EXAMTOPICS

- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

Which one of the following statements about the search command is true?

A. It does not allow the use of wildcards.

B. It treats field values in a case-sensitive manner.

C. It can only be used at the beginning of the search pipeline.

D. It behaves exactly like search strings before the first pipe.

Correct Answer: *D*

Reference:

https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand

Community vote distribution

D (100%)

oksey Highly Voted 4 years ago

The Correct Ans is D

upvoted 14 times

leonmflai4exam Highly Voted 3 years, 8 months ago

P.115 of F2. Behaves exactly like the search strings before the first pipe

upvoted 5 times

ComeUp 2 years, 7 months ago

This is correct

upvoted 2 times

a9f89d1 Most Recent 4 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

Uvasta 1 year, 9 months ago

A page 101 troubleshooting

upvoted 1 times

Uvasta 1 year, 9 months ago

Is it not A

upvoted 1 times

Dracula666 3 years ago

The correct answer is D. Slide 115

upvoted 3 times

sid2051 3 years, 12 months ago

D is correct

upvoted 2 times

qoijbztdtourbyuifo 4 years ago

Search command can also be used in second,third,... search pipeline.
like this:
`index="main" | search host=vendor_sales`
so the answer is D.

upvoted 4 times

Question #2 *Topic 1*

Which of the following actions can the eval command perform?

A. Remove fields from results.

B. Create or replace an existing field.

C. Group transactions by one or more fields.

D. Save SPL commands to be reused in other searches.

Correct Answer: *B*

Community vote distribution

B (100%)

abderrahimpro 1 year, 4 months ago

Selected Answer: B

The Correct is b.
The eval command calculates an expression and puts the resulting value into a search results field.

upvoted 2 times

34de54a 1 year, 6 months ago

i cinfirm it's B

upvoted 2 times

metromini 1 year, 9 months ago

just B, confirmed

upvoted 2 times

Uvasta 1 year, 9 months ago

The Correct is b

upvoted 2 times

Uvasta 1 year, 9 months ago

Best without wildcards

upvoted 1 times

TestingAccount900 1 year, 11 months ago

Selected Answer: B

B is right

upvoted 2 times

samtron 2 years, 7 months ago

Selected Answer: B

B correct

upvoted 1 times

andharep 2 years, 8 months ago

Its should be B

upvoted 1 times

cthulhu 2 years, 11 months ago

B is correct. Reference: https://docs.splunk.com/Documentation/Splunk/8.2.2/SearchReference/Eval

upvoted 1 times

Dracula666 3 years ago

Answer B.
Slide 97 Results of eval written to either new or existing field you specify. If the destination field exists, the value of the field are replaced by the result of eval

upvoted 1 times

Nanila 3 years, 6 months ago

It's B

upvoted 2 times

RyanDST 3 years, 6 months ago

"A" should be incorrect, "eval" can create or replace fields, but not remove.

upvoted 2 times

leonmflai4exam 3 years, 8 months ago

Is "A" True also?

upvoted 1 times

muraliecm 3 years, 8 months ago

Is "A" true?

upvoted 2 times

ggfsplunk 3 years, 9 months ago

"B" is also true.

upvoted 1 times

sid2051 3 years, 12 months ago

B is correct

upvoted 2 times

Shabhi16 3 years, 12 months ago

B is true

upvoted 1 times

Question #3 *Topic 1*

When can a pipe follow a macro?

A. A pipe may always follow a macro.

B. The current user must own the macro.

C. The macro must be defined in the current app.

D. Only when sharing is set to global for the macro.

Correct Answer: *A*

[Removed] Highly Voted 3 years, 9 months ago

A
Fund 2 - P.212: Using a basic macro - Pipe to more commands, or precede with a search string

upvoted 17 times

FK_AY Most Recent 10 months, 1 week ago

C: macro must be defined in the current app

upvoted 2 times

Uvasta 1 year, 9 months ago

The Correct is b

upvoted 1 times

Uvasta 1 year, 9 months ago

Index needs to be seleced

upvoted 1 times

qtygbapjpesdayazko 1 year, 9 months ago

I think is correct

upvoted 1 times

cthulhu 2 years, 11 months ago

The answer is A. Additional reference found here: https://books.google.com.mx/books?id=Ut18DwAAQBAJ&pg=PA173&lpg=PA173&dq=use+a+pipe+after+a+macro+splunk&source=bl&ots=VV76kboWQl&sig=ACfU3U0bfR3B9Sr7
SmHkFbavFyVeV3zw&hl=en&sa=X&ved=2ahUKEwiU077T_6TzAhVzkGoFHaQBAsoQ6AF6BAgQEAM#v=onepage&q=use%20a%20pipe%20after%
0a%20macro%20splunk&f=false

upvoted 1 times

mikey_76 3 years ago

The answer is A but the wording of B, C and D make it sound like the question is asking "WHO can use a macro?"

upvoted 1 times

leonmflai4exam 3 years, 8 months ago

Should it be A? since this question is asking for when will "pipe" be placed

upvoted 2 times

muraliecm 3 years, 8 months ago

"The macro must be defined in the current app"

upvoted 1 times

TeeCeeP 3 years, 9 months ago

I am thinking A. Nothing found anywhere?

upvoted 4 times

rishbah 3 years, 10 months ago

Correct answer is C

upvoted 3 times

> **jiaminyun** 3 years, 6 months ago
>
> C why ?
>
> upvoted 3 times

Question #4 *Topic 1*

Data models are composed of one or more of which of the following datasets? (Choose all that apply.)

A. Events datasets

B. Search datasets

C. Transaction datasets

D. Any child of event, transaction, and search datasets

Correct Answer: *ABC*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Community vote distribution

ABC (100%)

Powdered_Sugar Highly Voted 3 years, 9 months ago

I'm pretty sure all four of them are correct. The about data models page lists four types of datasets:
Event datasets,
Search datasets,
Transaction datasets,
Child datasets

https://docs.splunk.com/Documentation/Splunk/8.1.0/Knowledge/Aboutdatamodels

upvoted 22 times

Liberatus 3 years, 9 months ago

You are correct

upvoted 4 times

currotron 3 years, 4 months ago

It's true! Datasets break down into four types. These types are: Event datasets, search datasets, transaction datasets, and child datasets.
Ref.: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

upvoted 1 times

__x 2 years, 6 months ago

From the link provided:
Datasets break down into four types. These types are: Event datasets, search datasets, transaction datasets, and child datasets.

upvoted 1 times

__x 2 years, 6 months ago

Meanwhile, a data model derived from a heterogeneous system log might have several root datasets (events, searches, and transactions). Each of these root datasets can be the first dataset in a hierarchy of datasets with nested parent and child relationships. Each child dataset a dataset hierarchy can have new fields in addition to the fields they inherit from ancestor datasets.

upvoted 1 times

krishdee 3 years, 4 months ago

how to create child data set for Search data set?

upvoted 1 times

Glat Highly Voted 3 years, 8 months ago

Answer is ABC,
See p231 of F2

upvoted 15 times

DeltaPotato 3 years, 1 month ago

Test appears to be based off of the 7.x materials provided in Fund 2. Just finished class (July 2021). Can confirm pg 231 in 7.x course materials only lists ABC.

upvoted 5 times

vishal_gugale Most Recent 10 months, 3 weeks ago

ABC is correct

upvoted 1 times

kruasan 1 year ago

A,B,C,D
Splunk Data models are composed of one or more of the following datasets: Event Datasets, Search Datasets, Transaction Datasets, and Child Datasets1. So, the correct answer to your question is: A. Events datasets, B. Search datasets, C. Transaction datasets, and D. Any child of event, transaction, and search datasets.

upvoted 1 times

asarali 1 year, 3 months ago

Selected Answer: ABC

ABC - Datasets break down into four types. These types are: Event datasets, search datasets, transaction datasets, and child datasets.

D says child events...not child datasets

upvoted 3 times

test_12_12 1 year, 6 months ago

All four are correct -
" Child datasets of all three root dataset types--event, transaction, and search--are defined with simple constraints that narrow down the set of data that they inherit from their ancestor datasets.'

upvoted 1 times

Uvasta 1 year, 9 months ago

Index needs to be seleced

upvoted 2 times

Uvasta 1 year, 9 months ago

Is it not A

upvoted 1 times

SolventCourseisSCAM 1 year, 8 months ago

you commented the same question sentence under the many question. What are you trying to do? All of your selections are wrong

upvoted 6 times

shergar 1 year, 10 months ago

I'd pick ABCD too. You could argue against D based on the phrasing and that only a child dataset all by itself doesn't make up a data model. But child dataset literally can't exist by itself, so that argument doesn't make any sense.

I'd go for ABCD.

upvoted 1 times

PKUSER 1 year, 10 months ago

Datasets break down into four types. These types are: Event datasets, search datasets, transaction datasets, and child datasets.

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

upvoted 2 times

gabo1969 2 years, 9 months ago

ABC is correct!

upvoted 3 times

gabo1969 2 years, 9 months ago

Correct ABC
https://docs.splunk.com/Documentation/Splunk/8.2.3/Knowledge/Aboutdatamodels

upvoted 3 times

jackvn6 1 year, 11 months ago

Datasets break down into four types. These types are: Event datasets, search datasets, transaction datasets, and child datasets.

upvoted 1 times

Question #5 *Topic 1*

When using the Field Extractor (FX), which of the following delimiters will work? (Choose all that apply.)

A. Tabs

B. Pipes

C. Colons

D. Spaces

Correct Answer: *BD*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

Community vote distribution

AB (100%)

TeeCeeP Highly Voted 3 years, 9 months ago

I say ABCD, Colons can fall in the other category.

upvoted 42 times

gcalcaterra 3 years, 9 months ago

Correct

upvoted 2 times

antukin 3 years, 6 months ago

p152 - ...separated by delimiters (spaces, commas, pipes, tabs, or other characters).

upvoted 9 times

MxQ3 2 years, 2 months ago

ABCD is also my suggestion as in m Fundamentals 2 PDF dated Jan 2021, Delimiters used in events is Space, Comma, Tab Pipe and Other (whi
can be colons)

upvoted 2 times

sainfosec Highly Voted 3 years, 3 months ago

tested in my lab. ABCD is the current answer

upvoted 16 times

darNiz Most Recent 7 months ago

ABCD - according to documentation

upvoted 1 times

ANki_24 8 months, 1 week ago

Selected Answer: AB

All ABCD are correct

upvoted 1 times

Sankardevarajan1986 9 months ago

community vote distribution Answer AB, but Examtopics Answer BD, which one consider is right?

upvoted 1 times

jimil001 9 months, 1 week ago

Selected Answer: AB

ABC not colons!

upvoted 1 times

jimil001 9 months, 1 week ago

Correction ABD ! https://docs.splunk.com/Documentation/Splunk/7.3.0/Knowledge/FXRenameFieldsstep

upvoted 1 times

exampass999 11 months, 3 weeks ago

I think A, B, D. Because a comma, not a colon, is the correct answer.

upvoted 1 times

kruasan 1 year ago

ABCD

A. Tabs: Tabs can be used as delimiters for field extraction in Splunk. They are commonly used when data is separated by tab characters.

B. Pipes: Pipes (|) can be used as delimiters in Splunk's Field Extractor. This is especially useful when data is structured using pipe characters as separators.

C. Colons: Colons (:) can also be used as delimiters when defining field extractions in Splunk. If your data is separated by colons, you can specify this delimiter.

D. Spaces: Spaces can be used as delimiters as well. If your data is separated by spaces, you can configure the Field Extractor to recognize spaces delimiters.

So, all of the options (A, B, C, D) can work as delimiters when using the Field Extractor in Splunk, depending on how your data is structured and separated. You can choose the appropriate delimiter that matches the format of your data.

upvoted 1 times

Huslayer 1 year, 1 month ago

All of them

upvoted 2 times

n00r1 1 year, 2 months ago

According to Splunk, space, comma, tab, pipehttps://docs.splunk.com/Documentation/Splunk/9.0.5/Knowledge/FXRenameFieldsstep

upvoted 2 times

Mntman77 1 year, 2 months ago

So all the Splunk docs say " comma and space for sure" but the document reference below does include colons and tabs. (You can use the DELIM attribute in field transforms to configure field extractions for events where field values or field/value pairs are separated by delimiters such as commas, colons, tab spaces, and more.) = ABCD in my OP

upvoted 1 times

Harrysa 1 year, 5 months ago

ABCD is correct:When using the Field Extractor (FX) in Splunk, several delimiters can be used to extract fields from events, including:

Space ( ): Used to extract fields that are separated by spaces.
Comma (,): Used to extract fields that are separated by commas.
Tab (\t): Used to extract fields that are separated by tabs.
Pipe (|): Used to extract fields that are separated by pipes.
Semi-colon (;): Used to extract fields that are separated by semi-colons.

upvoted 5 times

mohanmk95 1 year, 5 months ago

I choose the all. because we can extract the data for any fields.

upvoted 1 times

tomhola 1 year, 5 months ago

ABCD
You can use the DELIMS attribute in field transforms to configure field extractions for events where field values or field/value pairs are separated l delimiters such as commas, colons, tab spaces, and more.
https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Exampleconfigurationsusingfieldtransforms

upvoted 2 times

Alexi2415 1 year, 6 months ago

https://kinneygroup.com/blog/a-lesson-on-splunk-field-extractions-and-rex-and-erex-commands/#:~:text=Delimiters%20are%20characters%20used%20to,pipes%2C%20tabs%2C%20and%20colons.

upvoted 1 times

Alexi2415 1 year, 5 months ago

ABCD are all correct

upvoted 1 times

metromini 1 year, 9 months ago

All the above

upvoted 3 times

fodder137 1 year, 9 months ago

Can we please have this corrected to A,B,C,D as reflected

upvoted 3 times

Question #6 *Topic 1*

Which group of users would most likely use pivots?

A. Users

B. Architects

C. Administrators

D. Knowledge Managers

Correct Answer: *D*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

Community vote distribution

A (60%) D (40%)

TeeCeeP Highly Voted 3 years, 9 months ago

A. Users.. Knowledge Managers build them.

upvoted 27 times

Glat 3 years, 8 months ago

Yes, see p142 of F2

upvoted 4 times

MxQ3 2 years, 2 months ago

Agree! Please change the answer moderator, it's users who uses them, knowledge managers build them! Unless the question is asking about who is building them

upvoted 4 times

Eli1982 Most Recent 1 month ago

Selected Answer: A

A for sure!

upvoted 1 times

samsam5136431 3 months ago

Selected Answer: A

A user !!! change the answer !

upvoted 2 times

Ulquiorrar 5 months, 1 week ago

Witch correct Knowledge Managers or User?

upvoted 1 times

tineboy46 7 months ago

a. USER is the correct answer. just took this class!

upvoted 1 times

darNiz 7 months ago

users USE pivots, and Knowledge Object managers - create them

upvoted 1 times

jimil001 9 months, 1 week ago

Selected Answer: A

Users!

upvoted 1 times

John199506 9 months, 2 weeks ago

Selected Answer: A

User is the beginner class of users. They level of knowledge is also minimum hence they are not creating SPL searches..

upvoted 1 times

exampass999 11 months, 3 weeks ago

I think D.
The prerequisite for using pivots is the design of the data model. The data model is created by the knowledge manager, not the user.

upvoted 2 times

psychezombie 1 year ago

Selected Answer: A

user is the correct ans

upvoted 2 times

Silas_Winterian 1 year, 2 months ago

A
Creation of data models for Pivot users. Splunk software offers the Pivot tool for users who want to quickly create tables, charts, and dashboards without having to write search strings that can sometimes be long and complicated. The Pivot tool is driven by data models--without a data mod Pivot has nothing to report on. Data models are designed by Splunk knowledge managers: people who understand the format and semantics of their indexed data, and who are familiar with the Splunk search language.

upvoted 2 times

mohanmk95 1 year, 4 months ago

Selected Answer: A

user is the correct one

upvoted 3 times

1988Greg 1 year, 4 months ago

Selected Answer: A

A. Users.. Knowledge Managers build them.

upvoted 1 times

solomone 1 year, 5 months ago

Selected Answer: D

Answer in the context of what they are looking for is D

upvoted 2 times

clapillo 1 year, 5 months ago

Selected Answer: D

Knowledge Managers is the correct one.

upvoted 2 times

Hasho 1 year, 6 months ago

Answer D, because the manger need use these features of (pivot) but for normal user no need it

upvoted 2 times

Requete 1 year, 6 months ago

Selected Answer: A

Answer is A

upvoted 1 times

Question #7 *Topic 1*

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?

A. Rank

B. Weight

C. Priority

D. Precedence

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes

Community vote distribution

C (100%)

Brandflakes Highly Voted 3 years, 9 months ago

Answer is C:

Page 206 of the PDF in the bubble

upvoted 11 times

> **RyanDST** 3 years, 6 months ago
>
> Which PDF are you referring to? Is it publicly available?
>
> upvoted 1 times
>
> > **antukin** 3 years, 6 months ago
> >
> > Splunk Fundamentals 2 PDF. Not publicly available though, at least not to my knowledge. Take the splunk fundamentals 2 course and you can download the PDF.
> >
> > upvoted 2 times

abderrahimpro Most Recent 1 year, 4 months ago

Selected Answer: C

https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/Abouteventtypepriorities

upvoted 1 times

metromini 1 year, 9 months ago

Selected Answer: C

It is confirmed. Search for event type color in fundamental study.

upvoted 3 times

dd188 1 year, 11 months ago

Selected Answer: C

Answer is C

upvoted 2 times

MxQ3 2 years, 2 months ago

From Fundamentals 2 PDF, "Priority controls which event type color displays for an event" so answer is C (Priority)

upvoted 1 times

Dutz 2 years, 5 months ago

C

New Link: https://docs.splunk.com/Documentation/SplunkCloud/8.2.2201/Knowledge/Abouteventtypepriorities

upvoted 1 times

mjl79 3 years, 4 months ago

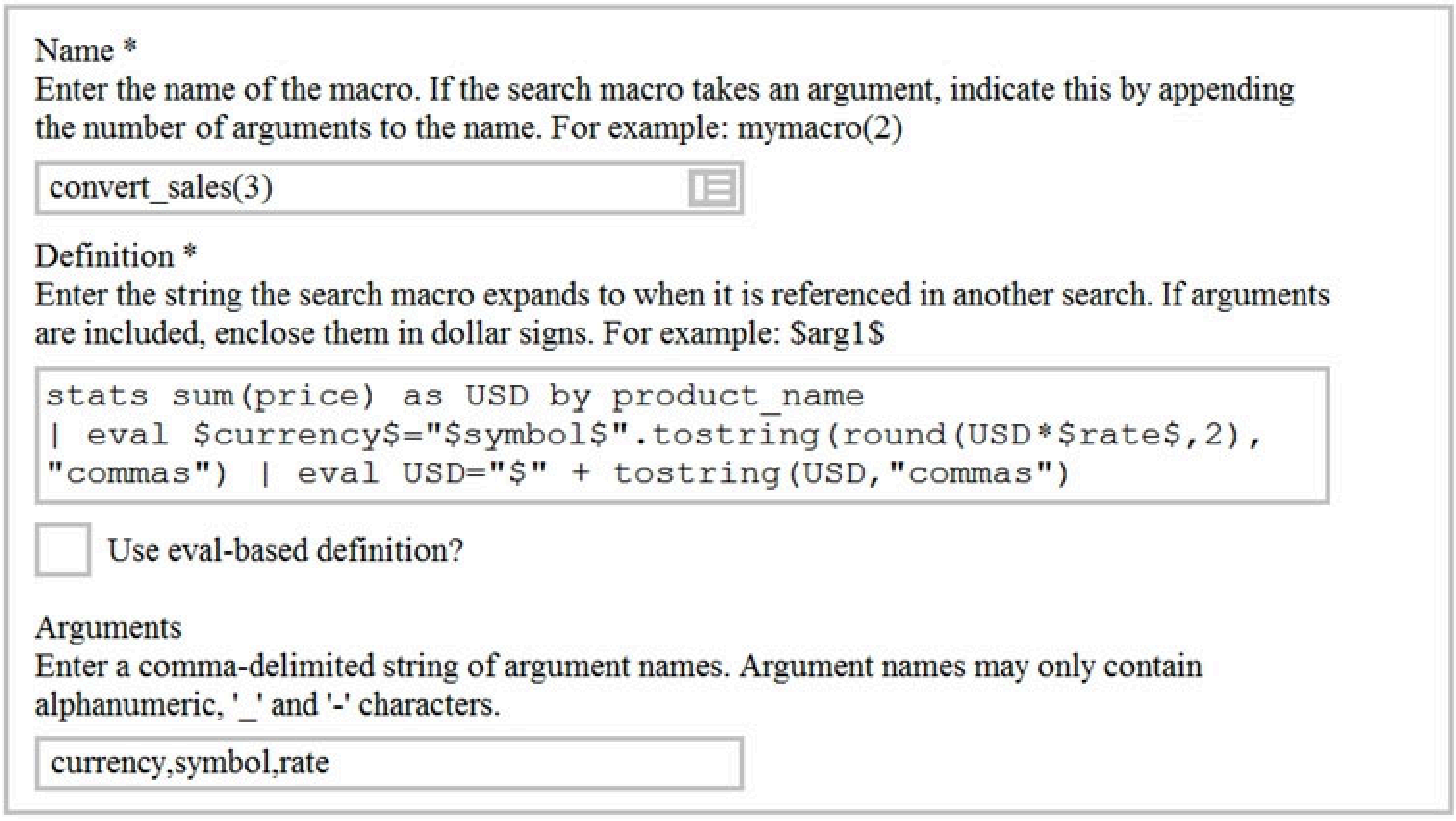
Brandflakes is correct, the answer is C - priority
"Priority determines the order of the event type listing in the expanded event. It also determines which color displays for the event type if two or more of the event types matching the event have a defined Color value.
For more see About event type priorities"

upvoted 2 times

> **othman** 3 years, 3 months ago
>
> May I know in what scenarios using event types is useful?
>
> upvoted 1 times

Question #8 *Topic 1*

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

convert_sales(3)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),
"commas") | eval USD="$" + tostring(USD,"commas")
```

□ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

currency,symbol,rate

A. "convert_sales(euro,79.,¬,ג)"

B. 'convert_sales(euro,79.,¬,ג)'

C. "convert_sales($euro$,79.$,$¬,ג)"

D. 'convert_sales($euro$,79.$,$¬,ג)'

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

Community vote distribution

B (100%)

antukin Highly Voted 3 years, 5 months ago

Currency,Symbol,Rate - answer should be somewhat like `convert_sales`(euro,€,0.79)

upvoted 18 times

antukin 3 years, 5 months ago

`convert_sales(euro,€,0.79)`

upvoted 14 times

Orion42 3 years, 1 month ago

yes, can confirm, the answers are malformed here, but the real (and correct) answer is this one

upvoted 4 times

gongiz Most Recent 1 year, 11 months ago

Selected Answer: B

As i can see there are 3 arguments "currency, sympol and rate.
The other dollar sign is just because they want it to be in USD, to excute this macro you should just write 'convert_sales'. But as many other say in there B is less wrong.

upvoted 2 times

Jack__ 2 years, 1 month ago

Selected Answer: B

All answers are wrong. B is the least wrong.
' and " are incorrect; should be `
additionally, there should only be 3 arguments, not 4.

upvoted 3 times

Nicker9 2 years, 1 month ago

yeah please correct the answers. Macros only work with backticks ` `

upvoted 1 times

MxQ3 2 years, 2 months ago

B is correct answer!

upvoted 1 times

gabo1969 2 years, 9 months ago

`convert_sales(euro,€,0.79)` Is Correct...review the PDF document.

upvoted 3 times

New_user 3 years, 5 months ago

There's 4 parameters in every answer, but only three in macro. Can someone explain how does it work?

upvoted 2 times

aosroyal 2 years, 4 months ago

the site is not properly displaying the answer.

upvoted 2 times

Question #9 *Topic 1*

There are several ways to access the field extractor.
Which option automatically identifies the data type, source type, and sample event?

A. Event Actions > Extract Fields

B. Fields sidebar > Extract New Fields

C. Settings > Field Extractions > New Field Extraction

D. Settings > Field Extractions > Open Field Extractor

Correct Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.4/Knowledge/Managesearch-timefieldextractions

Community vote distribution

A (100%)

carm8989 Highly Voted 3 years, 11 months ago
A its the correct answer
upvoted 23 times

Sartarus Highly Voted 4 years ago
A its correct
upvoted 10 times

kruasan Most Recent 1 year ago
Selected Answer: A
C, D - Settings > Field extractions does not exist
B - is not automatical
upvoted 1 times

mialux 1 year, 9 months ago
Selected Answer: A
A its the correct answer
upvoted 2 times

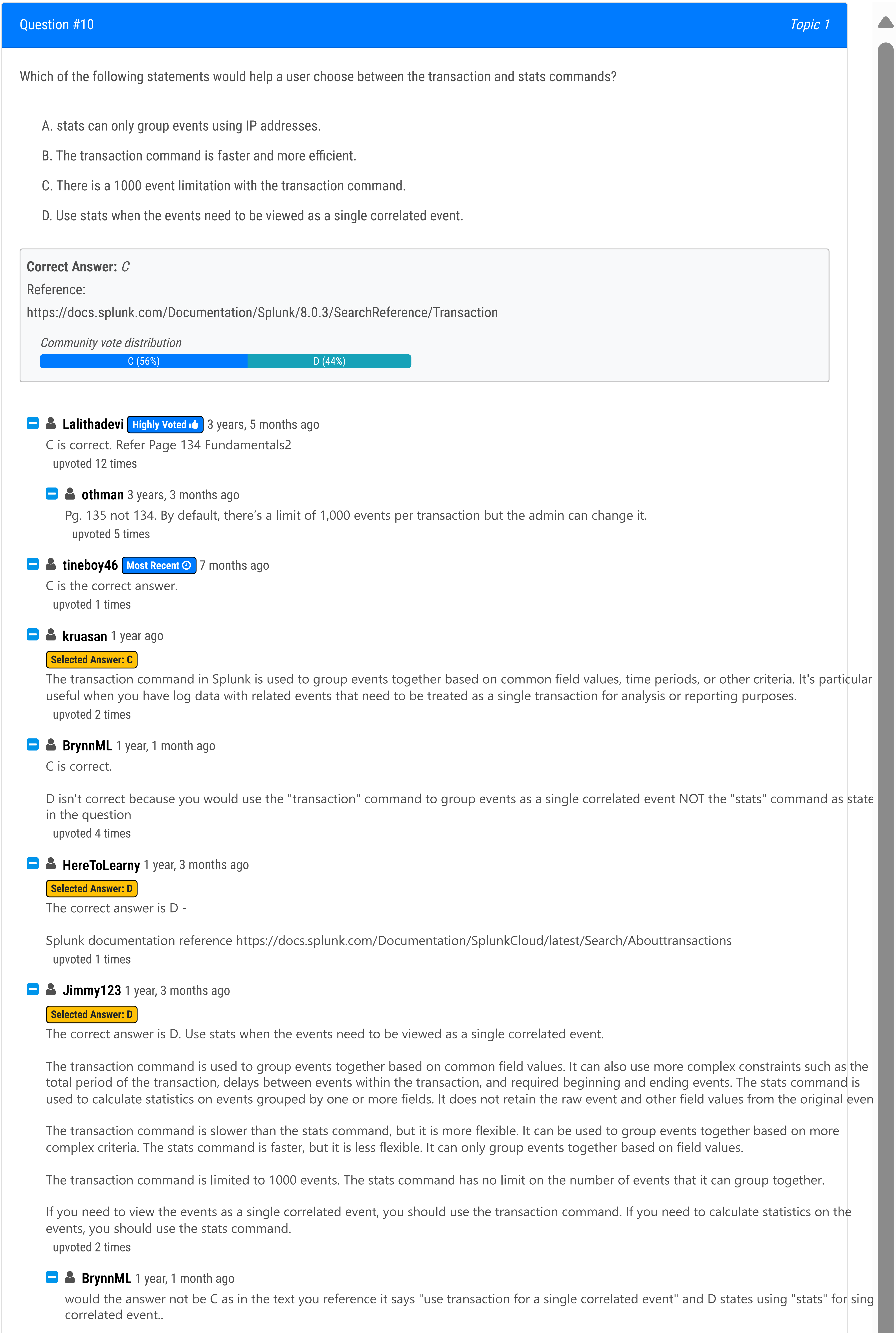
Azure_The_Tormentor 2 years, 10 months ago
A is the correct answer.
https://docs.splunk.com/Documentation/Splunk/8.2.3/Knowledge/ExtractfieldsinteractivelywithIFX

look at the picture
upvoted 6 times

Lalithadevi 3 years, 5 months ago
A is correct answer
upvoted 3 times

demarko 3 years, 11 months ago
AB are correct
upvoted 3 times

> **gcalcaterra** 3 years, 9 months ago
> B doesn't automatically identify the sample event to use.
> upvoted 4 times
>
> **othman** 3 years, 3 months ago
> B will open field extractor wizard
> upvoted 2 times



Question #10 *Topic 1*

Which of the following statements would help a user choose between the transaction and stats commands?

A. stats can only group events using IP addresses.

B. The transaction command is faster and more efficient.

C. There is a 1000 event limitation with the transaction command.

D. Use stats when the events need to be viewed as a single correlated event.

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

Community vote distribution

C (56%) D (44%)

Lalithadevi Highly Voted 3 years, 5 months ago

C is correct. Refer Page 134 Fundamentals2

upvoted 12 times

othman 3 years, 3 months ago

Pg. 135 not 134. By default, there's a limit of 1,000 events per transaction but the admin can change it.

upvoted 5 times

tineboy46 Most Recent 7 months ago

C is the correct answer.

upvoted 1 times

kruasan 1 year ago

Selected Answer: C

The transaction command in Splunk is used to group events together based on common field values, time periods, or other criteria. It's particular useful when you have log data with related events that need to be treated as a single transaction for analysis or reporting purposes.

upvoted 2 times

BrynnML 1 year, 1 month ago

C is correct.

D isn't correct because you would use the "transaction" command to group events as a single correlated event NOT the "stats" command as state in the question

upvoted 4 times

HereToLearny 1 year, 3 months ago

Selected Answer: D

The correct answer is D -

Splunk documentation reference https://docs.splunk.com/Documentation/SplunkCloud/latest/Search/Abouttransactions

upvoted 1 times

Jimmy123 1 year, 3 months ago

Selected Answer: D

The correct answer is D. Use stats when the events need to be viewed as a single correlated event.

The transaction command is used to group events together based on common field values. It can also use more complex constraints such as the total period of the transaction, delays between events within the transaction, and required beginning and ending events. The stats command is used to calculate statistics on events grouped by one or more fields. It does not retain the raw event and other field values from the original even

The transaction command is slower than the stats command, but it is more flexible. It can be used to group events together based on more complex criteria. The stats command is faster, but it is less flexible. It can only group events together based on field values.

The transaction command is limited to 1000 events. The stats command has no limit on the number of events that it can group together.

If you need to view the events as a single correlated event, you should use the transaction command. If you need to calculate statistics on the events, you should use the stats command.

upvoted 2 times

BrynnML 1 year, 1 month ago

would the answer not be C as in the text you reference it says "use transaction for a single correlated event" and D states using "stats" for sing correlated event..

upvoted 2 times

AlexSOC 1 year, 5 months ago

Selected Answer: C

C is correct.

upvoted 3 times

raizen11 1 year, 5 months ago

Ans is C
D statement cab be corrected by replacing stats with trasnaction.... Use Transaction when the events need to be viewed as a single correlated eve

upvoted 1 times

yaman778 1 year, 6 months ago

Selected Answer: D

As other people's comments the limitation of events quantity is changeable by admin. I think D is much better than C, But I didn't find evidence.
We have 2 specific cases refer to use transaction better.
1.unique ID alone is not sufficient to discriminate between 2 transactions.
2. When it is desirable to see the raw text of the events combined rather than analysis on constituent fields of events.

upvoted 1 times

MxQ3 2 years, 2 months ago

Limit of 1,000 events per transaciton to no limits when using stats.

upvoted 1 times

Question #11 *Topic 1*

By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

A. Turned off.

B. Turned on.

C. Determined automatically based on the sourcetype.

D. Determined automatically based on the data source.

Correct Answer: *A*

Community vote distribution

A (100%)

oksey Highly Voted 4 years ago

By default, the acceleration is turned off, So ans is A

upvoted 16 times

sid2051 Highly Voted 3 years, 12 months ago

Correct Answer is A ,Fundamental 2 Pdf page 273

upvoted 11 times

kruasan Most Recent 1 year ago

Selected Answer: A

All data models included in the CIM add-on have data model acceleration disabled by default.

https://docs.splunk.com/Documentation/CIM/5.1.1/User/Setup

upvoted 1 times

ggfsplunk 3 years, 9 months ago

based on the document "A" is correct answer, by default acceleration is off.

upvoted 4 times

Question #12 *Topic 1*

Which of the following statements describe the Common Information Model (CIM)? (Choose all that apply.)

A. CIM is a methodology for normalizing data.

B. CIM can correlate data from different sources.

C. The Knowledge Manager uses the CIM to create knowledge objects.

D. CIM is an app that can coexist with other apps on a single Splunk deployment.

Correct Answer: *ABD*

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

Community vote distribution

ABC (63%) AB (38%)

NLotus Highly Voted 3 years ago

As others have said,
A - Correct
B - Correct
Now for the interesting ones.
C - CIM can create reports, which are a type of saved search, which are knowledge objects. Also, yes it is the knowledge manager's role: "you can use the models to generate reports", from the Knowledge Management docs
https://docs.splunk.com/Documentation/Splunk/8.2.1/Knowledge/UnderstandandusetheCommonInformationModel
- Correct
D - Splunk's splexicon for add-on: "A type of app..." and the F2 pdf "The CIM add-on is a search time app..."
https://docs.splunk.com/Splexicon:Addon
- Correct

ABCD is correct

upvoted 27 times

Hudda Highly Voted 3 years, 2 months ago

Friends,finally ABC? could you please confirm this answer?

upvoted 8 times

achalm 2 years, 7 months ago

yes friend

upvoted 4 times

adella1031 Most Recent 1 month ago

I think ABC is correct. Yes, CIM add-on is an app that can be downloaded from splunkbase but as for CIM itself, it is a set of data models which yc can use during search time

upvoted 1 times

ANki_24 8 months, 1 week ago

Selected Answer: ABC

ABCD are correct

upvoted 2 times

SH_N 11 months, 4 weeks ago

what is the correct answer? ABD or just AB

upvoted 1 times

clapillo 1 year, 5 months ago

Selected Answer: ABC

"CIM is an app that can coexist with other apps on a single Splunk deployment" is not correct

upvoted 3 times

codemk 1 year, 8 months ago

A different perspective but it is A, C and D for me
A - yes
B - no because the CIM is used to normalise, not to correlate
C - yes
D - yes, according to the Splexicon, an add-on is a type of app therefore D is correct

upvoted 1 times

metromini 1 year, 9 months ago

Selected Answer: AB

It doesn't say it needs 3 answer, just A and B are the confirmed right answers.

upvoted 3 times

guilhermecervo 2 years, 4 months ago

This is a hard understandable and trick question. In my first read I thought it was ABC but after a while and doing some researches I end up with and B. Here is my explanation:

C - CIM is not a tool to create Knowledge OBjects. Knowledge manager use CIM to have a default start up of Knowledge OBjects.

D - Despite Add-on be a TYPE of APP, add-on is not equal to an app.
"Unlike an Add-on, App caters towards only a single perspective. It is used only for one common goal and it can be used for a specific thing."

https://dev.splunk.com/enterprise/docs/welcome/?_gl=1*1x7ca1c*_ga*MjA0MTE4MDA2OC4xNjQzMDI4MzEx*_gid*OTYwNjk3ODMxLjE2NTEwNjgwMDE.&_ga=2.11612092.960697831.1651068001-2041180068.1643028311#What-is-a-Splunk-app

https://dev.splunk.com/enterprise/docs/welcome/?_gl=1*1x7ca1c*_ga*MjA0MTE4MDA2OC4xNjQzMDI4MzEx*_gid*OTYwNjk3ODMxLjE2NTEwNjgwMDE.&_ga=2.11612092.960697831.1651068001-2041180068.1643028311#What-is-a-Splunk-add-on

upvoted 6 times

M9201715 2 years, 11 months ago

Agree with Ajames21 - option D is incorrect because CIM is an add-on, not an app. So correct answer is ABC
See this discussion on the differences between apps and add-ons:
https://www.splunk.com/en_us/blog/tips-and-tricks/what-are-splunk-apps-and-add-ons.html
and this page on the CIM add-on:
https://splunkbase.splunk.com/app/1621/#/details (App Type is listed as Add-on, bottom right corner of Details tab)

upvoted 7 times

teems5uk 2 years, 11 months ago

Option D is really confusing, but according to page 268: CIM only helps to ensure – Multiple apps can co-exist on a single Splunk deployment.

upvoted 2 times

teems5uk 2 years, 11 months ago

Fun2(page 268)
What is the Common Information Model (CIM)?
• The Splunk Common Information Model provides a methodology to
normalize data
• Leverage the CIM when creating field extractions, field aliases,
event types, and tags to ensure:
– Multiple apps can co-exist on a single Splunk deployment
– Object permissions can be set to global for the use of multiple
apps
– Easier and more efficient correlation of data from different
sources and source types

upvoted 3 times

Ajames21 3 years, 1 month ago

ABC is correct

A - Duh
B - page 268 fundamentals 2
C - reports and dashboards are knowledge objects,
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtocreatereportsanddashboards
D - CIM is an addon not an app, obvious trick wording
https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

upvoted 2 times

lGoddard90 3 years, 5 months ago

A lot of different responses for this question! It seems to be ambiguously worded, i thought ABC was correct

upvoted 2 times

utku461 3 years, 5 months ago

"The CIM add-on is a search time app..." so i guess D is kinda correct or am i mistaken?
I would say A,B and D

upvoted 2 times

robotn1k 3 years, 7 months ago

A and B are correct
D is incorrect as CIM is a framework that 'allows' apps to co-exist on a single instance

upvoted 2 times

lxlJustinlxl 3 years, 7 months ago

AB for sure.. but I am not sure about C
D is out (says CIM is an app but it is an add on)
The issue with C is that CIM is used to normalize data and then that normalized data can be used to create reports (a knowledge object) - I don't think CIM itself can be used to create the knowledge objects.

upvoted 3 times

Question #13 *Topic 1*

Which of the following knowledge objects represents the output of an eval expression?

A. Eval fields

B. Calculated fields

C. Field extractions

D. Calculated lookups

Correct Answer: *B*

Reference:

https://docs.splunk.com/Splexicon:Calculatedfield

Community vote distribution

B (100%)

Brandflakes Highly Voted 3 years, 9 months ago

B

Pg. 188 on the PDF

upvoted 9 times

kruasan Most Recent 1 year ago

Selected Answer: B

The knowledge object that represents the output of an eval expression in Splunk is typically referred to as "Calculated fields." When you use the eval command in Splunk, you are creating new fields or modifying existing fields based on expressions or calculations. These calculated fields can be used in searches, reports, and dashboards to analyze and visualize data in different ways.

upvoted 1 times

abderrahimpro 1 year, 4 months ago

Selected Answer: B

https://docs.splunk.com/Documentation/Splunk/9.0.4/Knowledge/definecalcfields

upvoted 1 times

linux_programmer46 2 years, 2 months ago

B for bravo!

upvoted 2 times

ravindraz 3 years, 2 months ago

b is the correct answer, f2 - p188

upvoted 2 times

Question #14 *Topic 1*

What do events in a transaction have in common?

A. All events in a transaction must have the same timestamp.

B. All events in a transaction must have the same sourcetype.

C. All events in a transaction must have the exact same set of fields.

D. All events in a transaction must be related by one or more fields.

Correct Answer: *D*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions

Community vote distribution

D (100%)

oksey Highly Voted 👍 4 years ago

All events in a transaction must be related by one or more fields.

upvoted 18 times

kbisht Highly Voted 👍 4 years ago

D is the correct ans

upvoted 13 times

abderrahimpro Most Recent 🕓 1 year, 4 months ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

erick165 2 years, 2 months ago

D is correct but B could be right too

upvoted 1 times

king1993 2 years, 5 months ago

Answer: D

upvoted 1 times

leonmflai4exam 3 years, 8 months ago

D, P.124 in F2

upvoted 5 times

ggfsplunk 3 years, 9 months ago

correct answer is "D"

upvoted 5 times

sid2051 3 years, 12 months ago

D is correct .

upvoted 6 times

Question #15 *Topic 1*

Which delimiters can the Field Extractor (FX) detect? (Choose all that apply.)

A. Tabs

B. Pipes

C. Spaces

D. Commas

Correct Answer: *BCD*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

Community vote distribution

ABC (44%) | ACD (33%) | BCD (22%)

oksey Highly Voted 4 years ago

ABCD is the ans

upvoted 52 times

sid2051 Highly Voted 3 years, 12 months ago

ABCD everything

upvoted 22 times

stevo1974 Most Recent 4 months ago

in an test environment in the delimiter you can choose :space, comma , tab, pipe and other so correct is ABCD

upvoted 2 times

tineboy46 7 months ago

abcd IS THE ANSWER.

upvoted 1 times

shanumani777 11 months, 3 weeks ago

Answer is none, Check the S in all the answers, not tabs commas spaces, It should be tab comma space, So answer is none

upvoted 2 times

> **10minaccount** 10 months, 2 weeks ago
>
> LMAOOOOOOOOOOOOO
>
> upvoted 1 times

abderrahimpro 1 year, 4 months ago

Selected Answer: ACD

The answer is ABCD. try to do it in a lab and you will find the 4 options.

upvoted 3 times

Harrysa 1 year, 5 months ago

The answer is ABCD all!

upvoted 4 times

tomhola 1 year, 5 months ago

Correct answer is BCD
"cleanly separated by a common delimiter, such as a space, a comma, or a pipe character."
See doc https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

upvoted 2 times

Nerzul007 1 year, 6 months ago

Selected Answer: BCD

"cleanly separated by a common delimiter, such as a space, a comma, or a pipe character" From
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

upvoted 2 times

UPTICKG 1 year, 6 months ago

ABD is the Answer! Commas not Colons

upvoted 1 times

metromini 1 year, 9 months ago

Selected Answer: ABC

Moderator, I cannot select all ABCD answers in here. ABCD is the answer.

upvoted 1 times

fodder137 1 year, 9 months ago

Its all of them ABCD

upvoted 2 times

gongiz 1 year, 11 months ago

I have just check it. Your options is all of them, its not even under "other" anymore. so the correct answers is ABCD

upvoted 2 times

jackvn6 1 year, 11 months ago

BCD Only, with A answer we need to do some tricks. FX can't detect
==> cleanly separated by a common delimiter, such as a space, a comma, or a pipe character.

upvoted 2 times

emlch 2 years, 2 months ago

Selected Answer: ABC

Basically with the "others" delimiters option any string might be detectable by de field extractor. However all of the listed options are available even if the "others" option didn't exist. ABCD is the correct answer

upvoted 3 times

fsanchezs 2 years, 4 months ago

ABCD is the correct

upvoted 2 times

adamsca 2 years, 5 months ago

ABCD is correct see https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXRenameFieldsstep

upvoted 2 times

Question #16

Topic 1

A data model consists of which three types of datasets?

A. Constraint, field, value.

B. Events, searches, transactions.

C. Field extraction, regex, delimited.

D. Transaction, session ID, metadata.

Correct Answer: *B*

Reference:

https://docs.splunk.com/Splexicon:Datamodeldataset

Community vote distribution

B (100%)

Brandflakes Highly Voted 3 years, 9 months ago

B:

Pg. 231 of the PDF

upvoted 14 times

kruasan Most Recent 1 year ago

Selected Answer: B

Data model can consist of 3 types of datasets - Events, Searches and Transactions so B is correct answer.

upvoted 1 times

MxQ3 2 years, 2 months ago

Per F2 pdf, Data model can consist of 3 types of datasets - Events, Searches and Transactions so B is correct answer.

upvoted 2 times

Nanila 3 years, 6 months ago

Events, searches, and transaction pg. 231

upvoted 3 times

t4ufiq 3 years, 7 months ago

B;

you can check on this web page:

https://docs.splunk.com/Splexicon:Datamodeldataset

upvoted 2 times

Question #17 *Topic 1*

Where are the results of eval commands stored?

A. In a field.

B. In an index.

C. In a KV Store.

D. In a database.

Correct Answer: *A*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Eval

Community vote distribution

A (100%)

Brandflakes Highly Voted 👍 3 years, 9 months ago

A:

Pg 238 of the PDF

upvoted 8 times

> **sainfosec** 3 years, 3 months ago
>
> what pdf are you referring here?
>
> upvoted 1 times
>
> > **cthulhu** 2 years, 11 months ago
> >
> > I know this is an old comment but for anyone wondering, it's the PDF included with the Splunk Fundamentals pt. 2 course.
> >
> > upvoted 1 times

SpTester Highly Voted 👍 3 years, 8 months ago

A. Fun2 pdf 97 - results of eval written to new or existing field

upvoted 6 times

Cyde Most Recent ⏲ 1 month, 1 week ago

Selected Answer: A

The correct answer is A - In a field

upvoted 1 times

kruasan 1 year ago

Selected Answer: A

results of eval written to new or existing field

upvoted 1 times

MxQ3 2 years, 2 months ago

A is correct. Results of eval is written to new or existing field you specify.

upvoted 2 times

Question #18 *Topic 1*

Which of the following statements describe calculated fields? (Choose all that apply.)

A. Calculated fields can be used in the search bar.

B. Calculated fields can be based on an extracted field.

C. Calculated fields can only be applied to host and sourcetype.

D. Calculated fields are shortcuts for performing calculations using the eval command.

Correct Answer: *ABD*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

Community vote distribution

ABD (100%)

oksey Highly Voted 4 years ago

ABD is the ans

upvoted 15 times

sid2051 Highly Voted 3 years, 12 months ago

ABD . A is also correct

upvoted 9 times

kruasan Most Recent 1 year ago

Selected Answer: ABD

A. Calculated fields can be used in the search bar.

True. Calculated fields can be referenced in the search bar like any other extracted field1.
B. Calculated fields can be based on an extracted field.

True. Calculated fields can use extracted fields in their calculations1.
C. Calculated fields can only be applied to host and sourcetype.

False. While you can select a host, source, or source type to apply to the calculated field2, it's not limited to only these options.
D. Calculated fields are shortcuts for performing calculations using the eval command.

True. Calculated fields are indeed used as shortcuts for performing repetitive, long, or complex transformations using the eval command1.

upvoted 2 times

emergency_gouda 2 years, 1 month ago

Selected Answer: ABD

ABD is correct

upvoted 4 times

emlch 2 years, 2 months ago

To answer this question you must pay attention at the search time operations sequence:
1. Extractions 2. Aliases 3. Calculated 4. Lookups 5. Event types 6. Tags

A. That's correct
B. Yes, since calculated fields are evaluate after field extractions
D. That's correct since this is the definition of calculated fields

upvoted 2 times

king1993 2 years, 5 months ago

Answer: ABD

upvoted 1 times

huu_nguyen 2 years, 7 months ago

ABD is correct

upvoted 2 times

gabo1969 2 years, 9 months ago

The documentation say:
"Select host, source or sourcetype to apply to the calculated field and specifi the related name", not only host and source, I have my doubts!

upvoted 1 times

gabo1969 2 years, 9 months ago

I think ABD is Correct
upvoted 1 times

M9201715 2 years, 11 months ago
I know that F2 says it MUST be based on extracted field, not CAN be based. But in reality it doesn't need to be. "| eval newField = 1" works just fir
no extracted field. So ABD is correct.
upvoted 1 times

Robo187 3 years, 5 months ago
"MUST be based on extracted field", not CAN be based on extracted field.
upvoted 3 times

Nanila 3 years, 6 months ago
ABD, 188-190 of the PDF
upvoted 3 times

IxlJustinlxl 3 years, 7 months ago
Might just be AD
B says it CAN be based on extracted field - which suggests other alternatives.
pg 187 of F2: "Must be based on an extracted field"
upvoted 7 times

leonmflai4exam 3 years, 8 months ago
F2, P188 + P189
upvoted 1 times

Question #19 *Topic 1*

Calculated fields can be based on which of the following?

A. Tags

B. Extracted fields

C. Output fields for a lookup

D. Fields generated from a search string

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

Community vote distribution

B (100%)

Brandflakes Highly Voted 3 years, 9 months ago

B

Pg. 188 of the PDF

upvoted 9 times

Robo187 3 years, 5 months ago

"MUST be based on an extracted field", which makes B wrong

upvoted 1 times

Atavius 3 years, 5 months ago

Yeah but no other answer makes sense, so probably the wording in the question is wrong and should must instead of can

upvoted 2 times

kruasan Most Recent 1 year ago

Selected Answer: B

In Splunk, calculated fields can use extracted fields in their calculations, but it is not a requirement. Calculated fields can perform calculations with the values of two or more fields already present in those events. These fields can be extracted fields or any other field present in the event data. S to answer your question, calculated fields can use extracted fields in their calculations, but it is not a must.

upvoted 1 times

Mntman77 1 year, 2 months ago

"D" is possible, but B is the best answer. "Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags."

upvoted 1 times

abderrahimpro 1 year, 4 months ago

Selected Answer: B

It's B.

upvoted 1 times

Ajames21 3 years, 1 month ago

It's B

"Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags."

upvoted 4 times

New_user 3 years, 1 month ago

Answer B means that you can't make calculated fields based on lookup fields, but that is not true. Answer is D - you can make calculated fields or fields generated by search string, including extracted fields, lookup fields and other calculated fields

upvoted 1 times

DeltaPotato 3 years, 1 month ago

B. From page 188 note, "Output fields from a lookup table or fields/columns generated from within a search string are not supported".

upvoted 5 times

Lalithadevi 3 years, 5 months ago

B is correct

upvoted 1 times

Question #20 *Topic 1*

When should transaction be used?

A. Only in a large distributed Splunk environment.

B. When calculating results from one or more fields.

C. When event grouping is based on start/end values.

D. When grouping events results in over 1000 events in each group.

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Abouttransactions

Community vote distribution

C (100%)

oksey Highly Voted 👍 4 years ago

When event grouping is based on start/end values.

upvoted 26 times

sid2051 Highly Voted 👍 3 years, 12 months ago

C is correct answer .

upvoted 21 times

KenNudho Most Recent ⊙ 2 weeks, 1 day ago

Answer is C, B can be done with the more efficient stats command.

upvoted 1 times

47e09fb 2 months ago

wow. will this exam be updated for correct answers? it's C!

upvoted 1 times

varmaTrainer 4 months ago

Selected Answer: C

Only use "transaction" when you- Need to see events correlated together,
- Must define event grouping based on start/end values or segment on time.

upvoted 1 times

tineboy46 7 months ago

C Is the correct answer

upvoted 1 times

gatundu_ 8 months ago

Correct answer is C. Transactions are events that span time hence the Start/ End values

upvoted 1 times

kruasan 1 year ago

Selected Answer: C

The transaction command is most useful in two specific cases:

When a unique ID (from one or more fields) alone is not sufficient to discriminate between two transactions. This is the case when the identifier is reused, for example web sessions identified by cookie or client IP2.
When event grouping is based on start/end values

upvoted 2 times

Dree_Dogg 1 year ago

Selected Answer: C

C is correct answer

upvoted 2 times

hawxxx 1 year, 1 month ago

C is the answer Page 135. Use transaction when you
- Need to see events correlated together
- Must define event grouping based on start/end values or segment on time

upvoted 3 times

jackvn6 1 year, 11 months ago

Only C NOT B

upvoted 3 times

emergency_gouda 2 years, 1 month ago

Selected Answer: C

B would be for stats. Answer is obviously C.

upvoted 2 times

Jack__ 2 years, 1 month ago

Selected Answer: C

| Search is more appropriate for B.

upvoted 2 times

MxQ3 2 years, 2 months ago

C is correct answer. ONLY use transaction when you
- Need to see events correlated together OR
- Must define event grouping based on start/end values or segment on time

upvoted 2 times

NightShark 2 years, 2 months ago

Selected Answer: C

Definately C

upvoted 2 times

gibla1929 2 years, 4 months ago

Selected Answer: C

answer is C

upvoted 2 times

fsanchezs 2 years, 4 months ago

Selected Answer: C

C is the correct

upvoted 2 times

Question #21 *Topic 1*

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.

B. The field being extracted will be required for all future events.

C. The events without the required field will not display in searches.

D. Only events with the required string will be included in the extraction.

Correct Answer: *D*

Community vote distribution

D (100%)

Sartarus Highly Voted 4 years ago

D it's correct ans

upvoted 12 times

limayi 3 years, 10 months ago

Splunk Fundamentals 2 page 158

upvoted 9 times

kruasan Most Recent 1 year ago

Selected Answer: D

When performing a regular expression (regex) field extraction using the Field Extractor (FX), the require option can be used to focus the field extraction on events that contain specific text1. This means that only events with the required string will be included in the extraction.

upvoted 1 times

emergency_gouda 2 years, 1 month ago

Selected Answer: D

It is D. Language is right from the PDF.

upvoted 1 times

MJD20 1 year, 3 months ago

how to get the PDF?

upvoted 1 times

MxQ3 2 years, 2 months ago

Require option : extraction is only executed on events that include the highlighted string

upvoted 1 times

huu_nguyen 2 years, 7 months ago

D IS CORRECT

upvoted 1 times

Lalithadevi 3 years, 5 months ago

D it's correct ans

upvoted 2 times

Question #22 *Topic 1*

When using | timechart by host, which field is represented in the x-axis?

A. date

B. host

C. time

D. _time

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

Community vote distribution

D (100%)

oksey Highly Voted 4 years ago

_time is the ANS

upvoted 27 times

Racgud 3 years, 12 months ago

"A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis"
Thus, ANS is Time
src: https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchReference/Timechart

upvoted 2 times

allansid 3 years, 10 months ago

is _time

upvoted 5 times

pabinajm 2 years, 8 months ago

Splunk docs (link above) clearly states "...with time used as the X-axis."
However, if you run "| timechart count", the field defaults to "_time". Thus, the visualization tab displays the "_time" on the X-axis. So thi seems to be the case where the question/answer is referring to the documentation.

upvoted 2 times

ctux 3 years, 8 months ago

if you look at any figure in the link you reported above where a timechart is represented, you can see that the indicated field is _time

upvoted 4 times

sid2051 Highly Voted 3 years, 12 months ago

_time ans is D

upvoted 9 times

DenaliAK Most Recent 5 days, 3 hours ago

It says field, so it is _time. Time is not a field.

upvoted 1 times

Cyde 1 month, 1 week ago

Selected Answer: D

Tested in my environment. The correct answer is "D - _time"

upvoted 1 times

osahin4 9 months, 1 week ago

Selected Answer: D

_time is the answer.

upvoted 1 times

kruasan 1 year ago

Selected Answer: D

D is correct. _time

upvoted 1 times

Dree_Dogg 1 year ago

_time is the ANS

upvoted 1 times

QuackingSteve 1 year, 1 month ago

Selected Answer: D

_time ans is D

upvoted 1 times

abderrahimpro 1 year, 3 months ago

Selected Answer: D

_time is the correct answer (verified in lab)

upvoted 1 times

Mntman77 1 year, 4 months ago

Timechart always has time on the X-axis
https://docs.splunk.com/Documentation/Splunk/latest/Search/Createtimebasedcharts#:~:text=The%20timechart%20command%20generates%20
%2
0table%20of%20summary,field%20as%20a%20separate%20series%20in%20the%20chart.

upvoted 1 times

mohanmk95 1 year, 4 months ago

_time is the correct answer

upvoted 1 times

igweifeanyi 2 years ago

D is the sure answer bro.

upvoted 1 times

emlch 2 years, 2 months ago

Selected Answer: D

Time will be the x-axis but we have remember which field stores time (_time). So the answer is D. That's a tricky question.

upvoted 2 times

soc_sts_exam 2 years, 3 months ago

100% D

upvoted 1 times

gibla1929 2 years, 4 months ago

Selected Answer: D

d _time

upvoted 2 times

Trafalgar_Law 2 years, 6 months ago

Selected Answer: D

D is the correct answer

upvoted 1 times

huu_nguyen 2 years, 7 months ago

D IS THE ANSWER

upvoted 2 times

Question #23 *Topic 1*

Which of the following is the correct way to use the datamodel command to search fields in the Web data model within the Web dataset?

A. | datamodel Web Web search | fields Web*

B. | search datamodel Web Web | fields Web*

C. | datamodel Web Web fields | search Web*

D. datamodel=Web | search Web | fields Web*

Correct Answer: *A*

kbisht Highly Voted 👍 4 years ago

Correct Ans is A

upvoted 9 times

RyanDST Highly Voted 👍 3 years, 6 months ago

| datamodel [data model name] [dataset name] [search mode {search, flat, accelerate_search}]

upvoted 8 times

Lalithadevi Most Recent 🕘 3 years, 5 months ago

A is correct

upvoted 3 times

_pasha 3 years, 8 months ago

A. | datamodel Web Web search | fields Web*

upvoted 1 times

Glat 3 years, 8 months ago

Answer is A.
See p279 of F2 PDF

upvoted 3 times

ggfsplunk 3 years, 9 months ago

agreed it's "A"

upvoted 3 times

sid2051 3 years, 12 months ago

A is correct answer

upvoted 4 times

Question #24 *Topic 1*

Which of the following statements describe the command below? (Choose all that apply.) sourcetype=access_combined | transaction JSESSIONID

A. An additional field named maxspan is created.

B. An additional field named duration is created.

C. An additional field named eventcount is created.

D. Events with the same JSESSIONID will be grouped together into a single event.

Correct Answer: *BCD*

Community vote distribution

BCD (100%)

kbisht Highly Voted 4 years ago

B C D is the correct ans

upvoted 17 times

Glat Highly Voted 3 years, 8 months ago

BCD is the answer.
See p129 of F2 PDF

upvoted 8 times

abderrahimpro Most Recent 1 year, 3 months ago

Selected Answer: BCD

https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchReference/Transaction

upvoted 1 times

igweifeanyi 2 years, 1 month ago

ANSWER IS BCD

upvoted 2 times

Lalithadevi 3 years, 5 months ago

B C D is the correct ans

upvoted 2 times

RyanDST 3 years, 6 months ago

The transaction command adds two fields to the raw events, duration and eventcount.

| transaction [<field-list>]
One or more field names. The events are grouped into transactions, based on the unique values in the fields.

upvoted 5 times

Sandy_1988 3 years, 10 months ago

BCD are the options

upvoted 4 times

sid2051 3 years, 12 months ago

BCD are correct

upvoted 4 times

Question #25 *Topic 1*

Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv

B. tag=Priv*

C. tag=priv*

D. tag=privileged

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

Community vote distribution

B (100%)

kbisht Highly Voted 👍 4 years ago

B is the correct ans

upvoted 21 times

Racgud 3 years, 12 months ago

D is the correct ans
"Verify that all privileged activity is returned. tag=privileged Returns privileged user activity data."
ref: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity
please don't comment the wrong answer, check the documentation before you post in the future :)

upvoted 5 times

adamforsythebartlett 3 years, 9 months ago

^that's an example for a tag "privileged," not "Privileged"

upvoted 4 times

SasnycoN 2 years, 9 months ago

Tags are CASE SENSITIVE and can use wildcard. So A: tag=Priv* is the correct anser.

upvoted 2 times

Bianchi 3 years, 1 month ago

"please don't comment the wrong answer, check the documentation before you post in the future :)" that's right Racgud, but take if for yourself since the ans is B!

upvoted 3 times

MxQ3 2 years, 2 months ago

lmao! Racgud got pwned hard. B is correct answer Tags are CaSe sentitive and can be used with wildards.

upvoted 3 times

allansid Highly Voted 👍 3 years, 10 months ago

the answer is B, tag are case sensitive. Privileged != privileged

upvoted 11 times

Nicker9 Most Recent 🕘 2 years, 1 month ago

Selected Answer: B

tags are case sensitive so it must be B

upvoted 1 times

geedawgie 2 years, 5 months ago

Selected Answer: B

Definitely B - done in a lab to make sure.

upvoted 3 times

MxQ3 2 years, 2 months ago

thank you

upvoted 1 times

huu_nguyen 2 years, 7 months ago

Selected Answer: B

B is the correct answer because Tag is case-sensitive

upvoted 2 times

M9201715 2 years, 11 months ago

Definitely B. Tags are case-sensitive

upvoted 2 times

Hudda 3 years, 1 month ago

agreed with D. pls confirm friends.

upvoted 2 times

mohanmk95 1 year, 4 months ago

Please do refer the this document
https://docs.splunk.com/Documentation/PCI/latest/Install/PrivilegedUserActivity

upvoted 1 times

Hudda 3 years, 1 month ago

Friends, the final answer is B or D?
Could you please confirm this answer?

upvoted 1 times

Sutanu_97 3 years ago

B is the right answer due to case sensitivity

upvoted 2 times

ravindraz 3 years, 2 months ago

p197 of f2

upvoted 1 times

Lalithadevi 3 years, 5 months ago

tag names are case sensitive. In this case B is correct ans. Ref Fund2 : 196

upvoted 3 times

Nanila 3 years, 6 months ago

D is the correct answer. Pg 197. The examples are listed

upvoted 1 times

ademide2 2 years, 4 months ago

Tags are case sensitive therefore Priv* is correct

upvoted 2 times

extea 3 years, 8 months ago

B
case sensitive

upvoted 3 times

Sandy_1988 3 years, 10 months ago

B should be the answer

upvoted 6 times

Taks 3 years, 11 months ago

Tricky one but I agree with "kbisht" Correct Answer is B. Tag names are case sensitive and the question is: Which of the following searches will return events containing a tag named Privileged?, Capital letter P..... For example, "Privileged" and "privileged" are two different words because th
"P" is uppercase in the first example and lowercase in the second example...See pages 194-196 in Splunk 7.X Fundamentals Part 2 PDF

upvoted 9 times

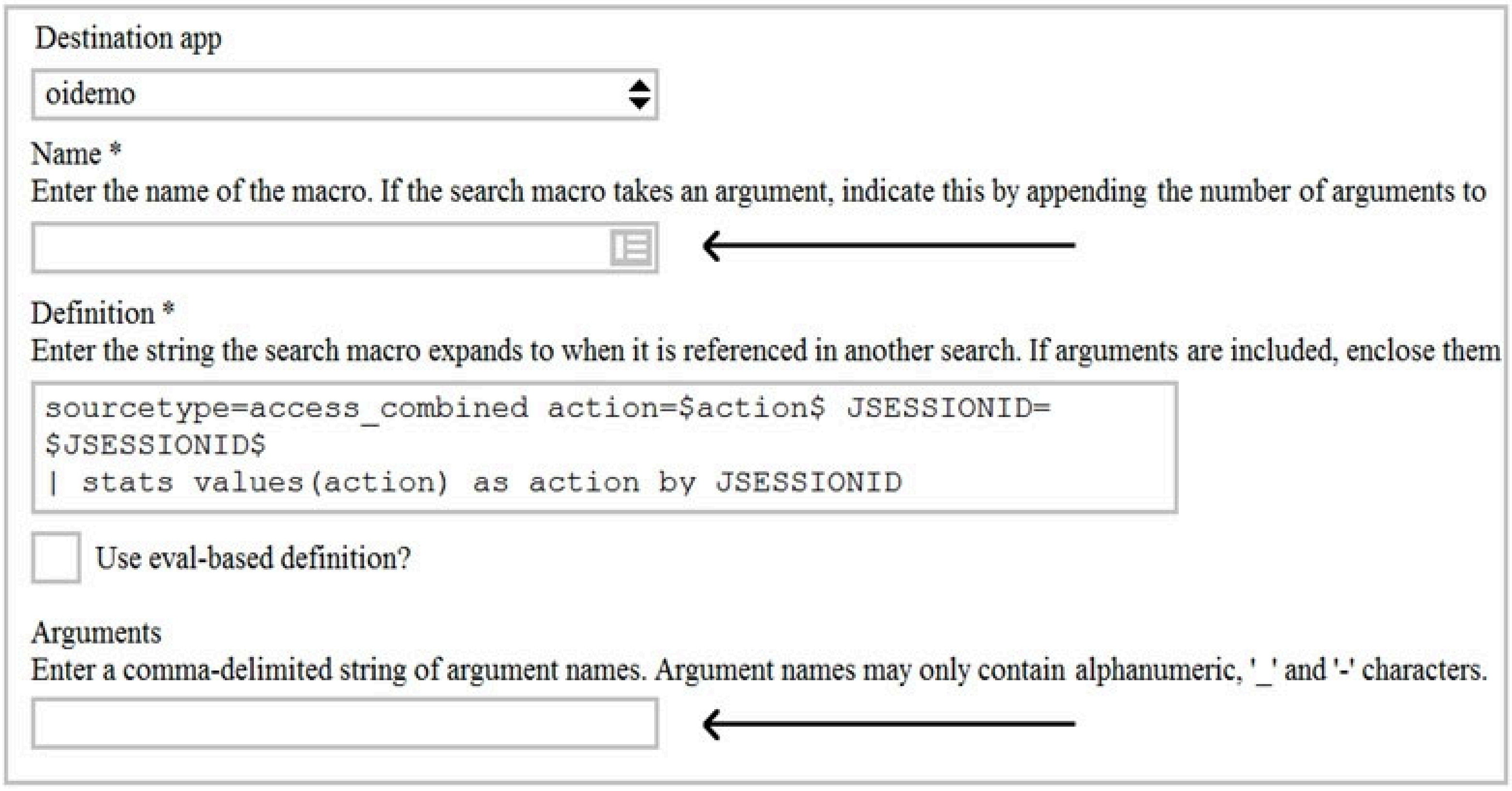
antukin 3 years, 6 months ago

page 193 shows that "Tags are case sensitive"
page 196-197 shows that tags can be searched through wildcard (*)

upvoted 2 times

Question #26 Topic 1

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configure the macro?



Destination app

oidemo

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them

```
sourcetype=access_combined action=$action$ JSESSIONID=
$JSESSIONID$
| stats values(action) as action by JSESSIONID
```

□ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

A. The macro name is sessiontracker and the arguments are action, JESSIONID.

B. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

C. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.

D. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

Community vote distribution

B (100%)

MxQ3 2 years, 2 months ago

B is correct.

upvoted 4 times

emlch 2 years, 2 months ago

Selected Answer: B

B is the correct answer.
If your macro have arguments you must specify them in parenthesis after the macro name (like <macroname>(<numberofarguments>))
When you specify the arguments you have to tell splunk what are the arguments name (without the $).

upvoted 3 times

ravindraz 3 years, 2 months ago

B is the correct answer, see p213 of f2

upvoted 2 times

sosevo2147 3 years, 5 months ago

B Is correct Answer

upvoted 2 times

> **Atavius** 3 years, 5 months ago
>
> And why it is not A? I mean there is nothing about macro name in that screen.
>
> upvoted 1 times
>
> > **Atavius** 3 years, 5 months ago
> >
> > Nevermind I just realized that it is number of arguments.
> >
> > upvoted 2 times

Lalithadevi 3 years, 5 months ago

B Is correct Answer

upvoted 3 times

Question #27 *Topic 1*

What is required for a macro to accept three arguments?

A. The macro's name ends with (3).

B. The macro's name starts with (3).

C. The macro's argument count setting is 3 or more.

D. Nothing, all macros can accept any number of arguments.

Correct Answer: *A*

Community vote distribution

A (57%) C (43%)

oksey Highly Voted 4 years ago

The macro's name ends with (3).A

upvoted 21 times

sid2051 Highly Voted 3 years, 12 months ago

A is correct

upvoted 6 times

tineboy46 Most Recent 7 months ago

A is the correct answer

upvoted 1 times

PrincePazol 7 months, 2 weeks ago

Selected Answer: A

When the macro name ends with (3)

upvoted 1 times

exampass999 11 months, 3 weeks ago

Selected Answer: A

A. is correct.
When creating a macro, there are two rules: "specify the number of arguments at the end of the macro name (not necessary if there are no arguments)" and "enclose the arguments in $$. If you forget these rules, Splunk will not recognize the macro.

upvoted 1 times

Dree_Dogg 1 year ago

A is correct Answer

upvoted 2 times

Mntman77 1 year, 2 months ago

A = Number () is required, arguments are optional
****
Enter a unique Name for the search macro.
If your search macro includes an argument, append the number of arguments to the name. For example, if your search macro mymacro includes two arguments, name it mymacro(2).
****
(Optional) Enter any Arguments for your search macro.

upvoted 2 times

Sam1289 1 year, 2 months ago

Selected Answer: C

C. The macro's argument count setting is 3 or more.

For a macro to accept three arguments, the macro's argument count setting needs to be configured to allow three or more arguments. The argument count setting determines the number of arguments that a macro can accept. By setting it to 3 or more, the macro becomes capable of receiving three specific arguments.

Option A, stating that the macro's name ends with (3), is not a requirement for a macro to accept three arguments. The name of the macro does not determine the number of arguments it can accept.

Option B, suggesting that the macro's name starts with (3), is also not a requirement. Again, the name of the macro does not dictate the number arguments it can receive.

Option D, claiming that nothing is required and all macros can accept any number of arguments, is incorrect. Macros in Splunk require explicit configuration of the argument count setting to define the number of arguments they can accept.

upvoted 3 times

Doflamingo 1 year, 2 months ago

As Mntman77 said, when you are adding a macro, the Name is a required field and comes with the legend:

"Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)"

upvoted 2 times

MxQ3 2 years, 2 months ago

A. Number of arguments in parenthese should be AFTER macro name

upvoted 1 times

fuchi_pixel 2 years, 4 months ago

Selected Answer: A

A is correct

upvoted 2 times

Lalithadevi 3 years, 5 months ago

A is correct Answer

upvoted 4 times

kikoololstyle 3 years, 8 months ago

A is correct; P213 from PDF

upvoted 6 times

Sandy_1988 3 years, 10 months ago

A should be the ans.

upvoted 5 times

Question #28 *Topic 1*

Which workflow action method can be used when the action type is set to link?

A. GET

B. PUT

C. Search

D. UPDATE

Correct Answer: *A*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction

Community vote distribution

A (100%)

sid2051 Highly Voted 3 years, 12 months ago

there are only three workflow get post and search .This leaves only get as answer

upvoted 10 times

amh111 Most Recent 8 months, 1 week ago

There are two workflow action types: Link and Search. For link, there are 2 methods: GET and POST. Hence, the answer is GET.

upvoted 1 times

jb844 10 months, 2 weeks ago

Sorry Get & Put.
Lack of coffee...

upvoted 1 times

jb844 10 months, 2 weeks ago

answer: GET & Post

Ref: https://docs.splunk.com/Documentation/Splunk/9.1.1/Admin/Workflow_actionsconf

upvoted 1 times

emlch 2 years, 2 months ago

Selected Answer: A

GET and POST action can use Link.

There's no POST within the listed possible answers. So the answer is GET.

upvoted 2 times

ravindraz 3 years, 2 months ago

A is correct answer, see p220 - 221 of f2

upvoted 4 times

Lalithadevi 3 years, 5 months ago

A is correct Ans

upvoted 2 times

ArDeKu 3 years, 5 months ago

GET & POST is correct..But as here PUT is given so only A is correct answer

upvoted 3 times

IxIJustinIxI 3 years, 7 months ago

If you follow these steps:
Navigate to Settings > Fields > Workflow Actions.
Click New to open up a new workflow action form.
You will see "action type" which can be Link or Search (because we want to know options when set to link, we can say C is not the correct answer)
Next, if you click "link method" you will see 2 options: GET and POST (because PUT and UPDATE are not options in the list we can say B and D are not correct)
This leaves the only possible answer as A: GET

upvoted 1 times

ctux 3 years, 8 months ago

Should be:
A) GET
C) Search

upvoted 1 times

ctux 3 years, 8 months ago

Sorry, action type is link, so only GET.

upvoted 4 times

Sandy_1988 3 years, 10 months ago

A and B. Both needs the link as option while creating the workflow action.

upvoted 1 times

nirmaljohnson 3 years, 10 months ago

GET is the answer.
The workflow actions are GET POST and SEARCH . No actions by the name PUT.
GET and POST come under the action type LINK and SEARCH under the action type Search.

upvoted 7 times

oksey 4 years ago

It's GET and PUT . A&B

upvoted 4 times

kbisht 4 years ago

There is no workflow named as PUT. The correct ans is GET

upvoted 9 times

Question #29 *Topic 1*

Which of the following statements about tags is true? (Choose all that apply.)

A. Tags are case-insensitive.

B. Tags are based on field/value pairs.

C. Tags categorize events based on a search.

D. Tags are designed to make data more understandable.

Correct Answer: *BD*

Community vote distribution

BD (100%)

Btee Highly Voted 3 years, 10 months ago

BD is the correct Answer
A says - Tags are case-insensitive.
Tags are case sensitive not case-insensitive.

upvoted 24 times

Glat 3 years, 8 months ago

Yes, see p.193 of F2

upvoted 6 times

abderrahimpro Most Recent 1 year, 3 months ago

Selected Answer: BD

BD correct.

upvoted 1 times

easy02 1 year, 3 months ago

answer is ABD

upvoted 1 times

emlch 2 years, 2 months ago

Selected Answer: BD

BD correct.
A. False
C. this is event types

upvoted 3 times

gabo1969 2 years, 9 months ago

BD is correct, tag are case-sensitive and the Event Types categorize events based on search terms

upvoted 2 times

Lalithadevi 3 years, 5 months ago

BD is correct. Refer Page Fun2:192

upvoted 3 times

lGoddard90 3 years, 5 months ago

BD is correct. Tags are case sensitive so A can't be correct

upvoted 1 times

Nanila 3 years, 6 months ago

ABD is correct. See pg 193 of the PDF

upvoted 2 times

idsej 3 years, 1 month ago

No A is wrong since tags are case sensitive.

upvoted 2 times

SrGhost 2 years, 4 months ago

on a quick read, you might get confused between case-sensitive and case-insensitive

upvoted 1 times

BMO 3 years, 7 months ago

BD is the correct answer

upvoted 1 times

Scrubsboy 3 years, 10 months ago

ABD is correct

upvoted 2 times

Question #30 *Topic 1*

Which of the following statements about macros is true? (Choose all that apply.)

A. Arguments are defined at execution time.

B. Arguments are defined when the macro is created.

C. Argument values are used to resolve the search string at execution time.

D. Argument values are used to resolve the search string when the macro is created.

Correct Answer: *AC*

Community vote distribution

BC (95%) 5%

oksey Highly Voted 4 years ago

I think BC is the Ans

upvoted 33 times

Glat Highly Voted 3 years, 8 months ago

Answer is BC.
See p210 and 213 of F2 PDF

upvoted 11 times

ANki_24 Most Recent 8 months, 1 week ago

Selected Answer: BC

BC are correct

upvoted 1 times

ANki_24 8 months, 1 week ago

BC are correct

upvoted 1 times

Dree_Dogg 1 year ago

Selected Answer: BC

B&C are the correct answers

upvoted 1 times

Sam1289 1 year, 2 months ago

Selected Answer: AC

A. Arguments are defined at execution time.
C. Argument values are used to resolve the search string at execution time.

The following statements about macros are true:

A. Arguments are defined at execution time: Macros allow you to define placeholders for arguments that can be filled in with specific values wher
the macro is executed. The values of these arguments are provided at runtime or execution time, allowing for flexibility and dynamic customizatic
of the macro's behavior.

C. Argument values are used to resolve the search string at execution time: Macros often include a search string as part of their definition. When the macro is executed and the argument values are provided, these values are used to resolve the search string, replacing the argument placeholders with the specified values. This allows the macro to generate a search string tailored to the specific use case or provided values.

upvoted 1 times

Hurshbabe 1 year ago

Sam, the arguments are defined during creation time, but the values are filled in during execution time. Dont get confused.

upvoted 2 times

c69ed2f 2 weeks, 5 days ago

Arguments are declared at creation time but defined at execution time. Don't get confused between variable declaration and definition. When a variable is defined in a programming language it means a value is being set.

upvoted 1 times

abderrahimpro 1 year, 3 months ago

Selected Answer: BC

Answer is BC.

upvoted 2 times

mohanmk95 1 year, 4 months ago

Selected Answer: BC

B and C are the correct answer

upvoted 2 times

metromini 1 year, 9 months ago

Selected Answer: BC

Answer is BC

upvoted 3 times

TestingAccount900 1 year, 11 months ago

Selected Answer: BC

BC is the answer, you define the arguments during macro creation, but you set their values during search time

upvoted 3 times

huu_nguyen 2 years, 7 months ago

BC is the final answers

upvoted 3 times

yuyulin 2 years, 8 months ago

Selected Answer: BC

I think BC is the Ans

upvoted 4 times

raflyalk 2 years, 9 months ago

Selected Answer: BC

Yeah BC is the answer

upvoted 5 times

SasnycoN 2 years, 9 months ago

Answer is BC

upvoted 1 times

teems5uk 2 years, 11 months ago

The correct answer is BC

upvoted 1 times

paro2 3 years, 3 months ago

B-C is clearly the correct answer

upvoted 1 times

Lalithadevi 3 years, 5 months ago

BC is correct

upvoted 3 times

Question #31 *Topic 1*

Information needed to create a GET workflow action includes which of the following? (Choose all that apply.)

A. A name for the workflow action.

B. A URI where the user will be directed at search time.

C. A label that will appear in the Event Action menu at search time.

D. A name for the URI where the user will be directed at search time.

Correct Answer: *ABC*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction

Community vote distribution

ABC (52%) | AC (38%) | 10%

oksey Highly Voted 4 years ago

ABC is the Ans

upvoted 27 times

lance_grown 10 months, 2 weeks ago

B is wrong because it is not directed at search time

upvoted 1 times

carnage1970 Highly Voted 2 years, 1 month ago

Selected Answer: AC

It's not redirected at search time.

upvoted 7 times

ANki_24 Most Recent 8 months ago

Selected Answer: ABC

correct

upvoted 2 times

jb844 8 months, 3 weeks ago

Selected Answer: AC

not redirected at search time,

upvoted 1 times

mohamedhaleem 11 months, 1 week ago

ABC makes sense

upvoted 2 times

JoAsiaGje 11 months, 2 weeks ago

ABC is the correct answer. Tested: Settings -> Fields » Workflow actions » Add new
mandatory fields (*):
- Name (Enter a unique name without spaces or special characters. This is used for identifying your workflow action later on within Splunk Settings.),
- Label (Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search f ticket number : $ticketnum$'.),
- Action Type (link, search),
- URI (Enter the location to link to. Optionally, specify fields by enclosing the field name in dollar signs, e.g. http://www.google.com/search?q=$host$.).

upvoted 1 times

Dree_Dogg 1 year ago

Selected Answer: ABC

ABC is the Ans

upvoted 2 times

Huslayer 1 year, 1 month ago

Selected Answer: ABC

you need name,label,uri i just tried it 7/18/23

upvoted 3 times

Sam1289 1 year, 2 months ago

Selected Answer: ABC

A. A name for the workflow action.
B. A URI where the user will be directed at search time.
C. A label that will appear in the Event Action menu at search time.

upvoted 4 times

asarali 1 year, 3 months ago

Selected Answer: BC

It doesn't require a Name..it requires only a Label and URI

upvoted 2 times

Doflamingo 1 year, 2 months ago

When you are adding a new Workflow action, you can see that the required fields (marked with asterisk) are: Name, Label, Action Type (link/search) and URI.

upvoted 1 times

SasnycoN 2 years, 9 months ago

I'm not sure about "B". THe user is not redirected at search time but when accessing it.

upvoted 3 times

SasnycoN 2 years, 9 months ago

"In URI provide a URI for the location of the external resource that you want to send your field values to." but it never mentiones a searchtime
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction

upvoted 3 times

NLotus 2 years, 12 months ago

B might be a trick. The user isn't directed to the URI, at search time, but when they activate the GET action, after search time.

upvoted 3 times

Lalithadevi 3 years, 5 months ago

ABC is correct Ref:P219

upvoted 2 times

Glat 3 years, 8 months ago

Answer is ABS
See p219 of F2 PDF

upvoted 2 times

nirmaljohnson 3 years, 10 months ago

A,B&C
Workflow Name, Label & URI are required.

upvoted 2 times

SasnycoN 2 years, 9 months ago

URI is required but not for user redirection at search time.

upvoted 1 times

oksey 4 years ago

A&B is the Ans

upvoted 1 times

Question #32 *Topic 1*

Which of the following can be used with the eval command tostring function? (Choose all that apply.)

A. "hex"

B. "commas"

C. "decimal"

D. "duration"

Correct Answer: *ABD*

Reference:

https://splunkonbigdata.com/2018/10/27/usage-of-splunk-eval-function-tostring/

Community vote distribution

ABD (100%)

Kool_Kid Highly Voted 3 years, 8 months ago

A,B,D. Page 105 of F2 slides.

upvoted 15 times

ComeUp 2 years, 7 months ago

correct

upvoted 1 times

teems5uk Highly Voted 2 years, 11 months ago

Fun2(page 105)

• Options:
– "commas":
applies commas
□ If the number includes decimals, it
rounds to two decimal places
– "duration":
formats the number as
"hh:mm:ss"
– "hex": formats the number
in hexadecimal

upvoted 5 times

sith Most Recent 12 months ago

https://splunkonbigdata.com/usage-of-splunk-eval-function-tostring/#:~:text=This%20functions%20converts%20inputs%20value,corresponding%20to%20the%20Boolean%20value.

upvoted 1 times

abderrahimpro 1 year, 3 months ago

Selected Answer: ABD

https://docs.splunk.com/Documentation/Splunk/9.0.4/SearchReference/ConversionFunctions

upvoted 2 times

tomhola 1 year, 5 months ago

If <value> is a number, the second argument <format> is optional and can be "hex", "commas", or "duration".

ABD

upvoted 1 times

JadeC 3 years, 9 months ago

https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.29

upvoted 1 times

Question #33 *Topic 1*

Which of the following searches show a valid use of a macro? (Choose all that apply.)

A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField

B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField

C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField

D. index=main source=mySource oldField=* | '"newField('makeMyField(oldField)')"' | table _time newField

Correct Answer: *AB*

Reference:

https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html

Community vote distribution

AC (100%)

Powdered_Sugar Highly Voted 3 years, 9 months ago

B can't be true, it has a malformed if statement. I think it's A & C.

upvoted 25 times

Steve2610 2 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/9.0.0/Knowledge/Usesearchmacros

upvoted 1 times

Steve2610 2 years, 1 month ago

Search macros can be any part of a search, such as an eval statement or search term and do not need to be a complete command. Macros inside of quoted values are not expanded.

upvoted 1 times

Teloif Most Recent 10 months ago

Selected Answer: AC

AC are correct

upvoted 3 times

Dree_Dogg 1 year ago

Selected Answer: AC

A, C
Can't be B because "if" takes 3 arguments.

upvoted 2 times

poubellelc66 1 year, 2 months ago

I'm I the only one that see there's no "NewField" in the A search and that would likely result in the search not working.
For me only C is working in terms of macro's and search.
But maybe I'm wrong.

upvoted 2 times

mohanmk95 1 year, 4 months ago

Selected Answer: AC

please check in splunk also

upvoted 2 times

Harrysa 1 year, 4 months ago

Only A works why are the others being suggested?

upvoted 1 times

TestingAccount900 1 year, 11 months ago

Selected Answer: AC

A and C are correct. Anyone saying C is wrong due to quotes is ignoring the fact macro's use ` ` syntax

upvoted 3 times

huu_nguyen 2 years, 7 months ago

Only A is correct
B is incorrect since the if statement was malformed
C is incorrect since the field value must be quoted by double-quotes, not single-quotes
D is incorrect obviously

upvoted 2 times

Iman1367 2 years, 11 months ago

AC are correct

upvoted 1 times

M9201715 2 years, 11 months ago

A and C are correct. A obviously, and C works because I just tried it

upvoted 2 times

Hudda 3 years, 1 month ago

which one is the final answer friends, could you pls confirm.

upvoted 2 times

Lalithadevi 3 years, 5 months ago

A is Correct

upvoted 4 times

IxlJustinlxl 3 years, 7 months ago

I think the only answer is A based off what I read here: https://community.splunk.com/t5/Knowledge-Management/How-to-pass-field-values-as-macro-arguments/m-p/164018
BD are for sure incorrect (improper use of back ticks (D) and no function following stats command (B))
C however, I think is also wrong because eval evaluates mathematical, string, and boolean expressions.. therefore eval newField='makeMyField(oldField)' would take oldField as a string and not as an argument.

upvoted 2 times

subham29 2 years, 7 months ago

if it was in single quote then it eval would have taken that as string.. but here it is in back tick

upvoted 1 times

_pasha 3 years, 8 months ago

A, C correct answers

upvoted 2 times

akkki 3 years, 11 months ago

@kbisht : Why not C or D?

upvoted 1 times

nirmaljohnson 3 years, 10 months ago

Not Sure what does D do ?
I think A & C are correct.
| eval n=`tostringnumber(15)` where as the macro is tostring($number$, "hex") , If I understood the option C correctly , this works.

upvoted 5 times

kbisht 4 years ago

Correct ans is A

upvoted 4 times

Question #34 *Topic 1*

A user wants to convert numeric field values to strings and also to sort on those values.
Which command should be used first, the eval or the sort?

A. It doesn't matter whether eval or sort is used first.

B. Convert the numeric to a string with eval first, then sort.

C. Use sort first, then convert the numeric to a string with eval.

D. You cannot use the sort command and the eval command on the same field.

Correct Answer: *B*

Community vote distribution

C (88%) 13%

oksey Highly Voted 4 years ago
Use sort first, then convert the numeric to a string with eval. C
upvoted 17 times

mybox1 Highly Voted 3 years, 10 months ago
To order numerically, first sort, then use eval - page 107
upvoted 12 times

MxQ3 2 years, 2 months ago
This is correct
upvoted 1 times

tatdatpham Most Recent 1 week, 4 days ago
Selected Answer: B
Tested and the answer is B. C does not sort on the values
upvoted 1 times

jsk46 11 months, 3 weeks ago
B and C return the same result so the correct anws is A
upvoted 1 times

mohanmk95 1 year, 4 months ago
Selected Answer: C
need to be sort out in numeric format only
upvoted 1 times

Harrysa 1 year, 4 months ago
C is wrong becasue If you use the sort command first and then the eval command, you need to ensure that the sort command is sorting the value in the desired way (i.e., as strings rather than numerically), and you need to use the str function within the sort command to force it to treat the values as strings. This can make the command more complicated and increase the likelihood of errors.
upvoted 2 times

solomone 1 year, 4 months ago
Selected Answer: C
Sort numerically first always.
upvoted 1 times

TestingAccount900 1 year, 11 months ago
Selected Answer: C
C is correct
upvoted 1 times

jdestinoble 2 years, 1 month ago
Selected Answer: C
C is correct
upvoted 1 times

Nicker9 2 years, 1 month ago
You have to sort first and then convert to a string. So Answer C.
upvoted 1 times

emlch 2 years, 2 months ago

If you convert to a string first you will have this kind of ordenation:
1, 11, 12, 13, 14, 15, 16, 17, 18, 19, 2, 20, 21...

upvoted 4 times

fsanchezs 2 years, 4 months ago

Selected Answer: C

The answer is C

upvoted 1 times

[Removed] 2 years, 4 months ago

Answer is C, sort first. Always.

upvoted 1 times

RoVasq3 2 years, 5 months ago

Selected Answer: C

Answer is C

upvoted 2 times

SasnycoN 2 years, 9 months ago

I think it's A as It doesn't matter if you are soring before or after as they are all numeric fields and the resutls will be the same.

upvoted 2 times

teems5uk 2 years, 11 months ago

Fun2(page) justifies option C

upvoted 1 times

mikey_76 3 years ago

the logical answer is C, sorting the numbers first and then converting to string. However the wording of the questions make it sound like they wa
to convert first and then sort alphanumerically so B is the answer. The wording on the question needs to be more clear

upvoted 2 times

Question #35 *Topic 1*

Which Knowledge Object does the Splunk Common Information Model (CIM) use to normalize data, in addition to field aliases, event types, and tags?

A. Macros

B. Lookups

C. Workflow actions

D. Field extractions

Correct Answer: *BD*

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

Community vote distribution

BD (46%) B (31%) D (23%)

sid2051 Highly Voted 3 years, 12 months ago

Lookup is wrong - Field Extraction shld be correct

upvoted 17 times

some_thing 3 years, 2 months ago

Lookup correct: https://docs.splunk.com/Documentation/CIM/4.6.0/User/UsetheCIMtonormalizedataatsearchtime
This one clearly states Lookups and field extractions.

upvoted 9 times

gabo1969 2 years, 9 months ago

I re-view..the correct is only B lookups..

upvoted 4 times

Networkingguy 1 year, 3 months ago

Seems like the answer is BD here, from the above link from some_thing, 5. Make your fields CIM-compliant. Normalize your data via the three methods, Lookup, Field Aliases and Field Extraction.

upvoted 2 times

[Removed] Highly Voted 3 years, 9 months ago

Reference: Fund 2 - P.268: Leverage CIM when creating field extractions, field aliases, event types and tags ... D is the best-fit in the answer set hei

upvoted 11 times

a9f89d1 Most Recent 4 months, 3 weeks ago

Selected Answer: BD

B & D
https://docs.splunk.com/Documentation/CIM/4.6.0/User/UsetheCIMtonormalizedataatsearchtime

upvoted 1 times

Alexi2415 7 months ago

B, D https://docs.splunk.com/Documentation/CIM/5.3.1/User/UsetheCIMtonormalizedataatsearchtime

upvoted 1 times

PrincePazol 7 months, 3 weeks ago

Selected Answer: BD

BD is the correct options. Link to the latest docs:
https://docs.splunk.com/Documentation/CIM/5.3.1/User/UsetheCIMtonormalizedataatsearchtime

upvoted 1 times

Dree_Dogg 1 year ago

Selected Answer: BD

It's B&D. See splunk doc here:
https://docs.splunk.com/Documentation/CIM/4.6.0/User/UsetheCIMtonormalizedataatsearchtime

upvoted 1 times

Doflamingo 1 year, 2 months ago

Does this question ask for multiple options? It doesn't say "Choose all that apply" as in the others. If it needs only one, I'd definitely go for D. Fielc Extraction. If I can choose more than one, I'd go with B and D.

upvoted 3 times

Sam1289 1 year, 2 months ago

Selected Answer: B

B is the answer

upvoted 1 times

Mntman77 1 year, 2 months ago

B&D: "field aliases, field extractions, and lookups."

upvoted 1 times

HereToLearny 1 year, 3 months ago

Selected Answer: D

The Answer is D. It can not be B because -
Sure. Lookups are used to map values from one field to another. They cannot be used to normalize data by extracting the same data from differe
events and storing it in the same field.

For example, a lookup could be used to map the value "John Doe" from the user_name field to the full_name field. This would not normalize the data, as the user_name and full_name fields would still contain different data.

Lookups can be used to normalize data in some cases, but they are not the only knowledge object that can be used for this purpose. Field extractions are a more powerful tool for normalizing data, as they can be used to extract data from events and store it in fields.

upvoted 3 times

Harrysa 1 year, 4 months ago

If a user wants to convert numeric field values to strings and then sort on those values, they should use the eval command first and then the sort command.

The eval command is used to add a new field to the search results that contains the string representation of the numeric field. For example, the following eval command converts the count field to a string: | eval count_str=tostring(count)

upvoted 1 times

lazer23 1 year, 5 months ago

Lookups : Fund 2 PG .277

upvoted 1 times

VijayReddy29 1 year, 5 months ago

Selected Answer: BD

B and D.
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime
In the above link- Under point 5a.
Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.

upvoted 3 times

test_12_12 1 year, 6 months ago

B - Lookups are a knowledge object; field extractions aren’t

upvoted 3 times

> **CRYSYS** 1 year, 5 months ago
>
> Lookups are, by definition, knowledge objects. https://docs.splunk.com/Splexicon:Knowledgeobject
>
> upvoted 1 times

guuillauume 1 year, 7 months ago

Selected Answer: B

B is the correct answer

upvoted 3 times

igweifeanyi 2 years, 1 month ago

Fund2, page 170;B and D are correct.

upvoted 2 times

Marianionut123 2 years, 1 month ago

i think is lookup -> B

d. Write lookups to add fields and normalize field values

https://docs.splunk.com/Documentation/CIM/5.0.1/User/UsetheCIMtonormalizedataatsearchtime

upvoted 2 times

Question #36 *Topic 1*

Which of the following statements describe data model acceleration? (Choose all that apply.)

A. Root events cannot be accelerated.

B. Accelerated data models cannot be edited.

C. Private data models cannot be accelerated.

D. You must have administrative permissions or the accelerate_datamodel capability to accelerate a data model.

Correct Answer: *BCD*

Community vote distribution

BCD (100%)

oksey Highly Voted 👍 4 years ago

BCD is the Ans

upvoted 16 times

Glat Highly Voted 👍 3 years, 8 months ago

BCD is the answer.
See p265 of F2

upvoted 8 times

Nicker9 Most Recent ⏲ 2 years, 1 month ago

Selected Answer: BCD

https://docs.splunk.com/Documentation/Splunk/9.0.0/Knowledge/Acceleratedatamodels

upvoted 1 times

MxQ3 2 years, 2 months ago

BDC is the right answer.

upvoted 1 times

fsanchezs 2 years, 4 months ago

Selected Answer: BCD

BCD is correct

upvoted 1 times

teems5uk 2 years, 11 months ago

(page 265)Accelerating a Data Model
• You must have administrative permissions or the
accelerate_datamodel capability to accelerate a data model
• Private data models cannot be accelerated
• Accelerated data models cannot be edited.

Note
• With persistent data model acceleration, all fields
Only root events can be
accelerated. If there are multiple
in the model become "indexed" fields
root events, only the first root
event is accelerated.

upvoted 1 times

Lalithadevi 3 years, 5 months ago

BCD is correct

upvoted 1 times

allansid 3 years, 10 months ago

BCD
Private data models cannot be accelerated.

upvoted 4 times

shervin2s 3 years, 10 months ago

BCD is true

upvoted 3 times

Medis 3 years, 10 months ago

Private datamodels can't be accelerated, Hence answer is BCD

upvoted 5 times

Question #37 *Topic 1*

How does a user display a chart in stack mode?

A. By using the stack command.

B. By turning on the Use Trellis Layout option.

C. By changing Stack Mode in the Format menu.

D. You cannot display a chart in stack mode, only a timechart.

Correct Answer: *C*

oksey Highly Voted 👍 4 years ago
By changing Stack Mode in the Format menu.
upvoted 17 times

DeltaPotato 3 years, 1 month ago
shown on pg 44
upvoted 1 times

sid2051 Highly Voted 👍 3 years, 12 months ago
C is the ans
upvoted 12 times

Lalithadevi Most Recent 🕒 3 years, 5 months ago
C is corrrect
upvoted 1 times

shervin2s 3 years, 10 months ago
C is true
upvoted 6 times

Question #38 *Topic 1*

If no value is specified with the fillnull command, what default value will be used?

A. 0

B. N/A

C. ג€"

D. NULL

Correct Answer: *A*

Reference:

https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html

needleskanya Highly Voted 3 years, 5 months ago

if no value= clause, default replacement value is 0
Fundamentals part 2, slide 122 for Fillnull command

upvoted 11 times

DeltaPotato 3 years, 1 month ago

page 119 in PDF

upvoted 4 times

Hudda Most Recent 3 years, 1 month ago

why not D. any comments friends?

upvoted 1 times

Bianchi 3 years, 1 month ago

Read the comment below :) from @needleskanya :)

upvoted 2 times

Question #39 *Topic 1*

What other syntax will produce exactly the same results as | chart count over vendor_action by user?

A. | chart count by vendor_action, user

B. | chart count over vendor_action, user

C. | chart count by vendor_action over user

D. | chart count over user by vendor_action

Correct Answer: *A*

kbisht Highly Voted 4 years ago

A is the correct ans

upvoted 20 times

sid2051 Highly Voted 3 years, 12 months ago

A is the correct answer it will produce exactly the same chart

upvoted 13 times

Harrysa Most Recent 1 year, 4 months ago

A is correct, "over" is used for time-based aggregation, while "by" is used for field-based aggregation.

upvoted 2 times

emlch 2 years, 2 months ago

Equivalent expressions:
by <field>, <field2>
over <field> by <field2>

upvoted 4 times

nupacniyiveli 2 years, 8 months ago

A is correct

upvoted 1 times

BengieQuesada 3 years, 1 month ago

A is correct, reference F2 page 52

upvoted 4 times

Lalithadevi 3 years, 5 months ago

A is correct

upvoted 1 times

robotn1k 3 years, 6 months ago

A is the correct answer
Chart syntax is: over = [row-split] by = [column-split]
By default, the first field name after the chart command is the [row-split] and the second is [column-split], so B would be the same as the example in the question
https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart

upvoted 3 times

allansid 3 years, 10 months ago

answer A

upvoted 7 times

oksey 4 years ago

I think B is correct

upvoted 1 times

Sartarus 4 years ago

B it's not possible

upvoted 1 times

Question #40 *Topic 1*

What are the two parts of a root event dataset?

A. Fields and variables.

B. Fields and attributes.

C. Constraints and fields.

D. Constraints and lookups.

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Designdatamodelobjects

ravindraz Highly Voted 3 years, 2 months ago

Answer is C, P232 of F2

upvoted 8 times

teems5uk Most Recent 2 years, 11 months ago

(Page 232) Data Model Events
• Event datasets contain constraints and fields
• Constraints are essentially the search broken down into a hierarchy
• Fields are properties
associated with the events

upvoted 3 times

Glat 3 years, 8 months ago

See p.236-237 in F2

upvoted 1 times

merte 3 years, 8 months ago

Answer is C!

upvoted 3 times

Question #41 *Topic 1*

When using timechart, how many fields can be listed after a by clause?

A. 0, because timechart doesn't support using a by clause.

B. 1, because _time is already implied as the x-axis.

C. 2, because one field would represent the x-axis and the other would represent the y-axis.

D. There is no limit specific to timechart.

Correct Answer: *B*

Community vote distribution

B (100%)

kbisht Highly Voted 4 years ago

B is the correct ans

upvoted 22 times

shervin2s Highly Voted 3 years, 10 months ago

B is true

upvoted 6 times

solomone Most Recent 1 year, 5 months ago

Selected Answer: B

Answer is B

upvoted 1 times

YYABABY 2 years ago

B IS CORRECT! :)

upvoted 1 times

Galrim 2 years ago

Selected Answer: B

Correct is B

upvoted 1 times

Lalithadevi 3 years, 5 months ago

B is correct

upvoted 3 times

BMO 3 years, 7 months ago

B is correct (F2, p.67)

upvoted 3 times

Question #42 *Topic 1*

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.

B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.

C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.

D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Correct Answer: *B*

Community vote distribution

B (100%)

oksey Highly Voted 4 years ago

I think B is the Ans

upvoted 19 times

Glat 3 years, 8 months ago

See p186 of F2

upvoted 4 times

AAMA Highly Voted 3 years, 10 months ago

B is true

upvoted 5 times

AmirSA92 Most Recent 1 year ago

Selected Answer: B

B is the correct answer

upvoted 1 times

autorun 3 years, 5 months ago

Why A is incorrect ?

upvoted 2 times

paro2 3 years, 3 months ago

Because you don't necessarily need to specify the alias in the search. If it appears in at least 20% of events, it will appear in the interesting fielc even if you didn't specify it in the search.

A would be correct only in case of "Fast Mode" enabled.

upvoted 2 times

gabo1969 2 years, 9 months ago

Correct!..

upvoted 1 times

BMO 3 years, 7 months ago

B is the correct answer

upvoted 2 times

Question #43 *Topic 1*

Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.

B. A macro is a reusable search string that must have a fixed time range.

C. A macro is a reusable search string that may have a flexible time range.

D. A macro is a reusable search string that must contain only a portion of the search.

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

Community vote distribution

C (100%)

Nobby123122222 Highly Voted 3 years, 11 months ago

C is the correct answer as Macros can be a full search string or portion of search while you can select the time range at search time so Answer is

upvoted 24 times

gabo1969 2 years, 9 months ago

Yes, also I think that C option is correct

upvoted 1 times

sid2051 Highly Voted 3 years, 12 months ago

C shld be the answer

upvoted 10 times

MxQ3 Most Recent 2 years, 2 months ago

Damn what a sneaky tricky question. My initial thoughts were either A or D but as others have pointed out it's only part of answer. C seems most likely correct

upvoted 1 times

emlch 2 years, 2 months ago

Selected Answer: C

A and D are half correct, macros can be a full or a portion of a search. But the most correct answer is that they may have flexible time range

upvoted 2 times

RoVasq3 2 years, 5 months ago

Selected Answer: C

I think that C option is correct

upvoted 1 times

adamsca 2 years, 6 months ago

Selected Answer: C

Yes, C is the correct Answer

upvoted 2 times

Glat 3 years, 8 months ago

Answer is C
See F2 p.210

upvoted 6 times

allansid 3 years, 10 months ago

the trick is must/may

upvoted 4 times

hahahah68 3 years, 11 months ago

I think A is the answer

upvoted 2 times

Question #44 *Topic 1*

In what order are the following knowledge objects/configurations applied?

A. Field Aliases, Field Extractions, Lookups

B. Field Extractions, Field Aliases, Lookups

C. Field Extractions, Lookups, Field Aliases

D. Lookups, Field Aliases, Field Extractions

Correct Answer: *B*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge

Community vote distribution

B (100%)

oksey Highly Voted 4 years ago

Field Extractions, Field Aliases, Lookups ..B

upvoted 10 times

leonmflai4exam Highly Voted 3 years, 8 months ago

B, F2 P181

upvoted 7 times

emlch Most Recent 2 years, 2 months ago

1. Fields Extractions
2. " Aliases
3. Calculated "
4. Lookups
5. Event Types
6. Tags

upvoted 4 times

adamsca 2 years, 5 months ago

Selected Answer: B

Ans is B -
Updated Link >https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Searchtimeoperationssequence

upvoted 3 times

Nanila 3 years, 6 months ago

Is Actually A

upvoted 1 times

paro2 3 years, 3 months ago

No, it's B.
https://docs.splunk.com/Documentation/SplunkCloud/8.2.2104/Knowledge/Searchtimeoperationssequence

upvoted 2 times

Noone04 3 years, 11 months ago

Ans is B - https://docs.splunk.com/Documentation/Splunk/8.0.6/Knowledge/Searchtimeoperationssequence

upvoted 5 times

Question #45 *Topic 1*

In which of the following scenarios is an event type more effective than a saved search?

A. When a search should always include the same time range.

B. When a search needs to be added to other users' dashboards.

C. When the search string needs to be used in future searches.

D. When formatting needs to be included with the search string.

Correct Answer: *C*

Reference:

https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html

Community vote distribution

C (86%) 14%

oksey Highly Voted 👍 4 years ago

C. When the search string needs to be used in future searches.

upvoted 21 times

TeeCeeP Highly Voted 👍 3 years, 9 months ago

c, slide 207

upvoted 8 times

Loupesko 3 years, 9 months ago

C, but the slide is 206 :)

upvoted 5 times

Paul7 Most Recent ⏲ 1 year, 12 months ago

For me, It's C

upvoted 1 times

emergency_gouda 2 years, 1 month ago

Selected Answer: C

Reports, not event types, have saved formatting, so the answer is not D. Event types, unlike reports, can be included in a search string. Answer is (

upvoted 4 times

RuiA2 1 year, 5 months ago

F2 P207. Saved formatting, shared with splunk users and added to dashboards are for Saved Reports. So answer is C.

upvoted 2 times

SrGhost 2 years, 2 months ago

Selected Answer: D

For me D is the correct answer.
A, B and C are scenarios where create a new search should is interesting, but a scenario where using a new search string is better than a search shuld is D

upvoted 1 times

SrGhost 2 years, 4 months ago

Selected Answer: C

It's C

upvoted 2 times

Hudda 3 years, 1 month ago

which one is the final answer friends, could you pls confirm.

upvoted 2 times

cthulhu 2 years, 11 months ago

It's C.

upvoted 1 times

igweifeanyi 2 years ago

the final answer is C

upvoted 1 times

sargeholik 3 years, 9 months ago

C is correct answer

upvoted 3 times

sid2051 3 years, 12 months ago

D is the correct answer

upvoted 2 times

RoGr 3 years, 5 months ago

D would be "Saved Reports" if you ask me....P.207

upvoted 3 times

kbisht 4 years ago

D is the correct ans

upvoted 3 times

Question #46 *Topic 1*

When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.

B. Sets the maximum length of all the events within a transaction.

C. Sets the maximum total time between the earliest and latest events in a transaction.

D. Sets the maximum length that any single event can reach to be included in the transaction.

Correct Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

Community vote distribution

C (100%)

Nobby123122222 Highly Voted 3 years, 11 months ago

Correct answer is C

upvoted 21 times

amsinha Highly Voted 3 years, 10 months ago

130 page of splk-1002. C is thee answer

upvoted 13 times

gandalfthegray Most Recent 2 years, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

yuyulin 2 years, 8 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

SasnycoN 2 years, 9 months ago

Answer is C:
maxspan Syntax: maxspan=<int>[s | m | h | d]
Description: Specifies the maximum length of time in seconds, minutes, hours, or days that the events can span. The events in the transaction mu
span less than integer specified for maxspan. Events that exceed the maxspan limit are treated as part of a separate transaction. If the value is negative, the maxspan constraint is disabled and there is no limit.
Default: -1 (no limit)

upvoted 2 times

Lalithadevi 3 years, 5 months ago

130 page of splk-1002. C is thee answer

upvoted 1 times

allansid 3 years, 10 months ago

maxspan -> first and last event
maxpause -> between the events

upvoted 10 times

shervin2s 3 years, 10 months ago

Total time means start time+end time,
i think max length make more sense so B is correct

upvoted 1 times

sandman310323 3 years, 11 months ago

I believe C as well

upvoted 7 times

carm8989 3 years, 11 months ago

B is the correct answer

upvoted 1 times

Question #47 *Topic 1*

When creating a Search workflow action, which field is required?

A. Search string

B. Data model name

C. Permission setting

D. An eval statement

Correct Answer: *A*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction

Glat Highly Voted 3 years, 8 months ago

Answer is A.
See F2 p.225

upvoted 12 times

Lalithadevi Most Recent 3 years, 5 months ago

Answer is A.
See F2 p.225

upvoted 1 times

Question #48 *Topic 1*

To identify all of the contributing events within a transaction that contain at least one REJECT event, which syntax is correct?

A. index=main REJECT | transaction sessionid

B. index=main | transaction sessionid | search REJECT

C. index=main | transaction sessionid | where transaction=reject

D. index=main | transaction sessionid | where transaction="REJECT*"

Correct Answer: *B*

Community vote distribution

B (100%)

gioojardines Highly Voted 3 years, 10 months ago

Yes, the correct answer is B, because in the page 133 you have a similar example.

upvoted 20 times

shervin2s Highly Voted 3 years, 10 months ago

yes B is true

upvoted 8 times

kirtak Most Recent 1 year, 5 months ago

A and B are correct actually, both return the exact same results when executed.

upvoted 1 times

Trafalgar_Law 2 years, 6 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

bapun17 2 years, 7 months ago

Selected Answer: B

B is the correct

upvoted 3 times

babusartop17 3 years, 8 months ago

A should be the correct answer

upvoted 1 times

> **paro2** 3 years, 3 months ago
>
> Identify the events WITHIN a transaction. B is the correct answer.
>
> upvoted 4 times

akkki 3 years, 11 months ago

Is B correct option?

upvoted 4 times

Question #49 *Topic 1*

After manually editing a regular expression (regex), which of the following statements is true?

A. Changes made manually can be reverted in the Field Extractor (FX) UI.

B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.

C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.

D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Correct Answer: *B*

Community vote distribution

B (100%)

kbisht Highly Voted 👍 4 years ago

I think B is correct ans

upvoted 18 times

Ascheros Highly Voted 👍 3 years, 10 months ago

B is the correct answer - page 166 fundamentals 2 pdf (upper right corner)

upvoted 15 times

bapun17 Most Recent 🕘 2 years, 7 months ago

Selected Answer: B

B is correct

upvoted 2 times

androki 2 years, 10 months ago

B is correct!

upvoted 1 times

ragulanand 3 years ago

B is correct

upvoted 1 times

Tajit 3 years, 6 months ago

B is correct

upvoted 1 times

sargeholik 3 years, 9 months ago

correct answer is D.

upvoted 1 times

> **sargeholik** 3 years, 9 months ago
>
> sorry, correct is B
>
> upvoted 6 times

Question #50 *Topic 1*

Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.

B. POST workflow actions can be configured to send email to the URI location.

C. By default, POST workflow actions are shown in both the event and field menus.

D. POST workflow actions can be configured to send POST arguments to the URI location.

Correct Answer: *D*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaPOSTworkflowaction

Community vote distribution

D (100%)

Sartarus Highly Voted 👍 4 years ago

D its correct ans

upvoted 9 times

Glat Highly Voted 👍 3 years, 8 months ago

Answer is D.
See F2 p.223

upvoted 7 times

berbersploit Most Recent 🕘 2 years, 2 months ago

Selected Answer: D

D is the correct one

upvoted 1 times

Qadir 2 years, 9 months ago

In some websites these options are given.The correct ans is D
A. POST workflow actions are always encrypted.
B. POST workflow actions cannot use field values in their URI.
C. POST workflow actions cannot be created on custom sourcetypes.
D. POST workflow actions can open a web page in either the same window or a new .

upvoted 1 times

Question #51 *Topic 1*

Which of the following statements is true, especially in large environments?

A. Use the stats command when you need to group events by two or more fields.

B. The stats command is faster and more efficient than the transaction command.

C. The transaction command is faster and more efficient than the stats command.

D. Use the transaction command when you want to see the results of a calculation.

Correct Answer: *B*

Reference:

https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html

kikoololstyle Highly Voted 3 years, 8 months ago

B, p135 from PDF

upvoted 16 times

yohi Highly Voted 2 years, 7 months ago

B is correct. "When you have a choice, always use stats as it is faster and more efficient, especially in large Splunk environments"

upvoted 5 times

Question #52 *Topic 1*

What does the following search do?
index=corndog type= mysterymeat action=eaten | stats count as corndog_count by user

A. Creates a table of the total count of users and split by corndogs.

B. Creates a table of the total count of mysterymeat corndogs split by user.

C. Creates a table with the count of all types of corndogs eaten split by user.

D. Creates a table that groups the total number of users by vegetarian corndogs.

Correct Answer: *B*

Community vote distribution

B (100%)

kbisht Highly Voted 4 years ago
B is the correct ans
upvoted 16 times

Medis Highly Voted 3 years, 10 months ago
Answer will be B , if corrected as below
Creates a table of total count of mysterymeat crondogs eaten split by user
upvoted 12 times

emergency_gouda Most Recent 2 years, 1 month ago
Selected Answer: B
lol, this is such a step down in difficulty compared to Sec+
upvoted 3 times

bmalin77 1 year, 8 months ago
You use this for sec+?
upvoted 2 times

Tajit 3 years, 6 months ago
B is the correct ans
upvoted 1 times

allansid 3 years, 10 months ago
answer B
can't be answer C
cause type=mysterymeat in search terms,
upvoted 5 times

Question #53 *Topic 1*

Which of the following statements about event types is true? (Choose all that apply.)

A. Event types can be tagged.

B. Event types must include a time range.

C. Event types categorize events based on a search.

D. Event types can be a useful method for capturing and sharing knowledge.

Correct Answer: *AC*

Reference:

https://www.edureka.co/blog/splunk-events-event-types-and-tags/

Community vote distribution

AC (50%) AD (25%) CD (25%)

oksey Highly Voted 4 years ago

ACD is the Ans

upvoted 28 times

ComeUp Highly Voted 2 years, 7 months ago

ACD is correct, Splunk F2 pg 201

upvoted 10 times

olino Most Recent 8 months ago

Since event types are knowledge object, the can be used for sharing knowledge. So the answers are: ACD

upvoted 1 times

ANki_24 8 months, 1 week ago

Selected Answer: AC

ACD is ans

upvoted 2 times

ltp1120 9 months, 1 week ago

Selected Answer: CD

ACD is correct

upvoted 2 times

Kasimkyo 1 year ago

Selected Answer: AD

ACD is correct

upvoted 2 times

TestingAccount900 1 year, 11 months ago

Selected Answer: AC

ACD is correct

upvoted 2 times

yohi 2 years, 7 months ago

ACD correct answer, because:
"• A method of categorizing events based on a search
• A useful method for institutional knowledge capturing and sharing
• Can be tagged to group similar types of events"

upvoted 7 times

mahfuzmonawwer 2 years, 10 months ago

ACD is correct :)

upvoted 6 times

Lalithadevi 3 years, 5 months ago

ACD. refer page no 207

upvoted 3 times

sargeholik 3 years, 9 months ago

ACD, correct answer

upvoted 3 times

sesanchez88 3 years, 10 months ago

Event Types does not include a time range. Page 207 Splunk Fundamentals 2 PDF

upvoted 4 times

gcalcaterra 3 years, 9 months ago

ACD, page 201 too

upvoted 7 times

Question #54 *Topic 1*

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization.
If another person in the organization runs the shared report and no results are returned, why might this be? (Choose all that apply.)

A. Fast mode is enabled.

B. The dashboard is private.

C. The extraction is private.

D. The person in the organization running the report does not have access to the index.

Correct Answer: *CD*

Community vote distribution

CD (100%)

sargeholik Highly Voted 3 years, 9 months ago

THE correct answer is CD

upvoted 17 times

TestingAccount900 Most Recent 1 year, 11 months ago

Selected Answer: CD

CD are correct

upvoted 1 times

Galrim 2 years ago

Selected Answer: CD

CD are correct

upvoted 1 times

RoVasq3 2 years, 5 months ago

Selected Answer: CD

Correct answer is "CD".

upvoted 1 times

marda 2 years, 7 months ago

Selected Answer: CD

Correct answer is "CD".

upvoted 1 times

Sutanu_97 3 years ago

C & D will be the answer here. But keep in mind that while sharing a report there is an option called "Run As" Owner/User . So in this scenario the report has to be shared with run as user otherwise Owner's permissions will be used.

upvoted 3 times

Hudda 3 years, 1 month ago

finall is CD friends?

upvoted 1 times

jakal12345 3 years, 2 months ago

Correct answer is "CD".
The option B, Cannot be correct , because the other user might not necessarily be accessing the report from a dashboard ... As we know that a report can also be directly shared. Hence the option B does not fit in.

upvoted 3 times

Kool_Kid 3 years, 8 months ago

Need some clarity for this.

upvoted 1 times

gcalcaterra 3 years, 9 months ago

Isn't it BCD?

upvoted 1 times

ctux 3 years, 8 months ago

If the dashboard was private, you couldn't run it. So the problem is only with the contained data, either because you don't have access to the index or because you can't extract it.

upvoted 3 times

carm8989 3 years, 11 months ago

BD is correct

upvoted 2 times

Question #55 *Topic 1*

Which of the following statements describe the search string below?
| datamodel Application_State All_Application_State search

A. Events will be returned from dataset named Application_State.

B. Events will be returned from the data model named Application_State.

C. Events will be returned from the data model named All_Application_State.

D. No events will be returned because the pipe should occur after the datamodel command.

Correct Answer: *A*

Community vote distribution

B (100%)

kbisht Highly Voted 4 years ago
B is correct ans
upvoted 24 times

sid2051 Highly Voted 3 years, 12 months ago
B is correct answer
upvoted 8 times

Dree_Dogg Most Recent 1 year ago
Selected Answer: B
B is correct
upvoted 1 times

Huslayer 1 year, 1 month ago
Selected Answer: B
The dataset is all_.....so A is totally wrong!
upvoted 1 times

Harrysa 1 year, 4 months ago
why cannot it be C? All_Application_State is being searched here?
upvoted 2 times

> **HaoDang01122000** 1 year, 2 months ago
> I think C is dataset name
> upvoted 1 times

monk85 2 years, 1 month ago
Selected Answer: B
B is correct
upvoted 2 times

emergency_gouda 2 years, 1 month ago
Selected Answer: B
It's B
upvoted 3 times

Nicker9 2 years, 1 month ago
datamodel <datamodel> <dataset>
You will see the fields of the dataset All_Application_State. A cannot be true because Application_State is the datamodel and not the dataset name
So B is correct (but still a stupid answer).
upvoted 4 times

berbersploit 2 years, 2 months ago
Selected Answer: B
B is correct answer
upvoted 2 times

huu_nguyen 2 years, 7 months ago
Selected Answer: B
B is a final answer
upvoted 1 times

yuyulin 2 years, 8 months ago

Selected Answer: B

B is correct ans

upvoted 1 times

sondj 2 years, 8 months ago

Selected Answer: B

B is correct:
| datamodel [data model name] [data model dataset name] | ....

upvoted 5 times

mahfuzmonawwer 2 years, 10 months ago

B is correct

upvoted 1 times

SJB0324 3 years, 1 month ago

n this example the data model is Application_State;
the dataset is All_Application_State;
the command is search

It should return events from the dataset All_Application_State within data model Application_State

Option B is the only one with the correct name. p.278

upvoted 2 times

manjumeti 3 years, 5 months ago

Syntax:
| datamodel [<data model name>] [<dataset name>] [<data model search mode>]

So answer is B.

upvoted 4 times

Kiran89045 3 years, 6 months ago

I think C is correct

upvoted 2 times

gcalcaterra 3 years, 9 months ago

Answer is B.

upvoted 1 times

Question #56 *Topic 1*

What is the correct syntax to search for a tag associated with a value on a specific field?

A. tag=<field>

B. tag=<field>(<tagname>)

C. tag=<field>::<tagname>

D. tag::<field>=<tagname>

Correct Answer: *D*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/TagandaliasfieldvaluesinSplunkWeb

Community vote distribution

D (100%)

Glat Highly Voted 3 years, 8 months ago

D is correct.
See p197 of F2

upvoted 10 times

marda Most Recent 2 years, 7 months ago

Selected Answer: D

D - p197

upvoted 3 times

yohi 2 years, 7 months ago

D is correct, because:
"To search for a tag associated with a value on a specific field:
tag::<field>=<tagname>
"

upvoted 3 times

Lalithadevi 3 years, 5 months ago

D is correct.
See p197 of F2

upvoted 4 times

Question #57 *Topic 1*

In most large Splunk environments, what is the most efficient command that can be used to group events by fields?

A. join

B. stats

C. streamstats

D. transaction

Correct Answer: *B*

Reference:

https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html

Community vote distribution

B (100%)

Ailen_Man 2 years, 4 months ago

answer is stats (B)

upvoted 3 times

marda 2 years, 7 months ago

Selected Answer: B

B - P135

upvoted 2 times

SasnycoN 2 years, 9 months ago

Answer is B

upvoted 2 times

SJB0324 3 years, 1 month ago

B. stats pg 135 in f2

upvoted 2 times

Hudda 3 years, 1 month ago

Friends, could you pls confirm the final answer friends.

upvoted 1 times

thomass 3 years, 7 months ago

ans: b

upvoted 2 times