EXAMTOPICS

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



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which search string only returns events from hostWWW3?

A. host=*

B. host=WWW3

C. host=WWW*

D. Host=WWW3

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

G4ct756 Highly Voted 4 years, 1 month ago

A. Will returns multiple field values from host field. C. Will return multiple field values starting with "WWW " D. will return nothing, as field name is case sensitive. Therefore, B is correct. field name fit metadata field name, and field value is specific.

upvoted 7 times

Xpens Most Recent 7 months, 1 week ago

Splunk is case sensitive, we need to type command "host" and we are looking for www3 = host=www3

upvoted 1 times

RoopashreeKatarluRajappa24 1 year, 4 months ago

host=WWW3

upvoted 1 times

techsdc 1 year, 6 months ago

B. host=WWW3 For events ONLY, so Ans is b

upvoted 1 times

splunker1211 1 year, 8 months ago

A. Will returns multiple field values from host field. C. Will return multiple field values starting with "WWW " D. will return nothing, as field name is case sensitive. B is correct one

upvoted 1 times

Nandhan28 1 year, 8 months ago

B. host=WWW3 is the right answer

upvoted 1 times

Sankardevarajan1986 2 years, 9 months ago

Ans : B host=WWW3

upvoted 1 times

JH94 3 years ago

B is correct; field names are case sensitive, field values are not

upvoted 1 times

cagdaskarabag 3 years, 3 months ago

correct answer: B

upvoted 1 times

Adri300 3 years, 4 months ago

b is correct

upvoted 2 times

Nikhilfwd 3 years, 6 months ago

B is the correct answer

upvoted 1 times

qtygbapjpesdayazko 3 years, 8 months ago

answer is correct

upvoted 1 times

qtygbapjpesdayazko 3 years, 8 months ago

Is correct

upvoted 1 times

HUGOTE 4 years, 7 months ago

B is the correct answer

upvoted 1 times

Royal7 5 years ago

B is the correct answer

upvoted 1 times

Alex_Cyber_Sec 5 years, 1 month ago

B is correct. host = * wildcard will return all possibilities www* - returns not only www3 Host = incorrect because it case sensitive

upvoted 2 times

Janna05 5 years, 5 months ago

B For sure

upvoted 2 times

Question #2 *Topic 1*

By default, how long does Splunk retain a search job?

A. 10 Minutes

B. 15 Minutes

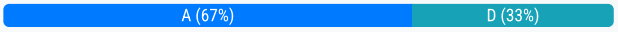
C. 1 Day

D. 7 Days

Suggested Answer: *A*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

Community vote distribution



Xpens Most Recent 7 months, 1 week ago

Splunk retains a search job is A. 10 Minutes

upvoted 1 times

computernew 1 year, 2 months ago

Can you change the default to retain search results for longer?

upvoted 1 times

techsdc 1 year, 6 months ago

Lifetime is 10 min . Ans:A

upvoted 1 times

Sankardevarajan1986 1 year, 9 months ago

Ans A 10 mins

upvoted 1 times

Nikhilfwd 2 years, 6 months ago

10 min is the correct answer

upvoted 1 times

G4ct756 3 years, 1 month ago

under "Default lifetimes for unscheduled searches" states, "the resulting search job has a default lifetime of 10 minutes." therefore A - 10 mins should be the correct answer

upvoted 3 times

HUGOTE 3 years, 7 months ago

is ok -

upvoted 1 times

nsisilya 3 years, 8 months ago

Job default Lifetime is 10 minutes,

upvoted 1 times

Alex_Cyber_Sec 4 years, 1 month ago

Lifetime 10min (page 69)

upvoted 1 times

bigmills 4 years, 9 months ago

A For Sure

upvoted 3 times

Question #3 *Topic 1*

What must be done before an automatic lookup can be created? (Choose all that apply.)

A. The lookup command must be used.

B. The lookup definition must be created.

C. The lookup file must be uploaded to Splunk.

D. The lookup file must be verified using the inputlookup command.

Suggested Answer: *B*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/DefineanautomaticlookupinSplunkWeb

Community vote distribution



oksey Highly Voted 5 years, 11 months ago

lookup file upload is optional. For instance, for KVstore and Scripted Lookup, you don't really need lookup file. So B is correct

upvoted 7 times

alisyed Highly Voted 5 years, 10 months ago

BCD... when we upload a file we need to test aswell if it actually displays the contents | inputlookup test.csv

upvoted 5 times

Shane_81 Most Recent 3 months ago

there are two foundational steps to complete: define the lookup table file and create the lookup definition. You can't automate the lookup until Splunk knows what file to read and how to interpret the data inside it.

upvoted 1 times

Xpens 7 months, 1 week ago

C. The lookup file must be uploaded to Splunk.

upvoted 1 times

Robert12 1 year, 1 month ago

Whats the difference between C and D inputlookup - Loads search results from a specified static lookup table The `inputlookup` command is used to load the entire lookup table into Splunk. review the contents of a specified static lookup file It looks like to me C and D are the same thing

upvoted 1 times

vagabontx 1 year, 9 months ago

Options A and D are not required steps for creating an automatic lookup: A. The lookup command must be used is incorrect because the lookup command itself isn't needed to set up the automatic lookup; it's only used if you want to apply the lookup manually in a search. D. The lookup file must be verified using the inputlookup command is also incorrect because verification is optional and not required for creating the automatic lookup.

upvoted 2 times

Goncaloc29 1 year, 11 months ago

B and C

upvoted 3 times

Splunkie007 3 years, 2 months ago

B, C (I think D is just optional)

upvoted 2 times

maxxxxx 3 years, 4 months ago

I asked ChatGPT, "To create an automatic lookup in Splunk, the following must be done: The lookup definition must be created. The lookup file must be uploaded to Splunk. The lookup file must be verified using the inputlookup command. Therefore, options B, C, and D are all correct. The lookup command is not necessary for creating an automatic lookup."

upvoted 1 times

G4ct756 4 years, 1 month ago

Under Prerequisites at the top , stated "A lookup definition that you have defined previously."

upvoted 2 times

HUGOTE 4 years, 7 months ago

B y C is the correct

upvoted 1 times

Janna05 5 years, 5 months ago

A lookup definition that you have defined previously. IS B

upvoted 1 times

YPR77 5 years, 6 months ago

Splunk fundamental page is 196 for Automatic Lookup

upvoted 1 times

mel101 5 years, 8 months ago

B,C . 189 in pdf

upvoted 3 times

SGBEB 5 years, 8 months ago

The answer is BC, slide 189 of Splunk Fundamentals 1

upvoted 3 times

labarcaremo635 5 years, 8 months ago

B is correct, if you test it the file is not required

upvoted 1 times

bigmills 5 years, 9 months ago

B For Sure

upvoted 1 times

igorg 5 years, 9 months ago

B, C, D

upvoted 2 times

Question #4 *Topic 1*

Which of the following Splunk components typically resides on the machines where data originates?

A. Indexer

B. Forwarder

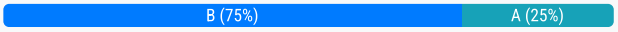
C. Search head

D. Deployment server

Suggested Answer: *B*

Official Answer: B

Community vote distribution



Shane_81 Most Recent 3 months ago

I think the answer is B: forwarder

upvoted 1 times

Xpens 7 months, 1 week ago

A. Indexer

upvoted 1 times

Vkah 1 year, 2 months ago

Forwarder

upvoted 2 times

Sankardevarajan1986 1 year, 9 months ago

Ans : B

upvoted 1 times

G4ct756 3 years, 1 month ago

Top line explaining Forwarders. " Forwarders require minimal resources and have little impact on performance, so they can usually reside on the machines where the data originates. "

upvoted 2 times

HUGOTE 3 years, 7 months ago

B is the im agree

upvoted 1 times

Janna05 4 years, 5 months ago

B For Sure

upvoted 1 times

bigmills 4 years, 9 months ago

C For Sure

upvoted 1 times

Question #5 *Topic 1*

What determines the scope of data that appears in a scheduled report?

A. All data accessible to the User role will appear in the report.

B. All data accessible to the owner of the report will appear in the report.

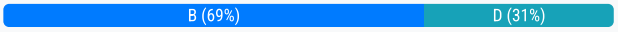
C. All data accessible to all users will appear in the report until the next time the report is run.

D. The owner of the report can configure permissions so that the report uses either the User role or the owner's profile at run time.

Suggested Answer: *D*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Managereportpermissions

Community vote distribution



Janna05 Highly Voted 4 years, 11 months ago

D is correct When you share a report with other users, you have the option of having it run with the permissions of the report "owner" (the person who created the report) or the report "user" (the person who is running the report) Scheduled reports and alerts can only run as Owner. If you share a report so that it runs as User and then schedule that report, its permissions change to run as Owner

upvoted 10 times

Shane_81 Most Recent 3 months ago

Ans B: perfectly matches Splunk's default behavior. Splunk runs the scheduled search using the security context and index constraints assigned to the report's owner.

upvoted 1 times

Xpens 7 months, 1 week ago

B. All data accessible to the owner of the report will appear in the report.

upvoted 1 times

mirko1976 1 year, 7 months ago

In Splunk, a scheduled report runs with the permissions and access level of its owner. This means the scope of data included in the report is determined by the data the owner has access to, including any restrictions on indexes, source types, or specific field-level access.

upvoted 1 times

udontknow 1 year, 7 months ago

Only option B is correct. 'Reports' can be created to run as both Owner or User. But when you set a schedule to a report, making it 'scheduled report' it will run only as the 'owner' of the report.

upvoted 1 times

yo23 2 years ago

D is correct. As documentation says the owner can configure it either way

upvoted 2 times

jb844 2 years, 4 months ago

"B" because of this the last sentence... Determine whether to run reports as the report owner or report user When you share a report with other users, you have the option of having it run with the permissions of the report "owner" (the person who created the report) or the report "user" (the person who is running the report). This setting is used for two reasons: It can allow access to search data that might otherwise be unavailable to the person running the report. It helps prevent situations where your concurrent search limit is reached when too many people run reports that you own. All reports run as Owner by default. Scheduled reports and alerts can only run as Owner. If you share a report so that it runs as User and then schedule that report, its permissions change to run as Owner.

upvoted 2 times

hamud_tanvir 2 years, 7 months ago

D is correct, slide 211 of Splunk Material

upvoted 1 times

aglopez 2 years, 4 months ago

owner is the default view, but but the permissions can be changed.

upvoted 1 times

hamud_tanvir 2 years, 7 months ago

D is correct, slide 211 of Splunk MaterialHi, any chance I can get the spunk material you referenced ? I'm a beginner and I want to write the certification exam asap, so any reading material I can get is appreciated.

upvoted 1 times

philophobia 2 years, 5 months ago

Hi, any chance I can get the spunk material you referenced ? I'm a beginner and I want to write the certification exam asap, so any reading material I can get is appreciated.

upvoted 2 times

JokerRWild 2 years, 9 months ago

Option D is not the better answer because it talks about permission configuration which is not related to determining the scope of data that appears in a scheduled report. The scope of data that appears in a scheduled report is determined by the filters and criteria set by the report owner at the time of scheduling the report. The report owner can set the filter criteria based on their requirement, and the report will display the data that matches the criteria. Thus, option B is a better answer because it explains that the data accessible to the owner of the report will appear in the scheduled report.

upvoted 2 times

JokerRWild 2 years, 9 months ago

B. All data accessible to the owner of the report will appear in the report.

upvoted 1 times

maxxxxx 2 years, 10 months ago

IT IS BOTH C + D.

upvoted 1 times

solomone 2 years, 10 months ago

Creator sets the permissions

upvoted 1 times

paparulo 2 years, 11 months ago

D, Agree

upvoted 1 times

carnage1970 3 years, 6 months ago

"Scheduled reports and alerts can only run as Owner. If you share a report so that it runs as User and then schedule that report, its permissions change to run as Owner."

upvoted 3 times

falssa 3 years, 6 months ago

D is correct. Yes, owner is the default, but the permissions set on a report after the report is saved is what determines who can see it.

upvoted 1 times

G4ct756 3 years, 7 months ago

Selected Answer: B

I believe answer should be B. Since for Scheduled Report, not matter how you configure the RunAs scope, it will default back to "Owner" base on the documentation. " Scheduled reports and alerts can only run as Owner. If you share a report so that it runs as User and then schedule that report, its permissions change to run as Owner. "

upvoted 1 times

igweifeanyi 3 years, 7 months ago

But here it says "what determines the scope..." so i think its D

upvoted 2 times

Question #6 *Topic 1*

When writing searches in Splunk, which of the following is true about Booleans?

A. They must be lowercase.

B. They must be uppercase.

C. They must be in quotations.

D. They must be in parentheses.

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

Xpens Most Recent 7 months, 1 week ago

B. They must be uppercase.

upvoted 1 times

SlyLamp 2 years ago

B = TRUE

upvoted 4 times

G4ct756 2 years, 1 month ago

B.

upvoted 3 times

HUGOTE 2 years, 7 months ago

B is the correct

upvoted 2 times

Alex_Cyber_Sec 3 years, 1 month ago

B is correct. AND OR NOT

upvoted 4 times

JanBanan 3 years, 5 months ago

B correct

upvoted 3 times

Question #7 *Topic 1*

Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

A. (index=netfw failure) AND index=netops warn OR critical

B. (index=netfw failure) OR (index=netops (warn OR critical))

C. (index=netfw failure) AND (index=netops (warn OR critical))

D. (index=netfw failure) OR index=netops OR (warn OR critical)

Suggested Answer: *B*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Aboutsubsearches

Community vote distribution

B (100%)

Xpens Most Recent 7 months, 1 week ago

B. (index=netfw failure) OR (index=netops (warn OR critical))

upvoted 1 times

JokerRWild 1 year, 9 months ago

This search uses the OR Boolean operator to search for events in either index=netfw with "failure" in it or in index=netops with "warn" or "critical" in it. The parentheses ensure that the warn and critical criteria are grouped together and only apply to the index=netops part of the search. The other options do not correctly group the criteria or use the AND operator incorrectly, which would not return the desired results.

upvoted 4 times

SlyLamp 2 years, 6 months ago

B-ware the wrong answers

upvoted 1 times

amarachi_amazone 2 years, 6 months ago

B. That is the correct answer

upvoted 1 times

atonui 2 years, 11 months ago

B. The brackets around (war OR critical) only would confuse the search.

upvoted 2 times

HUGOTE 3 years, 1 month ago

B is the correct

upvoted 2 times

Alex_Cyber_Sec 3 years, 7 months ago

B is correct (failure OR (warn OR critical))

upvoted 3 times

mikelord 3 years, 8 months ago

B is correct

upvoted 2 times

Question #8 *Topic 1*

Select the answer that displays the accurate placing of the pipe in the following search string: index=security sourcetype=access_* status=200 stats count by price

A. index=security sourcetype=access_* status=200 stats | count by price

B. index=security sourcetype=access_* status=200 | stats count by price

C. index=security sourcetype=access_* status=200 | stats count | by price

D. index=security sourcetype=access_* | status=200 | stats count by price

Suggested Answer: *B*

Official Answer: B

Community vote distribution



Vkah Most Recent 1 year, 2 months ago

Pipe should be infront of stats command

upvoted 2 times

JokerRWild 1 year, 9 months ago

The correct answer is B. The pipe in this search should be placed after the "status=200" criteria, as we want to select events where the status is 200 before we aggregate and count by price. Option A incorrectly places the pipe after "stats", which would not filter for events with status=200 before counting. Option C correctly uses the pipe but incorrectly places the count after the pipe instead of the stats command. Option D incorrectly places the pipe after "index=security sourcetype=access_*", resulting in no filtering for events with status=200.

upvoted 2 times

SlyLamp 2 years, 6 months ago

Could it B? I think it could.

upvoted 1 times

amarachi_amazone 2 years, 6 months ago

B for sure

upvoted 1 times

HUGOTE 3 years, 1 month ago

B is the correct

upvoted 1 times

Alex_Cyber_Sec 3 years, 7 months ago

B for sure

upvoted 1 times

mikelord 3 years, 8 months ago

B is correct

upvoted 1 times

Question #9 *Topic 1*

Which of the following constraints can be used with the top command?

A. limit

B. useperc

C. addtotals

D. fieldcount

Suggested Answer: *A*

Reference: https://answers.splunk.com/answers/339141/how-to-use-top-command-or-stats-with-sort-results.html

Community vote distribution

A (100%)

Robert12 Most Recent 1 year, 1 month ago

Maybe the question should specify if you have to choose more than 1 option. if userpec and addtotals are valid constraints according to JokeRWild9 the answer would have to be A,B & C

upvoted 1 times

JokerRWild 1 year, 10 months ago

The correct answer is A. limit. The "top" command is used in Splunk to identify the most common values for a field over a specified time range. It can be used with various constraints to customize its behavior. The "limit" constraint can be used with the top command to specify the maximum number of results to return. For example, "top limit=10 source" would return the top 10 most common values for the "source" field. The "useperc" constraint is used to specify whether to display the percentage of occurrences for each result. The "addtotals" constraint is used to add a row to the results that displays the total number of occurrences for all values. The "fieldcount" constraint is not a valid option to use with the top command.

upvoted 1 times

hatachino1 2 years, 10 months ago

A. limit is correct. The others options should be: showperc, countfield. The addtotals is an invalid option.

upvoted 1 times

SlyLamp 4 years ago

A is correct

upvoted 2 times

amarachi_amazone 4 years ago

A is correct

upvoted 1 times

bob456Big 4 years, 6 months ago

A is correct

upvoted 1 times

HUGOTE 4 years, 7 months ago

A is the correct

upvoted 1 times

Alex_Cyber_Sec 5 years, 1 month ago

A for sure

upvoted 1 times

mikelord 5 years, 2 months ago

A is Correct

upvoted 1 times

Question #10 *Topic 1*

When editing a dashboard, which of the following are possible options? (Choose all that apply.)

A. Add an output.

B. Export a dashboard panel.

C. Modify the chart type displayed in a dashboard panel.

D. Drag a dashboard panel to a different location on the dashboard.

Suggested Answer: *C*

Official Answer: C

Community vote distribution



siddiquip Highly Voted 6 years ago

C&D both correct

upvoted 15 times

gith27 Highly Voted 6 years ago

optionD is also correct i think. Ans C&D

upvoted 9 times

Robert12 Most Recent 1 year, 1 month ago

In a previous comment i stated i believe the answer to be BCD , i now think the answer to be CD .

upvoted 1 times

Robert12 1 year, 1 month ago

Among the options to Edit , i can't see an option to Export the dashboard panel

upvoted 1 times

Robert12 1 year, 1 month ago

The Question states "Choose all that Apply" . Therefore i believe BCD all apply

upvoted 1 times

2dd1c50 1 year, 2 months ago

When editing a dashboard, which of the following are possible options? (Choose all that apply.) A. Add an output. B. Export a dashboard panel. C. Modify the chart type displayed in a dashboard panel. D. Drag a dashboard panel to a different location on the dashboard.

upvoted 1 times

Dharam123 1 year, 3 months ago

BCD are correct option for this.

upvoted 1 times

mirko1976 1 year, 7 months ago

Correct Answers: B. Export a dashboard panel. C. Modify the chart type displayed in a dashboard panel. D. Drag a dashboard panel to a different location on the dashboard. B. Export a dashboard panel. This is correct. Many Splunk dashboards allow you to export the data or chart from a panel (e.g., as a CSV file or other formats) depending on permissions and configuration. C. Modify the chart type displayed in a dashboard panel. This is correct. When editing a dashboard, you can modify a panel's visualization type (e.g., changing a bar chart to a line chart or pie chart) by accessing the panel's settings. D. Drag a dashboard panel to a different location on the dashboard. This is correct. Dashboards in Splunk have a drag-and-drop interface, allowing you to rearrange panels for better organization. Incorrect answer A. This option is incorrect in the context of editing dashboards. The term "output" is more relevant to creating searches, lookups, or reports, but it is not an option when editing dashboards directly.

upvoted 2 times

JokerRWild 1 year, 10 months ago

C and D is the correct answer. A. Add an output - This option is not available when editing a dashboard in Splunk. B. Export a dashboard panel - This is not an option when editing a dashboard, but you can export a dashboard as a whole. C. Modify the chart type displayed in a dashboard panel - This is possible when editing a dashboard in Splunk. You can change the chart type from the Visualization tab in a panel's Edit menu. D. Drag a dashboard panel to a different location on the dashboard - This is also possible when editing a dashboard in Splunk. You can move dashboard panels around by dragging and dropping them to a new location.

upvoted 3 times

Sankardevarajan1986 2 years, 9 months ago

Answer is C

upvoted 1 times

Hurshbabe 3 years ago

C is the correct answer, D has nothing to do with editing it even though it is something you can do with a panel

upvoted 1 times

Alexi2415 3 years, 5 months ago

B,C,D are all correct??

upvoted 1 times

Alexi2415 3 years, 5 months ago

B,C,D are all correct??just C, D since "when editing" B will not be correct

upvoted 1 times

Alexi2415 3 years, 5 months ago

just C, D since "when editing" B will not be correct

upvoted 2 times

hurryupfool123 3 years, 8 months ago

How is B not an option? The source code is available for export?

upvoted 1 times

DePat 3 years, 11 months ago

C&D. Keys: Drag and Modify

upvoted 4 times

phosphor 3 years, 11 months ago

C & D are both correct

upvoted 3 times

SlyLamp 4 years ago

C&D is the correct path, young Jedi.

upvoted 3 times

igweifeanyi 4 years, 1 month ago

C and D are the correct answers

upvoted 4 times

Question #11 *Topic 1*

When running searches, command modifiers in the search string are displayed in what color?

A. Red

B. Blue

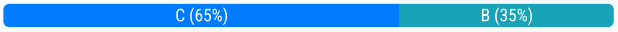
C. Orange

D. Highlighted

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Parsingsearches

Community vote distribution



JokerRWild Highly Voted 3 years, 3 months ago

The answer is B. blue because the question is talking about command modifiers and not keyword modifiers. Keyword modifiers are used to modify the search terms that are used in a query in order to narrow down the results. Examples of keyword modifiers include: - Boolean operators (AND, OR, NOT) to combine or exclude terms - Wildcard characters (*, ?) to match partial words or unknown characters - Field qualifiers (fieldname:value) to search within specific fields Command modifiers, on the other hand, modify the behavior of individual search commands, affecting how the search results are processed and displayed. Examples of command modifiers include: - The stats command modifier, which calculates statistics based on the search results - The sort command modifier, which orders the search results based on specific fields - The top command modifier, which returns the most frequent values for a specific field

upvoted 6 times

2dd1c50 Most Recent 1 year, 2 months ago

In Splunk, when running searches, command modifiers (like stats, table, where, eval, etc.) are typically displayed in orange within the Search Processing Language (SPL) syntax highlighting.

upvoted 2 times

Only12go 1 year, 2 months ago

Blue is command , Modifier is Orange

upvoted 2 times

Dharam123 1 year, 3 months ago

Its orange--checked in splunk

upvoted 2 times

anurag3011 1 year, 6 months ago

C. Orange

upvoted 1 times

EA88 1 year, 9 months ago

C. Orange

upvoted 1 times

teeec 2 years ago

C. Orange

upvoted 1 times

imnewtothis 2 years, 5 months ago

In Splunk, there isn't a formal distinction between "command modifiers" and "keyword modifiers" as separate concepts. https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Parsingsearches#Color_codes Keyword modifiers and Boolean operators: Orange

upvoted 1 times

dickchappy 2 years, 8 months ago

Commands are blue, MODIFIERS to commands are orange.

upvoted 3 times

Xtian 2 years, 9 months ago

B blue.

upvoted 1 times

SlyLamp 4 years ago

Hear me and see that C be thee answer for ye.

upvoted 3 times

amarachi_amazone 4 years ago

C is the right one

upvoted 2 times

igweifeanyi 4 years, 1 month ago

the right answer is B.

upvoted 1 times

HUGOTE 4 years, 7 months ago

C is the correct

upvoted 2 times

Janna05 5 years, 5 months ago

C is correct BOOLEAN OPERATORS and COMMAND MODIFIERS are in orange

upvoted 2 times

Joker20 5 years, 6 months ago

Boolean and command modifiers : Orange

upvoted 3 times

SpTester 5 years, 7 months ago

Orange indeed. Fun1 PDF page 101

upvoted 3 times

Question #12 *Topic 1*

Which of the following represents the Splunk recommended naming convention for dashboards?

A. Description_Group_Object

B. Group_Description_Object

C. Group_Object_Description

D. Object_Group_Description

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/Developnamingconventionsforknowledgeobjecttitles

Community vote distribution

C (100%)

SlyLamp Highly Voted 4 years ago

C. Remember the acronym is GOD.

upvoted 7 times

SlyLamp Highly Voted 4 years ago

C. Remember the acronym is GOD.The ending of the words is ALMSIVI.

upvoted 7 times

StudyBuddy_ Most Recent 1 year, 11 months ago

The ending of the words is ALMSIVI.

upvoted 1 times

Steve2610 4 years, 1 month ago

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

upvoted 1 times

HUGOTE 4 years, 7 months ago

C is the correct

upvoted 1 times

tintin_ 4 years, 9 months ago

https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Developnamingconventionsforknowledgeobjecttitles

upvoted 1 times

Janna05 5 years, 5 months ago

C is correct For example, you can create something simple like this: – _ _

upvoted 3 times

Question #13 *Topic 1*

How can search results be kept longer than 7 days?

A. By scheduling a report.

B. By creating a link to the job.

C. By changing the job settings.

D. By changing the time range picker to more than 7 days.

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

Community vote distribution

A (100%)

Noone04 Highly Voted 6 years ago

Guys, here keyword is longer than 7 days. changing job settings will allow only up to 7 days so if you want to go more than that then you have to schedule a report.

upvoted 28 times

Noone04 Highly Voted 6 years ago

Guys, here keyword is longer than 7 days. changing job settings will allow only up to 7 days so if you want to go more than that then you have to schedule a report.ExactlyAgree it can be longer than 7 days by scheduling a report

upvoted 28 times

Mahmoudhi 5 years, 1 month ago

Exactly

upvoted 6 times

linux_programmer46 4 years, 1 month ago

Agree it can be longer than 7 days by scheduling a report

upvoted 4 times

Janna05 5 years, 5 months ago

A is correct • Lifetime – Default is 10 minutes – Can be extended to 7 days – To keep your search results longer, schedule a report

upvoted 11 times

Nandhan28 Most Recent 1 year, 8 months ago

Scheduling a report in Splunk allows you to extend the retention period of search results beyond the default 7 days.

upvoted 1 times

hamud_tanvir 3 years, 1 month ago

Its A, Page 70 of Splunk official guide

upvoted 2 times

WhalerTom 3 years, 4 months ago

A is correct

upvoted 2 times

Gabbyx 3 years, 5 months ago

Correct answer is A. Schedule as a report. Edit on Job settings only has a max of 7 days and the question says more than 7 days

upvoted 4 times

SlyLamp 4 years ago

A is the one you want to go fors

upvoted 2 times

amarachi_amazone 4 years ago

A is correct

upvoted 3 times

G4ct756 4 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes Ad-hoc search, can only retain results either 10min or 7days Only Scheduled searches can extend the search result beyond 7 days. "By default, these jobs are retained for the interval of the scheduled search

multiplied by two."

upvoted 4 times

veroncafe 4 years, 2 months ago

A is correct, you have to schedule a report.

upvoted 2 times

HUGOTE 4 years, 7 months ago

A is correct

upvoted 3 times

g0nes03 5 years, 8 months ago

if : A is correct, like per page 70 from PDF (can somebody add the link to this PDF file) thanks

upvoted 3 times

labarcaremo635 5 years, 8 months ago

A is correct, page 70 from PDF

upvoted 1 times

alisyed 5 years, 10 months ago

Page 70.. PDF File Answer is A

upvoted 3 times

kbisht 5 years, 11 months ago

A is correct ans

upvoted 2 times

razzorb 6 years ago

Select Edit Job Settings to display the Job Settings.

upvoted 2 times

gabo1969 6 years, 1 month ago

A is correct

upvoted 3 times

Question #14 *Topic 1*

Which of the following is a Splunk search best practice?

A. Filter as early as possible.

B. Never specify more than one index.

C. Include as few search terms as possible.

D. Use wildcards to return more search results.

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

Janna05 Highly Voted 4 years, 5 months ago
A is correct, pag 92 • Filter as early as possible
upvoted 5 times

sc0ne Most Recent 2 years, 2 months ago
Filtering early limits the amount of events your other operations will have to process, improving efficiency
upvoted 1 times

G4ct756 3 years, 1 month ago
https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Quicktipsforoptimization " Filter the data as early as possible in the search, so that processing is done on the minimum amount of data necessary. "
upvoted 2 times

linux_programmer46 3 years, 1 month ago
A is correct
upvoted 2 times

HUGOTE 3 years, 7 months ago
A is the correct
upvoted 2 times

Question #15 *Topic 1*

When looking at a dashboard panel that is based on a report, which of the following is true?

A. You can modify the search string in the panel, and you can change and configure the visualization.

B. You can modify the search string in the panel, but you cannot change and configure the visualization.

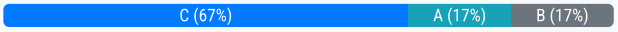
C. You cannot modify the search string in the panel, but you can change and configure the visualization.

D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels

Community vote distribution



Janna05 Highly Voted 5 years, 5 months ago

C is correct When using a panel from a report, you cannot modify the search string in the panel, but you can change and configure the visualization. If the report search changes, the panel using that report updates accordinglyHi Janna, pls can you verify if this is in "edit" mode or not cos am confused. So i tried to look at it on my instance but its only possible in edit mode. Kindly verify pls. Thanxx.

upvoted 8 times

Janna05 Highly Voted 5 years, 5 months ago

C is correct When using a panel from a report, you cannot modify the search string in the panel, but you can change and configure the visualization. If the report search changes, the panel using that report updates accordingly

upvoted 8 times

igweifeanyi 4 years, 1 month ago

Hi Janna, pls can you verify if this is in "edit" mode or not cos am confused. So i tried to look at it on my instance but its only possible in edit mode. Kindly verify pls. Thanxx.

upvoted 1 times

2dd1c50 Most Recent 1 year, 2 months ago

When a dashboard panel is based on a saved report in Splunk: The search string is locked because it is tied to the saved report. If you want to change the search, you must edit the report itself. However, you can modify how the results are visualized (e.g., change from a table to a bar chart, adjust chart settings) within the dashboard.

upvoted 1 times

s4t4 1 year, 6 months ago

The documentation says "When using a panel from a report, you cannot modify the search string in the panel, but you can change and configure the visualization." So C is correct.

upvoted 1 times

anurag3011 1 year, 6 months ago

When viewing a dashboard panel based on a report in Splunk, you can modify the search string within the panel, but you cannot change or configure the visualization; the visualization is typically inherited from the original report.

upvoted 1 times

cyberWoof 1 year, 8 months ago

The Answer is C Ignore the previous comment, the keyword is based on the report

upvoted 2 times

cyberWoof 1 year, 8 months ago

the answer to this question is A These answers need to be revisited it was a while back that you couldn't make changes to the search string, but with the latest releases these features are available and add lot of flexibility, yes you can edit the search string and run the report in the dashboard panel to see the new changes. Tried it.

upvoted 1 times

HUGOTE 4 years, 7 months ago

C is correct

upvoted 1 times

Question #16 *Topic 1*

Which of the following are common constraints of the top command?

A. limit, count

B. limit, showpercent

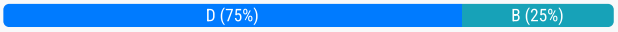
C. limits, countfield

D. showperc, countfield

Suggested Answer: *A*

Official Answer: A

Community vote distribution



DaddyP Highly Voted 5 years, 11 months ago

Top Command has commond constraints that can be remembered as LCS (Limit, Countfield, Showperc).

upvoted 11 times

amrit12345 Highly Voted 6 years, 1 month ago

D Ref - https://docs.splunk.com/Documentation/SplunkCloud/8.0.2004/SearchReference/Top

upvoted 10 times

LaurenM Most Recent 1 year ago

Even though limit IS a constraint for top command, showpercent isn't the proper name, it's showperc, making it D. In this case, it's about specifics.

upvoted 1 times

2dd1c50 1 year, 2 months ago

The top command in Splunk is used to display the most common values of a field. It has several options (also known as constraints or modifiers) to control how results are shown. Two of the most common constraints are: limit – Specifies the maximum number of top values to return. The default is 10. showpercent – A boolean flag (true or false) to show percentages alongside counts. Default is true.

upvoted 1 times

mirko1976 1 year, 7 months ago

The top command in Splunk is used to find the most frequently occurring values in a dataset. Common constraints (arguments) for the top command include: limit: Specifies the maximum number of results to return. For example, limit=10 will show the top 10 results. showpercent: Controls whether percentages are displayed in the results. For example, showpercent=true will include a column showing the percentage of each value relative to the total. Other options like countfield and showperc are not valid parameters for the top command. Let me know if you'd like further examples or clarifications!

upvoted 1 times

lahk 1 year, 10 months ago

"B" is the answer, as The question is asking about the common constraints that can be used with the top command in Splunk.By "valid constraint," I mean a parameter or option that is officially recognized and accepted by a specific command or function—in this case, the top command in Splunk. Valid constraints allow users to modify the behavior or output of the command according to their needs.Here's a breakdown of the options: A. limit, count: limit specifies how many of the top values to return. count is not a standard constraint for the top command. B. limit, showpercent: limit is valid. showpercent indicates whether to show the percentage of each value relative to the total. This is also a valid constraint. C. limits, countfield: limits is similar to limit, but countfield is not a recognized constraint. D. showperc, countfield: showperc is similar to showpercent, but again, countfield is not a valid constraint.

upvoted 1 times

Yelib 2 years, 5 months ago

Syntax: countfield= | limit= | otherstr= | percentfield= | showcount= | showperc= | useother=

upvoted 1 times

m_s_ 3 years, 3 months ago

Selected Answer: B

The common constraints would be limit, showperc and countfield. The options are vague so either B or D seems like the same thing - count is a field and not the constraint so A is definitely wrong -"limits" does not exist so C is wrong - between B and D, limits + showperc > countfield + showperc in terms of "common-ness" so I would mark B but D isn't incorrect either.

upvoted 1 times

m_s_ 3 years, 3 months ago

The common constraints would be limit, showperc and countfield. The options are vague so either B or D seems like the same thing - count is a field and not the constraint so A is definitely wrong -"limits" does not exist so C is wrong - between B and D, limits + showperc > countfield + showperc in terms of "common-ness" so I would mark B but D isn't incorrect either.showpercent is not a valid option - showperc needs to be used therefore the answer is DI think you mean the answer is A...Bruh moment. Answer is definitly D.

upvoted 1 times

sc0ne 3 years, 2 months ago

showpercent is not a valid option - showperc needs to be used therefore the answer is D

upvoted 1 times

sc0ne 3 years, 2 months ago

showpercent is not a valid option - showperc needs to be used therefore the answer is DI think you mean the answer is A...Bruh moment. Answer is definitly D.

upvoted 1 times

z3phyr 2 years, 8 months ago

I think you mean the answer is A...

upvoted 1 times

z3phyr 2 years, 8 months ago

I think you mean the answer is A...Bruh moment. Answer is definitly D.

upvoted 1 times

z3phyr 2 years, 8 months ago

Bruh moment. Answer is definitly D.

upvoted 1 times

Alexi2415 3 years, 5 months ago

common constraints ..should be A ???ignore me no count so D would be appropriated ..Top options : countfield , limit , otherstr, percentfield, showcount, showperc,useother.....count would be the "field" that will appear when you run top command

upvoted 1 times

Alexi2415 3 years, 5 months ago

common constraints ..should be A ???

upvoted 1 times

Alexi2415 3 years, 5 months ago

ignore me no count so D would be appropriated ..Top options : countfield , limit , otherstr, percentfield, showcount, showperc,useother.....count would be the "field" that will appear when you run top command

upvoted 1 times

Chris_Be 4 years, 1 month ago

D has 2 of the common constraints - limit is the other

upvoted 1 times

Steve2610 4 years, 1 month ago

there is no"Limits", "count" options in the top command: https://docs.splunk.com/Documentation/Splunk/9.0.0/SearchReference/TopWrong answer there is a limits/ countfield option https://docs.splunk.com/Documentation/SplunkCloud/9.0.2205/SearchReference/Top

upvoted 1 times

Steve2610 4 years, 1 month ago

Selected Answer: D

there is no"Limits", "count" options in the top command: https://docs.splunk.com/Documentation/Splunk/9.0.0/SearchReference/Top

upvoted 1 times

exam__Man 3 years, 11 months ago

Wrong answer there is a limits/ countfield option https://docs.splunk.com/Documentation/SplunkCloud/9.0.2205/SearchReference/Top

upvoted 1 times

Solemn_Tornado 4 years, 1 month ago

limit, showperc, countfield are valid options for Top

upvoted 1 times

linux_programmer46 4 years, 1 month ago

The keyword is limits of the top command: countfield and showperc

upvoted 1 times

cagdaskarabag 4 years, 3 months ago

https://docs.splunk.com/Documentation/SplunkCloud/8.0.2004/SearchReference/Top

upvoted 2 times

emlch 4 years, 3 months ago

D The others are present on top command but used other syntax. The options available are: countfield= , limit= , otherstr= (boolean to allow or string to name the column), percentfield= or showperc=false... a.o. https://docs.splunk.com/Documentation/SplunkCloud/8.2.2202/SearchReference/Top

upvoted 1 times

andycondeg 4 years, 4 months ago

answer D

upvoted 3 times

HUGOTE 4 years, 7 months ago

Yes, D is Correct

upvoted 2 times

Question #17 *Topic 1*

When displaying results of a search, which of the following is true about line charts?

A. Line charts are optimal for single and multiple series.

B. Line charts are optimal for single series when using Fast mode.

C. Line charts are optimal for multiple series with 3 or more columns.

D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/LineAreaCharts

Community vote distribution



nonee125 Highly Voted 6 years, 2 months ago

A is Correct

upvoted 9 times

Chakhak Most Recent 2 years, 1 month ago

Option A is true, but D is more specific about the minimum number of series. Option B is not necessarily true. Line charts can handle both single and multiple series efficiently. Option C restricts the number of columns to 3 or more, which is inaccurate. Even with 2 columns (representing two trends), a line chart is a good choice.

upvoted 1 times

Yelib 2 years, 5 months ago

Typically, line or area charts represent multiple series. Line charts can also be used for a single data series, but area charts cannot. A is correct

upvoted 2 times

Lonny 2 years, 8 months ago

A is correct

upvoted 1 times

DevilJewels 2 years, 9 months ago

A is Correct

upvoted 1 times

TheRealSplunkie 3 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/LineAreaCharts "Typically, line or area charts represent multiple series."

upvoted 1 times

Huslayer 3 years, 1 month ago

A is the best answer

upvoted 1 times

BrynnML 3 years, 1 month ago

Selected Answer: C

I would say due to the word "optimal", C is the answer as Line charts are best suited for multiple series. But it does say in Splunk docs that Line charts can be used for both single and multiple series. I think they phrase the question differently.

upvoted 1 times

BrynnML 3 years, 1 month ago

I would say due to the word "optimal", C is the answer as Line charts are best suited for multiple series. But it does say in Splunk docs that Line charts can be used for both single and multiple series. I think they phrase the question differently.The problem is that the word "optimal" isn't listed on their own document in any way. Not even a synonym of it. It states "typically" but that doesn't mean it's the best.*need to

upvoted 1 times

imnewtothis 2 years, 5 months ago

The problem is that the word "optimal" isn't listed on their own document in any way. Not even a synonym of it. It states "typically" but that doesn't mean it's the best.

upvoted 1 times

BrynnML 3 years, 1 month ago

*need to

upvoted 2 times

Steve2610 4 years, 1 month ago

Typically, line or area charts represent multiple series. Line charts can also be used for a single data series.
https://docs.splunk.com/Documentation/Splunk/9.0.0/Viz/LineAreaCharts

upvoted 1 times

Solemn_Tornado 4 years, 1 month ago

"Line charts can represent one or more data series. Area charts represent multiple data series."
https://docs.splunk.com/Documentation/DashApp/0.9.0/DashApp/chartsArea

upvoted 2 times

cagdaskarabag 4 years, 3 months ago

Line charts can represent one or more data series. https://docs.splunk.com/Documentation/SplunkCloud/8.0.2001/Viz/LineAreaCharts

upvoted 2 times

emlch 4 years, 3 months ago

A is correct

upvoted 3 times

Requete 4 years, 3 months ago

A is Correct

upvoted 3 times

Cheroti 4 years, 4 months ago

On the documentation we not have any information about 3 or more columns

upvoted 2 times

Benny_On 4 years, 5 months ago

A is answer - "Typically, line or area charts represent multiple series. Line charts can also be used for a single data series, but area charts cannot."

upvoted 2 times

Howizzle 4 years, 6 months ago

Personally, I think it's C, and it's due to the wording, they can be used for single series, but they are not optimal for it

upvoted 1 times

HUGOTE 4 years, 7 months ago

A is correct

upvoted 2 times

Question #18 *Topic 1*

How are events displayed after a search is executed?

A. In chronological order.

B. Randomly by default.

C. In reverse chronological order.

D. Alphabetically according to field name.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

Janna05 Highly Voted 2 years, 11 months ago

C is correct pag 58 Displayed in reverse chronological order (newest first)

upvoted 6 times

emlch Most Recent 1 year, 9 months ago

C for sure

upvoted 3 times

Safra 1 year, 9 months ago

C is correct

upvoted 2 times

HUGOTE 2 years, 1 month ago

C is OK

upvoted 2 times

Question #19 *Topic 1*

Which of the following is true about user account settings and preferences?

A. Search & Reporting is the only app that can be set as the default application.

B. Full names can only be changed by accounts with a Power User or Admin role.

C. Time zones are automatically updated based on the setting of the computer accessing Splunk.

D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

akamit225 2 years, 2 months ago

Option B: D is incorrect, as we cannot edit NAme https://vceguide.com/which-of-the-following-is-true-about-user-account-settings-and-preferences/The comments from your link clarify that D is the correct answer.Name can indeed be edited.

upvoted 1 times

akamit225 2 years, 2 months ago

Option B:

D is incorrect, as we cannot edit NAme https://vceguide.com/which-of-the-following-is-true-about-user-account-settings-and-preferences/

upvoted 1 times

yezup2 2 years ago

The comments from your link clarify that D is the correct answer.

upvoted 2 times

m_s_ Most Recent 1 year, 9 months ago

Name can indeed be edited.

upvoted 1 times

emlch 2 years, 9 months ago

Not sure about the others (except C that is completely incorrect) but D is def correct.

upvoted 2 times

HUGOTE 3 years, 1 month ago

D is correct

upvoted 1 times

Janna05 3 years, 11 months ago

D is correct

upvoted 3 times

rakusu 4 years ago

D confirmed

upvoted 1 times

labarcaremo635 4 years, 2 months ago

Tested, I say D

upvoted 1 times

TeeCeeP 4 years, 3 months ago

I tested it out and say D

upvoted 3 times

thinhtin 4 years, 3 months ago

Is it B or D?

upvoted 1 times

Question #20 *Topic 1*

What is a primary function of a scheduled report?

A. Auto-detect changes in performance.

B. Auto-generated PDF reports of overall data trends.

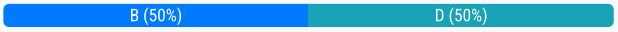
C. Regularly scheduled archiving to keep disk space use low.

D. Triggering an alert in your Splunk instance when certain conditions are met.

Suggested Answer: *D*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports

Community vote distribution



Robert12 Most Recent 1 year, 1 month ago

A scheduled report is a report that runs on a scheduled interval, and which can trigger an action each time it runs. You can define up to four actions for a scheduled report: Send a report summary by email Write the report results to a CSV lookup file Set up a webhook that sends a message to an external web resource, such as a chatroom Log and index searchable events

upvoted 1 times

udontknow 1 year, 7 months ago

B. Auto-generated PDF reports of overall data trends. D is certainly not true. In Schedules reports you can trigger alerts at specified time in the schedulre, NOT 'when certain conditions are met'.

upvoted 1 times

HUGOTE 2 years, 1 month ago

D. Triggering an alert in your Splunk instance when certain conditions are met.

upvoted 2 times

amar_scorpio 2 years, 5 months ago

A, as alert can trigger action not scheduled report. You can have an alert action as scheduled report

upvoted 3 times

Janna05 2 years, 11 months ago

D is correct A scheduled report is a report that runs on a scheduled interval, and which can trigger an action each time it runs.

upvoted 2 times

Nanila 3 years ago

A scheduled report is a report that runs on a scheduled interval, and which can trigger an action each time it runs.

upvoted 1 times

iguessillsignup 3 years, 3 months ago

I think it is meant to say "action" and not "report"I meant to say "alert" not "report"

upvoted 4 times

iguessillsignup 3 years, 3 months ago

I think it is meant to say "action" and not "report"

upvoted 4 times

iguessillsignup 3 years, 3 months ago

I meant to say "alert" not "report"

upvoted 2 times

gcalcaterra 3 years, 4 months ago

It can triggers an alert when the report run

upvoted 1 times

Question #21 *Topic 1*

After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.

B. Filters current search results.

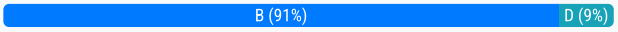
C. Moves to past or future events.

D. Expands the time range of the search.

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethetimeline

Community vote distribution



nonee125 Highly Voted 5 years, 8 months ago

B is CORRECT.

upvoted 18 times

stallone Highly Voted 5 years, 6 months ago

B is correct. Dragging across series of bars filters the current result. Doesn't re-execute the search.

upvoted 10 times

Lonny Most Recent 2 years, 1 month ago

B is the right answer

upvoted 1 times

DevilJewels 2 years, 3 months ago

B is correct When you select a set of bars on the timeline and click Zoom to Selection, your search results are filtered to show only the selected time period. The timeline and events list update to show the results of your selection.

upvoted 1 times

Huslayer 2 years, 7 months ago

B Is correct !!!

upvoted 1 times

foxx99 3 years, 4 months ago

It's B

upvoted 3 times

kennethbrown4542 3 years, 6 months ago

B is correct.

upvoted 2 times

Steve2610 3 years, 7 months ago

When you use the timeline to investigate events, you are not running a new search. You are filtering the existing search results.
https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Usethetimeline

upvoted 2 times

Solemn_Tornado 3 years, 7 months ago

"When you use the timeline to investigate events...You are filtering the existing search results." "When you select a set of bars on the timeline...your search results are filtered to show only the selected time period." ref - https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Usethetimeline

upvoted 2 times

cagdaskarabag 3 years, 9 months ago

How do you have data to search from the Future!

upvoted 6 times

Requete 3 years, 9 months ago

B is CORRECT.

upvoted 4 times

mansamusa 3 years, 11 months ago

answer is D. TESTED

upvoted 2 times

RaTix 4 years, 7 months ago

It has to be B. How do you have data to search from the Future? Unless you have a time machine. All data is in the past. Even if you have monitoring enabled on a search, by the time it hits Splunk it is now in the past.

upvoted 2 times

Janna05 4 years, 11 months ago

B is correct pag 67 To select a narrower time range, click and drag across a series of bars – This action filters the current search results Does not re-execute the search

upvoted 4 times

rakusu 4 years, 11 months ago

I SAY B IS CORRECT

upvoted 1 times

TeeCeeP 5 years, 3 months ago

page 67, slide show. B

upvoted 1 times

alisyed 5 years, 4 months ago

B as future events not possible ?

upvoted 4 times

Question #22 *Topic 1*

Which command is used to review the contents of a specified static lookup file?

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

Suggested Answer: *C*
Official Answer: C

linux_programmer46 Most Recent 2 years, 1 month ago

C is correct, it is InputLookup

upvoted 3 times

Janna05 3 years, 5 months ago

C is correct pag 191 Use the inputlookup command to load the results from a specified static lookup

upvoted 4 times

Question #23 *Topic 1*

What must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.

B. The contents of the lookup file must be copied and pasted into the search bar.

C. The lookup file must be uploaded to Splunk and a lookup definition must be created.

D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Suggested Answer: *C*
Official Answer: C

JanBanan Highly Voted 4 years, 11 months ago
C correct
upvoted 5 times

XiomaraRoRod Most Recent 2 years, 2 months ago
"All lookup types require a lookup definition. After you create a lookup definition you can invoke the lookup in a search with the lookup command."
https://docs.splunk.com/Documentation/Splunk/9.1.2/Knowledge/Aboutlookupsandfieldactions
upvoted 1 times

HUGOTE 4 years, 1 month ago
C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
upvoted 3 times

Question #24 *Topic 1*

When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?

A. |

B. $

C. !

D. ,

Suggested Answer: *D*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Sort

amrit12345 Highly Voted 2 years, 7 months ago

"List of fields to sort by and the sort order. Use a minus sign (-) for descending order and a plus sign (+) for ascending order. When specifying more than one field, separate the field names with commas. " Answer is "D"

upvoted 5 times

Janna05 Most Recent 1 year, 11 months ago

D is correct Description: List of fields to sort by and the sort order. Use a minus sign (-) for descending order and a plus sign (+) for ascending order. When specifying more than one field, separate the field names with commas

upvoted 3 times

Question #25 *Topic 1*

Which time range picker configuration would return real-time events for the past 30 seconds?

A. Preset - Relative: 30-seconds ago

B. Relative - Earliest: 30-seconds ago, Latest: Now

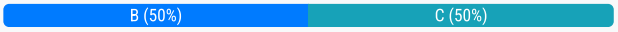
C. Real-time - Earliest: 30-seconds ago, Latest: Now

D. Advanced - Earliest: 30-seconds ago, Latest: Now

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Selecttimerangestoapply

Community vote distribution



Janna05 Highly Voted 5 years, 5 months ago

C is correct https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Selecttimerangestoapply

upvoted 6 times

udontknow Most Recent 1 year, 7 months ago

C. Real-time - Earliest: 30-seconds ago, Latest: Now Real-time time picker option is available in Splunk out-of.box.

upvoted 1 times

cyberWoof 1 year, 8 months ago

The option Real-time is no longer present in the Time Range picker, in this scenario the Relative time picker makes sense

https://docs.splunk.com/Documentation/Splunk/9.3.2/Search/Selecttimerangestoapply

upvoted 1 times

Flqm 2 years, 8 months ago

Not sure why people are saying C, since in the time picker there is no "real-time" option - just presets, relative, date range, date and time range, and advanced. The only option that works with "earliest" and "latest" options using "30-seconds ago" and "Now" values, respectively, is the relative option; so B.

upvoted 2 times

Rider2053 3 years, 3 months ago

C is the right answer

upvoted 2 times

HUGOTE 4 years, 7 months ago

C. Real-time - Earliest: 30-seconds ago, Latest: Now

upvoted 3 times

Question #26 *Topic 1*

What is the correct syntax to count the number of events containing a vendor_action field?

A. count stats vendor_action

B. count stats (vendor_action)

C. stats count (vendor_action)

D. stats vendor_action (count)

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

sedative 2 years, 3 months ago

Selected Answer: C

yo it's C frfr no cap bet on GOd

upvoted 1 times

sedative 2 years, 3 months ago

yo it's C frfr no cap bet on GOdshut up!!!!

upvoted 1 times

rome981 Most Recent 2 years, 1 month ago

shut up!!!!

upvoted 2 times

Martin_SS 3 years, 4 months ago

C is correct

upvoted 1 times

igweifeanyi 3 years, 7 months ago

C is correct

upvoted 1 times

Leinnad 4 years ago

C is right

upvoted 2 times

mikelord 4 years, 8 months ago

C is Correct

upvoted 3 times

Question #27 *Topic 1*

What is one benefit of creating dashboard panels from reports?

A. Any newly created dashboard will include that report.

B. There are no benefits to creating dashboard panels from reports.

C. It makes the dashboard more efficient because it only has to run one search string.

D. Any change to the underlying report will affect every dashboard that utilizes that report.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
D (89%) C (11%)

nonee125 Highly Voted 5 years, 2 months ago
D is correct
upvoted 12 times

amrit12345 Highly Voted 5 years, 1 month ago
"When using a panel from a report, you cannot modify the search string in the panel, but you can change and configure the visualization. If the report search changes, the panel using that report updates accordingly." "D"
upvoted 8 times

TheRealSplunkie 2 years, 1 month ago
" It makes the dashboard more efficient because it only has to run one search string." This might be true only if there is one panel in the Dashboard. It is rare a Dashboard has less than one panel, in my experience.
upvoted 1 times

assfedassfinished 2 years, 3 months ago
My vote is C. What makes D a benefit? Frankly, C is the only benefit in the multiple choices.
upvoted 1 times

assfedassfinished 2 years, 3 months ago
My vote is C. What makes D a benefit? Frankly, C is the only benefit in the multiple choices.Dashboard can have multiple panels that can have multiple searches.so it's not true to say " it only has to run one search string."
upvoted 1 times

SH_N 1 year, 11 months ago
Dashboard can have multiple panels that can have multiple searches.
upvoted 1 times

SH_N 1 year, 11 months ago
Dashboard can have multiple panels that can have multiple searches.so it's not true to say " it only has to run one search string."
upvoted 1 times

SH_N Most Recent 1 year, 11 months ago
so it's not true to say " it only has to run one search string."
upvoted 2 times

m_s_ 2 years, 3 months ago
Both C and D are correct
upvoted 1 times

dreamnet 2 years, 4 months ago
D is correct
upvoted 2 times

Sunsil 2 years, 8 months ago
D is correct
upvoted 1 times

igweifeanyi 3 years, 1 month ago
D is correct

upvoted 1 times

Solemn_Tornado 3 years, 1 month ago

D - The other three options are just flat out false.

upvoted 1 times

cagdaskarabag 3 years, 3 months ago

Any change to the underlying report will affect every dashboard that utilizes that report.

upvoted 2 times

Himadhar1997 3 years, 3 months ago

D is correct answer

upvoted 1 times

Benny_On 3 years, 5 months ago

"When using a panel from a report, you cannot modify the search string in the panel, but you can change and configure the visualization. If the report search changes, the panel using that report updates accordingly."

upvoted 2 times

jake7 3 years, 10 months ago

D without question

upvoted 1 times

Tinus5135 3 years, 12 months ago

Yes, D is the correct answer. Why it this commented more than 1 year ago and is C still the right answer? Should be fixed imho.

upvoted 3 times

Janna05 4 years, 5 months ago

D is correct pag 154 Any change to the underlying report affects every dashboard panel that utilizes that report

upvoted 3 times

SpTester 4 years, 7 months ago

Answer D - Page 132 Fun1 PDF. Why Create Dashboard panel - it is efficient to use 1 report across several dashboards and when the report changes any dashboard using it will change too.Page 154 Fun 1 PDF not 132. D is the correct answer.

upvoted 3 times

SpTester 4 years, 7 months ago

Answer D - Page 132 Fun1 PDF. Why Create Dashboard panel - it is efficient to use 1 report across several dashboards and when the report changes any dashboard using it will change too.

upvoted 3 times

thioseck 4 years, 6 months ago

Page 154 Fun 1 PDF not 132. D is the correct answer.

upvoted 3 times

bpasquale42 4 years, 8 months ago

Exam keywords here are likely "one benefit"; D seems to be a fact/constraint/given

upvoted 4 times

Question #28 *Topic 1*

By default, which of the following fields would be listed in the fields sidebar under interesting Fields?

A. host

B. index

C. source

D. sourcetype

Suggested Answer: *A*

Reference: https://answers.splunk.com/answers/185864/selected-fields-in-fields-side-bar.html

Community vote distribution

B (100%)

nonee125 Highly Voted 6 years, 2 months ago

B is correct

upvoted 15 times

Cyde Most Recent 2 years, 1 month ago

B - index (is the correct answer) "By default, host, source, and sourcetype are displayed under Selected Fields"

upvoted 1 times

Lonny 2 years, 8 months ago

B is correct

upvoted 1 times

TheRealSplunkie 3 years, 1 month ago

host, source and sourcetype are listed under "Selected Fields" not "interesting fields".

upvoted 3 times

Huslayer 3 years, 1 month ago

Index is the correct answer, try it out!!

upvoted 1 times

Sunsil 3 years, 8 months ago

index is the correct answer

upvoted 1 times

Steve2610 4 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/9.0.0/SearchTutorial/Aboutthesearchapp

upvoted 2 times

cagdaskarabag 4 years, 3 months ago

index is not preselected that's why it's in interesting fields.

upvoted 2 times

Cheroti 4 years, 4 months ago

host, source & sourcetype are displayed, by default, under Selected Fields

upvoted 1 times

rakusu 5 years, 5 months ago

ANSWER IS B

upvoted 3 times

marty 5 years, 6 months ago

host, source & sourcetype are displayed, by default, under Selected Fields, so these answers are incorrect. Index is the correct answer, because it's the only one that is left and also because under Interesting Fields, all the fields are displayed that are present in at least 20% of the results. This would be the case for index, because all events are always part of an index. So the correct answer is B

upvoted 2 times

SGBEB 5 years, 8 months ago

It is ACD slide 60 of Splunk Fundamentals 1

upvoted 1 times

Nanila 5 years, 8 months ago

Instead of "Interesting Fields", it should say "Selected Fields"

upvoted 1 times

Nanila 5 years, 8 months ago

This question is confusing.nteresting fields are key-value pairs that Splunk extracts when searching the data. When you dispatch a search, Splunk will try to identify delimiters such as an equal sign or colon and assign the value on the left as the field and the value on the right as the value. It will then take these key-value pairs and list them under interesting fields if that fields is atleast 20% of the search range by default. You can pop open the fields at the bottom of the selection and select any fields that you want at the top and they become selected fields.https://community.splunk.com/t5/Archive/What-is-an-interesting-field/m-p/417956. I think the correct answer is A, C,D

upvoted 1 times

Nanila 5 years, 8 months ago

This question is confusing.nteresting fields are key-value pairs that Splunk extracts when searching the data. When you dispatch a search, Splunk will try to identify delimiters such as an equal sign or colon and assign the value on the left as the field and the value on the right as the value. It will then take these key-value pairs and list them under interesting fields if that fields is atleast 20% of the search range by default. You can pop open the fields at the bottom of the selection and select any fields that you want at the top and they become selected fields.https://community.splunk.com/t5/Archive/What-is-an-interesting-field/m-p/417956. I think the correct answer is A, C,DIt would have been. if that is multiple questions. It is a trick question however. And thats is why A,C,D fields are Selected by default. Whereas Index is not and it is located in Interesting fields by default. Hence Correct answer is B

upvoted 1 times

SpTester 5 years, 7 months ago

It would have been. if that is multiple questions. It is a trick question however. And thats is why A,C,D fields are Selected by default. Whereas Index is not and it is located in Interesting fields by default. Hence Correct answer is B

upvoted 2 times

Oduro 5 years, 10 months ago

SELECTED FIELDS host 2 source 2 sourcetype Answer is B. Index doesn't fall under selected field.

upvoted 3 times

sid2051 6 years ago

index is correct answer

upvoted 2 times

stallone 6 years ago

Question says which (all) fields? Answer is: host, source, sourcetype A, C, D

upvoted 1 times

stallone 6 years ago

Question says which (all) fields? Answer is: host, source, sourcetype A, C, DMy mistake...didn't see the interesting Fields. Answer is index. B.Question says Whcih of the Following !

upvoted 1 times

stallone 6 years ago

My mistake...didn't see the interesting Fields. Answer is index. B.

upvoted 2 times

alisyed 5 years, 11 months ago

Question says Whcih of the Following !

upvoted 1 times

Question #29 *Topic 1*

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

Suggested Answer: *B*

Reference: https://answers.splunk.com/answers/65/are-field-values-case-sensitive.html

Community vote distribution

B (100%)

Cyde Most Recent 2 years, 1 month ago

B - Field names ARE case sensitive; field values are NOT (is the correct answer)

upvoted 1 times

rashidsahito 3 years, 10 months ago

src_ip=" " is correct. SRC_IP= " " is wrong

upvoted 2 times

Janna05 5 years, 5 months ago

B is correct pag 84 Field names ARE case sensitive; field values are NOT

upvoted 4 times

Question #30 *Topic 1*

What does the rare command do?

A. Returns the least common field values of a given field in the results.

B. Returns the most common field values of a given field in the results.

C. Returns the top 10 field values of a given field in the results.

D. Returns the lowest 10 field values of a given field in the results.

Suggested Answer: *A*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Rare

SimonR2 Highly Voted 2 years, 3 months ago
I was trying to work out why this wasn't D, the wording is very subtle and the "lowest 10" bit caught me out. Basically, values of a field can be low, but that doesn't make them "uncommon". The value of a field can be the highest value in the dataset and still be considered "rare". So the answer is definitely A!
upvoted 5 times

HUGOTE Most Recent 2 years ago
A is correct
upvoted 3 times

Janna05 2 years, 11 months ago
A is correct pag 119 The rare command returns the least common field values of a given field in the results
upvoted 3 times

rakusu 2 years, 11 months ago
WHY NOT D?
upvoted 1 times

rakusu 2 years, 11 months ago
WHY NOT D?Probably because of the language used. The specific term "least common" is the answer they want.
upvoted 1 times

SecurityPaul 2 years, 8 months ago
Probably because of the language used. The specific term "least common" is the answer they want.
upvoted 1 times

Question #31 *Topic 1*

When an alert action is configured to run a script, Splunk must be able to locate the script.
Which is one of the directories Splunk will look in to find the script?

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/scripts

C. $SPLUNK_HOME/bin/etc/scripts

D. $SPLUNK_HOME/etc/scripts/bin

Suggested Answer: *A*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Configuringscriptedalerts

amrit12345 Highly Voted 2 years, 7 months ago
"A" The script or batch file that an alert triggers must be at either of the following locations: $SPLUNK_HOME/bin/scripts $SPLUNK_HOME/etc/apps/ /bin/scripts
upvoted 8 times

JanBanan Most Recent 1 year, 11 months ago
A correct
upvoted 3 times

Question #32 *Topic 1*

Which Boolean operator is always implied between two search terms, unless otherwise specified?

A. OR

B. NOT

C. AND

D. XOR

Suggested Answer: *C*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Booleanexpressions

JanBanan Most Recent 1 year, 11 months ago

C correct

upvoted 1 times

amrit12345 2 years, 7 months ago

The AND operator is always implied between terms, that is: web error is the same as web AND error. So unless you want to include it for clarity reasons, you should not need to specify the AND operator.

upvoted 3 times

Question #33 *Topic 1*

What does the values function of the stats command do?

A. Lists all values of a given field.

B. Lists unique values of a given field.

C. Returns a count of unique values for a given field.

D. Returns the number of events that match the search.

Suggested Answer: *C*
Official Answer: C

Community vote distribution
B (100%)

gabo1969 Highly Voted 6 years, 2 months ago
Only list, not count, B iws correct
upvoted 7 times

gabo1969 Highly Voted 6 years, 2 months ago
In the curse Fundamemtals 1 Splunk say: The Stats Command Value Function Returns unique values for a given field The correct is B
upvoted 5 times

Cyde Most Recent 2 years, 1 month ago
B - Lists unique values of a given field (is the correct answer) "only list, not count"
upvoted 1 times

Lonny 2 years, 8 months ago
It's B
upvoted 1 times

Sunsil 3 years, 8 months ago
B is correct
upvoted 1 times

yawdeals 3 years, 9 months ago
B is the correct answer
upvoted 2 times

aguilard 3 years, 9 months ago
B is correct
upvoted 1 times

osakalocka 4 years ago
B is correct
upvoted 1 times

G4ct756 4 years, 1 month ago
https://docs.splunk.com/Documentation/SplunkCloud/latest/SearchReference/Multivaluefunctions "Returns the list of all distinct values of the field X as a multivalue entry. "
upvoted 1 times

cagdaskarabag 4 years, 3 months ago
Selected Answer: B
B Page 120 of the Class PDF - Splunk 7.X Fundamentals Part 1 (eLearning).pdf document. just look and you'll see. no rocket science there.
upvoted 2 times

cagdaskarabag 4 years, 3 months ago
B Page 120 of the Class PDF - Splunk 7.X Fundamentals Part 1 (eLearning).pdf document. just look and you'll see. no rocket science there.its page 162. B is correct. only list
upvoted 2 times

igweifeanyi 4 years, 1 month ago
its page 162. B is correct. only list

upvoted 1 times

emlch 4 years, 3 months ago

B, | stats value(field) gives unique values from a field A, | status list(field) gives ALL the values from a field (even if its duplicated)

upvoted 2 times

Cheroti 4 years, 4 months ago

command | stats value(field) only list, not count

upvoted 1 times

Janna05 5 years, 5 months ago

B is correct pag 120 list – lists all values of a given field

upvoted 1 times

bpasquale42 5 years, 8 months ago

I just ran it and it's B, returns the list of unique values

upvoted 1 times

Nanila 5 years, 8 months ago

- Distinct_count, dc – returns a count of unique values for a given filed.That will be answer C

upvoted 1 times

Nanila 5 years, 8 months ago

The answer Is B -- Values – list unique values of a given field.- Count – returns the number of events that match the search criteria - Distinct_count, dc – returns a count of unique values for a given filed. - Sum – returns a sum of numeric values - Avg – returns an average of numeric values - List – lists all values of a given field - Values – list unique values of a given field.

upvoted 4 times

labarcaremo635 5 years, 8 months ago

B is correct, page 129 of PDF

upvoted 2 times

Question #34 *Topic 1*

Which stats command function provides a count of how many unique values exist for a given field in the result set?

A. dc(field)

B. count(field)

C. count-by(field)

D. distinct-count(field)

Suggested Answer: *A*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Usethestatscommandandfunctions

Community vote distribution

A (100%)

amrit12345 Highly Voted 4 years, 1 month ago

Answer "A" his example creates a chart of how many new users go online each hour of the day. ... | sort _time | streamstats dc(userid) as dcusers | delta dcusers as deltadcusers | timechart sum(deltadcusers) The dc (or distinct_count) function returns a count of the unique values of userid and renames the resulting field dcusers.

upvoted 5 times

yawdeals Most Recent 1 year, 9 months ago

dc() means distinct count. A is the correct answer

upvoted 1 times

G4ct756 2 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/9.0.0/SearchReference/Aggregatefunctions "Returns the count of distinct values of the field X. This function processes field values as strings. To use this function, you can specify distinct_count(X), or the abbreviation dc(X). "

upvoted 1 times

Janna05 3 years, 5 months ago

A is correct pag 120 distinct_count, dc – returns a count of unique values for a given field

upvoted 1 times

SpTester 3 years, 7 months ago

"A" (D is a dash NOT underscore, hence wrong) page 120 pdf

upvoted 3 times

Nanila 3 years, 8 months ago

A or B is correct

upvoted 1 times

Nanila 3 years, 8 months ago

A or B is correctThe question wants unique values, so it has to be A

upvoted 1 times

msn_aden 2 years, 10 months ago

The question wants unique values, so it has to be A

upvoted 2 times

Question #35 *Topic 1*

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

A. An app

B. JSON

C. A role

D. An enhanced solution

Suggested Answer: *A*
Official Answer: A

HUGOTE Most Recent 2 years ago
is correct
upvoted 1 times

marianex 2 years, 9 months ago
A, page 9
upvoted 1 times

Question #36 *Topic 1*

Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.

B. Alerts are based on searches and when triggered will only send an email notification.

C. Alerts are based on searches and require cron to run on scheduled interval.

D. Alerts are based on searches that are run exclusively as real-time.

Suggested Answer: *A*
Official Answer: A

Darren4737 Most Recent 1 year, 8 months ago
it's actually 221 pg on the Splunk fundamental pdf
upvoted 1 times

learner_2022 3 years, 2 months ago
A is the answer according to me.
upvoted 1 times

Janna05 4 years, 5 months ago
A is correct pag 213 Splunk alerts are based on searches that can run either: – On a regular scheduled interval – In real-timepage 213 of which document please?Splunk-7-X-Fundamentals-Part-1-Presentation.pdfit's actually 221 pg on the Splunk fundamental pdf
upvoted 4 times

Janna05 4 years, 5 months ago
A is correct pag 213 Splunk alerts are based on searches that can run either: – On a regular scheduled interval – In real-time
upvoted 4 times

amksa 3 years, 7 months ago
page 213 of which document please?Splunk-7-X-Fundamentals-Part-1-Presentation.pdf
upvoted 2 times

amksa 3 years, 7 months ago
page 213 of which document please?
upvoted 2 times

Stoops 2 years, 8 months ago
Splunk-7-X-Fundamentals-Part-1-Presentation.pdf
upvoted 1 times

Question #37 *Topic 1*

What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.

B. To compute numerical statistics on each field.

C. To specify how the values in a list are delimited.

D. To partition the input data based on the split-by fields.

Suggested Answer: *A*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Stats#1._Compare_the_difference_between_using_the_stats_and_chart_commands

Janna05 Most Recent 2 years, 11 months ago

A is correct pag 123 by clause returns a count for each value of a named field or set of fields

upvoted 3 times

Question #38 *Topic 1*

How do you add or remove fields from search results?

A. Use field +to add and field -to remove.

B. Use table +to add and table -to remove.

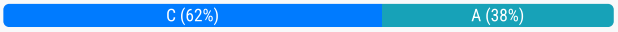
C. Use fields +to add and fields ɹ€"to remove.

D. Use fields Plus to add and fields Minus to remove.

Suggested Answer: *C*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Fields

Community vote distribution



Fred4N6 Most Recent 2 years ago

The minus symbol for the correct answer is not displayed correctly

upvoted 1 times

Cyde 2 years, 1 month ago

C - Use fields + to add and fields - to remove (is the correct answer) "field is not a Splunk command, it is fields"

upvoted 1 times

ANki_24 2 years, 8 months ago

fields + and fields - are used

upvoted 1 times

ANki_24 2 years, 8 months ago

C is correct

upvoted 1 times

dickchappy 2 years, 8 months ago

"field" is not a valid Splunk command, it's "fields"

upvoted 1 times

jb844 2 years, 10 months ago

typo "fields-"

upvoted 1 times

TheRealSplunkie 3 years, 1 month ago

I have to go with C. "fields" is plural in the Splunk documentation not singular. In answer C, there is no minus sign to remove, but 2 symbols and a quotation mark in the answer. My assumption is that is a misprint.

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2203/SearchReference/Fields#Syntax

upvoted 2 times

Alexi2415 3 years, 5 months ago

use fields + to add add fields - to minus ..testedfields - to remove**

upvoted 2 times

Alexi2415 3 years, 5 months ago

use fields + to add add fields - to minus ..tested

upvoted 2 times

Alexi2415 3 years, 5 months ago

fields - to remove**

upvoted 1 times

warlitos 3 years, 6 months ago

Correct answer C. The command is "fields" and not "field"

upvoted 4 times

Amish0123 3 years, 7 months ago

A is correct

upvoted 2 times

Sunsil 3 years, 8 months ago

A is the correct answer

upvoted 2 times

aguilard 3 years, 9 months ago

A is correct

upvoted 2 times

Solemn_Tornado 4 years, 1 month ago

Not sure what '" is supposed to be but C is not correct. A is. ref - https://docs.splunk.com/Documentation/SplunkCloud/8.2.2203/SearchReference/Fields#SyntaxAlso as jake7 pointed out, none are technically correct. A is closest, add s to make fields and the answer is there.

upvoted 2 times

Solemn_Tornado 4 years, 1 month ago

Selected Answer: A

Not sure what '" is supposed to be but C is not correct. A is. ref - https://docs.splunk.com/Documentation/SplunkCloud/8.2.2203/SearchReference/Fields#Syntax

upvoted 2 times

Solemn_Tornado 4 years, 1 month ago

Also as jake7 pointed out, none are technically correct. A is closest, add s to make fields and the answer is there.

upvoted 1 times

igweifeanyi 4 years, 1 month ago

the correct answer is A for sure bcos you use + to add and - to remove. You dont type "plus" or "minus" cos splunk wont recognize it.

upvoted 3 times

millyb_hig 4 years, 4 months ago

I completely agree with jake7, fields - is to remove

upvoted 3 times

sathyaDeva 4 years, 7 months ago

C.Use fields +to add and fields -to remove.

upvoted 4 times

jake7 4 years, 10 months ago

Technically none of them are correct. The answer is fields + to add and fields - to remove. I keep seeing C as the answer but at least the way the answer is displayed to me it shows fields '" as to remove and that is not correct

upvoted 3 times

Question #39 *Topic 1*

A field exists in search results, but isn't being displayed in the fields sidebar.
How can it be added to the fields sidebar?

A. Click All Fields and select the field to add it to Selected Fields.

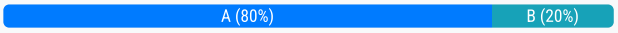
B. Click Interesting Fields and select the field to add it to Selected Fields.

C. Click Selected Fields and select the field to add it to Interesting Fields.

D. This scenario isn't possible because all fields returned from a search always appear in the fields sidebar.

Suggested Answer: *A*
Official Answer: A

Community vote distribution



foxx99 Most Recent 1 year, 10 months ago
A is correct
upvoted 1 times

yawdeals 2 years, 3 months ago
The answer is A
upvoted 2 times

shergar 2 years, 4 months ago
It's A when it is not showing at all. The question isn't about Interesting Fields or Selected Fields, it's about making it visible if it's hidden.
upvoted 2 times

soc_sts_exam 2 years, 5 months ago
A is right
upvoted 1 times

yaman778 2 years, 6 months ago
to add fields to the selected fields list, click all fields at the top of the fields sidebar Reference:
https://docs.splunk.com/Documentation/Splunk/9.0.0/SearchTutorial/Usefieldstosearch
upvoted 1 times

sborisv 2 years, 6 months ago
A is right. You cannot click "Interesting Fields", however you can click "All FIelds" and select field.
upvoted 1 times

BeckyC 2 years, 8 months ago
A is correct
upvoted 2 times

qtygbapjpesdayazko 2 years, 9 months ago
Is not B?no its not
upvoted 1 times

qtygbapjpesdayazko 2 years, 9 months ago
Selected Answer: B
Is not B?
upvoted 1 times

igweifeanyi 2 years, 7 months ago
no its not
upvoted 2 times

Janna05 3 years, 11 months ago
A is correct PAG 82
upvoted 2 times

Question #40 *Topic 1*

In the fields sidebar, which character denotes alphanumeric field values?

A. #

B. %

C. a

D. a#

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

spartello Highly Voted 2 years, 6 months ago

The answer is C, a is alpha-numeric whereas # is just numeric

upvoted 6 times

techsdc Most Recent 1 year, 6 months ago

The character that typically denotes alphanumeric field values is C. a. Letter 'a' is used to represent alphanumeric values

upvoted 1 times

raghavkulkarni 1 year, 9 months ago

C is Correct

upvoted 1 times

kjwqhdwheijoiw 2 years, 7 months ago

a = string # = numeric % = alphanumeric So answer is BIncorrect! a indicates the field values are alphanumeric # indicates the values are numeric Page 77 of Splunk fundamentals 1 You can also read more about how it categories the fields into these two categories here: https://community.splunk.com/t5/Splunk-Search/Field-categorization/m-p/87018

upvoted 4 times

kjwqhdwheijoiw 2 years, 7 months ago

a = string # = numeric % = alphanumeric So answer is B

upvoted 4 times

SimonR2 1 year, 9 months ago

Incorrect! a indicates the field values are alphanumeric # indicates the values are numeric Page 77 of Splunk fundamentals 1 You can also read more about how it categories the fields into these two categories here: https://community.splunk.com/t5/Splunk-Search/Field-categorization/m-p/87018

upvoted 3 times

CC1123 2 years, 7 months ago

It's C, pdf 79

upvoted 4 times

Nanila 2 years, 8 months ago

The answer is D. If you look at the interesting and Selected fields, you will see these symbols: #a

upvoted 3 times

TeeCeeP 2 years, 9 months ago

Has anyone seen % as the answer?

upvoted 1 times

Question #41 *Topic 1*

What is the main requirement for creating visualizations using the Splunk UI?

A. Your search must transform event data into Excel file format first.

B. Your search must transform event data into XML formatted data first.

C. Your search must transform event data into statistical data tables first.

D. Your search must transform event data into JSON formatted data first.

Suggested Answer: *B*
Official Answer: B

Community vote distribution
C (100%)

AMRIT475 Highly Voted 4 years, 6 months ago
C is correct
upvoted 13 times

nonee125 Highly Voted 4 years, 8 months ago
C is correct
upvoted 11 times

Sunsil Most Recent 2 years, 2 months ago
C is the correct answer
upvoted 2 times

TestingAccount900 2 years, 5 months ago
C, is correct, I don't understand B would make sense in any way.
upvoted 2 times

Solemn_Tornado 2 years, 7 months ago
Idk why all these sites all have the same wrong answers, but I guess it makes me feel ready for the exam since I spend most of my time submitting the correct answers. ref - https://docs.splunk.com/Documentation/Splunk/9.0.0/Viz/Datastructurerequirementsforvisualizations
upvoted 4 times

BeckyC 2 years, 8 months ago
Answer is C
upvoted 2 times

cagdaskarabag 2 years, 9 months ago
Hopefully someone will update the answer. it's obvious that the answer is C!
upvoted 3 times

qtygbapjpesdayazko 2 years, 9 months ago
Is C !!
upvoted 1 times

sathyaDeva 3 years ago
C is the correct answer
upvoted 1 times

sathyaDeva 3 years, 1 month ago
C is Correct
upvoted 1 times

Tinus5135 3 years, 6 months ago
C is correct, why is still the wrong answer displayed? It is great that this website and tests are free, but they should be giving at least the right answer to students.
upvoted 4 times

Nanila 4 years, 2 months ago
The answer is C :To create charts visualizations, your search must transform event data into statistical data tables.
https://docs.splunk.com/Documentation/Splunk/8.0.5/Search/Aboutreportingcommands

upvoted 3 times

Flavour 4 years, 3 months ago

C is the correct answer

upvoted 4 times

Scott13183 4 years, 6 months ago

C https://docs.splunk.com/Documentation/Splunk/8.0.5/Search/Aboutreportingcommands "To create charts visualizations, your search must transform event data into statistical data tables. These statistical tables are required for charts and other kinds of data visualizations. This section discusses how to use transforming commands to transform event data."

upvoted 6 times

sid2051 4 years, 6 months ago

C is correct

upvoted 4 times

stallone 4 years, 6 months ago

C is correct.

upvoted 5 times

Question #42 *Topic 1*

What syntax is used to link key/value pairs in search strings?

A. action+purchase

B. action=purchase

C. action | purchase

D. action equal purchase

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

2dd1c50 Most Recent 1 year, 2 months ago

The correct answer is: B. action=purchase □ □ Explanation: In Splunk search syntax, key/value pairs are written using the = sign

upvoted 1 times

mikelord 2 years, 2 months ago

B is Correct

upvoted 1 times

Question #43 *Topic 1*

What user interface component allows for time selection?

A. Time summary

B. Time range picker

C. Search time picker

D. Data source time statistics

Suggested Answer: *B*
Official Answer: B

G4ct756 Most Recent 2 years, 1 month ago
https://docs.splunk.com/Splexicon:Timerangepicker
upvoted 1 times

kr57 3 years, 9 months ago
B is correct
upvoted 1 times

Question #44 *Topic 1*

Which of the following searches will return results where fail, 400, and error exist in every event?

A. error AND (fail AND 400)

B. error OR (fail and 400)

C. error AND (fail OR 400)

D. error OR fail OR 400

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (100%)

stallone Highly Voted 6 years ago

A is correct answer. AND is the keyword here.

upvoted 13 times

Fred4N6 Most Recent 2 years ago

Why does it say the correct answer is C? If everyone says it is A ?

upvoted 1 times

Lonny 2 years, 8 months ago

A is the right answer

upvoted 1 times

jayfourkay17 3 years, 1 month ago

This is a badly worded question, I would have lost a point for this..

upvoted 1 times

assfedassfinished 3 years, 3 months ago

It's still A

upvoted 2 times

Sunsil 3 years, 8 months ago

A is the correct answer

upvoted 1 times

yawdeals 3 years, 9 months ago

A is the correct Answer

upvoted 1 times

osakalocka 4 years ago

A is correct based on the inclusive 'and'

upvoted 1 times

Solemn_Tornado 4 years, 1 month ago

C will only return two of the three (error AND one or the other). The question asks for all 3. We need the inclusive AND, not the exclusive OR. The parentheses are unnecessary but acceptable.

upvoted 1 times

igweifeanyi 4 years, 1 month ago

A is the very right answer pls.

upvoted 1 times

thefoque 4 years, 1 month ago

A is correct.

upvoted 2 times

BeckyC 4 years, 2 months ago

A is the correct answer

upvoted 2 times

cagdaskarabag 4 years, 3 months ago

A! simple logic man.

upvoted 3 times

Requete 4 years, 3 months ago

A is correct answer.

upvoted 1 times

sathyaDeva 4 years, 7 months ago

A is correct because if no Boolean is mentioned default AND will applicable

upvoted 2 times

bpasquale42 5 years, 8 months ago

A is correct.

upvoted 3 times

kr57 5 years, 9 months ago

A is correct

upvoted 3 times

Question #45 *Topic 1*

When placed early in a search, which command is most effective at reducing search execution time?

A. dedup

B. rename

C. sort -

D. fields +

Suggested Answer: *A*

Official Answer: A

Community vote distribution

D (60%) A (40%)

SimonR2 Highly Voted 4 years, 9 months ago

Reducing search execution time is the key phrase here. On page 107 of the pdf it shows reduced execution time by adding fields +. Dedup would reduce the amount of data but we still need to retrieve it first. It wouldn't actually do anything to reduce the execution time.

upvoted 11 times

falssa Highly Voted 4 years ago

D is Correct. Dedup command removes duplicates. Sometimes your data will not have duplicates so this does not guarantee any search optimization. Fields command specifies fields you want to include in the search. Inclusion is better then exclusion. Fields command improves performance and executes before field extraction. Document on search optimization:https://docs.splunk.com/Documentation/Splunk/8.0.4/Search/Quicktipsforoptimization

upvoted 6 times

LaurenM Most Recent 1 year ago

If you actually input it into splunk, using dedup is faster than using fields +

upvoted 1 times

2dd1c50 1 year, 2 months ago

The correct answer is: D. fields + □ □ Explanation: Placing the **fields +** command early in a Splunk search helps reduce search execution time because: It limits the amount of data returned by discarding unnecessary fields. This reduces memory usage and improves performance, especially with large datasets. □ Why the others are less effective: A. dedup – Helps remove duplicates, but still processes more data upfront. B. rename – Has no impact on performance; it's just a label change. C. sort - – Sorting large datasets early can actually slow down your search.

upvoted 1 times

vagabontx 1 year, 9 months ago

The dedup command is less effective at reducing search execution time because it works only after all events have been retrieved. Its purpose is to remove duplicate events based on specified fields, which helps in organizing results but doesn't impact the initial data retrieval process. Since dedup is a post-processing command, placing it early in a search doesn't reduce the volume of data initially retrieved or processed. In contrast, fields + limits the fields retrieved at the very start, reducing memory usage and processing time, which directly impacts search speed.

upvoted 1 times

Arrowseven 3 years, 1 month ago

I would say A is correct. We want to minimise the amount of time it will take for the search job and removing duplicates is the best way to do it.

upvoted 4 times

arthursabino20 3 years, 2 months ago

A is the correct answer.

upvoted 3 times

asarali 3 years, 2 months ago

I will bet on ans A - because the question says when placed early in search. It should be Dedup. This improves the search which otherwise would have taken more time.

upvoted 2 times

Koove 3 years, 6 months ago

A. dedup (deduplicate) is most effective at reducing search execution time when placed early in a search. This is because dedup removes duplicate events from the results, reducing the amount of data that needs to be processed. By removing duplicates, the search can be more efficient, reducing

search execution time. The other commands (rename, sort, and fields) also have their uses, but they are not as effective at reducing search execution time as dedup when placed early in a search.

upvoted 2 times

G4ct756 4 years, 1 month ago

fields + , will only include fields from the field-list. dedup, will only start sorting (de duplication) process after all the results is collected. so fields + is the most efficient.

upvoted 4 times

cagdaskarabag 4 years, 3 months ago

A is correct based on the way of the question is asked. Document P106 --> Field extraction is the most costly part of a search, adding / removing does not change the fact.

upvoted 1 times

Requete 4 years, 3 months ago

A is correct.

upvoted 1 times

Cheroti 4 years, 4 months ago

Fileds + will search only the fields that you need and does not do any extraction on other fields

upvoted 1 times

atonui 4 years, 4 months ago

D (fields +) is correct. This is because the fields command is a Distributable streaming command (https://docs.splunk.com/Documentation/Splunk/8.2.5/SearchReference/Fields) i.e. it is executed on the indexer before field extraction occurs and the results sent to the search head for further processing. The dedup command is a streaming command or a dataset processing command, depending on which arguments are specified with the command. Thus it does not serve to optimize searches, in fact in some instances it may negatively impact performance (https://docs.splunk.com/Documentation/Splunk/8.2.5/SearchReference/Dedup).

upvoted 4 times

nimanami 5 years ago

A is correct. P.92

upvoted 3 times

H1_ 5 years, 2 months ago

100% sure dedup is correct

upvoted 1 times

Janna05 5 years, 5 months ago

D is correct pag 106 To include, use fields + (default) – Occurs before field extraction – Improves performance

upvoted 3 times

Question #46 *Topic 1*

Which of the following is the most efficient filter for running searches in Splunk?

A. Time

B. Fast mode

C. Sourcetype

D. Selected Fields

Suggested Answer: *C*
Official Answer: C

Community vote distribution
A (100%)

nonee125 Highly Voted 5 years, 8 months ago
A is correct
upvoted 10 times

Lonny Most Recent 2 years, 1 month ago
It's A
upvoted 1 times

TheRealSplunkie 2 years, 7 months ago
DUH!!!!
upvoted 1 times

Sunsil 3 years, 2 months ago
A is correct
upvoted 2 times

kiki533 3 years, 3 months ago
A correct
upvoted 2 times

hawxxx 3 years, 6 months ago
A should be correct not sourcetype
upvoted 3 times

arcsw 3 years, 7 months ago
Its A, even the guy in the videos mention it a lot
upvoted 2 times

cagdaskarabag 3 years, 9 months ago
time is the most efficient filter.
upvoted 1 times

Cheroti 3 years, 10 months ago
Time is the most efficient filter, not sourcetype
upvoted 1 times

sathyaDeva 4 years, 1 month ago
A is correct
upvoted 1 times

DanielVA 4 years, 1 month ago
A is correct
upvoted 1 times

Janna05 4 years, 11 months ago
A is correct pag 91 Time is the most efficient filter
upvoted 3 times

SpTester 5 years, 1 month ago

Time - because of how splunk stores indexes. Each bucket (index) is stored as a file with Epoch Time in its name. And the more limiting your time the less files Splunk need to search in.

upvoted 2 times

Nanila 5 years, 2 months ago

A is accurate - Time is the most efficient filter. Page 91 of fundamental 1 PDF

upvoted 1 times

Nanila 5 years, 2 months ago

A is accurate - Time is the most efficient filter. Page 91 of fundamental 1 PDFwhat is the pdf ur referring to ? is it available online

upvoted 1 times

vasanthi77 2 years, 9 months ago

what is the pdf ur referring to ? is it available online

upvoted 1 times

kr57 5 years, 2 months ago

A is correct

upvoted 1 times

asultan20 5 years, 3 months ago

A is correct.

upvoted 1 times

alisyed 5 years, 4 months ago

pAGE -91 PDF.. Answer is A

upvoted 1 times

Question #47 *Topic 1*

How does Splunk determine which fields to extract from data?

A. Splunk only extracts the most interesting data from the last 24 hours.

B. Splunk only extracts fields users have manually specified in their data.

C. Splunk automatically extracts any fields that generate interesting visualizations.

D. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

2dd1c50 Most Recent 1 year, 2 months ago

The correct answer is: D. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data. Explanation: Splunk uses automatic field extraction during indexing and searching: It relies on the sourcetype to determine how data is structured. It scans for key/value patterns (like user=john, status=200) and extracts fields accordingly. These extracted fields appear in the Fields Sidebar during a search. Why the others are incorrect: A: Time range (like last 24 hours) doesn't affect field extraction. B: Users can manually define fields, but Splunk does automatic extraction too. C: Visualizations don't drive field extraction—field data enables visualizations.

upvoted 1 times

atonui 1 year, 10 months ago

D is correct. B may seem correct but according to the pdf pg. 77, Prior to search time, some fields are already stored with the event in the index: meta fields like host, source, sourcetype and index as well as internal fields such as _time and _raw.

upvoted 1 times

kr57 3 years, 2 months ago

D is correct

upvoted 1 times

Question #48 *Topic 1*

Which of the following file types is an option for exporting Splunk search results?

A. PDF

B. JSON

C. XLS

D. RTF

Suggested Answer: *A*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/ExportdatausingSplunkWeb

Community vote distribution

B (100%)

Robert12 Most Recent 1 year, 1 month ago

Im currently on my splunk UI and you have the following options: CSV, XML, and JSON

upvoted 1 times

oussa_ama 1 year, 12 months ago

B is correct.

upvoted 1 times

BrynnML 3 years, 1 month ago

XML/JSON/CSV

upvoted 1 times

TestingAccount900 3 years, 12 months ago

You can only export via PDF for a saved search within a report, if it's a direct search it can only be XML/JSON/CSV and Raw Data if statistical data isn't contained in it

upvoted 2 times

cagdaskarabag 4 years, 3 months ago

B. Export file type options: csv, json, xml.

upvoted 2 times

Cheroti 4 years, 4 months ago

B. Export file type options: csv, json, xml.

upvoted 2 times

atonui 4 years, 4 months ago

B. There are three file type options: csv, json, xml.

upvoted 1 times

HUGOTE 4 years, 7 months ago

B is correct JSON

upvoted 2 times

sathyaDeva 4 years, 7 months ago

B is right...because the options available are csv, json, xml

upvoted 2 times

DanielVA 4 years, 7 months ago

B is correct JSON

upvoted 1 times

ayotundet 4 years, 10 months ago

The answer is A PDF, saving is CSV, XML and JSON format

upvoted 1 times

nifasecu 5 years, 1 month ago

it's B, page 72 in fundamentals part 1 learning-pdf

upvoted 3 times

Nanila 5 years, 8 months ago

B is accurate

upvoted 1 times

SGBEB 5 years, 8 months ago

It is B, you can export search results to Raw Events (text file), CSV, XML or JSON format

upvoted 4 times

labarcaremo635 5 years, 8 months ago

Answer is B, page 72 from PDF

upvoted 1 times

kr57 5 years, 9 months ago

B is correct

upvoted 1 times

alisyed 5 years, 10 months ago

B is correct A cannot be correct as Pdf can be saved for Saved searches only

upvoted 2 times

Question #49 *Topic 1*

What syntax is used to link key/value pairs in search strings?

A. Parentheses

B. @ or # symbols

C. Quotation marks

D. Relational operators such as =,

Suggested Answer: *D*
Official Answer: D

mikelord Most Recent 2 years, 2 months ago

D is Correct

upvoted 1 times

Question #50 *Topic 1*

Which search string returns a filed containing the number of matching events and names that field Event Count?

A. index=security failure | stats sum as ɹ€Event Countɹ€

B. index=security failure | stats count as ɹ€Event Countɹ€

C. index=security failure | stats count by ɹ€Event Countɹ€

D. index=security failure | stats dc(count) as ɹ€Event Countɹ€

Suggested Answer: *C*

Official Answer: C

Community vote distribution

B (92%) C (8%)

shergar Highly Voted 3 years, 4 months ago

By is how grouping occurs, AS renames the field. The question ask for the search string that names the number of matching events (count) Event Count.

upvoted 6 times

dwuanklk Most Recent 1 year, 10 months ago

B is the correct

upvoted 1 times

b0d4564 1 year, 12 months ago

Looks like C to me

upvoted 1 times

Lonny 2 years, 1 month ago

It's B

upvoted 1 times

hashed_pony 2 years, 2 months ago

"stats count AS" will rename the field given, "stats count BY" will count the number of instances of the field given. Right answer is C.

upvoted 1 times

wolfsense 2 years, 3 months ago

B has the only correct syntax that also renames the field to Event Count.

upvoted 1 times

sridevi3018 2 years, 4 months ago

C is the correct answer...

upvoted 2 times

Sunsil 3 years, 2 months ago

B is the correct answer

upvoted 2 times

Ufuk_Ari 3 years, 4 months ago

Definitely B

upvoted 2 times

Question #51 *Topic 1*

Which search would return events from the access_combined sourcetype?

A. Sourcetype=access_combined

B. Sourcetype=Access_Combined

C. sourcetype=Access_Combined

D. SOURCETYPE=access_combined

Suggested Answer: *A*

Official Answer: A

Community vote distribution

C (100%)

sid2051 Highly Voted 4 years, 6 months ago

C is correct answer ,field name is case sensitive not values

upvoted 10 times

nonee125 Highly Voted 4 years, 8 months ago

C is correct

upvoted 8 times

loop3r_11 Most Recent 1 year, 9 months ago

field names are sensitive not values

upvoted 2 times

assfedassfinished 1 year, 9 months ago

If all the answers were right on this exam, I imagine that these exam questions would not be available for long.

upvoted 1 times

warlitos 2 years ago

C correct. field name (sourcetype) -> case sensitive field value (Acces_Combined) -> NOT case sensitive

upvoted 2 times

Sunsil 2 years, 2 months ago

C is correct

upvoted 1 times

M4L34 2 years, 7 months ago

Field name is case sensitive and field value is not

upvoted 2 times

G4ct756 2 years, 7 months ago

field value is not case sensitive.

upvoted 1 times

BeckyC 2 years, 8 months ago

Field name is case sensitive so the correct answer is C

upvoted 1 times

Requete 2 years, 9 months ago

C is correct.

upvoted 1 times

ITgmoney 2 years, 11 months ago

C is correct

upvoted 1 times

HUGOTE 3 years, 1 month ago

C is correct

upvoted 1 times

sathyaDeva 3 years, 1 month ago

C because field names are case sensitive field values are not

upvoted 1 times

kr57 4 years, 2 months ago

C is correct

upvoted 1 times

asultan20 4 years, 3 months ago

C is correct.

upvoted 1 times

alisyed 4 years, 4 months ago

C is correct

upvoted 1 times

stallone 4 years, 6 months ago

C is correct. Field names are case sensitive.

upvoted 4 times

Question #52 *Topic 1*

Which of the following index searches would provide the most efficient search performance?

A. index=*

B. index=web OR index=s*

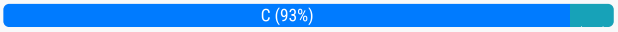
C. (index=web OR index=sales)

D. *index=sales AND index=web*

Suggested Answer: *B*

Official Answer: B

Community vote distribution



HUGOTE Highly Voted 3 years, 7 months ago

C is correct. Wild cards are always expensive.

upvoted 11 times

yukilee 3 years, 4 months ago

C is correct

upvoted 5 times

2dd1c50 Most Recent 1 year, 2 months ago

The correct answer is: C. (index=web OR index=sales) □ □ Explanation: When it comes to search performance in Splunk, efficiency is achieved by: Narrowing the search scope (specific indexes, sources, sourcetypes) Avoiding wildcards at the beginning of terms (e.g., index=*sales is inefficient) Why C is most efficient: spl Copy Edit (index=web OR index=sales) This query explicitly specifies two indexes. It's optimized for Splunk's indexing engine. Searches only the relevant data, which improves speed and performance. □ Why the others are inefficient: A. Searches all indexes—very resource-intensive and slow. B. The index=s* includes a leading wildcard, which forces Splunk to scan more index names = less efficient. D. Invalid syntax; also uses wildcards improperly, making it both incorrect and inefficient.

upvoted 1 times

hashed_pony 1 year, 8 months ago

I have no idea who tagged the right answers for these but please stop, there are so many wrong answers.

upvoted 4 times

SnakeTech 1 year, 9 months ago

Another mistake, ExamTopics, could you please correct ...

upvoted 1 times

kiuh 2 years, 1 month ago

C is the correct ans

upvoted 1 times

Mr__d__ 2 years, 3 months ago

C is correct

upvoted 2 times

sjb0001 2 years, 8 months ago

Wildcards are very inefficient.

upvoted 2 times

ITgmoney 3 years, 4 months ago

C gives you the most details to specify the search the most. using * brings you everything under the sun and would be the least efficient.

upvoted 4 times

Sam_cipher 3 years, 8 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

Sam_cipher 3 years, 8 months ago

A is the right answerWhat do you base this of? They say you get better search performance by including more fields and being more specific. A is nothing but a wildcard, i'd say its the least efficient when it comes to search performance

upvoted 1 times

lwoved Highly Voted 3 years, 8 months ago

What do you base this of? They say you get better search performance by including more fields and being more specific. A is nothing but a wildcard, i'd say its the least efficient when it comes to search performance

upvoted 7 times

asultan20 4 years, 9 months ago

C is correct.

upvoted 2 times

sid2051 5 years ago

C should be correct as it is not using regex

upvoted 3 times

stallone 5 years ago

C is correct. Wild cards are always expensive.

upvoted 2 times

parelo 5 years, 1 month ago

C is right, to improve performance in searches you have to be specific, wildcards makes searches more expensive

upvoted 2 times

nonee125 5 years, 2 months ago

C is correct

upvoted 3 times

Question #53 *Topic 1*

What is a suggested Splunk best practice for naming reports?

A. Reports are best named using many numbers so they can be more easily sorted.

B. Use a consistent naming convention so they are easily separated by characteristics such as group and object.

C. Name reports as uniquely as possible with no overlap to differentiate them from one another.

D. Any naming convention is fine as long as you keep an external spreadsheet to keep track.

Suggested Answer: *B*
Official Answer: B

marianex Most Recent 1 year, 9 months ago

B, page 134

upvoted 1 times

Question #54 *Topic 1*

In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

A. No events will be returned.

B. Splunk will prompt you to specify an index.

C. All non-indexed events to which the user has access will be returned.

D. Events from every index searched by default to which the user has access will be returned.

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (100%)

Janna05 Highly Voted 4 years, 5 months ago
D is correct pag 42 Splunk applies defaults if not specified
upvoted 5 times

FrancoPepe Most Recent 2 years ago
I have 2 indexes in my test deployment. (Splunk enterprise) 9.1.0.2. By running a simple search with the word "error" or a sourcetype specified does not return any event. To me it's A
upvoted 1 times

BrynnML 2 years, 1 month ago
D is correct
upvoted 2 times

Niketes 2 years, 1 month ago
Splunk Cloud, version 9. Tried a search putting a sourcetype before, then one with only a word after, without telling the index: I got result. So for me D is the correct one.
upvoted 1 times

daniele_pepe 2 years, 5 months ago
A. Splunk 9 returns no event
upvoted 1 times

SimonR2 3 years, 9 months ago
Just tested this and it returned all results from indexes I had access to. Answer is D.
upvoted 4 times

Sanket3 4 years, 2 months ago
D is correct it will take default index if not specified
upvoted 4 times

ShreeshaKM 4 years, 5 months ago
Answer is A. Splunk will not return any events.
upvoted 2 times

pabinajm 4 years, 6 months ago
Using Splunk 8.1.1, when I don't specify an index, I don't get results. I've created two new indexes, both which contain data, but neither are searched by default.In order to establish new indexes as "default", edit the Role > Indexes, check the indexes to be made default.
upvoted 1 times

pabinajm 4 years, 6 months ago
Using Splunk 8.1.1, when I don't specify an index, I don't get results. I've created two new indexes, both which contain data, but neither are searched by default.
upvoted 1 times

pabinajm 4 years, 6 months ago
In order to establish new indexes as "default", edit the Role > Indexes, check the indexes to be made default.
upvoted 1 times

Nanila 4 years, 8 months ago

Page 42 of the PDF says, Splunk applies default if not specified. So D is accurate

upvoted 2 times

alisyed 4 years, 10 months ago

Because you only have one index in your Lab. Try to create a test Index and then search. It will search both the test and default index

upvoted 1 times

gcalcaterra 4 years, 10 months ago

In my lab with splunk 8, when I don't specify any index param it only brings me data from the default index "main". So I'm confused with this one? any other tests?Is the assumption that you have access to all/remaining Indexes?

upvoted 1 times

gcalcaterra 4 years, 10 months ago

In my lab with splunk 8, when I don't specify any index param it only brings me data from the default index "main". So I'm confused with this one? any other tests?

upvoted 1 times

yury 3 years, 4 months ago

Is the assumption that you have access to all/remaining Indexes?

upvoted 1 times

Question #55 *Topic 1*

When looking at a statistics table, what is one way to drill down to see the underlying events?

A. Creating a pivot table.

B. Clicking on the visualizations tab.

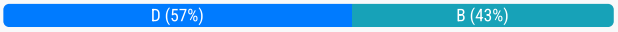
C. Viewing your report in a dashboard.

D. Clicking on any field value in the table.

Suggested Answer: *D*

Official Answer: D

Community vote distribution



babusartop17 Highly Voted 4 years, 1 month ago

Nope -- should be D. To see the underlying event you can click on field to add to search

upvoted 11 times

Alexi2415 Most Recent 1 year, 11 months ago

I vote for B

upvoted 1 times

SlyLamp 2 years, 6 months ago

Vote for D

upvoted 1 times

nqthien041292 2 years, 6 months ago

Vote D

upvoted 1 times

arcsw 2 years, 7 months ago

Is D, because you can´t see detailed events in a visualization, if you clic on any event in a statistcs table you can choose the option "View events" wich is the same as drilldown underlying event

upvoted 2 times

Osa_ 2 years, 8 months ago

D is correct Cagdaskarabag is right

upvoted 1 times

cagdaskarabag 2 years, 9 months ago

Read the question again: It says, in the "Statistics tab" In the Statistics tab you can run a drilldown search when you click on a field value or calculated search result. https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Drilldownonstatisticaltablerowsandcells

upvoted 4 times

Requete 2 years, 9 months ago

B is correct

upvoted 2 times

H1_ 3 years, 8 months ago

b is 100%

upvoted 1 times

marianex 3 years, 9 months ago

B, page 180 Fun1

upvoted 2 times

SpTester 4 years, 1 month ago

D - page 158 Fun1 pdf

upvoted 3 times

Sab123 4 years, 1 month ago

B is correct.Tried & when I clicked on the visualizations tab it drill down the events.

upvoted 2 times

Sravs_24 4 years, 1 month ago

Correct Answer: B

upvoted 1 times

Question #56 *Topic 1*

In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type

B. App, Owner, Priority, and Status

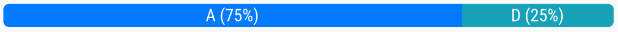
C. App, Dashboard, Severity, and Type

D. App, Time Window, Type, and Severity

Suggested Answer: *D*

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

Community vote distribution



Only12go Most Recent 1 year, 2 months ago

D is correct answer from this doc https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 2 times

SnakeTech 1 year, 9 months ago

Selected Answer: A

"by nonee125" and in comment nonee123 : "A is correct". Could you correct this answer ?

upvoted 1 times

SnakeTech 1 year, 9 months ago

"by nonee125" and in comment nonee123 : "A is correct". Could you correct this answer ?125 not 123

upvoted 1 times

SnakeTech 1 year, 9 months ago

125 not 123

upvoted 1 times

TheStudiousPeepz 1 year, 9 months ago

A is correct. If you look on the Alerts page in a Splunk instance, the options to filter triggered alerts are: App, Owner, Severity and Alert (version 9.11)

upvoted 2 times

Hurshbabe 2 years ago

D is correct answer from this doc https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 2 times

Derag 2 years, 3 months ago

D is Correct, as On the Triggered Alerts page, details appear in the following categories: Time: Trigger date and time. Fired alerts: Triggered alert name(s). App: Alert app context. Type: Alert type. Severity: Assigned alert severity level. Severity levels can help you sort or filter alerts on this page. Mode: Alert triggering configuration mode. "Per-result" means that the alert triggered because of a single event. "Digest" means that the alert triggered because of a group of events.

upvoted 2 times

arcsw 3 years, 1 month ago

In the new Splunk versions you can only filter by Owner and App, but the PDF is based on an older version thus you can filter by App, Owner, Severity and Type(Alert), page 224 PDF Splunk Fundamentals 1, so the right aswer is A

upvoted 4 times

Himadhar1997 3 years, 2 months ago

A "Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name)." as per Splunk docs

upvoted 1 times

cagdaskarabag 3 years, 3 months ago

fundementals 1 pdf, p224 time, fired alerts, app, type, severity, mode, actions (enterprise v7X) answer is D

upvoted 1 times

Requete 3 years, 3 months ago

A is correct

upvoted 1 times

CC1123 4 years, 7 months ago

A, from the link below: Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name).

upvoted 4 times

CC1123 4 years, 7 months ago

A, from the link below: Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name).checks out; https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 4 times

PoundingCode 3 years, 10 months ago

checks out; https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 1 times

Nanila 4 years, 8 months ago

A is accurate

upvoted 1 times

Asirpa 4 years, 8 months ago

On the Alerts page, there's a Title, Actions, Owner, App, Sharing, and Status column for each alert, but not for Severity or Time Window. In the Splunk documentation, you can filter TRIGGERED alerts by App, Owner, Severity, and Alert (alert name). So is there a typo or omitted phrase in this question? Or are none of the answers correct?

upvoted 4 times

kr57 4 years, 9 months ago

Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name).

upvoted 2 times

sid2051 5 years ago

A is correcthttps://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/ReviewtriggeredalertsD is correct.

upvoted 1 times

sid2051 5 years ago

A is correct

upvoted 1 times

Nanakj 5 years ago

https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/ReviewtriggeredalertsD is correct.

upvoted 1 times

Nanakj 5 years ago

https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 1 times

Nanakj 5 years ago

D is correct.

upvoted 2 times

stallone 5 years ago

A is correct. Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name).there is no owner Time Trigger date and time. Fired alerts Triggered alert name(s). App Alert app context. Type Alert type. Severity Assigned alert severity level. Severity levels can help you sort or filter alerts on this page. Mode Alert triggering configuration mode. "Per-result" means that the alert triggered because of a single event. "Digest" means that the alert triggered because of a group of eventshttps://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 1 times

stallone 5 years ago

A is correct. Filter any displayed alerts according to App, Owner, Severity, and Alert (alert name).

upvoted 1 times

razzorb 5 years ago

there is no owner Time Trigger date and time. Fired alerts Triggered alert name(s). App Alert app context. Type Alert type. Severity Assigned alert severity level. Severity levels can help you sort or filter alerts on this page. Mode Alert triggering configuration mode. "Per-result" means that the alert triggered because of a single event. "Digest" means that the alert triggered because of a group of events

upvoted 2 times

razzorb 5 years ago

there is no owner Time Trigger date and time. Fired alerts Triggered alert name(s). App Alert app context. Type Alert type. Severity Assigned alert severity level. Severity levels can help you sort or filter alerts on this page. Mode Alert triggering configuration mode. "Per-result" means that the alert triggered because of a single event. "Digest" means that the alert triggered because of a group of eventshttps://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 2 times

razzorb 5 years ago

https://docs.splunk.com/Documentation/Splunk/7.2.6/Alert/Reviewtriggeredalerts

upvoted 1 times

nonee125 5 years, 2 months ago

A is correct

upvoted 2 times

Question #57 *Topic 1*

What are the steps to schedule a report?

A. After saving the report, click Schedule.

B. After saving the report, click Event Type.

C. After saving the report, click Scheduling.

D. After saving the report, click Dashboard Panel.

Suggested Answer: *A*
Official Answer: A

Janna05 Most Recent 1 year, 11 months ago

A is correct pag 204 After the report is created, click Schedule

upvoted 3 times

Question #58 *Topic 1*

In the fields sidebar, what indicates that a field is numeric?

A. A number to the right of the field name.

B. A # symbol to the left of the field name.

C. A lowercase n to the left of the field name.

D. A lowercase n to the right of the field name.

Suggested Answer: *B*
Official Answer: B

marianex Most Recent 1 year, 9 months ago

B,page 79

upvoted 1 times

Question #59 *Topic 1*

Which of the following are functions of the stats command?

A. count, sum, add

B. count, sum, less

C. sum, avg, values

D. sum, values, table

Suggested Answer: *C*
Official Answer: C

marianex Most Recent 1 year, 9 months ago

C, page 120

upvoted 1 times

Question #60 *Topic 1*

At index time, in which field does Splunk store the timestamp value?

A. time

B. _time

C. EventTime

D. timestamp

Suggested Answer: *B*
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Data/HowSplunkextractstimestamps

HUGOTE Most Recent 2 years ago
is ok b
upvoted 1 times

marianex 2 years, 9 months ago
B, page 199
upvoted 1 times

Question #61 *Topic 1*

Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms.

B. Include at least one function as this is a search requirement.

C. Include the search terms at the beginning of the search string.

D. Avoid using formatting clauses, as they add too much overhead.

Suggested Answer: *D*

Official Answer: D

Community vote distribution

C (100%)

alisyed Highly Voted 4 years, 10 months ago

C is correct Admin please start correcting the Errors !!

upvoted 16 times

Khuli_Dolly Most Recent 1 year, 11 months ago

c is correct

upvoted 1 times

Rider2053 2 years, 2 months ago

C is right answer

upvoted 1 times

warlitos 2 years, 6 months ago

C is correct

upvoted 1 times

igweifeanyi 3 years, 1 month ago

C is very correct

upvoted 1 times

cagdaskarabag 3 years, 3 months ago

admin, wake up! fix those errors!

upvoted 3 times

DanielVA 3 years, 7 months ago

C is correct

upvoted 3 times

kr57 4 years, 9 months ago

C is correct

upvoted 2 times

Glat 4 years, 11 months ago

Answer is C

upvoted 3 times

gabo1969 5 years ago

I think that is C Splunk say "Apply filtering commands as early as possible in your search"

upvoted 4 times

edev 5 years ago

isn't it C?

upvoted 3 times

Question #62 *Topic 1*

What type of search can be saved as a report?

A. Any search can be saved as a report.

B. Only searches that generate visualizations.

C. Only searches containing a transforming command.

D. Only searches that generate statistics or visualizations.

Suggested Answer: *A*
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Aboutsavingandsharingreports#Save_a_search_as_a_report

mikelord Most Recent 2 years, 2 months ago

A is Correct

upvoted 1 times

Question #63 *Topic 1*

What can be included in the All Fields option in the sidebar?

A. Dashboards

B. Metadata only

C. Non-interesting fields

D. Field descriptions

Suggested Answer: *D*

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/ExtractfieldsinteractivelywithIFX#Access_the_field_extractor_from_the_All_Fields_dialog_box

Community vote distribution

C (100%)

BrynnML Most Recent 2 years, 1 month ago

C is correct

upvoted 3 times

Amish0123 2 years, 7 months ago

selected fields , interesting fields are displayed by default. All-Fields must be selected to see non interesting fields

upvoted 3 times

Sunsil 2 years, 8 months ago

C is correct option

upvoted 2 times

G4ct756 3 years, 1 month ago

Non-interesting fields, are listed in the All-Fields option window.

upvoted 1 times

igweifeanyi 3 years, 1 month ago

the answer is C for sure

upvoted 1 times

Joker20 4 years, 6 months ago

C , check page 79

upvoted 2 times

kr57 4 years, 9 months ago

C is correct

upvoted 4 times

Cameron808 4 years, 11 months ago

This question is so vague...i would guess C also

upvoted 1 times

kbisht 4 years, 11 months ago

I guess the ans is C

upvoted 3 times

Question #64 *Topic 1*

When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event.

B. A field that appears in every event.

C. A field that appears in the top 10 events.

D. A field that appears in at least 20% of the events.

Suggested Answer: *D*
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch

marianex Most Recent 1 year, 9 months ago

D, page 79

upvoted 1 times

Question #65 *Topic 1*

When a Splunk search generates calculated data that appears in the Statistics tab, in what formats can the results be exported?

A. CSV, JSON, PDF

B. CSV, XML, JSON

C. Raw Events, XML, JSON

D. Raw Events, CSV, XML, JSON

Suggested Answer: *B*

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Exportsearchresults

Community vote distribution

B (100%)

Asirpa Highly Voted 4 years, 8 months ago

The key word here is Statistics Tab. According to the Splunk Documentation: "If the search generates calculated data that appears on the Statistics tab, you cannot export using the Raw Events format." PDF is only available for saved searches. Therefore, the answer is B.
https://docs.splunk.com/Documentation/Splunk/8.1.0/Search/ExportdatausingSplunkWeb

upvoted 11 times

AMRIT475 Highly Voted 5 years ago

B. CSV, XML, JSON

upvoted 5 times

SnakeTech Most Recent 1 year, 9 months ago

B is correct. For Raw Évents : "If the search generates calculated data that appears on the Statistics tab, you cannot export using the Raw Events format. "

upvoted 1 times

viciousbeast 2 years, 1 month ago

Answer is D. The dropdown for formats include Raw Events, CSV, XML, & JSON.

upvoted 1 times

igweifeanyi 3 years, 1 month ago

the sure answer is B

upvoted 1 times

Himadhar1997 3 years, 2 months ago

Supported export formats answer will be different based on the question asked see the conditions below: You can export Splunk data into the following formats: Raw Events (for search results that are raw events and not calculated fields) CSV JSON XML PDF (for saved searches, using Splunk Web)

upvoted 2 times

jubi 3 years, 6 months ago

Ans is B If the search generates calculated data that appears on the Statistics tab, you cannot export using the Raw Events format.

upvoted 1 times

thepebble_97 4 years, 1 month ago

PAGE 72 IN FUND 1 - D

upvoted 3 times

GDanger 4 years, 5 months ago

72 PDF - D

upvoted 1 times

TeeCeeP 4 years, 9 months ago

tested ANS = B

upvoted 4 times

asultan20 4 years, 9 months ago

C is the correct answer.

upvoted 1 times

stallone 5 years ago

Raw Events (for search results that are raw events and not calculated fields) CSV JSON XML PDF (for saved searches, using Splunk Web)

upvoted 4 times

Question #66 *Topic 1*

Which search matches the events containing the terms `error` and `fail`?

A. index=security Error Fail

B. index=security error OR fail

C. index=security ɹ€error failureɹ€

D. index=security NOT error NOT fail

Suggested Answer: *B*

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Search

Community vote distribution

A (100%)

hashed_pony Most Recent 1 year, 8 months ago

Admin please fix these errors. At this point I'm scared of failing the exam because you keep flagging the wrong answers as the right ones.

upvoted 4 times

Khuli_Dolly 1 year, 11 months ago

Admin, please fix these errors

upvoted 3 times

BrynnML 2 years, 1 month ago

A is correct because the Boolean expression "AND" is implied between 2 search terms. (so doesn't need to be written here

upvoted 4 times

Inimitable 2 years, 5 months ago

A because this search is not case sensitive.

upvoted 2 times

Archu88 2 years, 6 months ago

A looks correct

upvoted 1 times

Sunsil 2 years, 8 months ago

A is correct

upvoted 1 times

tandelmanish34 2 years, 9 months ago

The correct answer should be A

upvoted 2 times

foxx99 2 years, 10 months ago

A is correct

upvoted 1 times

SlyLamp 2 years, 11 months ago

The correct answer is A

upvoted 2 times

Question #67 *Topic 1*

Which of the following is an option after clicking an item in search results?

A. Saving the item to a report.

B. Adding the item to the search.

C. Adding the item to a dashboard.

D. Saving the Search to a JSON file.

Suggested Answer: *B*
Official Answer: B

A077 Most Recent 1 year, 10 months ago
B, page 61Fun1
upvoted 1 times

mikelord 3 years, 2 months ago
B is Correct
upvoted 2 times

Question #68 *Topic 1*

Which of the following fields is stored with the events in the index?

A. user

B. source

C. location

D. sourceIp

Suggested Answer: *B*
Reference: https://answers.splunk.com/answers/609626/is-there-a-way-to-check-if-makeresults-stored-the.html

mikelord Most Recent 2 years, 2 months ago

B is correct

upvoted 1 times

Question #69 *Topic 1*

Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

A. Save the search as a report and use it in multiple dashboards as needed.

B. Save the search as a dashboard panel for each dashboard that needs the data.

C. Save the search as a scheduled alert and use it in multiple dashboards as needed.

D. Export the results of the search to an XML file and use the file as the basis of the dashboards.

Suggested Answer: *D*

Reference: https://answers.splunk.com/answers/231429/can-i-have-multiple-panels-using-the-same-inline-s.html

Community vote distribution

A (100%)

labarcaremo635 Highly Voted 4 years, 8 months ago

Answer is A. Page 154 in PDF

upvoted 12 times

SnakeTech Most Recent 1 year, 9 months ago

AAAAAAAAAAAAAAAA

upvoted 4 times

TheRealSplunkie 2 years, 1 month ago

Running the report once is less taxing on Splunk when it is used in multiple dashboards.

upvoted 4 times

arthursabino20 2 years, 2 months ago

A is the correct

upvoted 1 times

Rider2053 2 years, 3 months ago

Answer is A

upvoted 2 times

Mobyd 2 years, 3 months ago

A but which PDF are people on about?

upvoted 4 times

Sunsil 2 years, 8 months ago

A is correct

upvoted 2 times

Requete 3 years, 3 months ago

A is correct

upvoted 2 times

Avah 4 years, 4 months ago

B is correct

upvoted 1 times

kr57 4 years, 9 months ago

A is correct

upvoted 2 times

Glat 4 years, 11 months ago

Answer is A

upvoted 3 times

oksey 4 years, 11 months ago

Ans is A

upvoted 4 times

Question #70 *Topic 1*

What does the following specified time range do?
earliest=-72h@h latest=@d

A. Look back 3 days ago and prior.

B. Look back 72 hours, up to one day ago.

C. Look back 72 hours, up to the end of today.

D. Look back from 3 days ago, up to the beginning of today.

Suggested Answer: *C*
Reference: https://answers.splunk.com/answers/149904/find-earliest-and-latest-event-per-day-for-a-time-range.html

Community vote distribution
D (100%)

stallone Highly Voted 6 years ago
D is correct. It's always beginning of the day, not end of the day.
upvoted 10 times

fa03337 Most Recent 2 years, 1 month ago
It's D
upvoted 1 times

Lonny 2 years, 8 months ago
It's D
upvoted 1 times

SnakeTech 2 years, 9 months ago
Correction ?
upvoted 1 times

Khuli_Dolly 2 years, 11 months ago
the @ always snaps at the beginning of the specified period
upvoted 2 times

Sunsil 3 years, 8 months ago
D is correct
upvoted 3 times

Requete 4 years, 3 months ago
D is correct.
upvoted 3 times

ademide2 4 years, 11 months ago
C is correct, @d means day, so we want the day inclusive
upvoted 1 times

Joker20 5 years, 6 months ago
D , check PDF 65
upvoted 1 times

Nanila 5 years, 8 months ago
D is correct
upvoted 1 times

labarcaremo635 5 years, 8 months ago
D is correct, page 65 from PDF
upvoted 2 times

bigmills 5 years, 9 months ago
Who sat for this exam recently?
upvoted 3 times

asultan20 5 years, 9 months ago

D is correct.

upvoted 2 times

sangramrelekar 6 years ago

D is correct

upvoted 3 times

parelo 6 years, 1 month ago

D is right @month for the beginning of the month -- will be the same for day

upvoted 3 times

nonee125 6 years, 2 months ago

D is correct

upvoted 4 times

Question #71 *Topic 1*

Which events will be returned by the following search string? host=www3 status=503

A. All events that either have a host of www3 or a status of 503.

B. All events with a host of www3 that also have a status of 503.

C. We need more information; we cannot tell without knowing the time range.

D. We need more information; a search cannot be run without specifying an index.

Suggested Answer: *B*
Reference: https://answers.splunk.com/answers/617772/why-am-i-getting-a-http-503-error-when-using-threa.html

bmalin77 Most Recent 2 years ago
B. And is implied.
upvoted 1 times

saikkat7ghosh 2 years, 6 months ago
Answer: B
upvoted 1 times

Question #72 *Topic 1*

What does the stats command do?

A. Automatically correlates related fields.

B. Converts field values into numerical values.

C. Calculates statistics on data that matches the search criteria.

D. Analyzes numerical fields for their ability to predict another discrete field.

Suggested Answer: *C*
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Stats

marianex Most Recent 1 year, 9 months ago

C, page 120

upvoted 1 times