Free Questions for SPLK-2001 by dumpshq

Shared by Smith on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In order to successfully accelerate a report, which criteria must the search meet? (Select all that apply.)

Options:

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:

A, B, D

Question 2

Question Type: MultipleChoice

There is a global search named "global_search" defined on a form as shown below:

index-_internal source-*splunkd.log | stats count by component, log_level

Which of the following would be a valid post-processing search? (Select all that apply.)

Options:

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:

C, D

Question 3

Question Type: MultipleChoice

What application security best practices should be adhered to while developing an app for Splunk? (Select all that apply.)

Options:

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:

A, C

Question 4

Question Type: MultipleChoice

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

Options:

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

Question 5

Question Type: MultipleChoice

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?

Options:

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

Question 6

Question Type: MultipleChoice

What must be done when calling the serviceNS endpoint?

Options:

A- Authenticate with an admin user.

B- Specify the user and app context in the URI.

C- Authenticate with the user of the required context.

D- Pass the user and app context in the request payload.

Answer:

B

Question 7

Question Type: MultipleChoice

Which of the following is true of a namespace?

Options:

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

Question 8

Question Type: MultipleChoice

Which of the following options would be the best way to identify processor bottlenecks of a search?

Options:

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