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
Which of the following endpoints is used to authenticate with the Splunk REST API?

A. /services/auth/login
B. /services/session/login
C. /services/auth/session/login
D. /servicesNS/authentication/login

Answer: A

NEW QUESTION 4
Given a dashboard with a Simple XML extension in myApp, what is the XML reference for the file myJS.js located in myOtherApp in the location shown below?
$SPLUNK_HOME/etc/apps/myOtherApp/appserver/static/javascript/

A. <dashboard script=??myJs.js??>
B. <dashboard script=??myOtherApp/myJS.js??>
C. <dashboard script=??myOtherApp:javascript/myJS.js??>
D. <dashboard script=??myOtherApp:appserver/static/javascript/myJS.js??>

Answer: A

NEW QUESTION 5
Using Splunk Web to modify config settings for a shared object, a revised config file with those changes is placed in which directory?

A. $SPLUNK_HOME/etc/apps/myApp/local
B. $SPLUNK_HOME/etc/system/default/
C. $SPLUNK_HOME/etc/system/local
D. $SPLUNK_HOME/etc/apps/myApp/default

Answer: A

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 is a customization option for the Open in Search panel link button?

A. Display the refresh time.
B. Show the Export Results button.
C. Show link buttons at the bottom of a panel.
D. Define an alternative search or target view to use.

Answer: D

NEW QUESTION 8
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.

Answer: AC

NEW QUESTION 9
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 10
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: CD

NEW QUESTION 10
When using the Splunk REST API, which of the following containers is/are included in the Atom Feed response? (Select all that apply.)

A. <feed>
B. <entry>
C. <content>
D. <namespace>

Answer: BC

NEW QUESTION 13
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 17
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 19
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 21
Which of the following are ways to get a list of search jobs? (Select all that apply.)

A. Access Activity > Jobs with Splunk Web.
B. Use Splunk REST to query the /services/search/jobs endpoint.
C. Use Splunk REST to query the /services/saved/searches endpoint.
D. Use Splunk REST to query the /services/search/sid/results endpoint.

Answer: AB

NEW QUESTION 25
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 28
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 29
Which Splunk REST endpoint is used to create a KV store collection?

A. /storage/collections
B. /storage/kvstore/create
C. /storage/collections/config
D. /storage/kvstore/collections

Answer: A

NEW QUESTION 34
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 39
When output_mode is not used, which element of a feed is a human readable name for a returned entry?

A. Author
B. Title
C. Link
D. Id

Answer: B

NEW QUESTION 44
Which type of command is tstats?

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

Answer: A

NEW QUESTION 48
Which of the following ensures that quotation marks surround the value referenced by the token?

A. $token_name|s$
B. ??$token_name$??
C. ($token_name$)
D. \??$token_name$\??

Answer: A

NEW QUESTION 52
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: CD

NEW QUESTION 57
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 61
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 64
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 66
When added to an app??s default.meta file, which of the following makes one of its views available to other apps?

A. export = app
B. export = none
C. export = view
D. export = system

Answer: D

NEW QUESTION 71
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 76
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 81
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 85
There is a global search named ??global_search?? defined on a form as shown below:
<search id=??global_search??>
<query>
index-_internal source-*splunkd.log | stats count by component, log_level
</query>
</search>
Which of the following would be a valid post-processing search? (Select all that apply.)

A. | tstats count
B. sourcetype=mysourcetype
C. stats sum(count) AS count by log level
D. search log_level=error | stats sum(count) AS count by component

Answer: CD

NEW QUESTION 90
After updating a dashboard in myApp, a Splunk admin moves myApp to a different Splunk instance. After logging in to the new instance, the dashboard is not seen. What could have happened? (Select all that apply.)

A. The dashboard??s permissions were set to private.
B. User role permissions are different on the new instance.
C. The admin deleted the myApp/local directory before packaging.
D. Changes were placed in: $SPLUNK_HOME/etc/apps/search/default/data/ui/nav

Answer: AB

NEW QUESTION 92
Which of these URLs could be used to construct a REST request to search the employee KV store collection to find records with a rating greater than or equal to 2 and less than 5?

A. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={$and:[{rating:{$gte:2}},{rating:{$lt:5}}]}&output_mode-json??
B. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={$and:[{rating:$gte:2}},{rating:{$lt:5}}]}&output_mode=json??
C. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={%22rating%22:{%22$gte%22:2}},{%22$and%22},{%22rating%22:{% 22$lt%22:5}}}&output_mode=json??
D. ??http://localhost:8089/servicesNS/nobody/search/storage/collections/data/employees?query={%22$and%22:[{%22rating%22:{%22$gte%22:2}},{%22rating%22:{% 22$lt%22:5}}]}&output_mode=json??

Answer: C

NEW QUESTION 94
A dashboard is taking too long to load. Several searches start with the same SPL. How can the searches be optimized in this dashboard? (Select all that apply.)

A. Convert searches to include NOT expressions.
B. Restrict the time range of the search as much as possible.
C. Replace | stats command with | transaction command wherever possible.
D. Convert the common SPL into a Global Search and convert the other searches to post-processing searches.

Answer: CD

NEW QUESTION 98
......