SPLK-2001.VCEplus.premium.exam.70q

Number: SPLK-2001
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

SPLK-2001

Splunk Certified Developer

Version 1.0

Exam A

QUESTION 1

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>
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/BuildandeditdashboardswithSimplifiedXML

QUESTION 2 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 3 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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Search/SupervisejobswiththeJobspage

QUESTION 4 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/visualizedata/usewebframework/modifydashboards/

QUESTION 5 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”.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/UsetheHTTPEventCollector

QUESTION 6 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`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/DashboardPermissions

QUESTION 7 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.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
QUESTION 8 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/devtools/java/sdk-java/howtousesdkjava/howtoworkjobjava/

QUESTION 10 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"`.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11 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.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
QUESTION 12 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 13
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`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 14
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Admin/Howtoeditaconfigurationfile

QUESTION 15
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.

Correct Answer: AC
Section: (none)
Explanation
Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/

QUESTION 16
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`

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/Savedsearches

QUESTION 17 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.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Knowledge/Manageacceleratedsearchsummaries

QUESTION 18 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which type of command is `tstats`?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats

QUESTION 20 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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/

QUESTION 21 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Search/Specifytimemodifiersinyoursearch

QUESTION 24 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25 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`

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/setpermissionsforobjects/

QUESTION 26
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 27 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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/usetherestapitomanagekv/

QUESTION 28 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 Which of the following are types of event handlers? (Select all that apply.)

A. Search
B. Set token
C. Form input
D. Visualization

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/EventHandlerReference

QUESTION 30
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/AdvancedDev/CustomVizTutorial

QUESTION 31
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`

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 Which of the following are reserved field names in a KV Store? (Select all that apply.)

A. `_key`
B. `_time`
C. `_user`
D. `_source`

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/aboutkvstorecollections/

QUESTION 33 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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 34
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'`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35 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`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Troubleshooting/WhatSplunklogsaboutitself

QUESTION 36 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>`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens

QUESTION 37
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>`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/SplunkCloud/latest/Viz/DrilldownLinkToURL

QUESTION 38 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 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>`

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 40 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`

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.splunk.com/t5/Getting-Data-In/How-to-create-Search-via-REST-api-in-verbose-mode/td-p/406400

QUESTION 41
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’)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/

QUESTION 42 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`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/HECExamples

QUESTION 44
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 45 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. `$token_name|u$`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens

QUESTION 46 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/EventHandlerReference

QUESTION 48 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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/VisualizationTrellis

QUESTION 49
How can event logs be collected from a remote Windows machine using a standard Splunk installation and no customization? (Select all that apply.)

A. By configuring a WMI input.
B. By using HTTP event collector.
C. By using a Windows heavy forwarder.
D. By using a Windows universal forwarder.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51 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`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Troubleshooting/Whatdatagetslogged

QUESTION 52 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`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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">`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/visualizedata/usewebframework/modifydashboards/

QUESTION 54 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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/

QUESTION 55 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 56 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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 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. `\"$token_name$\"`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens

QUESTION 58 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/FormateventsforHTTPEventCollector

QUESTION 59
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.

Correct Answer: AB
Section: (none)
Explanation
Explanation/Reference:

QUESTION 60 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61 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>
```

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 In a `DELETE` request, what would omitting the value of `_key` from the REST endpoint do?

A. Clean the KV store, deleting all content.
B. Produce the syntax error `"Key value missing"`.
C. Cause all records in a collection to be deleted.
D. Mean that the `_key` value must be passed as an argument.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64 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`

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/devtools/customsearchcommands/manageaccesstocustom/

QUESTION 65 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67 Which of the following search commands can be used to perform statistical queries on indexed fields in TSIDX files?

A. `stats`
B. `tstats`
C. `tscollect`
D. `transaction`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats

QUESTION 68 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>`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.splunk.com/t5/Dashboards-Visualizations/Unset-a-token-if-it-is-equal-to-a-value/m-p/353512

QUESTION 69 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/usingconfigurationfiles/

QUESTION 70
For a KV store, a lookup stanza in the `transforms.conf` file must contain which of the following? (Select all that apply.)
A. `collection`
B. `fields_list`
C. `external_type`
D. `internal_type`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Knowledge/ConfigureKVstorelookups