Question #1 *Topic 1*

Which statement about tsidx files is accurate?

A. Splunk updates tsidx files every 30 minutes.

B. Splunk removes outdated tsidx files every 5 minutes.

C. A tsidx file consists of a lexicon and a posting list.

D. Each bucket in each index may contain only one tsidx file.

**Suggested Answer:** *C*

**voiddraco** Most Recent 2 years ago

Anybody took this recently? i plan on taking it in a couple weeks... I also checked that site that NOTYOURGIRL said and it's BS lol they dont even have this exam on there

upvoted 1 times

**jaemon22** 2 years, 2 months ago

Selected Answer: C

The answer is C

upvoted 2 times

**emlch** 2 years, 3 months ago

The TSIDX is an index file such as a book summary. It contains a Lexicon and a Posting List. The TSIDX is updated every 5 minutes and gets clean up for outdated data every 30 minutes. What is outdated data? We can think for example in data model acceleration, we have to select a timerange which our datamodel will be accelerate. D is false, you have naturally one tsidx file, when you accelerate your DM you have two.

upvoted 1 times

Question #2 *Topic 1*

Repeating JSON data structures within one event will be extracted as what type of fields?

A. Single value

B. Lexicographical

C. Multivalue

D. Mvindex

**Suggested Answer:** *C*

**jaemon22** Most Recent 1 year, 9 months ago

Selected Answer: C

the answer is multi value

upvoted 1 times

**emlch** 1 year, 9 months ago

Selected Answer: C

the other answer make no sense at all, A might be, but we're talking about repeating data structures

upvoted 1 times

Question #3 *Topic 1*

What default Splunk role can use the Log Event alert action?

A. Power

B. User

C. can_delete

D. Admin

**Suggested Answer:** *A*

**Soccerfan** 1 year, 10 months ago

A - https://docs.splunk.com/Documentation/Splunk/9.3.1/Security/Rolesandcapabilitiesthis - power users can - edit_log_alert_event Lets a user log an event when an alert condition is met. Also lets the user select the "Log an event" option for an alert action in Splunk Web.

upvoted 2 times

**marinatedcohort** Most Recent 1 year, 10 months ago

this - power users can - edit_log_alert_event Lets a user log an event when an alert condition is met. Also lets the user select the "Log an event" option for an alert action in Splunk Web.

upvoted 1 times

**AnE_splunk** 2 years ago

Using the log event alert action requires the edit_tcp capability for users without the admin role.

upvoted 1 times

**jaemon22** 2 years, 2 months ago

Selected Answer: A

Correction answer is A, the answer C i provided earlier was for anoher question.

upvoted 2 times

**jaemon22** 2 years, 2 months ago

Selected Answer: C

It's C

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: D

Correct answer is the Admin user. Power user needs the edit_tcp capability. See Fundamentals 3 slide 108.

upvoted 1 times

**Derag** 2 years, 4 months ago

A power user with edit_tcp capability can use the log event. The Admin role is required to edit/modify it.

upvoted 1 times

Question #4 *Topic 1*

When running a search, which Splunk component retrieves the individual results?

A. Indexer

B. Search head

C. Universal forwarder

D. Master node

**Suggested Answer:** *A*

**assfedassfinished** Most Recent 1 year, 9 months ago

Selected Answer: A

Definitely A. I worked in an environment with not enough CPUs on the indexer. Everytime you would refresh a dashboard, you'd get the iowait alert with a red exclamation mark advising that the indexer is tired, boss.

upvoted 1 times

**NagaoShingo** 2 years, 2 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

**jaemon22** 2 years, 2 months ago

Selected Answer: A

A indexer The indexer is responsible for retrieving and processing the raw data, returning the individual results to the search head, which then formats and presents them to the user.

upvoted 1 times

**emlch** 2 years, 3 months ago

Tricky question. Might fall in an interpreation issue here. In a distributed search model, the SH dispatches the searches and the indexers perform the searches individually in the data stored in each instance. Them, the SH merges all results. I would go with A.

upvoted 2 times

Question #5 *Topic 1*

What order of incoming events must be supplied to the transaction command to ensure correct results?

A. Reverse lexicographical order

B. Ascending lexicographical order

C. Ascending chronological order

D. Reverse chronological order

**Suggested Answer:** *D*

**Soccerfan** Most Recent 1 year, 10 months ago

D - https://docs.splunk.com/Documentation/Splunk/9.3.1/SearchReference/Transaction

upvoted 1 times

Question #6 *Topic 1*

What type of drilldown passes a value from a user click into another dashboard or external page?

A. Visualization

B. Event

C. Dynamic

D. Contextual

**Suggested Answer:** *C*

**RoaaAttalla** Most Recent 9 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

**cagdaskarabag** 1 year, 9 months ago

Dynamic drilldowns in Splunk are used to pass values from user interactions (like clicks) to another dashboard or an external page, enabling more interactive and contextual navigation.

upvoted 1 times

**slayqueeenslay** 2 years, 2 months ago

Selected Answer: C

Dynamic Drilldown - Link to dashboard ◦ Set tokens ◦ Pass values as tokens from a user click to another dashboard - Specify a path to a URL ◦ Relative path to a dashboard in another app ◦ Absolute path to an external website

upvoted 1 times

**adamsca** 2 years, 2 months ago

Selected Answer: C

C is Correct

upvoted 1 times

**adpafer** 2 years, 3 months ago

D. The question is about passing values to another dashboard or URL !Sorry for that but I thought about DYNAMIC which is C :)

upvoted 1 times

**adpafer** 2 years, 3 months ago

Sorry for that but I thought about DYNAMIC which is C :)

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: C

C. Contextual Drilldown to pass values as tokens from a user click to visualizations on the same dashboard. Dynamic Drilldown specify a path to a URL to a relative path to a dashboard in another app or to an Absolute path to an external website.

upvoted 1 times

Question #7 *Topic 1*

What file types does Splunk use to define geospatial lookups?

A. GPX or GML files

B. TXT files

C. KMZ or KML files

D. CSV files

**Suggested Answer:** *C*

**Rounaldo** Most Recent 1 year, 7 months ago

Selected Answer: C

KML or KMZ files

upvoted 1 times

Question #8 *Topic 1*

How can form inputs impact dashboard panels using inline searches?

A. A token in a search can be replaced by a form input value.

B. Panels powered by an inline search require a minimum of one form input.

C. Form inputs can not impact panels using inline searches.

D. Adding a form input to a dashboard converts all panels to prebuilt panels.

**Suggested Answer:** *A*

**cagdaskarabag** Most Recent 1 year, 9 months ago

Selected Answer: A

The correct answer is A. A token in a search can be replaced by a form input value. According to Splunk documentation, form inputs can dynamically impact dashboard panels by capturing user selections or inputs as tokens. These tokens can then be used to replace parts of the inline search query within the dashboard panel, allowing the panel's data and visualizations to update based on the user's interaction with the form input. This functionality enables dynamic and interactive dashboards. For example: A dropdown or text input can populate a token, which is then substituted into an inline search to filter or modify the search results displayed in the panel

upvoted 1 times

Question #9 *Topic 1*

How can a lookup be referenced in an alert?

A. Use the lookup dropdown in the alert configuration window.

B. Follow a lookup with an alert command in the search bar.

C. Run a search that uses a lookup and save as an alert.

D. Upload a lookup file directly to the alert.

**Suggested Answer:** *C*

**cagdaskarabag** Most Recent 1 year, 9 months ago

Selected Answer: C

C. Run a search that uses a lookup and save as an alert. In Splunk, lookups are used within searches to enrich or filter data. To reference a lookup in an alert, you must first create a search that incorporates the lookup (e.g., using the inputlookup or lookup command). Once the search is defined and tested, it can be saved as an alert to trigger based on specific conditions.

upvoted 1 times

**emlch** 2 years, 3 months ago

Selected Answer: C

You can either use the | outputlookup command in the alert search or select the "Output results to lookup". My first tought was A. But this doesn't seem to be the topic. Apparantly this question is talking about using a lookup in an alert, not outputing results, C is correct. Something like | lookup OUTPUT ...

upvoted 1 times

Question #10 *Topic 1*

What is an example of the simple XML syntax for a base search and its post-process search?

A. ,

B. ,

C. ,

D. ,

**Suggested Answer:** *A*

**marinatedcohort** Most Recent 1 year, 10 months ago

Selected Answer: A

if your search id is "myBaseSearch", then your base search should reference "myBaseSearch". Answer A is correct

upvoted 1 times

**emlch** 2 years, 3 months ago

For base search Post-process if your search id is "name", then your base search should reference "name". Answer A is correct

upvoted 1 times

**marinatedcohort** 1 year, 10 months ago

if your search id is "name", then your base search should reference "name". Answer A is correct

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: A

Correct answer is A. See example under Basic post-process search on

https://docs.splunk.com/Documentation/Splunk/latest/Viz/Savedsearches#Post-process_searches_2

upvoted 2 times

Question #11 *Topic 1*

What qualifies a report for acceleration?

A. Fewer than 100k events in search results, with transforming commands used in the search string.

B. More than 100k events in search results, with only a search command in the search string.

C. More than 100k events in the search results, with a search and transforming command used in the search string.

D. Fewer than 100k events in search results, with only a search and transaction command used in the search string.

**Suggested Answer:** *C*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: C

 search must include a transforming command (stats, timechart, top)  only distributable streaming commands before the transforming command (or none).  More than 100k events in the summary range

upvoted 3 times

**Derag** 1 year, 10 months ago

This could be unclear, but each bucket should be 100k or more, with search and transforming commands. So that would be C.

upvoted 2 times

Question #12 *Topic 1*

What happens to panels with post-processing searches when their base search is refreshed?

A. The panels are deleted.

B. The panels are only refreshed if they have also been configured.

C. The panels are refreshed automatically.

D. Nothing happens to the panels.

**Suggested Answer:** *C*

**emlch** Most Recent 1 year, 9 months ago

post-process searches automatically refresh when their base search is refreshed

upvoted 2 times

Question #13 *Topic 1*

How is a cascading input used?

A. As part of a dashboard, but not in a form.

B. Without token notation in the underlying XML.

C. As a way to filter other input selections.

D. As a default way to delete a user role.

**Suggested Answer:** *C*

**emlch** Most Recent 1 year, 9 months ago

C. A cascading input is a way to filter other input selections Think in a dashboard with 3 filters COUNTRY | STATE | CITY For a specific country, states are filtered to only show states of that country, same with city.

upvoted 1 times

Question #14 *Topic 1*

Which commands can run on both search heads and indexers?

A. Transforming commands

B. Centralized streaming commands

C. Dataset processing commands

D. Distributable streaming commands

**Suggested Answer:** *D*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: D

d

upvoted 2 times

**emlch** 2 years, 3 months ago

Selected Answer: D

Correct, distriutable streaming commands are executed both on SH and IDX (It depends on the order of commands). If any of the preceding commands execute on the SH then the distributable streaming command als oexecutes on SH (i.e. if we have a centralized streaming command BEFORE)

upvoted 2 times

Question #15 *Topic 1*

If a nested macro expands to a search string that begins with a generating command, what additional syntax is needed?

A. Double tick marks around the nested macro.

B. A comma before the nested macro.

C. Square brackets around the nested macro.

D. A pipe character before the nested macro.

**Suggested Answer:** *D*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: D

This question follows a best practice and it isn't true for all. But if the macro starts with a generating command (or any command) you have to put | before calling the macro Example: `macro` = stats count by something | `macro`

upvoted 1 times

**Derag** 1 year, 10 months ago

There could be confusion between pipe and square brackets; just to be apparent, it is a pipe. sourcetype=access_* | `mymacro`

upvoted 1 times

Question #16 *Topic 1*

When using a nested search macro, how can an argument value be passed to the inner macro?

A. The argument value may be passed to the outer macro.

B. An argument cannot be used with an inner nested macro.

C. An argument cannot be used with an outer nested macro.

D. The argument value must be specified in the outer macro.

**Suggested Answer:** *A*

**Bob_Hob** Most Recent 1 year, 6 months ago

Selected Answer: D

When any search is ran the parsing stage expands the macro. There is no reason they cant be nested

upvoted 1 times

**emlch** 1 year, 9 months ago

Selected Answer: D

D is correct. For example macro(1) -> `macro` => index=web sourcetype=access_combine `macro2($field$)` macro2(1) -> `macro2` | stats count by $field$ see that the first macro (outer macro) is receiving the $field$ argument and passing to the second macro (inner macro)

upvoted 1 times

**Derag** 1 year, 10 months ago

Correct answer is D. option A, it is not the correct answer to the question about passing an argument value to an inner macro. Option A suggests that the argument value may be passed to the outer macro, but the question asks about passing the argument value to the inner macro.

upvoted 1 times

Question #17 *Topic 1*

Which is a regex best practice?

A. Use complex expressions rather than simple ones.

B. Avoid backtracking.

C. Use greedy operators (.*) instead of non-greedy operators (.*?).

D. Use * rather than +.

**Suggested Answer:** *B*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: B

Other answers are the opposite of best practice. No need to extra knowledge on regex.

upvoted 1 times

Question #18 *Topic 1*

What does the query | makeresults generate?

A. A timestamp

B. A results field

C. An error message

D. The results of the previously run search

**Suggested Answer:** *A*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: A

The makeresults command generates a result with the _time field set to the current time.
https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Makeresults

upvoted 1 times

**Vidomina** 2 years, 3 months ago

Selected Answer: A

| makeresults alone generates "_time" only

upvoted 1 times

**emlch** 2 years, 3 months ago

Selected Answer: A

Makeresults generates a timestamp so you can create an event with that timestamp, mainly for purposes (i.e. testing an alert). Generates a single event in memory with only the _time field. You can add event fields using eval. Must be the first command in search succeeding a pipe

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

It generates the specified number of search results in temporary memory. With a single field, _time.

upvoted 2 times

Question #19 *Topic 1*

Why use the tstats command?

A. As an alternative to the summary command.

B. To generate statistics on indexed fields.

C. To generate an accelerated datamodel.

D. To generate statistics on search-time fields.

**Suggested Answer:** *B*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: B

Use the tstats command to perform statistical queries on indexed fields in tsidx files. The indexed fields can be from indexed data or accelerated data models. Because it searches on index-time fields instead of raw events, the tstats command is faster than the stats command.

upvoted 1 times

Question #20 *Topic 1*

Which of the following can be used to access external lookups?

A. Perl and Python

B. Python and Ruby

C. Perl and binary executable

D. Python and binary executable

**Suggested Answer:** *D*

**Soccerfan** Most Recent 1 year, 10 months ago

D - https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/DefineanexternallookupinSplunkWeb

upvoted 1 times

Question #21 *Topic 1*

Where does the output of an append command appear in the search results?

A. Added as a column to the right of the search results.

B. Added as a column to the left of the search results.

C. Added to the beginning of the search results.

D. Added to the end of the search results.

**Suggested Answer:** *D*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: D

Correct, append command adds results of the subsearch in the end of the current result set. appendpipe also does this appendcols adds a new column

upvoted 1 times

Question #22 *Topic 1*

What XML element is used to pass multiple fields into another dashboard using a dynamic drilldown?

A.

B.

C.

D.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

How is regex passed to the makemv command?

A. makemv must be preceded by the erex command.

B. It is specified by the delim argument.

C. It is specified by the tokenizer argument.

D. makemv must be preceded by the rex command.

**Suggested Answer:** *C*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: C

| makemv [delim= | tokenizer= ] you can use delimiter or regex. To use regex, use the tokenizer option.

upvoted 1 times

Question #24 *Topic 1*

Which of the following are potential string results returned by the typeof function?

A. True, False, Unknown

B. Number, String, Bool

C. Number, String, Null

D. Field, Value, Lookup

**Suggested Answer:** *C*

**Soccerfan** Most Recent 1 year, 10 months ago

B - https://docs.splunk.com/Documentation/SCS/current/SearchReference/InformationalFunctions

upvoted 2 times

**slayqueeenslay** 2 years, 2 months ago

Selected Answer: B

Its B, Splunk Fundementals 3 page 58 says: typeof: returns a string that represents the data type of X – Possible results: number, string, or bool

upvoted 2 times

**adamsca** 2 years, 2 months ago

Ans is C C. Number, String, Null

upvoted 1 times

**poorisubash** 2 years, 2 months ago

The answer is C. C. Number, String, Null

upvoted 1 times

**Derag** 2 years, 4 months ago

Its B. The following example takes one argument and returns a string representation of its type. This example returns "NumberStringBoolInvalid"

upvoted 2 times

Question #25 *Topic 1*

If a search contains a subsearch, what is the order of execution?

A. The order of execution depends on whether either search uses a stats command.

B. The inner search executes first.

C. The outer search executes first.

D. The two searches are executed in parallel.

**Suggested Answer:** *B*

**emlch** Most Recent 1 year, 9 months ago

inner search (subsearch) executed first and passes the results to the outer (basic or primary search)

upvoted 2 times

Question #26 *Topic 1*

What are the four types of event actions?

A. stats, target, set, and unset

B. stats, target, change, and clear

C. eval, link, change, and clear

D. eval, link, set, and unset

**Suggested Answer:** *D*

**ashutoshab** Most Recent 6 months, 3 weeks ago

Selected Answer: D

Correction from previous answer, The answer is D (Eval , Link, Set, Unset)

upvoted 1 times

**ashutoshab** 6 months, 3 weeks ago

Selected Answer: C

The answer is C

upvoted 1 times

Question #27 *Topic 1*

How is a multivalue field created from product="a,b,c,d"?

A. ...| makemv delim(product, ",")

B. ...| eval mvexpand(makemv(product, ","))

C. ...| mvexpand product

D. ...| makemv delim="," product

**Suggested Answer:** *D*

**98488b3** Most Recent 1 year ago

Selected Answer: D

the delim argument only accepts strings, A would result in an error

upvoted 1 times

**emlch** 1 year, 9 months ago

yep, D is correct. mvexpand creates a different event for each value in a mv field.

upvoted 2 times

**Eddie_exam** 1 year, 10 months ago

Selected Answer: D

Correct answer is D. makemv [delim= | tokenizer= ] [allowempty= ] [setsv= ] . See https://docs.splunk.com/Documentation/SplunkCloud/latest/SearchReference/Makemv

upvoted 2 times

Question #28 *Topic 1*

Which field is required for an event annotation?

A. annotation category

B. _time

C. eventtype

D. annotation label

**Suggested Answer:** *B*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: B

https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Viz/ChartEventAnnotations _time is an mandatory but the annotation category and annotation label is optional

upvoted 1 times

**Derag** 2 years, 4 months ago

B. _time is the only field that is required.

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: B

Correct answer is B. Only _time is a required field. See https://docs.splunk.com/Documentation/SplunkCloud/latest/Viz/ChartEventAnnotations

upvoted 2 times

Question #29 *Topic 1*

Which stats function is used to return a sorted list of unique field values?

A. values

B. sum

C. count

D. list

**Suggested Answer:** *A*

**a50b9c8** Most Recent 1 year, 9 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

**emlch** 2 years, 3 months ago

sum -> sum of values of a specified field count -> count of values of specified field (or all events) list -> list all values of a specified field (even if its repeated) values -> list unique values of a specified field

upvoted 2 times

Question #30 *Topic 1*

Which of the following is an event handler action?

A. Run an eval statement based on a user clicking a value on a form.

B. Set a token to select a value from the time range picker.

C. Pass a token from a drilldown to modify index settings.

D. Cancel all jobs based on the number of search job results captured.

**Suggested Answer:** *A*

**ashutoshab** Most Recent 6 months, 3 weeks ago

Selected Answer: A

This will be confusing between A & B. However A is the correct answer. Here is an explanation why B is not the answer: While event handlers can set tokens that are then used by a time range picker, they do not directly "select a value from" the picker as an action; rather, they manage the tokens that drive the dashboard's time parameters.

upvoted 1 times

**succulentchinesemeal** 1 year, 5 months ago

Selected Answer: B

Its tough but i would go with B

upvoted 1 times

**teeec** 1 year, 7 months ago

Selected Answer: B

I am in between of A and B as answer. I ended up choosing B because setting a token to select a value from time range picker is definitely an event handler action. I am not sure

upvoted 1 times

Question #31 *Topic 1*

What is a performance improvement technique unique to dashboards?

A. Using stats instead of transaction

B. Using global searches

C. Using report acceleration

D. Using datamodel acceleration

**Suggested Answer:** *B*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: B

This is unique to dashboards. Global searches allow multiple panels to share the same search results, reducing the number of searches that need to be run and improving overall dashboard performance.

upvoted 2 times

**desamfisher** 2 years ago

Selected Answer: B

CORRECT ANSWER IS B

upvoted 2 times

**poorisubash** 2 years, 2 months ago

Correct answer is B : using global searches

upvoted 2 times

**emlch** 2 years, 3 months ago

The others are not unique to dashboards, global searches are.

upvoted 4 times

**Derag** 2 years, 4 months ago

The correct answer is B. This technique is unique to dashboards and involves sharing search results across multiple panels within the same dashboard, which can significantly improve performance by avoiding redundant searches and data fetching operations.

upvoted 2 times

Question #32 *Topic 1*

When and where do search debug messages appear to help with troubleshooting views?

A. In the Dashboard Editor, while the search is running.

B. In the Search Job Inspector, after the search completes.

C. In the Search Job Inspector, while the search is running.

D. In the Dashboard Editor, after the search completes.

**Suggested Answer:** *B*

**ashutoshab** Most Recent 6 months, 3 weeks ago

Selected Answer: B

DEBUG messages appear at the top after the search job has completed. https://help.splunk.com/en/splunk-enterprise/search/search-manual/9.1/manage-jobs/view-search-job-properties#:~:text=The%20Search%20Job%20Inspector%20displays%20DEBUG%20messages%20at%20the%20top%20of%20the%20Search%20Job%20Inspector%20window%2C%20after%20the%20search%20has%20completed.

upvoted 1 times

**Rounaldo** 1 year, 7 months ago

Selected Answer: B

B. Debug messages appear after the search has completed Intro to Dashboards page 21

upvoted 1 times

**teeec** 1 year, 7 months ago

Selected Answer: B

The question ask about "troubleshooting views". A lot of people have missed this point. Esentially views are finished product/results, so the answer should be B - In the search job inspector, AFTER the search completes. You can't see the finished product/results when the search is running. Definition: A view is essentially a page or interface that presents search results, visualizations, and forms in Splunk. It can be part of a dashboard or a standalone interface within an app.

upvoted 1 times

**poorisubash** 1 year, 8 months ago

The correct option is : C Search debug messages appear in the Search Job Inspector during the search execution to help with troubleshooting.

upvoted 1 times

**adamsca** 1 year, 8 months ago

Selected Answer: C

C is correct While the Search Job Inspector can show search results after completion, debug messages are often most helpful while the search is running to pinpoint issues. you do not have to wait until search is completed.

upvoted 1 times

**adpafer** 1 year, 9 months ago

Job Inspector displays messages while the search is running. You do not have to wait untili search is completed.

upvoted 2 times

**emlch** 1 year, 9 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

**Derag** 1 year, 10 months ago

The correct answer is B. Look at the job inspector after completing the search.

upvoted 1 times

Question #33 *Topic 1*

Which statement about the coalesce function is accurate?

A. It can take only a single argument.

B. It can take a maximum of two arguments.

C. It can be used to create a new field in the results set.

D. It can return null or non-null values.

**Suggested Answer:** *D*

**J4ckrau** Most Recent 1 year, 2 months ago

Selected Answer: D

It can return the first non-null value from the fields but if all are null, then the output is also null.

upvoted 1 times

**emlch** 1 year, 9 months ago

Selected Answer: C

This kind of question is not nice. But let's see the options A. No, coalesce can take one or more values B. No, one or more values C. Yes, it creates a field with the first non-null value of any argument passed D. I'm not sure about this, because if any argument isn't contained in that event, the field my guess is that the field wouldn't be created in that event. But anyway, it isn't as accurate as C. So C is my final answer. https://docs.splunk.com/Documentation/SCS/current/SearchReference/ConditionalFunctions#coalesce.28.26lt.3Bvalues.26gt.3B.29Ah, just adding that C is valid due to the nature of the eval command, that can create new fieldsTest it, C is the correct answer. | makeresults | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip -------> No results find (i.e. coalesce doesnt return non-null values). | makeresults | eval s_ip="10.0.0.1" | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip --------> Result-> ipfield = s_ip (the first non-null value)

upvoted 1 times

**emlch** 1 year, 9 months ago

Ah, just adding that C is valid due to the nature of the eval command, that can create new fieldsTest it, C is the correct answer. | makeresults | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip -------> No results find (i.e. coalesce doesnt return non-null values). | makeresults | eval s_ip="10.0.0.1" | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip --------> Result-> ipfield = s_ip (the first non-null value)

upvoted 2 times

**emlch** 1 year, 9 months ago

Test it, C is the correct answer. | makeresults | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip -------> No results find (i.e. coalesce doesnt return non-null values). | makeresults | eval s_ip="10.0.0.1" | eval ip_field = coalesce(clientip, s_ip) | table ip_field, clientip, s_ip --------> Result-> ipfield = s_ip (the first non-null value)

upvoted 4 times

**Derag** 1 year, 10 months ago

No, it is D. Option C is not correct because the coalesce function can indeed be used to create a new field in the results set. The coalesce function returns the first non-null value from a list of arguments, and it can be used with the eval command to create a new field in the results set.

upvoted 2 times

**Eddie_exam** 1 year, 10 months ago

Selected Answer: C

Correct answer is C. When used in combination with eval command to create a new field. This function takes one or more values and returns the first value that is not NULL. See https://docs.splunk.com/Documentation/SCS/current/SearchReference/ConditionalFunctions

upvoted 1 times

Question #34 *Topic 1*

Which commands should be used in place of a subsearch if possible?

A. untable and/or xyseries

B. stats and/or eval

C. mvexpand and/or where

D. bin and/or where

**Suggested Answer:** *B*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: B

stats and eval are more efficient with many results in a subsearch

upvoted 2 times

Question #35 *Topic 1*

Which of the following has a schema or structure embedded in the data itself?

A. Dark data

B. Unstructured data

C. Embedded data

D. Self-describing data

**Suggested Answer:** *D*

**emlch** Most Recent 1 year, 9 months ago

Selected Answer: D

self describing data (XML,JSON) contains a schema

upvoted 3 times

Question #36 *Topic 1*

What arguments are required when using the spath command?

A. input, output, index

B. input, output, path

C. No arguments are required.

D. field, host, source

**Suggested Answer:** *B*

**chuzpah** Most Recent 6 months, 1 week ago

Selected Answer: C

None required for the structured path command

upvoted 1 times

**emlch** 1 year, 9 months ago

C, optional arguments are input= (where to extract structured data), output= (data will be stored in this field), path= path location to the vlaue you want to extract

upvoted 2 times

**Derag** 1 year, 10 months ago

It is C. No arguments are required; however, the optional arguments: fieldpath, input and output can be used.

upvoted 2 times

**Eddie_exam** 1 year, 10 months ago

Selected Answer: C

The correct answer is C. Input, output, and path are all optional. See Fundamentals 3 slide 152.

upvoted 2 times

Question #37 *Topic 1*

What is the recommended way to create a field extraction that is both persistent and precise?

A. Use the rex command.

B. Use the Field Extractor and manually edit the generated regular expression.

C. Use the Field Extractor and let it automatically generate a regular expression.

D. Use the erex command.

**Suggested Answer:** *B*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: B

B

upvoted 1 times

**MaxGamer** 1 year, 11 months ago

Selected Answer: B

The correct answer is B Answer A & D are not persistent Answer C could give wrong results as it is not perfect

upvoted 2 times

**emlch** 2 years, 3 months ago

IMHO B would be the answer. C would seem correct if field extractor were perfect (which isn't)

upvoted 1 times

Question #38 *Topic 1*

What capability does a power user need to create a Log Event alert action?

A. edit_search_server

B. edit_udp

C. edit_tcp

D. edit_alerts

**Suggested Answer:** *C*

**teeec** Most Recent 1 year, 7 months ago

Selected Answer: C

The edit_tcp capability allows users to configure TCP inputs, which is necessary for setting up certain alert actions, including the Log Event alert action. Assigning this capability to a power user enables them to create and manage Log Event alert actions effectively. Would be D if the D option is edit_log_alert_event

upvoted 1 times

**cagdaskarabag** 1 year, 9 months ago

Selected Answer: C

To create a "Log Event" alert action in Splunk, a user without the admin role requires the edit_tcp capability. This is necessary to ensure that the log event action functions properly, as highlighted in the Splunk Community discussion and documentation

upvoted 1 times

**ykamalharsha** 1 year, 9 months ago

Selected Answer: D

To create a Log Event alert action in Splunk, a power user needs the edit_alerts capability. This capability allows users to create, edit, and manage alert actions, including Log Event alerts

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: C

Correct answer is C. See Fundamentals 3 slide 108.

upvoted 2 times

**Derag** 2 years, 4 months ago

It is C. If not admin, a power user should have edit_tcp to create a log event alert.

upvoted 1 times

Question #39 *Topic 1*

How can the Inspect button be disabled on a dashboard panel?

A. Set inspect.link.disabled to 1

B. Set link.inspect.visible to 0

C. Set link.inspect.Search.visible to 0

D. Set link.search.disabled to 1

**Suggested Answer:** *B*

**Rounaldo** Most Recent 1 year, 7 months ago

Selected Answer: C

link.inspectSearch.visible Show the Inspect button at the bottom of the panel. Type=Boolean Defaults to the value of link.visible

upvoted 1 times

**Derag** 1 year, 10 months ago

The correct answer is C. false

upvoted 2 times

Question #40 *Topic 1*

Which of the following is accurate regarding predefined drilldown tokens?

A. They capture data from a form input.

B. They vary by visualization type.

C. There are eight categories of predefined drilldown tokens.

D. They are defined by a panel's base search.

**Suggested Answer:** *D*

**Rounaldo** Most Recent 1 year, 7 months ago

Selected Answer: B

B is correct

upvoted 1 times

**ykamalharsha** 1 year, 9 months ago

Selected Answer: B

predefined drilldown tokens are not defined by the base search of a panel. Instead, they are predefined by Splunk to capture specific user interactions with visualizations. Predefined drilldown tokens in Splunk are designed to capture user actions or other values from a dashboard, and their availability and behavior can vary depending on the type of visualization being used

upvoted 1 times

**Derag** 2 years, 4 months ago

Correct option is B. Predefined drilldown tokens can vary depending on the visualization type used in the panel, as different visualizations may support different types of drilldown actions.

upvoted 3 times

Question #41 *Topic 1*

What is returned when Splunk finds fewer than the minimum matches for each lookup value?

A. The default value NULL until the minimum match threshold is reached.

B. The default match value until the minimum match threshold is reached.

C. The first match unless the time_field attribute is specified.

D. Only the first match.

**Suggested Answer:** *A*

**succulentchinesemeal** Most Recent 1 year, 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

**Soccerfan** 1 year, 10 months ago

B - https://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Usefieldlookupstoaddinformationtoyourevents#:~:text=The%20table%20in%20the%20CSV,rows%20that%20exceed%204096%20characters.

upvoted 1 times

**adpafer** 2 years, 3 months ago

B is correct

upvoted 1 times

**emlch** 2 years, 3 months ago

B is correct

upvoted 2 times

Question #42 *Topic 1*

Assuming a standard time zone across the environment, what syntax will always return events from between 2:00am and 5:00am?

A. date hour>=2 AND date_hour<5

B. earliest==2h@h AND latests-5h@h

C. time_hour>=2 AND time_hour>=5

D. earliest-2h@h AND latest=5h@h

**Suggested Answer:** *B*

**succulentchinesemeal** Most Recent 1 year, 5 months ago

Selected Answer: A

A agree

upvoted 1 times

**marinatedcohort** 1 year, 10 months ago

Selected Answer: A

A - assuming a typo in date_hour

upvoted 1 times

**poorisubash** 2 years, 2 months ago

The correct answer is: A. date hour>=2 AND date_hour =2 AND date_hour<5, it ensures that events from 2:00am to 4:59am are returned, effectively capturing the timeframe between 2:00am and 5:00am.

upvoted 3 times

**Derag** 2 years, 4 months ago

I think there is a typo, the correct answer is A. It's just missing the _ from the statement.

upvoted 2 times

Question #43 *Topic 1*

What does using the tstats command with summariesonly=false do?

A. Returns results from only non-summarized data.

B. Returns results from both summarized and non-summarized data.

C. Prevents use of wildcard characters in aggregate functions.

D. Returns no results.

**Suggested Answer:** *B*

**Soccerfan** Most Recent 1 year, 10 months ago

B - It quickly returns results from the summarized data, and returns results more slowly from the raw, unsummarized data that exists outside of the data model summary range.

upvoted 1 times

Question #44 *Topic 1*

A report named "Linux logins" populates a summary index with the search string sourcetype=linux secure | sitop src ip user. Which of the following correctly searches against the summary index for this data?

A. index=summary sourcetype="linux_secure" | top src_ip user

B. index=summary search name="Linux logins" | top src ip user

C. index=summary search_name="Linux logins" | stats count by src_ip user

D. index=summary sourcetype="linux secure" | stats count by src_ip user

**Suggested Answer:** *D*

**Betoemihtevas** Most Recent 1 year ago

Selected Answer: D

Why D is correct It uses the correct index: summary It matches the original sourcetype: "linux secure" It uses stats count by src_ip user, which is appropriate for summarizing login activity  Why the others are incorrect A uses an incorrect sourcetype "linux_secure" (underscore instead of space) B uses search name="Linux logins" which is not valid syntax for summary index searches C uses search_name="Linux logins" which is also not valid unless you're using a saved search reference in a different context

upvoted 1 times

**adamsca** 1 year, 8 months ago

Selected Answer: B

B is the correct answer. https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Sitop

upvoted 1 times

**Derag** 1 year, 10 months ago

Please ignore my previous comment, It is B. It also states it needs to be filtered by the top IP user.

upvoted 2 times

**Derag** 1 year, 10 months ago

It is C. I have verified it by myself.

upvoted 1 times

**Eddie_exam** 1 year, 10 months ago

Selected Answer: C

Correct answer is C. The name of the report should be the value for the field search_name. See Splunk Fundamentals 3 slide 220.the same slide deck you mention shows the answer at page 225. if you're using | sitop to create an summary you would search | top

upvoted 1 times

**emlch** 1 year, 9 months ago

the same slide deck you mention shows the answer at page 225. if you're using | sitop to create an summary you would search | top

upvoted 1 times

Question #45 *Topic 1*

Which of the following is accurate about cascading inputs?

A. They can be reset by an event handler.

B. The final input has no impact on previous inputs.

C. Only the final input of the sequence can supply a token to searches.

D. Inputs added to panels can not participate.

**Suggested Answer:** *A*

**Soccerfan** Most Recent 1 year, 10 months ago

A - https://www.splunk.com/en_us/blog/tips-and-tricks/dashboards-beta-v0-9-all-things-inputs.html

upvoted 1 times

**Derag** 2 years, 4 months ago

No, its B. Event handlers are used to trigger actions based on user interactions, such as clicking a button or selecting a value from a dropdown. While event handlers can be used to reset the value of an input, they cannot be used to reset the value of a cascading input sequence.A, reason: event handler to reset a menu when another menu is changed Final input does affect the previous inputs. Reference, Splunk video: Click on first input shows the list of players, who played game X. When clicking on a player for game X, will show Player Y's game list

upvoted 1 times

**DevinArchie** 2 years, 1 month ago

A, reason: event handler to reset a menu when another menu is changed Final input does affect the previous inputs. Reference, Splunk video: Click on first input shows the list of players, who played game X. When clicking on a player for game X, will show Player Y's game list

upvoted 1 times

Question #46 *Topic 1*

What is the correct hierarchy of XML elements in a dashboard panel?

A.

B.

C.

D.

**Suggested Answer:** *B*

**ykamalharsha** Most Recent 1 year, 9 months ago

Selected Answer: B

Simple XML Reference - Splunk Documentation

upvoted 2 times

**SnakeTech** 2 years ago

Selected Answer: B

Good answer

upvoted 2 times

**emlch** 2 years, 3 months ago

upvoted 2 times

Question #47 *Topic 1*

When possible, what is the best choice for summarizing data to improve search performance?

A. Use the fieldsummary command

B. Data model acceleration

C. Report acceleration

D. Summary indexing

**Suggested Answer:** *D*

**Rounaldo** Most Recent 1 year, 7 months ago

Selected Answer: B

Data model acceleration

upvoted 1 times

**ykamalharsha** 1 year, 9 months ago

Selected Answer: D

Summary indexing is designed to improve search performance by precomputing and storing summarized data in a separate index. This allows you to run searches on the smaller, summarized dataset rather than the full raw data, significantly speeding up search times.

upvoted 1 times

**Eddie_exam** 2 years, 4 months ago

Selected Answer: B

Correct answer is B. Data model acceleration is the easiest and most efficient acceleration option and should be your first choice. From Splunk Fundamentals 3 slide 230.

upvoted 1 times