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
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
Consider the following Python code snippet used in a Splunk add-on:
if not os.path.exists(full_path): self.doAction(full_path, header) else: f = open (full_path) oldORnew = f.readline().split(??,??) f.close()
An attacker could create a denial of service by causing an error in either the open() or readline() commands. What type of vulnerability is this?

A. CWE-693: Protection Mechanism Failure
B. CWE-562: Return of Stack Variable Address
C. CWE-404: Improper Resource Shutdown or Release
D. CWE-636: Not Failing Securely (??Failing Open??)

Answer: C

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
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 6
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

Answer: A

NEW QUESTION 7
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 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
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 10
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

Answer: BC

NEW QUESTION 10
Which of the following is a security best practice?

A. Enable XSS.
B. Eliminate all escape characters.
C. Ensure the app passes App Certification.
D. Ensure components have no Common Vulnerabilities and Exposures (CVE) vulnerabilities.

Answer: D

NEW QUESTION 15
Which HTTP Event Collector (HEC) endpoint should be used to collect data in the following format?
{??message??:??Hello World??, ??foo??:??bar??, ??pony??:??buttercup??}

A. data/inputs/http/{name}
B. services/collector/raw
C. services/collector
D. data/inputs/http

Answer: B

NEW QUESTION 18
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 24
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 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 29
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 30
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 33
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 38
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 39
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 44
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 49
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 53
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 56
Which of the following Simple XML elements configure panel link buttons? (Select all that apply.)

A. <title>Open In Search</title>
B. <option name=??link.visible??>true</option>
C. <option name=??trellis.enabled??>false</option>
D. <option name=??refresh.link.visible??>false</option>

Answer: AB

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
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 63
Assuming permissions are set appropriately, which REST endpoint path can be used by someone with a power user role to access information about mySearch, a saved search owned by someone with a user role?

A. /servicesNS/-/data/saved/searches/mySearch
B. /servicesNS/object/saved/searches/mySearch
C. /servicesNS/search/saved/searches/mySearch
D. /servicesNS/-/search/saved/searches/mySearch

Answer: D

NEW QUESTION 67
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-2001 Practice Exam Features:

* SPLK-2001 Questions and Answers Updated Frequently

* SPLK-2001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year