Actual exam question from Splunk's SPLK-2001

Question #: 1

Topic #: 1

[All SPLK-2001 Questions]

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 ג€link.openSearch.viewTarget">$row.link$</option>

B. <drilldown> <link target=ג€ blank">$$row.link$$</link> </drilldown>

C. <drilldown> <link target="_blank">$row.link|n$</link> </drilldown>

D. <drilldown> <link target ג€_blank">http://localhost:8000/debug/refresh</link> </drilldown>

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 2

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 3

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 4

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 5

Topic #: 1

[All SPLK-2001 Questions]

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 ı€Enable indexer acknowledgementı€.

D. When the Global Settings for HEC are updated in Splunk Web, select the checkbox labeled ı€Enable indexer acknowledgementı€.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 6

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 7

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 8

Topic #: 1

[All SPLK-2001 Questions]

Which of the following are characteristics of an add-on? (Select all that apply.)

A. Requires navigation file.

B. Occupies a unique namespace within Splunk.

C. Can depend on add-ons for correct operation.

D. Contains technology or components not intended for reuse by other apps.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 9

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 10

Topic #: 1

[All SPLK-2001 Questions]

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=ɹ€ internalɹ€.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 11

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 12

Topic #: 1

[All SPLK-2001 Questions]

What must be done when calling the serviceNS endpoint?

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 13

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 14

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 15

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 16

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 17

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 18

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 19

Topic #: 1

[All SPLK-2001 Questions]

Which type of command is tstats?

A. Generating

B. Transforming

C. Centralized streaming

D. Distributable streaming

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 20

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 21

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 22

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 23

Topic #: 1

[All SPLK-2001 Questions]

Which of the following is an example of a valid syntax for specifying an absolute time range modifier in a search?

A. earliest=01/01/2019:00:00:00

B. earliest=01/01/2019T00:00:00

C. earliest=2019-01-01 00:00:00

D. earliest=2019-01-01T00:00:00

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 24

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 25

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 26

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 27

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 28

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 29

Topic #: 1

[All SPLK-2001 Questions]

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

A. Search

B. Set token

C. Form input

D. Visualization

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 30

Topic #: 1

[All SPLK-2001 Questions]

Which of the following describes a Splunk custom visualization?

A. A visualization with custom colors.

B. Any visualization available in Splunk.

C. A visualization in Splunk modified by the user.

D. A visualization that uses the Splunk Custom Visualization API.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 31

Topic #: 1

[All SPLK-2001 Questions]

Searching `index=_internal metrics | head 3` from Splunk Web returned the following events:

04-12-2018 18:39:43.514 +0200 INFO Metrics `" group=thruput, name=thruput, instantaneous_kbps=0.9651774014563425, instantaneous_eps=5.645638802094809, average_kbps=1.198995639527069, total_k_processed=2676, kb=29.91796875, ev=175, load_average=3.85888671875

04-12-2018 18:39:43.514 +0200 INFO Metrics `" group_thruput, name_syslog_output, instantaneous_kbps=0, instantaneous_eps_0, average_kbps=0, total_k_processed=0, kb=0, ev=0

04-12-2018 18:39:43.513 +0200 INFO Metrics `" group_thruput, name_index_thruput, instantaneous_kbps=0.9651773703189551, instantaneous_eps=4.87137960922438, average_kbps=1.1985932324065556, total_k_processed=2675, kb=29.91796875, ev=151

When the same search is required from a REST API call, which fields will be given? (Select all that apply.)

A. _raw

B. name

C. sourcetype

D. instantaneous_kbps

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 32

Topic #: 1

[All SPLK-2001 Questions]

Which of the following are reserved field names in a KV Store? (Select all that apply.)

A. _key

B. _time

C. _user

D. _source

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 33

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 34

Topic #: 1

[All SPLK-2001 Questions]

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'

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 35

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 36

Topic #: 1

[All SPLK-2001 Questions]

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>

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 37

Topic #: 1

[All SPLK-2001 Questions]

Which of the following Simple XML elements configure panel link buttons? (Select all that apply.)

A. <title>Open In Search</title>

B. <option name=ı€link.visibleı€>true</option>

C. <option name=ı€trellis.enabledı€>false</option>

D. <option name=ı€refresh.link.visibleı€>false</option>

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 38

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 39

Topic #: 1

[All SPLK-2001 Questions]

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>

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 40

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 41

Topic #: 1

[All SPLK-2001 Questions]

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')

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 42

Topic #: 1

[All SPLK-2001 Questions]

Which of the following formats are valid for a Splunk REST URI?

A. host:port/endpoint

B. scheme://host/servicesNS/*/

C. $SPLUNK HOME/services/endpoint

D. scheme://host:port/services/endpoint

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 43

Topic #: 1

[All SPLK-2001 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 44

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 45

Topic #: 1

[All SPLK-2001 Questions]

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. $token_name|u$

Show Suggested Answer

Actual exam question from Splunk's SPLK-2001

Question #: 46

Topic #: 1

[All SPLK-2001 Questions]

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.

Show Suggested Answer