Question #1 *Topic 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 ɹ€link.openSearch.viewTarget">$row.link$</option>

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

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

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

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/BuildandeditdashboardswithSimplifiedXML

Community vote distribution
C (100%)

mohanmk95 1 year, 10 months ago

Selected Answer: C

PLEASE do refer the drilldown concepts
upvoted 2 times

New_user 3 years, 7 months ago

Answer is C. "A" is not a drilldown option
upvoted 2 times

ucsdmiami2020 3 years, 4 months ago

Agreed Answer is C. Using the Splunk Reference URLs https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/DrilldownLinkToURL

"To customize the content that opens in the browser, you can include query parameters with the URL that you use. You can configure a drilldown to capture a clicked or other value in the source dashboard and pass it as a parameter to a target. As an example, you might have drilldown enabled on a table visualization. The $click.value2$ predefined token gives you access to the value in a clicked table cell."

https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens
"Drilldown. Use tokens to configure drilldown behavior. Prefined and custom token let you customize content in linked searches, dashboards, or URLs. You can also use tokens to create interactive behavior in the same dashbaord."
upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

ucsdmiami2020 3 years, 4 months ago

Agreed Answer is A. Per the provided Splunk Reference URL, Scroll down to the section titled, "Access Control List"
https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

"The following properties represent configured permissions for a resource. app - The app context for the resource. Required for updating saved search ACP properties. Allowed values are: The name of an app OR system"
Example 3. Make the saved search available to all users and change the context to a different app.

curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/myapp/saved/searches/mysearch/move
-d user=nobody
-d app=otherapp

upvoted 3 times

Question #3 *Topic 1*

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.

Suggested Answer: *AB*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Search/SupervisejobswiththeJobspage

ucsdmiami2020 3 years, 4 months ago

Agreed A and B. Per the Splunk Reference URLs. https://docs.splunk.com/Documentation/Splunk/8.2.2/Search/SupervisejobswiththeJobspage "Manage Search jobs. You can use the Jobs page to review and manage any job that you own. In Splunk Web, to view a list of your jobs select Activity > Jobs. This opens the jobs page."

https://docs.splunk.com/Documentation/Splunk/8.2.2/RESTTUT/RESTsearches
"/saved/searches --> Create or access the configuration of saved searches.
/search/jobs --> Create searches or access the results of search jobs."

https://docs.splunk.com/Documentation/Splunk/8.2.2/RESTREF/RESTsearch#GET_search.2Fjobs

search/jobs
https://<host>:<mPort>/services/search/jobs
List search jobs.

saved/searchs
https://<host>:<mPort>/services/saved/searches
Access and create saved searches.
"Does not explicitly state that it lists searches"

upvoted 3 times

Question #4 *Topic 1*

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.

Suggested Answer: *AC*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/visualizedata/usewebframework/modifydashboards/

New_user Highly Voted 3 years, 7 months ago

Answer is ABC. According to text of provided link: "You can modify layout, add new visualizations, and customize behaviors for a dashboard"
upvoted 5 times

ucsdmiami2020 3 years, 4 months ago

Agreed A, B, and C. Providing another Splunk reference URL to further support the answers
https://dev.splunk.com/enterprise/docs/developapps/visualizedata

"Simple XML extensions. Use extensions to modify the appearance and behavior of a dashboard that was created using the Dashboard Editor or by using Simple XML. Extensions are CSS and JavaScript files that you add to your app then reference from the dashboard's Simple XML code."
upvoted 2 times

Question #5 *Topic 1*

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 ɹ€Enable indexer acknowledgementɹ€.

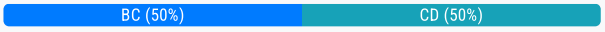
D. When the Global Settings for HEC are updated in Splunk Web, select the checkbox labeled ɹ€Enable indexer acknowledgementɹ€.

Suggested Answer: *CD*

Reference:

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

Community vote distribution



qtygbapjpesdayazko 1 year, 5 months ago

Selected Answer: BC

BC is the way

upvoted 1 times

shabamichael 1 year, 9 months ago

The correct answer is BC.

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”.

upvoted 2 times

aninhapipol 2 years, 10 months ago

Selected Answer: CD

Its CD.

A - It is only default if set as in option D.

B - When indexer acknowledgement is on you pass a guid in the header, but to turn on you must set in the token, not in the request.

upvoted 1 times

kraljko 2 years, 10 months ago

it is BC

"Can be enabled/disabled using Splunk Web or by sending a REST request"

upvoted 2 times

gsplunker 3 years, 7 months ago

Guess answer is C and D

https://docs.splunk.com/Documentation/Splunk/8.1.2/Data/AboutHECIDXAck

upvoted 2 times

New_user 3 years, 7 months ago

Answer is C. Global settings n Splunk web don't have such option, so D is wrong

upvoted 3 times

shabamichael 1 year, 11 months ago

Correct

upvoted 1 times

Question #6 *Topic 1*

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

Suggested Answer: *AB*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/DashboardPermissions

Community vote distribution
AB (100%)

shabamichael 1 year, 7 months ago
The correct answer is AB
A. The dashboard's permissions were set to private. B. User role permissions are different on the new instance.
upvoted 1 times

aninhapipol 2 years, 10 months ago
Selected Answer: AB
It's AB.
C - Is wrong because this would delete modifications made to the dashboard, not the dashboard itself.
D - It's wrong because dashboards are stored in the views folder. Not nav.
upvoted 4 times

qtygbapjpesdayazko 1 year, 5 months ago
AB is the way.
D, Dashboard, if it was created in local this will be true.
upvoted 1 times

Question #7 *Topic 1*

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

aninhapipol 2 years, 10 months ago

Selected Answer: A

It's A according to the discussion below:
https://community.splunk.com/t5/Getting-Data-In/REST-API-with-namespace/m-p/9596
upvoted 4 times

Question #8 *Topic 1*

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.

Suggested Answer: *AD*

New_user 3 years, 7 months ago

Answer is C.

- (A) Add-ons don't have own navigation menu
- (B) Namespace is a combination of user and app. Add-on is an app, so there must be several namespaces
- (D) Add-on are created to provide new abilities to other apps

upvoted 4 times

Question #9 *Topic 1*

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.

Suggested Answer: *BC*
Reference:
https://dev.splunk.com/enterprise/docs/devtools/java/sdk-java/howtousesdkjava/howtoworkjobjava/

Community vote distribution
BC (100%)

shabamichael 1 year, 7 months ago
Ans is BC
B. Can specify csv as an output format. C. Stream all results upon search completion.
Specifies the output format of the results (XML, JSON, JSON_COLS, JSON_ROWS, CSV, ATOM, or RAW).
ref:- https://dev.splunk.com/enterprise/docs/devtools/java/sdk-java/howtousesdkjava/howtoworkjobjava/
For those searches that stream the results (oneshot and export), the search results are not retained on the server. If the stream is interrupted for any reason, the results are not recoverable without running the search again.
upvoted 1 times

aninhapipol 2 years, 10 months ago
Selected Answer: BC
It's BC.
A - It's wrong because a oneshot search is a synchronous search as we get the results upon making the request without the need for complementary requests in order to get the results
D - It's wrong becaus according to the domumentation auto_cancel refers to inactivity not to timeout (timeout is set by the timeout parameter).
upvoted 3 times

qtygbapjpesdayazko 1 year, 5 months ago
BC is the way
upvoted 1 times

Question #10 *Topic 1*

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=ɔ€ internalɔ€.

Suggested Answer: *C*

Community vote distribution

B (100%)

qtygbapjpesdayazko 1 year, 6 months ago

Selected Answer: B

search job inspector, is the way

upvoted 1 times

splnk24 1 year, 11 months ago

Current answer B

upvoted 2 times

Question #11 *Topic 1*

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.

Suggested Answer: *D*

shabamichael 1 year, 7 months ago

The correct answer is C

C. The namespace filters the knowledge objects returned by the REST API.

upvoted 2 times

qtygbapjpesdayazko 1 year, 5 months ago

this is the way

upvoted 1 times

splnk24 1 year, 11 months ago

Correct answer C

upvoted 2 times

splnk24 2 years, 6 months ago

Correct is B

upvoted 3 times

Question #12 *Topic 1*

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.

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

shabamichael 1 year, 7 months ago
The correct Ans is
B. Specify the user and app context in the URI
upvoted 2 times

qtygbapjpesdayazko 1 year, 5 months ago
this is the way
upvoted 1 times

guilhermecervo 2 years, 3 months ago
In my opinion is letter A, once that is possible to ommit user and app. Ex: serviceNS/-/search/savedSearch....
upvoted 2 times

Question #13 *Topic 1*

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

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

splnk24 1 year, 11 months ago
Correct Answer D
upvoted 4 times

qtygbapjpesdayazko 1 year, 5 months ago
D. /servicesNS/-/search/saved/searches/mySearch
This is the way
upvoted 1 times

splnk24 1 year, 11 months ago
Correct Answer A
upvoted 2 times

Question #14 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Admin/Howtoeditaconfigurationfile

shabamichael 1 year, 10 months ago
https://docs.splunk.com/Documentation/Splunk/9.0.4/Admin/Configurationfiledirectories
upvoted 1 times

shabamichael 1 year, 10 months ago
Correct Answer is A
upvoted 1 times

splnk24 1 year, 11 months ago
Correct Answer D
upvoted 1 times

Question #15 *Topic 1*

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.

Suggested Answer: *AC*

Reference:

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

Community vote distribution

AC (100%)

shabamichael 1 year, 7 months ago

Yes ACD is the answer

A. Review the OWASP Top Ten List. 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.

upvoted 2 times

qtygbapjpesdayazko 1 year, 6 months ago

ACD, this is the way

upvoted 1 times

shabamichael 1 year, 10 months ago

Selected Answer: AC

The answer is AC, because it is during development

upvoted 1 times

aninhapipol 2 years, 10 months ago

Selected Answer: AC

It's ACD.

upvoted 2 times

gsplunker 3 years, 7 months ago

Yes ACD is the answer

upvoted 2 times

New_user 3 years, 7 months ago

Answer is ACD. D s also included to the list accessable by provided link

upvoted 3 times

Question #16 *Topic 1*

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

Suggested Answer: *CD*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/Savedsearches

Community vote distribution
CD (100%)

guilhermecervo Highly Voted 2 years, 3 months ago
Only D is the correct answer. Letter C do not have underscore in the log level field.
upvoted 5 times

qtygbapjpesdayazko 1 year, 5 months ago
This is the way
upvoted 1 times

aninhapipol Most Recent 2 years, 10 months ago
Selected Answer: CD
It's CD.
upvoted 1 times

New_user 3 years, 7 months ago
Answer is ACD. Tstats is also valid function
upvoted 1 times

New_user 3 years, 7 months ago
Sorry, answer CD is right. The tstats command can't be used after stats command
upvoted 2 times

Question #17 *Topic 1*

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.

Suggested Answer: *ABD*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Knowledge/Manageacceleratedsearchsummaries

Community vote distribution
ABD (100%)

qtygbapjpesdayazko 1 year, 6 months ago

Selected Answer: ABD

For a report to qualify for acceleration its search must meet three criteria:

The search string must use a transforming command (such as chart, timechart, stats, and top).
If the search string has any commands before the first transforming command, they must be streamable.
The search cannot use event sampling.

upvoted 1 times

nosavotor 1 year, 6 months ago

Im not sure how to respond to that

upvoted 2 times

Question #18 *Topic 1*

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.

Suggested Answer: *AC*

Community vote distribution

AB (100%)

aninhapipol 2 years, 10 months ago

Selected Answer: AB

It's ABD.

A - Splunk does not limit indexes or sourcetypes in token creation.

B - It's correct according to the documentation(edit_token_http):

https://docs.splunk.com/Documentation/Splunk/8.2.6/Security/Rolesandcapabilities

D - Splunl allows you to update tokens through this endpoint:

https://docs.splunk.com/Documentation/Splunk/8.2.6/Data/HECRESTendpoints

upvoted 2 times

New_user 3 years, 7 months ago

Answer is AD. To create a token, is used the "data/inputs/http" endpoint

upvoted 3 times

Question #19 *Topic 1*

Which type of command is tstats?

A. Generating

B. Transforming

C. Centralized streaming

D. Distributable streaming

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats

New_user 3 years, 7 months ago

A is right https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Commandsbytype#Transforming_commands

upvoted 4 times

qtygbapjpesdayazko 1 year, 6 months ago

this is the way, a tstats is a generating command.

upvoted 1 times

Question #20 *Topic 1*

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.

Suggested Answer: *AB*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/

New_user Highly Voted 3 years, 7 months ago
Answer is ABD. The D is also included to page provided by link
upvoted 5 times

qtygbapjpesdayazko 1 year, 6 months ago
This is the way
upvoted 1 times

Question #21 *Topic 1*

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.

Suggested Answer: *D*

nosavotor 1 year, 6 months ago

Someone please verify the accuracy of this answer

upvoted 1 times

Question #22 *Topic 1*

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

Suggested Answer: *BC*

shabamichael 1 year, 7 months ago
To correct my previous ans,
The correct ans is ABCD
This is because file path $SPLUNK_HOME/etc/apps/app_name/local/data/ui/nav/default/xml doesnt exist in splunk
upvoted 1 times

shabamichael 1 year, 10 months ago
Answer is ACD. is the correct answer, in Splunk, the default.xml takes precedence and does not merge the content of files as in .config files
upvoted 1 times

guilhermecervo 2 years, 3 months ago
Since the local directory is wrong, I'm going with ABCD.
upvoted 1 times

New_user 3 years, 7 months ago
Answer is ACD. Files in the "local" folder have precendance over ones in the "default"
upvoted 4 times

New_user 3 years, 7 months ago
Of course, if name of the second file is "default.xml"
upvoted 3 times

qtygbapjpesdayazko 1 year, 6 months ago
This is the way
upvoted 1 times

Question #23 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Search/Specifytimemodifiersinyoursearch

shabamichael 1 year, 10 months ago

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

upvoted 2 times

Question #24 *Topic 1*

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.

Suggested Answer: *BC*

guilhermecervo 2 years, 3 months ago

I know that A and C are correct.

Letter B I think is wrong because we can set auto refresh editing directly the report. Not needing to go in the xml tab.

Letter D is wrong because post-processing searchs cannot be apart refreshed;

upvoted 3 times

qtygbapjpesdayazko 1 year, 5 months ago

AC, This is the way

upvoted 1 times

New_user 3 years, 7 months ago

Answer is ABD

upvoted 1 times

Question #25 *Topic 1*

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

Suggested Answer: *D*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/setpermissionsforobjects/

qtygbapjpesdayazko 1 year, 5 months ago
D. export = system
upvoted 1 times

nosavotor 1 year, 6 months ago
Im not sure how to respond to that
upvoted 1 times

Question #26 *Topic 1*

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

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

qtygbapjpesdayazko 1 year, 5 months ago
B. Title
upvoted 1 times

nosavotor 1 year, 6 months ago
Someone please verify the accuracy of this answer
upvoted 1 times

Question #27 *Topic 1*

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

Suggested Answer: *A*

Reference:

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

Community vote distribution

C (100%)

qtygbapjpesdayazko 1 year, 5 months ago

Selected Answer: C

C. /storage/collections/config

upvoted 1 times

New_user 3 years, 7 months ago

C is the answer. A new collection is creted via POST method and endpoint /storage/collections/config

upvoted 4 times

Question #28 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

A (100%)

qtygbapjpesdayazko 1 year, 5 months ago

Selected Answer: A

A. Nobody

upvoted 1 times

New_user 3 years, 7 months ago

Answer is A, "Nobody". See examples here

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

upvoted 2 times

Question #29 *Topic 1*

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

A. Search

B. Set token

C. Form input

D. Visualization

Suggested Answer: *CD*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/EventHandlerReference

Community vote distribution
AC (100%)

Farshid 1 year, 5 months ago
A & B
"You can use the following event handlers to specify token settings within the <init> tags.
<condition>
<eval>
<link>
<set>
<unset>"
https://docs.splunk.com/Documentation/Splunk/9.1.1/Viz/tokens
upvoted 1 times

Farshid 1 year, 5 months ago
ACD is correct actually
upvoted 1 times

qtygbapjpesdayazko 1 year, 5 months ago
Selected Answer: AC
A. Search
C. Form input
D. Visualization
upvoted 1 times

New_user 3 years, 7 months ago
Answer is ACD. "Set token" is just an operation used by event handlers
upvoted 4 times

Question #30 *Topic 1*

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.

Suggested Answer: *D*

Reference:

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

Community vote distribution

D (100%)

qtygbapjpesdayazko 1 year, 5 months ago

Selected Answer: D

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

upvoted 1 times

guilhermecervo 2 years, 3 months ago

Letter D is correct according with the documentation mentioned in the answer.

upvoted 3 times

New_user 3 years, 7 months ago

Answer is C

upvoted 1 times

Question #31 *Topic 1*

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

Suggested Answer: *AC*

guilhermecervo 2 years, 3 months ago
AC correct.
upvoted 2 times

qtygbapjpesdayazko 1 year, 5 months ago
This is the way
upvoted 1 times

Question #32 *Topic 1*

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

A. _key

B. _time

C. _user

D. _source

Suggested Answer: *BC*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/manageknowledge/kvstore/aboutkvstorecollections/

gsplunker Highly Voted 3 years, 7 months ago
Yes it's A and C
upvoted 5 times

qtygbapjpesdayazko 1 year, 5 months ago
A. _key
C. _user
upvoted 1 times

New_user Most Recent 3 years, 7 months ago
Answer is AC. See the link under queston
upvoted 3 times

Question #33 *Topic 1*

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

Suggested Answer: *A*

Reference:

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

Community vote distribution

A (100%)

qtygbapjpesdayazko 1 year, 5 months ago

Selected Answer: A

curl -k https://localhost:8089/services/auth/login --data-urlencode username=admin --data-urlencode password=pass

upvoted 1 times

guilhermecervo 2 years, 3 months ago

Letter A is correct.

upvoted 1 times

Question #34 *Topic 1*

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'

Suggested Answer: *C*

Tt90 3 years, 2 months ago
Answer is D
upvoted 3 times

guilhermecervo 2 years, 3 months ago
Agree.
upvoted 3 times

qtygbapjpesdayazko 1 year, 5 months ago
D, the only one with correct JSON in the request
upvoted 1 times

New_user 3 years, 7 months ago
Answer is A. See "Queries" header here https://docs.splunk.com/Documentation/Splunk/8.2.1/RESTREF/RESTkvstore
upvoted 2 times

gsplunker 3 years, 7 months ago
No because output_mode should be followed by =
https://docs.splunk.com/Documentation/Splunk/8.2.1/Search/ExportdatausingRESTAPI
upvoted 2 times