their base searches are refreshed.
D. Each post-processing search using the same base search can have a different refresh time.

Answer: BC

NEW QUESTION 20
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??.

Answer: C

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 27
Data can be added to a KV store collection in which of the following format(s)?

A. JSON
B. JSON, XML
C. JSON, XML, CSV
D. JSON, XML, CSV, TXT

Answer: A

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 37
Which type of command is tstats?

A. Generating
B. Transforming
C. Centralized streaming
D. Distributable streaming

Answer: A

NEW QUESTION 38
Which event handler uses the <selection> element to support pan and zoom functionality?

A. Visualization event handler
B. Form input event handler
C. Condition event handler
D. Search event handler

Answer: A

NEW QUESTION 43
The response message from a successful Splunk REST call includes an <entry> element. What is contained in an <entry> element?

A. A dictionary of <eai:acl> elements.
B. Metadata encapsulating the <content> element.
C. A response code indicating success or failure.
D. An individual element in an <entries> collection.

Answer: B

NEW QUESTION 48
A fellow Splunk administrator is reviewing an app that has been downloaded from splunkbase and deployed in an organization. The admin has e-mailed the following configuration snippet with a brief note that says ??fix the permissions??.
In what configuration file should the snippet be placed? []
access = read : [*], write : [admin] export - system
(Assume that $APP_HOME refers to the path that the app is installed, e.g. $SPLUNK_HOME/etc/apps/<app name>)

A. $APP_HOME/default/app.conf
B. $APP_HOME/local/default.meta
C. $APP_HOME/metadata/local.meta
D. $SPLUNK_HOME/etc/system/local/server.conf

Answer: D

NEW QUESTION 49
Which of the following statements define a namespace?

A. The namespace is a combination of the user and the app.
B. The namespace is a combination of the user, the app, and the role.
C. The namespace is a combination of the user, the app, the role, and the sharing level.
D. The namespace is a combination of the user, the app, the role, the sharing level, and the permissions.

Answer: A

NEW QUESTION 50
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.

Answer: ABD

NEW QUESTION 53
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 54
Place content to set on page load inside which of the following Simple XML tags?

A. <set></set>
B. <eval></eval>
C. <init></init>
D. <value></value>

Answer: C

NEW QUESTION 58
Which of the following are valid parent elements for the event action shown below? (Select all that apply.)
<set token=??Token Name??>sourcetype=$click.value|s$</set>

A. <eval>
B. <change>
C. <change><condition>
D. <drilldown><condition>

Answer: AC

NEW QUESTION 59
......

Relate Links

100% Pass Your SPLK-2001 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-2001-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/