



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

Which search string only returns events from hostWWW3?

- A. host=\*
- B. host=WWW3
- C. host=WWW\*
- D. Host=WWW3

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **G4ct756** Highly Voted 3 years 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

🗳️ 👤 **RoopashreeKatarluRajappa24** Most Recent 3 months ago

Selected Answer: B

host=WWW3  
upvoted 1 times

🗳️ 👤 **techsdc** 4 months, 2 weeks ago

Selected Answer: B

B. host=WWW3  
For events ONLY, so Ans is b  
upvoted 1 times

🗳️ 👤 **splunker1211** 6 months, 2 weeks ago

Selected Answer: B

- 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** 7 months ago

Selected Answer: B

B. host=WWW3 is the right answer  
upvoted 1 times

🗳️ 👤 **Sankardevarajan1986** 1 year, 7 months ago

Ans : B host=WWW3  
upvoted 1 times

🗳️ 👤 **JH94** 1 year, 10 months ago

B is correct; field names are case sensitive, field values are not  
upvoted 1 times

🗳️ 👤 **cagdaskarabag** 2 years, 1 month ago

Selected Answer: B

correct answer: B  
upvoted 1 times

🗳️ 👤 **Adri300** 2 years, 2 months ago

Selected Answer: B

b is correct

upvoted 2 times

🗨️ 👤 **Nikhilfwd** 2 years, 5 months ago

B is the correct answer

upvoted 1 times

🗨️ 👤 **qtygbapjpesdayazko** 2 years, 7 months ago

**Selected Answer: B**

answer is correct

upvoted 1 times

🗨️ 👤 **qtygbapjpesdayazko** 2 years, 7 months ago

Is correct

upvoted 1 times

🗨️ 👤 **HUGOTE** 3 years, 5 months ago

B is the correct answer

upvoted 1 times

🗨️ 👤 **Royal7** 3 years, 10 months ago

B is the correct answer

upvoted 1 times

🗨️ 👤 **Alex\_Cyber\_Sec** 3 years, 12 months 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** 4 years, 3 months ago

B For sure

upvoted 2 times

🗨️ 👤 **labarcaremo635** 4 years, 7 months ago

B is correct. it asks for ONLY events from host WWW3

upvoted 1 times

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>

🗲️ 👤 **computernew** 3 weeks, 5 days ago

**Selected Answer: D**

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

upvoted 1 times

🗲️ 👤 **techsdc** 4 months, 2 weeks ago

**Selected Answer: A**

Lifetime is 10 min . Ans:A

upvoted 1 times

🗲️ 👤 **Sankardevarajan1986** 7 months, 3 weeks ago

Ans A 10 mins

upvoted 1 times

🗲️ 👤 **Nikhilfwd** 1 year, 5 months ago

10 min is the correct answer

upvoted 1 times

🗲️ 👤 **G4ct756** 2 years 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** 2 years, 5 months ago

is ok -

upvoted 1 times

🗲️ 👤 **nsisilya** 2 years, 6 months ago

Job default Lifetime is 10 minutes,

upvoted 1 times

🗲️ 👤 **Alex\_Cyber\_Sec** 2 years, 12 months ago

Lifetime 10min (page 69)

upvoted 1 times

🗲️ 👤 **bigmills** 3 years, 7 months ago

A For Sure

upvoted 3 times

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*

B (100%)

🗳️ 👤 **oksey** Highly Voted 4 years, 10 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 4 years, 8 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

🗳️ 👤 **vagabontx** Most Recent 7 months, 3 weeks ago

**Selected Answer: C**

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 1 times

🗳️ 👤 **Goncaloc29** 10 months ago

B and C  
upvoted 2 times

🗳️ 👤 **Splunkie007** 2 years ago

**Selected Answer: B**

B, C ( I think D is just optional)  
upvoted 2 times

🗳️ 👤 **maxxxx** 2 years, 2 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** 3 years ago

Under Prerequisites at the top , stated

"A lookup definition that you have defined previously."

upvoted 2 times

🗨️ 👤 **HUGOTE** 3 years, 5 months ago

B y C is the correct

upvoted 1 times

🗨️ 👤 **Janna05** 4 years, 3 months ago

A lookup definition that you have defined previously. IS B

upvoted 1 times

🗨️ 👤 **YPR77** 4 years, 4 months ago

Splunk fundamental page is 196 for Automatic Lookup

upvoted 1 times

🗨️ 👤 **mel101** 4 years, 6 months ago

B,C . 189 in pdf

upvoted 3 times

🗨️ 👤 **SGBEB** 4 years, 6 months ago

The answer is BC, slide 189 of Splunk Fundamentals 1

upvoted 3 times

🗨️ 👤 **labarcaremo635** 4 years, 7 months ago

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

upvoted 1 times

🗨️ 👤 **igorg** 4 years, 7 months ago

B, C, D

upvoted 2 times

🗨️ 👤 **bigmills** 4 years, 7 months ago

B For Sure

upvoted 1 times

🗨️ 👤 **alisyed** 4 years, 8 months ago

Apologies please ignore my previous comment. Correct answer is B.

The explanation from "oksey" is correct

upvoted 2 times

🗨️ 👤 **oksey** 4 years, 10 months ago

lookup file is optional. For instance, for KVlookup ypu don't really need lookup file

upvoted 3 times

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*

🗨️ 👤 **Vkah** 3 weeks, 5 days ago

**Selected Answer: B**

Forwarder

upvoted 1 times

🗨️ 👤 **Sankardevarajan1986** 7 months, 3 weeks ago

Ans : B

upvoted 1 times

🗨️ 👤 **G4ct756** 2 years 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** 2 years, 5 months ago

B is the im agree

upvoted 1 times

🗨️ 👤 **Janna05** 3 years, 3 months ago

B For Sure

upvoted 1 times

🗨️ 👤 **bigmills** 3 years, 7 months ago

C For Sure

upvoted 1 times

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

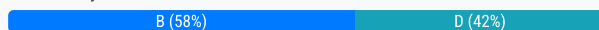
- A. All data accessible to the User role will appear in the report.
- B. All data accessible to the owner of the report will appear in the report.
- C. All data accessible to all users will appear in the report until the next time the report is run.
- D. The owner of the report can configure permissions 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 3 years, 9 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

**mirko1976** Most Recent 5 months, 3 weeks ago

**Selected Answer: B**

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** 6 months ago

**Selected Answer: B**

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** 10 months, 3 weeks ago

**Selected Answer: D**

D is correct.

As documentation says the owner can configure it either way

upvoted 2 times

**jb844** 1 year, 2 months ago

**Selected Answer: B**

"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

**aglopez** 1 year, 2 months ago



**Selected Answer: D**

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

upvoted 1 times

🗨️ **hamud\_tanvir** 1 year, 5 months ago

D is correct, slide 211 of Splunk Material

upvoted 1 times

🗨️ **philophobia** 1 year, 3 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** 1 year, 7 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** 1 year, 7 months ago

**Selected Answer: B**

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

upvoted 1 times

🗨️ **maxxxxx** 1 year, 8 months ago

IT IS BOTH C + D.

upvoted 1 times

🗨️ **solomone** 1 year, 9 months ago

**Selected Answer: D**

Creator sets the permissions

upvoted 1 times

🗨️ **paparulo** 1 year, 9 months ago

D, Agree

upvoted 1 times

🗨️ **carnage1970** 2 years, 5 months ago

**Selected Answer: B**

"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** 2 years, 5 months ago

**Selected Answer: D**

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

🗨️ **igweifeanyi** 2 years, 5 months ago

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

upvoted 2 times

🗨️ **G4ct756** 2 years, 6 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

🗨️ **HUGOTE** 2 years, 11 months ago

D. Im agree

upvoted 1 times

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*

*Community vote distribution*

B (100%)

🗲️ 👤 **SlyLamp** 10 months, 2 weeks ago

B = TRUE

upvoted 4 times

🗲️ 👤 **G4ct756** 1 year ago

**Selected Answer: B**

B.

upvoted 3 times

🗲️ 👤 **HUGOTE** 1 year, 5 months ago

B is the correct

upvoted 2 times

🗲️ 👤 **Alex\_Cyber\_Sec** 1 year, 12 months ago

B is correct. AND OR NOT

upvoted 4 times

🗲️ 👤 **JanBanan** 2 years, 3 months ago

B correct

upvoted 3 times

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%)

🗳️ 👤 **JokerRWild** 7 months, 4 weeks ago

**Selected Answer: B**

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** 1 year, 4 months ago

B-were the wrong answers

upvoted 1 times

🗳️ 👤 **amarachi\_amazone** 1 year, 5 months ago

B. That is the correct answer

upvoted 1 times

🗳️ 👤 **atonui** 1 year, 9 months ago

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

upvoted 2 times

🗳️ 👤 **HUGOTE** 1 year, 11 months ago

B is the correct

upvoted 2 times

🗳️ 👤 **Alex\_Cyber\_Sec** 2 years, 5 months ago

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

upvoted 3 times

🗳️ 👤 **mikelord** 2 years, 6 months ago

B is correct

upvoted 2 times

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**

Community vote distribution

B (100%)

🗳️ 👤 **Vkah** 3 weeks, 5 days ago

**Selected Answer: B**

Pipe should be in front of stats command  
upvoted 2 times

🗳️ 👤 **JokerRWild** 7 months, 4 weeks ago

**Selected Answer: B**

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** 1 year, 4 months ago

Could it B? I think it could.  
upvoted 1 times

🗳️ 👤 **amarachi\_amazone** 1 year, 5 months ago

B for sure  
upvoted 1 times

🗳️ 👤 **HUGOTE** 1 year, 11 months ago

B is the correct  
upvoted 1 times

🗳️ 👤 **Alex\_Cyber\_Sec** 2 years, 5 months ago

B for sure  
upvoted 1 times

🗳️ 👤 **mikelord** 2 years, 6 months ago

B is correct  
upvoted 1 times

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%)

🗳️ 👤 **JokerRWild** 9 months ago

**Selected Answer: A**

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** 1 year, 8 months ago

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

upvoted 1 times

🗳️ 👤 **SlyLamp** 2 years, 10 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

🗳️ 👤 **amarachi\_amazone** 2 years, 11 months ago

A is correct

upvoted 1 times

🗳️ 👤 **bob456Big** 3 years, 4 months ago

A is correct

upvoted 1 times

🗳️ 👤 **HUGOTE** 3 years, 5 months ago

A is the correct

upvoted 1 times

🗳️ 👤 **Alex\_Cyber\_Sec** 3 years, 12 months ago

A for sure

upvoted 1 times

🗳️ 👤 **mikelord** 4 years ago

A is Correct

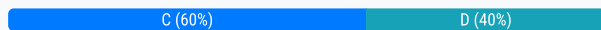
upvoted 1 times

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

Community vote distribution



**siddiquip** Highly Voted 4 years, 10 months ago

C&D both correct  
upvoted 14 times

**gith27** Highly Voted 4 years, 11 months ago

optionD is also correct i think. Ans C&D  
upvoted 9 times

**2dd1c50** Most Recent 1 week, 5 days ago

**Selected Answer: B**

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 month, 2 weeks ago

**Selected Answer: B**

BCD are correct option for this.  
upvoted 1 times

**mirko1976** 5 months, 3 weeks ago

**Selected Answer: B**

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** 9 months ago

**Selected Answer: C**

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** 1 year, 7 months ago

Answer is C

upvoted 1 times

🗲️ 👤 **Hurshbabe** 1 year, 10 months 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** 2 years, 3 months ago

B,C,D are all correct??

upvoted 1 times

🗲️ 👤 **Alexi2415** 2 years, 3 months ago

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

upvoted 2 times

🗲️ 👤 **hurryupfool123** 2 years, 6 months ago

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

upvoted 1 times

🗲️ 👤 **DePat** 2 years, 9 months ago

C&D. Keys: Drag and Modify

upvoted 4 times

🗲️ 👤 **phosphor** 2 years, 10 months ago

**Selected Answer: C**

C & D are both correct

upvoted 3 times

🗲️ 👤 **SlyLamp** 2 years, 10 months ago

C&D is the correct path, young Jedi.

upvoted 3 times

🗲️ 👤 **igweifeanyi** 2 years, 12 months ago

**Selected Answer: D**

C and D are the correct answers

upvoted 4 times

🗲️ 👤 **arcsrw** 3 years ago

C and D for sure, B is incorrect because that option is outside the "Edit" mode

upvoted 3 times

🗲️ 👤 **cagdaskarabag** 3 years, 1 month ago

C&D

tested & documentation reviewed.

upvoted 2 times

🗲️ 👤 **bmalin77** 3 years, 3 months ago

C and D are definitely right. B is tricky. You can't really "export the panel", but you can export the data to a CSV, so somewhat misleading.

upvoted 1 times

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

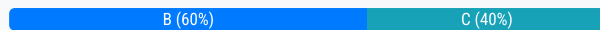
- A. Red
- B. Blue
- C. Orange
- D. Highlighted

**Suggested Answer:** C

Reference:

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

Community vote distribution



**JokerRWild** Highly Voted 2 years, 1 month ago

**Selected Answer: B**

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 3 weeks, 3 days ago

**Selected Answer: C**

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 month, 1 week ago

**Selected Answer: C**

Blue is command , Modifier is Orange

upvoted 2 times

**Dharam123** 1 month, 2 weeks ago

**Selected Answer: C**

Its orange--checked in splunk

upvoted 2 times

**anurag3011** 5 months ago

**Selected Answer: C**

C. Orange

upvoted 1 times

**EA88** 7 months, 3 weeks ago

C. Orange

upvoted 1 times

**teeec** 11 months, 1 week ago

C. Orange

upvoted 1 times



🗳️ 👤 **imnewtothis** 1 year, 3 months ago

**Selected Answer: C**

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](https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Parsingsearches#Color_codes)

Keyword modifiers and Boolean operators: Orange

upvoted 1 times

🗳️ 👤 **dickchappy** 1 year, 6 months ago

**Selected Answer: C**

Commands are blue, MODIFIERS to commands are orange.

upvoted 3 times

🗳️ 👤 **Xtian** 1 year, 8 months ago

B blue.

upvoted 1 times

🗳️ 👤 **SlyLamp** 2 years, 10 months ago

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

upvoted 3 times

🗳️ 👤 **amarachi\_amazone** 2 years, 11 months ago

C is the right one

upvoted 2 times

🗳️ 👤 **igweifeanyi** 2 years, 11 months ago

the right answer is B.

upvoted 1 times

🗳️ 👤 **HUGOTE** 3 years, 5 months ago

C is the correct

upvoted 2 times

🗳️ 👤 **Janna05** 4 years, 3 months ago

C is correct

BOOLEAN OPERATORS and

COMMAND MODIFIERS are in orange

upvoted 2 times

🗳️ 👤 **Joker20** 4 years, 4 months ago

Boolean and command modifiers : Orange

upvoted 3 times

🗳️ 👤 **SpTester** 4 years, 5 months ago

Orange indeed. Fun1 PDF page 101

upvoted 3 times

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 2 years, 10 months ago

C. Remember the acronym is GOD.

upvoted 7 times

🗲️ 👤 **StudyBuddy\_** 9 months, 3 weeks ago

The ending of the words is ALMSIVI.

upvoted 1 times

🗲️ 👤 **Steve2610** Most Recent 2 years, 11 months ago

Selected Answer: C

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

upvoted 1 times

🗲️ 👤 **HUGOTE** 3 years, 5 months ago

C is the correct

upvoted 1 times

🗲️ 👤 **tintin\_** 3 years, 8 months ago

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

upvoted 1 times

🗲️ 👤 **Janna05** 4 years, 3 months ago

C is correct

For example, you can create something simple like this:

– <group>\_<object>\_<description>

upvoted 3 times

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 4 years, 10 months 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

🗳️ 👤 **Mahmoudhi** 4 years ago

Exactly

upvoted 6 times

🗳️ 👤 **linux\_programmer46** 3 years ago

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

upvoted 4 times

🗳️ 👤 **Janna05** Highly Voted 4 years, 3 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 7 months ago

Selected Answer: A

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** 1 year, 12 months ago

Its A, Page 70 of Splunk official guide

upvoted 2 times

🗳️ 👤 **WhalerTom** 2 years, 3 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗳️ 👤 **Gabbyx** 2 years, 4 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** 2 years, 10 months ago

A is the one you want to go for

upvoted 2 times

🗨️ 👤 **amarachi\_amazone** 2 years, 11 months ago

A is correct

upvoted 3 times

🗨️ 👤 **G4ct756** 3 years ago

**Selected Answer: A**

<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** 3 years, 1 month ago

**Selected Answer: A**

A is correct, you have to schedule a report.

upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 1 month ago

**Selected Answer: A**

The keyword is 7 days.

upvoted 4 times

🗨️ 👤 **HUGOTE** 3 years, 5 months ago

A is correct

upvoted 3 times

🗨️ 👤 **g0nes03** 4 years, 7 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** 4 years, 7 months ago

A is correct, page 70 from PDF

upvoted 1 times

🗨️ 👤 **alisyed** 4 years, 8 months ago

Page 70.. PDF File

Answer is A

upvoted 3 times

🗨️ 👤 **kbisht** 4 years, 10 months ago

A is correct ans

upvoted 2 times

🗨️ 👤 **razzorb** 4 years, 11 months ago

Select Edit Job Settings to display the Job Settings.

upvoted 2 times

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**

*Community vote distribution*

A (100%)

🗲️ 👤 **Janna05** Highly Voted 👍 3 years, 3 months ago

A is correct, pag 92 • Filter as early as possible  
upvoted 5 times

🗲️ 👤 **sc0ne** Most Recent 🕒 1 year ago

Selected Answer: A

Filtering early limits the amount of events your other operations will have to process, improving efficiency  
upvoted 1 times

🗲️ 👤 **G4ct756** 2 years ago

Selected Answer: A

<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** 2 years ago

A is correct  
upvoted 2 times

🗲️ 👤 **HUGOTE** 2 years, 5 months ago

A is the correct  
upvoted 2 times

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>

🗨️ 👤 **Janna05** Highly Voted 4 years, 3 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** 2 years, 12 months 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 3 weeks, 3 days ago

Selected Answer: C

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** 4 months, 2 weeks ago

Selected Answer: C

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** 5 months ago

Selected Answer: B

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** 6 months, 3 weeks ago

Selected Answer: C

The Answer is C

Ignore the previous comment, the keyword is based on the report

upvoted 2 times

🗨️ 👤 **cyberWoof** 6 months, 3 weeks ago

Selected Answer: A

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** 3 years, 5 months ago

C is correct

upvoted 1 times

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**

Community vote distribution

D (90%)

10%

 **DaddyP** Highly Voted 4 years, 9 months ago

Top Command has common constraints that can be remembered as LCS (Limit, Countfield, Showperc).  
upvoted 11 times

 **amrit12345** Highly Voted 4 years, 11 months ago

D  
Ref - <https://docs.splunk.com/Documentation/SplunkCloud/8.0.2004/SearchReference/Top>  
upvoted 10 times

 **2dd1c50** Most Recent 3 weeks, 3 days ago

**Selected Answer: B**

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** 5 months, 3 weeks ago

**Selected Answer: B**

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** 8 months, 3 weeks 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** 1 year, 3 months ago

Syntax: countfield=<string> | limit=<int> | otherstr=<string> | percentfield=<string> | showcount=<bool> | showperc=<bool> | useother=<bool>

upvoted 1 times

  **m\_s\_** 2 years, 2 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

  **sc0ne** 2 years ago



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

upvoted 1 times

  **z3phyr** 1 year, 7 months ago

I think you mean the answer is A...

upvoted 1 times

  **z3phyr** 1 year, 7 months ago

Bruh moment. Answer is definitely D.

upvoted 1 times

  **Alexi2415** 2 years, 3 months ago



common constraints ..should be A ???

upvoted 1 times

  **Alexi2415** 2 years, 3 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** 2 years, 11 months ago

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

upvoted 1 times

  **Steve2610** 2 years, 11 months 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** 2 years, 9 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** 3 years ago

**Selected Answer: D**

limit, showperc, countfield are valid options for Top

upvoted 1 times

  **linux\_programmer46** 3 years ago

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



upvoted 1 times

  **cagdaskarabag** 3 years, 1 month ago

**Selected Answer: D**

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

upvoted 2 times

  **emlch** 3 years, 1 month ago

**Selected Answer: D**


D

The others are present on top command but used other syntax.

The options available are: countfield=<string>, limit=<int>, otherstr=<string> (boolean to allow or string to name the column), percentfield=<string> or showperc=false... a.o.

<https://docs.splunk.com/Documentation/SplunkCloud/8.2.2202/SearchReference/Top>



upvoted 1 times

  **[Removed]** 3 years, 1 month ago

**Selected Answer: D**

please refer to <https://docs.splunk.com/Documentation/SplunkCloud/8.2.2202/SearchReference/Top>

upvoted 2 times

  **andycondeg** 3 years, 2 months ago

**Selected Answer: D**

answer D

upvoted 3 times

  **HUGOTE** 3 years, 5 months ago

Yes, D is Correct

upvoted 2 times

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

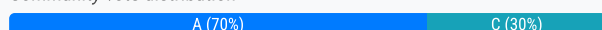
- A. Line charts are optimal for single and multiple series.
- B. Line charts are optimal for single series when using Fast mode.
- C. Line charts are optimal for multiple series with 3 or more columns.
- D. Line charts are optimal for multiseriess searches with at least 2 or more columns.

**Suggested Answer: C**

Reference:

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

Community vote distribution



🗳️ 👤 **nonee125** Highly Voted 5 years ago

A is Correct

upvoted 9 times

🗳️ 👤 **Chakhak** Most Recent 11 months, 3 weeks 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** 1 year, 3 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** 1 year, 6 months ago

A is correct

upvoted 1 times

🗳️ 👤 **DevilJewels** 1 year, 7 months ago

A is Correct

upvoted 1 times

🗳️ 👤 **TheRealSplunkie** 1 year, 11 months ago

Selected Answer: A

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

"Typically, line or area charts represent multiple series."

upvoted 1 times

🗳️ 👤 **Huslayer** 1 year, 11 months ago

A is the best answer

upvoted 1 times

🗳️ 👤 **BrynnML** 1 year, 12 months 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

🗳️ 👤 **imnewtothis** 1 year, 3 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** 1 year, 12 months ago

\*need to

upvoted 2 times

🗄️ 👤 **Steve2610** 2 years, 11 months ago

**Selected Answer: A**

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** 3 years ago

**Selected Answer: A**

"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** 3 years, 1 month 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** 3 years, 1 month ago

**Selected Answer: A**

A is correct

upvoted 3 times

🗄️ 👤 **Requete** 3 years, 1 month ago

**Selected Answer: A**

A is Correct

upvoted 3 times

🗄️ 👤 **[Removed]** 3 years, 1 month ago

**Selected Answer: C**

The keyword is "optimal." Line charts are typically used for multiple data series.

upvoted 4 times

🗄️ 👤 **Cheroti** 3 years, 3 months ago

**Selected Answer: A**

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

upvoted 2 times

🗄️ 👤 **Benny\_On** 3 years, 4 months ago

**Selected Answer: A**

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** 3 years, 4 months ago

**Selected Answer: C**

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

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

*Community vote distribution*

C (100%)

  **Janna05** Highly Voted 1 year, 9 months ago

C is correct

pag 58 Displayed in reverse chronological order (newest first)

upvoted 6 times

  **emlch** Most Recent 7 months, 2 weeks ago

**Selected Answer: C**

C for sure



upvoted 3 times

  **Safra** 7 months, 3 weeks ago

**Selected Answer: C**

C is correct

upvoted 2 times

  **HUGOTE** 11 months, 2 weeks ago

C is OK

upvoted 2 times

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

Community vote distribution

D (100%)

🗳️ 👤 **akamit225** 1 year, 1 month 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** 10 months, 3 weeks ago

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

upvoted 2 times

🗳️ 👤 **m\_s\_** 8 months ago

Name can indeed be edited.

upvoted 1 times

🗳️ 👤 **emlch** 1 year, 7 months ago

**Selected Answer: D**

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

upvoted 2 times

🗳️ 👤 **HUGOTE** 1 year, 11 months ago

D is correct

upvoted 1 times

🗳️ 👤 **Janna05** 2 years, 9 months ago

D is correct

upvoted 3 times

🗳️ 👤 **rakusu** 2 years, 11 months ago

D confirmed

upvoted 1 times

🗳️ 👤 **labarcaremo635** 3 years, 1 month ago

Tested, I say D

upvoted 1 times

🗳️ 👤 **TeeCeeP** 3 years, 1 month ago

I tested it out and say D

upvoted 3 times

🗳️ 👤 **thinhtin** 3 years, 1 month ago

Is it B or D?

upvoted 1 times

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>

🗲️ 👤 **udontknow** 6 months ago

**Selected Answer: B**

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 schedule, NOT 'when certain conditions are met'.  
upvoted 1 times

🗲️ 👤 **HUGOTE** 11 months, 2 weeks ago

D. Triggering an alert in your Splunk instance when certain conditions are met.  
upvoted 2 times

🗲️ 👤 **amar\_scorpio** 1 year, 4 months ago

A, as alert can trigger action not scheduled report. You can have an alert action as scheduled report  
upvoted 3 times

🗲️ 👤 **Janna05** 1 year, 9 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** 1 year, 11 months 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** 2 years, 1 month ago

I think it is meant to say "action" and not "report"  
upvoted 4 times

🗲️ 👤 **iguessillsignup** 2 years, 1 month ago

I meant to say "alert" not "report"  
upvoted 2 times

🗲️ 👤 **gcalcaterra** 2 years, 2 months ago

It can triggers an alert when the report run  
upvoted 1 times

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

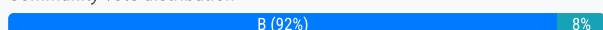
- A. Executes a new search.
- B. Filters current search results.
- C. Moves to past or future events.
- D. Expands the time range of the search.

**Suggested Answer: C**

Reference:

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

Community vote distribution



nonee125 **Highly Voted** 4 years, 6 months ago

B is CORRECT.

upvoted 18 times

stallone **Highly Voted** 4 years, 5 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** 1 year ago

B is the right answer

upvoted 1 times

DevilJewels 1 year, 1 month 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 1 year, 5 months ago

**Selected Answer: B**

B Is correct !!!

upvoted 1 times

foxx99 2 years, 2 months ago

**Selected Answer: B**

It's B

upvoted 3 times

kennethbrown4542 2 years, 4 months ago

**Selected Answer: B**

B is correct.

upvoted 2 times

Steve2610 2 years, 5 months ago

**Selected Answer: B**

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 2 years, 6 months ago

**Selected Answer: B**

"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** 2 years, 7 months ago

**Selected Answer: B**

How do you have data to search from the Future!

upvoted 6 times

🗨️ 👤 **Requete** 2 years, 7 months ago

**Selected Answer: B**

B is CORRECT.

upvoted 4 times

🗨️ 👤 **[Removed]** 2 years, 8 months ago

**Selected Answer: B**

"Mouse over and click on one of the bars or drag your mouse over a cluster of bars in the timeline. The events list updates to display only the events that occurred in that selected time range. The time range picker also updates to the selected time range."

upvoted 2 times

🗨️ 👤 **mansamusa** 2 years, 10 months ago

**Selected Answer: D**

answer is D. TESTED

upvoted 2 times

🗨️ 👤 **RaTix** 3 years, 6 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** 3 years, 9 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** 3 years, 9 months ago

I SAY B IS CORRECT

upvoted 1 times

🗨️ 👤 **TeeCeeP** 4 years, 1 month ago

page 67, slide show. B

upvoted 1 times

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*

🗉 👤 **linux\_programmer46** 11 months ago

C is correct, it is InputLookup  
upvoted 3 times

🗉 👤 **Janna05** 2 years, 2 months ago

C is correct pag 191  
Use the inputlookup command to load the results from a specified static lookup  
upvoted 4 times

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

  **JanBanan** Highly Voted 3 years, 9 months ago

C correct



upvoted 5 times

  **XiomaraRoRod** Most Recent 1 year 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** 2 years, 11 months ago

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

upvoted 3 times

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 1 year, 5 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 9 months, 4 weeks 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

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>

  **Janna05** Highly Voted 4 years, 3 months ago

C is correct

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

upvoted 6 times



  **udontknow** Most Recent 6 months ago

**Selected Answer: C**

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** 6 months, 4 weeks ago

**Selected Answer: B**

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** 1 year, 6 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** 2 years, 2 months ago

C is the right answer

upvoted 2 times

  **HUGOTE** 3 years, 5 months ago

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

upvoted 3 times

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

*Community vote distribution*

C (100%)

🗳️ 👤 **sedative** 1 year, 2 months ago

**Selected Answer: C**

yo it's C frfr no cap bet on G0d

upvoted 1 times

🗳️ 👤 **rome981** 11 months, 2 weeks ago

shut up!!!!

upvoted 2 times

🗳️ 👤 **Martin\_SS** 2 years, 2 months ago

C is correct ✓

upvoted 1 times

🗳️ 👤 **igweifeanyi** 2 years, 5 months ago

C is correct

upvoted 1 times

🗳️ 👤 **Leinnad** 2 years, 11 months ago

C is right

upvoted 2 times

🗳️ 👤 **mikelord** 3 years, 6 months ago

C is Correct

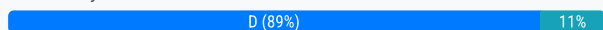
upvoted 3 times

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**

Community vote distribution



**nonee125** Highly Voted 4 years ago

D is correct

upvoted 12 times

**amrit12345** Highly Voted 3 years, 11 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."

"D"

upvoted 8 times

**TheRealSplunkie** Most Recent 11 months, 2 weeks ago

**Selected Answer: D**

"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** 1 year, 2 months ago

My vote is C.

What makes D a benefit? Frankly, C is the only benefit in the multiple choices.

upvoted 1 times

**SH\_N** 9 months, 2 weeks ago

Dashboard can have multiple panels that can have multiple searches.

upvoted 1 times

**SH\_N** 9 months, 2 weeks ago

so it's not true to say "it only has to run one search string."

upvoted 2 times

**m\_s\_** 1 year, 2 months ago

**Selected Answer: C**

Both C and D are correct

upvoted 1 times

**dreamnet** 1 year, 3 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

**Sunsil** 1 year, 6 months ago

D is correct

upvoted 1 times

**igweifeanyi** 1 year, 12 months ago

D is correct

upvoted 1 times

☒  **Solemn\_Tornado** 1 year, 12 months ago

**Selected Answer: D**

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

upvoted 1 times

☒  **cagdaskarabag** 2 years, 1 month ago

**Selected Answer: D**

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

upvoted 2 times

☒  **Himadhar1997** 2 years, 1 month ago

D is correct answer


upvoted 1 times

☒  **Benny\_On** 2 years, 4 months ago

**Selected Answer: D**

"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** 2 years, 8 months ago

D without question

upvoted 1 times

☒  **Tinus5135** 2 years, 10 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** 3 years, 3 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** 3 years, 5 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** 3 years, 5 months ago

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

upvoted 3 times

☒  **bpasquale42** 3 years, 7 months ago

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

upvoted 4 times



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** 5 years ago

B is correct

upvoted 15 times

Cyde **Most Recent** 1 year ago

B - index (is the correct answer)

"By default, host, source, and sourcetype are displayed under Selected Fields"

upvoted 1 times

Lonny 1 year, 6 months ago

B is correct

upvoted 1 times

TheRealSplunkie 1 year, 11 months ago

**Selected Answer: B**

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

upvoted 3 times

Huslayer 1 year, 11 months ago

**Selected Answer: B**

Index is the correct answer, try it out!!

upvoted 1 times

Sunsil 2 years, 6 months ago

index is the correct answer

upvoted 1 times

Steve2610 2 years, 11 months ago

**Selected Answer: B**

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

upvoted 2 times

cagdaskarabag 3 years, 1 month ago

**Selected Answer: B**

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

upvoted 2 times

[Removed] 3 years, 1 month ago

**Selected Answer: B**

Host, source, and sourcetype are in the selected field section by default. Which leaves index for the interesting fields section right below on the sidebar.

upvoted 3 times

Cheroti 3 years, 3 months ago

**Selected Answer: B**

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

upvoted 1 times

🗨️ 👤 **rakusu** 4 years, 3 months ago

ANSWER IS B

upvoted 3 times

🗨️ 👤 **marty** 4 years, 5 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** 4 years, 6 months ago

It is ACD slide 60 of Splunk Fundamentals 1

upvoted 1 times

🗨️ 👤 **Nanila** 4 years, 7 months ago

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

upvoted 1 times

🗨️ 👤 **Nanila** 4 years, 7 months ago

This question is confusing. Interesting 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 field is at least 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

🗨️ 👤 **SpTester** 4 years, 5 months ago

It would have been. if that is multiple questions. It is a trick question however. And that 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** 4 years, 8 months ago

SELECTED FIELDS

host 2

source 2

sourcetype

Answer is B. Index doesn't fall under selected field.

upvoted 3 times

🗨️ 👤 **sid2051** 4 years, 10 months ago

index is correct answer

upvoted 2 times

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** 1 year ago

**Selected Answer: B**

B - Field names ARE case sensitive; field values are NOT (is the correct answer)  
upvoted 1 times

🗲️ 👤 **rashidsahito** 2 years, 8 months ago

src\_ip=" " is correct. SRC\_IP=" " is wrong  
upvoted 2 times

🗲️ 👤 **[Removed]** 3 years, 1 month ago

**Selected Answer: B**

refer to <https://docs.splunk.com/Documentation/SplunkCloud/latest/SearchTutorial/Usefieldstosearch>  
upvoted 2 times

🗲️ 👤 **Janna05** 4 years, 3 months ago

B is correct  
pag 84 Field names ARE case sensitive; field values are NOT  
upvoted 4 times

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 1 year, 1 month 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 11 months, 2 weeks ago

A is correct



upvoted 3 times

  **Janna05** 1 year, 9 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** 1 year, 9 months ago

WHY NOT D?

upvoted 1 times

  **SecurityPaul** 1 year, 6 months ago

Probably because of the language used. The specific term "least common" is the answer they want.

upvoted 1 times



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**  1 year, 5 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/<AppName>/bin/scripts

upvoted 8 times

  **JanBanan**  9 months, 3 weeks ago

A correct

upvoted 3 times



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** 9 months, 3 weeks ago

C correct

upvoted 1 times

  **amrit12345** 1 year, 5 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

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**

Community vote distribution

B (100%)

🗳️ 👤 **gabo1969** Highly Voted 5 years ago

Only list, not count, B iws correct  
upvoted 7 times

🗳️ 👤 **gabo1969** Highly Voted 5 years ago

In the curse Fundamentals 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 1 year ago

**Selected Answer: B**

B - Lists unique values of a given field (is the correct answer)  
"only list, not count"  
upvoted 1 times

🗳️ 👤 **Lonny** 1 year, 6 months ago

It's B  
upvoted 1 times

🗳️ 👤 **Sunsil** 2 years, 6 months ago

B is correct  
upvoted 1 times

🗳️ 👤 **yawdeals** 2 years, 8 months ago

B is the correct answer  
upvoted 2 times

🗳️ 👤 **aguilard** 2 years, 8 months ago

**Selected Answer: B**

B is correct  
upvoted 1 times

🗳️ 👤 **osakalocka** 2 years, 11 months ago

B is correct  
upvoted 1 times

🗳️ 👤 **G4ct756** 2 years, 11 months ago

**Selected Answer: B**

<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** 3 years, 1 month 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

  **igweifeanyi** 2 years, 12 months ago

its page 162. B is correct. only list

upvoted 1 times



  **emlch** 3 years, 1 month ago

**Selected Answer: B**

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** 3 years, 3 months ago

**Selected Answer: B**

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

upvoted 1 times

  **Janna05** 4 years, 3 months ago

B is correct



pag 120 list – lists all values of a given field

upvoted 1 times

  **bpasquale42** 4 years, 7 months ago


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

upvoted 1 times

  **Nanila** 4 years, 7 months ago

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

upvoted 1 times

  **Nanila** 4 years, 7 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** 4 years, 7 months ago

B is correct, page 129 of PDF

upvoted 2 times



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)



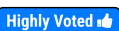
**Suggested Answer: A**

Reference:

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

Community vote distribution

A (100%)

  **amrit12345**  2 years, 11 months 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**  8 months ago

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

upvoted 1 times

  **G4ct756** 11 months, 4 weeks ago

 **Selected Answer: A**

<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** 2 years, 3 months ago

A is correct


pag 120 distinct\_count, dc – returns a count of unique values for a given field

upvoted 1 times

  **SpTester** 2 years, 5 months ago

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

upvoted 3 times

  **Nanila** 2 years, 7 months ago

A or B is correct

upvoted 1 times

  **msn\_aden** 1 year, 8 months ago

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

upvoted 2 times

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

🗨️ 👤 **HUGOTE** 11 months, 2 weeks ago

is correct

upvoted 1 times

🗨️ 👤 **marianex** 1 year, 7 months ago

A, page 9

upvoted 1 times

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**

🗨️ 👤 **Darren4737** 7 months, 1 week ago

it's actually 221 pg on the Splunk fundamental pdf  
upvoted 1 times

🗨️ 👤 **learner\_2022** 2 years ago

A is the answer according to me.  
upvoted 1 times

🗨️ 👤 **Janna05** 3 years, 3 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

🗨️ 👤 **Darren4737** 7 months, 1 week ago

it's actually 221 pg on the Splunk fundamental pdf  
upvoted 1 times

🗨️ 👤 **amksa** 2 years, 5 months ago

page 213 of which document please?  
upvoted 2 times

🗨️ 👤 **Stoops** 1 year, 6 months ago

Splunk-7-X-Fundamentals-Part-1-Presentation.pdf  
upvoted 1 times

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](https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Stats#1._Compare_the_difference_between_using_the_stats_and_chart_commands)

*Community vote distribution*

A (100%)

🗲️ 👤 **[Removed]** 8 months ago

**Selected Answer: A**

refer to <https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Stats>  
upvoted 1 times

🗲️ 👤 **Janna05** 1 year, 9 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

How do you add or remove fields from search results?

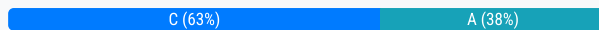
- A. Use field +to add and field -to remove.
- B. Use table +to add and table -to remove.
- C. Use fields +to add and fields -to remove.
- D. Use fields Plus to add and fields Minus to remove.

**Suggested Answer: C**

Reference:

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

Community vote distribution



🗳️ **Fred4N6** 10 months, 3 weeks ago

The minus symbol for the correct answer is not displayed correctly  
upvoted 1 times

🗳️ **Cyde** 1 year ago

**Selected Answer: C**

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** 1 year, 6 months ago

**Selected Answer: C**

fields + and fields - are used  
upvoted 1 times

🗳️ **ANki\_24** 1 year, 6 months ago

C is correct  
upvoted 1 times

🗳️ **dickchappy** 1 year, 6 months ago

**Selected Answer: C**

"field" is not a valid Splunk command, it's "fields"  
upvoted 1 times

🗳️ **jb844** 1 year, 8 months ago

**Selected Answer: C**

typo "fields-"  
upvoted 1 times

🗳️ **TheRealSplunkie** 1 year, 11 months ago

**Selected Answer: C**

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** 2 years, 3 months ago

use fields + to add  
fields - to minus ..tested  
upvoted 2 times

🗳️ **Alexi2415** 2 years, 3 months ago

fields - to remove\*\*  
upvoted 1 times

🗨️ 👤 **warlitos** 2 years, 4 months ago

**Selected Answer: C**

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

upvoted 4 times

🗨️ 👤 **Amish0123** 2 years, 5 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

🗨️ 👤 **Sunsil** 2 years, 6 months ago

A is the correct answer

upvoted 2 times

🗨️ 👤 **aguilard** 2 years, 8 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

🗨️ 👤 **Solemn\_Tornado** 2 years, 11 months 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** 2 years, 11 months 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** 2 years, 12 months ago

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

upvoted 3 times

🗨️ 👤 **millyb\_hig** 3 years, 2 months ago

I completely agree with jake7, fields - is to remove

upvoted 3 times

🗨️ 👤 **sathyaDeva** 3 years, 5 months ago

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

upvoted 4 times

🗨️ 👤 **jake7** 3 years, 8 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

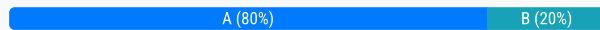
upvoted 3 times

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**

*Community vote distribution*



🗳️ **foxx99** 8 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗳️ **yawdeals** 1 year, 2 months ago

The answer is A

upvoted 2 times

🗳️ **shergar** 1 year, 3 months ago

**Selected Answer: A**

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** 1 year, 4 months ago

**Selected Answer: A**

A is right

upvoted 1 times

🗳️ **yaman778** 1 year, 4 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** 1 year, 4 months ago

A is right. You cannot click "Interesting Fields", however you can click "All Fields" and select field.

upvoted 1 times

🗳️ **BeckyC** 1 year, 6 months ago

A is correct

upvoted 2 times

🗳️ **qtygbapjpesdayazko** 1 year, 7 months ago

**Selected Answer: B**

Is not B?

upvoted 1 times

🗳️ **igweifeanyi** 1 year, 5 months ago

no its not

upvoted 2 times

🗳️ **Janna05** 2 years, 9 months ago

A is correct

PAG 82

upvoted 2 times

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


- A. #
- B. %
- C. a
- D. a#

**Suggested Answer:** C

  **spartello**  1 year, 4 months ago

The answer is C, a is alpha-numeric whereas # is just numeric  
upvoted 6 times

  **techsdc**  4 months, 1 week ago



 **Selected Answer: C**  
The character that typically denotes alphanumeric field values is C. a.  
Letter 'a' is used to represent alphanumeric values  
upvoted 1 times

  **raghavgulkarni** 7 months, 1 week ago

C is Correct  
upvoted 1 times

  **kjqhhdwheijoiw** 1 year, 5 months ago

a = string  
# = numeric  
% = alphanumeric So answer is B  
upvoted 4 times

  **SimonR2** 7 months, 2 weeks 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 categorizes the fields into these two categories here: <https://community.splunk.com/t5/Splunk-Search/Field-categorization/m-p/87018>  
upvoted 3 times

  **CC1123** 1 year, 6 months ago

It's C, pdf 79  
upvoted 4 times

  **Nanila** 1 year, 7 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** 1 year, 7 months ago

Has anyone seen % as the answer?  
upvoted 1 times



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**

Community vote distribution

C (100%)

AMRIT475 Highly Voted 3 years, 4 months ago

C is correct

upvoted 13 times

nonee125 Highly Voted 3 years, 6 months ago

C is correct

upvoted 11 times

Sunsil Most Recent 1 year ago

C is the correct answer

upvoted 2 times

TestingAccount900 1 year, 4 months ago

**Selected Answer: C**

C, is correct, I don't understand B would make sense in any way.

upvoted 2 times

Solemn\_Tornado 1 year, 5 months ago

**Selected Answer: C**

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 1 year, 6 months ago

**Selected Answer: C**

Answer is C

upvoted 2 times

cagdaskarabag 1 year, 7 months ago

**Selected Answer: C**

Hopefully someone will update the answer.

it's obvious that the answer is C!

upvoted 3 times

qtygbapjpesdayazko 1 year, 7 months ago

**Selected Answer: C**

Is C !!

upvoted 1 times

sathyaDeva 1 year, 11 months ago

C is the correct answer

upvoted 1 times

sathyaDeva 1 year, 11 months ago

C is Correct

upvoted 1 times

🗨️ 👤 **Tinus5135** 2 years, 4 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** 3 years 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** 3 years, 1 month ago

C is the correct answer

upvoted 4 times

🗨️ 👤 **Scott13183** 3 years, 4 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** 3 years, 4 months ago

C is correct

upvoted 4 times

🗨️ 👤 **stallone** 3 years, 5 months ago

C is correct.

upvoted 5 times

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*

🗨️ 👤 **2dd1c50** 2 weeks, 5 days ago

**Selected Answer: B**

The correct answer is: B. action=purchase ✓

📖 Explanation:

In Splunk search syntax, key/value pairs are written using the = sign  
upvoted 1 times

🗨️ 👤 **mikelord** 1 year ago

B is Correct

upvoted 1 times

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*

🗉 👤 **G4ct756** 11 months, 4 weeks ago  
<https://docs.splunk.com/Splexicon:Timerangepicker>  
upvoted 1 times

🗉 👤 **kr57** 2 years, 7 months ago  
B is correct  
upvoted 1 times

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**

Community vote distribution


A (100%)

 **stallone** Highly Voted 4 years, 11 months ago

A is correct answer. AND is the keyword here.  
upvoted 13 times

 **Fred4N6** Most Recent 10 months, 3 weeks ago

Why does it say the correct answer is C? If everyone says it is A ?  
upvoted 1 times

 **Lonny** 1 year, 6 months ago

A is the right answer  
upvoted 1 times


 **jayfourkay17** 1 year, 11 months ago

This is a badly worded question, I would have lost a point for this..  
upvoted 1 times

 **assfedassfinished** 2 years, 2 months ago

Selected Answer: A

It's still A  
upvoted 2 times

 **Sunsil** 2 years, 6 months ago

A is the correct answer  
upvoted 1 times

 **yawdeals** 2 years, 8 months ago

A is the correct Answer  
upvoted 1 times

 **osakalocka** 2 years, 11 months ago

A is correct based on the inclusive 'and'  
upvoted 1 times


 **Solemn\_Tornado** 2 years, 11 months ago

Selected Answer: A

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** 2 years, 11 months ago

A is the very right answer pls.  
upvoted 1 times

 **thefoque** 2 years, 11 months ago

Selected Answer: A

A is correct.  
upvoted 2 times

 **BeckyC** 3 years ago

Selected Answer: A

A is the correct answer  
upvoted 2 times

🗨️ 👤 **cagdaskarabag** 3 years, 1 month ago

Selected Answer: A

A! simple logic man.  
upvoted 3 times

🗨️ 👤 **Requete** 3 years, 1 month ago

Selected Answer: A

A is correct answer.  
upvoted 1 times

🗨️ 👤 **sathyaDeva** 3 years, 5 months ago

A is correct because if no Boolean is mentioned default AND will applicable  
upvoted 2 times

🗨️ 👤 **bpasquale42** 4 years, 6 months ago

A is correct.  
upvoted 3 times

🗨️ 👤 **kr57** 4 years, 7 months ago

A is correct  
upvoted 3 times

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**

Community vote distribution

D (61%)

A (39%)

🗳️ 👤 **SimonR2** Highly Voted 3 years, 7 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 2 years, 11 months ago

**Selected Answer: D**

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 than 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

🗳️ 👤 **2dd1c50** Most Recent 2 weeks, 5 days ago

**Selected Answer: D**

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** 8 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** 1 year, 11 months 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** 2 years, 1 month ago

**Selected Answer: A**

A is the correct answer.

upvoted 3 times

🗳️ 👤 **asarali** 2 years, 1 month ago

**Selected Answer: A**

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** 2 years, 4 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** 2 years, 11 months ago

**Selected Answer: D**

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** 3 years, 1 month ago

**Selected Answer: A**

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** 3 years, 1 month ago

**Selected Answer: A**

A is correct.

upvoted 1 times

🗳️ 👤 **Cheroti** 3 years, 3 months ago

**Selected Answer: D**

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

upvoted 1 times

🗳️ 👤 **atonui** 3 years, 3 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** 3 years, 11 months ago

A is correct. P.92

upvoted 3 times

🗳️ 👤 **H1\_** 4 years ago

100% sure dedup is correct

upvoted 1 times

🗳️ 👤 **Janna05** 4 years, 3 months ago

D is correct



pag 106 To include, use fields + (default)

– Occurs before field extraction

– Improves performance

upvoted 3 times



  **rakusu** 4 years, 3 months ago

A, NOT D

upvoted 1 times

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**

*Community vote distribution*

A (100%)

nonee125 **Highly Voted** 4 years, 6 months ago

A is correct  
upvoted 10 times

Lonny **Most Recent** 1 year ago

It's A  
upvoted 1 times

TheRealSplunkie 1 year, 5 months ago

**Selected Answer: A**  
DUH!!!!  
upvoted 1 times

Sunsil 2 years ago

**Selected Answer: A**  
A is correct  
upvoted 2 times

kiki533 2 years, 1 month ago

**Selected Answer: A**  
A correct  
upvoted 2 times

hawxxx 2 years, 4 months ago

**Selected Answer: A**  
A should be correct not sourcetype  
upvoted 3 times

arcs 2 years, 6 months ago

**Selected Answer: A**  
Its A, even the guy in the videos mention it a lot  
upvoted 2 times

cagdaskarabag 2 years, 7 months ago

time is the most efficient filter.  
upvoted 1 times

Cheroti 2 years, 9 months ago

**Selected Answer: A**  
Time is the most efficient filter, not sourcetype  
upvoted 1 times

sathyaDeva 2 years, 11 months ago

A is correct  
upvoted 1 times

DanielVA 2 years, 12 months ago

**Selected Answer: A**

A is correct



upvoted 1 times

  **Janna05** 3 years, 9 months ago

A is correct

pag 91 Time is the most efficient filter

upvoted 3 times

  **SpTester** 3 years, 12 months 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** 4 years ago



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

upvoted 1 times

  **vasanthi77** 1 year, 7 months ago

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

upvoted 1 times

  **kr57** 4 years, 1 month ago



A is correct

upvoted 1 times

  **asultan20** 4 years, 2 months ago

A is correct.

upvoted 1 times

  **alisyed** 4 years, 2 months ago

pAGE -91 PDF..

Answer is A

upvoted 1 times

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

🗨️ 👤 **2dd1c50** 2 weeks, 5 days ago

**Selected Answer: D**

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** 9 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** 2 years, 1 month ago

D is correct

upvoted 1 times

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** 1 week, 2 days ago

Selected Answer: B

Im currently on my splunk UI and you have the following options: CSV, XML, and JSON  
upvoted 1 times

🗳️ 👤 **oussa\_ama** 10 months, 2 weeks ago

Selected Answer: B

B is correct.  
upvoted 1 times

🗳️ 👤 **BrynnML** 1 year, 12 months ago

Selected Answer: B

XML/JSON/CSV  
upvoted 1 times

🗳️ 👤 **TestingAccount900** 2 years, 10 months ago

Selected Answer: B

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** 3 years, 1 month ago

B. Export file type options: csv, json, xml.  
upvoted 2 times

🗳️ 👤 **Cheroti** 3 years, 3 months ago

Selected Answer: B

B. Export file type options: csv, json, xml.  
upvoted 2 times

🗳️ 👤 **atonui** 3 years, 3 months ago

B. There are three file type options: csv, json, xml.  
upvoted 1 times

🗳️ 👤 **HUGOTE** 3 years, 5 months ago

B is correct JSON  
upvoted 2 times

🗳️ 👤 **sathyaDeva** 3 years, 5 months ago

B is right...because the options available are csv, json, xml  
upvoted 2 times

🗳️ 👤 **DanielVA** 3 years, 5 months ago

Selected Answer: B

B is correct JSON

upvoted 1 times

🗨️ 👤 **ayotundet** 3 years, 8 months ago

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

upvoted 1 times

🗨️ 👤 **nifasecu** 4 years ago

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

upvoted 3 times

🗨️ 👤 **Nanila** 4 years, 6 months ago

B is accurate

upvoted 1 times

🗨️ 👤 **SGBEB** 4 years, 6 months ago

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

upvoted 4 times

🗨️ 👤 **labarcaremo635** 4 years, 7 months ago

Answer is B, page 72 from PDF

upvoted 1 times

🗨️ 👤 **kr57** 4 years, 7 months ago

B is correct

upvoted 1 times

🗨️ 👤 **alisyed** 4 years, 8 months ago

B is correct

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

upvoted 2 times

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 =, <, or >

**Suggested Answer:** *D*

  **mikelord** 1 year ago

D is Correct

upvoted 1 times

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

- A. index=security failure | stats sum as 1Event Count1
- B. index=security failure | stats count as 1Event Count1
- C. index=security failure | stats count by 1Event Count1
- D. index=security failure | stats dc(count) as 1Event Count1

**Suggested Answer: C**

Community vote distribution

B (92%)

8%

  **shergar**  2 years, 3 months ago

**Selected Answer: B**


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**  8 months, 3 weeks ago

B is the correct

upvoted 1 times

  **b0d4564** 10 months, 2 weeks ago

**Selected Answer: C**

Looks like C to me

upvoted 1 times

  **Lonny** 1 year ago

It's B

upvoted 1 times

  **hashed\_pony** 1 year 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** 1 year, 2 months ago

**Selected Answer: B**

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

upvoted 1 times

  **sridevi3018** 1 year, 2 months ago

C is the correct answer...

upvoted 2 times

  **Sunsil** 2 years ago

**Selected Answer: B**

B is the correct answer

upvoted 2 times

  **Ufuk\_Ari** 2 years, 3 months ago

**Selected Answer: B**

Definitely B

upvoted 2 times



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**

Community vote distribution

C (100%)

sid2051 **Highly Voted** 3 years, 4 months ago

C is correct answer ,field name is case sensitive not values  
upvoted 10 times

nonee125 **Highly Voted** 3 years, 6 months ago

C is correct  
upvoted 8 times

loop3r\_11 **Most Recent** 7 months, 1 week ago

**Selected Answer: C**  
field names are sensitive not values  
upvoted 2 times

assfedassfinished 8 months ago

**Selected Answer: C**  
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 10 months, 3 weeks ago

**Selected Answer: C**  
C correct.  
field name (sourcetype) -> case sensitive  
field value (Acces\_Combined) -> NOT case sensitive  
upvoted 2 times

Sunsil 1 year ago

**Selected Answer: C**  
C is correct  
upvoted 1 times

M4L34 1 year, 5 months ago

**Selected Answer: C**  
Field name is case sensitive and field value is not  
upvoted 2 times

G4ct756 1 year, 5 months ago

**Selected Answer: C**  
field value is not case sensitive.  
upvoted 1 times

BeckyC 1 year, 6 months ago

**Selected Answer: C**  
Field name is case sensitive so the correct answer is C  
upvoted 1 times

Requete 1 year, 7 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

🗨️ 👤 **ITgmoney** 1 year, 9 months ago

C is correct

upvoted 1 times

🗨️ 👤 **HUGOTE** 1 year, 11 months ago

C is correct

upvoted 1 times

🗨️ 👤 **sathyaDeva** 1 year, 11 months ago

C because field names are case sensitive field values are not

upvoted 1 times

🗨️ 👤 **kr57** 3 years, 1 month ago

C is correct

upvoted 1 times

🗨️ 👤 **asultan20** 3 years, 2 months ago

C is correct.

upvoted 1 times

🗨️ 👤 **alisyed** 3 years, 2 months ago

C is correct

upvoted 1 times

🗨️ 👤 **stallone** 3 years, 5 months ago

C is correct. Field names are case sensitive.

upvoted 4 times

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**

Community vote distribution

C (93%)

7%


 **HUGOTE** Highly Voted 2 years, 5 months ago

C is correct. Wild cards are always expensive.  
upvoted 11 times

 **yukilee** Highly Voted 2 years, 3 months ago

**Selected Answer: C**

C is correct  
upvoted 5 times

 **2dd1c50** Most Recent 2 weeks, 5 days ago

**Selected Answer: C**

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** 6 months, 3 weeks 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** 7 months, 3 weeks ago

Another mistake, ExamTopics, could you please correct ...  
upvoted 1 times

 **kiuh** 1 year ago

C is the correct ans  
upvoted 1 times

 **Mr\_\_d\_\_** 1 year, 1 month ago

**Selected Answer: C**

C is correct  
upvoted 2 times

 **sjb0001** 1 year, 7 months ago

**Selected Answer: C**

Wildcards are very inefficient.

upvoted 2 times

🗨️ 👤 **ITgmoney** 2 years, 3 months ago

**Selected Answer: C**

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** 2 years, 7 months ago

**Selected Answer: A**

A is the right answer

upvoted 1 times

🗨️ 👤 **Iwoved** 2 years, 7 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** 3 years, 8 months ago

C is correct.

upvoted 2 times

🗨️ 👤 **sid2051** 3 years, 10 months ago

C should be correct as it is not using regex

upvoted 3 times

🗨️ 👤 **stallone** 3 years, 11 months ago

C is correct. Wild cards are always expensive.

upvoted 2 times

🗨️ 👤 **parelo** 4 years ago

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

upvoted 2 times

🗨️ 👤 **nonee125** 4 years ago



C is correct

upvoted 3 times

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*

  **marianex** 7 months, 1 week ago

B, page 134

upvoted 1 times

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

Community vote distribution

D (100%)

🗳️ 👤 **Janna05** Highly Voted 3 years, 3 months ago

D is correct

pag 42 Splunk applies defaults if not specified

upvoted 5 times

🗳️ 👤 **FrancoPepe** Most Recent 10 months, 2 weeks 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** 12 months ago

Selected Answer: D

D is correct

upvoted 2 times

🗳️ 👤 **Niketes** 1 year 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** 1 year, 4 months ago

A. Splunk 9 returns no event

upvoted 1 times

🗳️ 👤 **SimonR2** 2 years, 7 months ago

Just tested this and it returned all results from indexes I had access to. Answer is D.

upvoted 4 times

🗳️ 👤 **Sanket3** 3 years ago

D is correct it will take default index if not specified

upvoted 4 times

🗳️ 👤 **ShreeshKM** 3 years, 4 months ago

Answer is A. Splunk will not return any events.

upvoted 2 times

🗳️ 👤 **pabinajm** 3 years, 5 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** 3 years, 5 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** 3 years, 6 months ago

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

upvoted 2 times

  **alisyed** 3 years, 8 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** 3 years, 8 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** 2 years, 2 months ago

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

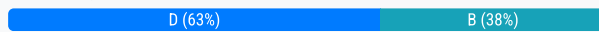
upvoted 1 times

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**

*Community vote distribution*



🗳️ **babusartop17** Highly Voted 2 years, 12 months 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 9 months, 2 weeks ago

I vote for B  
upvoted 1 times

🗳️ **SlyLamp** 1 year, 4 months ago

**Selected Answer: D**

Vote for D  
upvoted 1 times

🗳️ **ngthien041292** 1 year, 4 months ago

**Selected Answer: D**

Vote D  
upvoted 1 times

🗳️ **arcsu** 1 year, 6 months ago

**Selected Answer: D**

Is D, because you can't see detailed events in a visualization, if you clic on any event in a statistocs table you can choose the option "View events" wich is the same as drilldown underlying event  
upvoted 2 times

🗳️ **Osa\_** 1 year, 6 months ago

D is correct  
Cagdaskarabag is right  
upvoted 1 times

🗳️ **cagdaskarabag** 1 year, 7 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 3 times

🗳️ **Requete** 1 year, 7 months ago

**Selected Answer: B**

B is correct  
upvoted 2 times

🗳️ **[Removed]** 10 months, 3 weeks ago

No it's not. Visualizations will not show underlying events  
upvoted 1 times

🗳️ **Requete** 1 year, 7 months ago

**Selected Answer: B**

B is correct



upvoted 1 times

🗋️ 👤 **[Removed]** 1 year, 8 months ago

**Selected Answer: D**

refer to <https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Drilldownnonstatisticaltablerowsandcells>

upvoted 1 times

🗋️ 👤 **[Removed]** 1 year, 7 months ago

CORRECTION: The answer is B. "Statistics and visualizations allow you to drill down by default to see the underlying events."

upvoted 2 times

🗋️ 👤 **arcs\_w** 1 year, 6 months ago

Nope, that only means that Statistics and Visualizations are both capable of show you underlaying events, but the question is clear "If you ARE at statistics table", Visualization tab IS a different tab

upvoted 2 times

🗋️ 👤 **H1\_** 2 years, 6 months ago

b is 100%

upvoted 1 times

🗋️ 👤 **marianex** 2 years, 7 months ago

B, page 180 Fun1

upvoted 2 times

🗋️ 👤 **SpTester** 2 years, 12 months ago

D - page 158 Fun1 pdf

upvoted 3 times

🗋️ 👤 **Sab123** 2 years, 12 months ago

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

upvoted 2 times

🗋️ 👤 **Sravs\_24** 3 years ago

Correct Answer: B

upvoted 1 times

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*

A (100%)

🗳️ 👤 **Only12go** 1 month, 1 week ago

**Selected Answer: D**

D is correct answer from this doc

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

upvoted 1 times

🗳️ 👤 **SnakeTech** 7 months, 2 weeks ago

**Selected Answer: A**

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

upvoted 1 times

🗳️ 👤 **SnakeTech** 7 months, 2 weeks ago

125 not 123

upvoted 1 times

🗳️ 👤 **TheStudiosPeepz** 8 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** 10 months, 3 weeks ago

D is correct answer from this doc

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

upvoted 1 times

🗳️ 👤 **Derag** 1 year, 1 month 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

🗳️ 👤 **arcsnw** 2 years ago

**Selected Answer: A**

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 answer is A

upvoted 4 times

🗳️ 👤 **Himadhar1997** 2 years, 1 month ago

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

upvoted 1 times

🗲️ 👤 **cagdaskarabag** 2 years, 1 month ago

fundamentals 1 pdf, p224

time, fired alerts, app, type, severity, mode, actions (enterprise v7X)

answer is D

upvoted 1 times

🗲️ 👤 **Requete** 2 years, 1 month ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗲️ 👤 **CC1123** 3 years, 6 months ago

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

upvoted 4 times

🗲️ 👤 **PoundingCode** 2 years, 9 months ago

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

upvoted 1 times

🗲️ 👤 **Nanila** 3 years, 6 months ago

A is accurate

upvoted 1 times

🗲️ 👤 **Asirpa** 3 years, 7 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** 3 years, 7 months ago

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

upvoted 2 times

🗲️ 👤 **sid2051** 3 years, 10 months ago

A is correct

upvoted 1 times

🗲️ 👤 **Nanakj** 3 years, 10 months ago

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

upvoted 1 times

🗲️ 👤 **Nanakj** 3 years, 10 months ago

D is correct.

upvoted 2 times

🗲️ 👤 **stallone** 3 years, 11 months ago

A is correct.

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

upvoted 1 times

🗲️ 👤 **razzorb** 3 years, 11 months 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** 3 years, 11 months ago

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

upvoted 1 times



🗲️ 👤 **nonee125** 4 years ago

A is correct  
upvoted 2 times

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

  **Janna05** 9 months, 3 weeks ago

A is correct



pag 204 After the report is created, click Schedule

upvoted 3 times

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*

  **marianex** 7 months, 1 week ago

B,page 79

upvoted 1 times

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*

  **marianex** 7 months, 1 week ago

C, page 120

upvoted 1 times

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** 11 months, 2 weeks ago

is ok b

upvoted 1 times

🗨️ 👤 **marianex** 1 year, 7 months ago

B, page 199

upvoted 1 times



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

*Community vote distribution*

C (100%)

🗳️ 👤 **alisyed** Highly Voted 👍 3 years, 8 months ago

C is correct

Admin please start correcting the Errors !!

upvoted 15 times

🗳️ 👤 **Khuli\_Dolly** Most Recent 🕒 9 months, 3 weeks ago

Selected Answer: C

c is correct

upvoted 1 times

🗳️ 👤 **Rider2053** 1 year, 1 month ago

C is right answer

upvoted 1 times

🗳️ 👤 **warlitos** 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **igweifeanyi** 1 year, 11 months ago

C is very correct

upvoted 1 times

🗳️ 👤 **cagdaskarabag** 2 years, 1 month ago

Selected Answer: C

admin, wake up! fix those errors!

upvoted 3 times

🗳️ 👤 **DanielVA** 2 years, 5 months ago

Selected Answer: C

C is correct

upvoted 3 times

🗳️ 👤 **kr57** 3 years, 7 months ago

C is correct

upvoted 2 times

🗳️ 👤 **Glat** 3 years, 9 months ago

Answer is C

upvoted 3 times

🗳️ 👤 **gabo1969** 3 years, 11 months ago

I think that is C

Splunk say "Apply filtering commands as early as possible in your search"

upvoted 4 times

🗳️ 👤 **edev** 3 years, 11 months ago

isn't it C?

upvoted 3 times

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](https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Aboutsavingandsharingreports#Save_a_search_as_a_report)

  **mikelord** 1 year ago

A is Correct

upvoted 1 times

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/](https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/ExtractfieldsinteractivelywithIFX#Access_the_field_extractor_from_the_All_Fields_dialog_box)

[ExtractfieldsinteractivelywithIFX#Access\\_the\\_field\\_extractor\\_from\\_the\\_All\\_Fields\\_dialog\\_box](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** 12 months ago

**Selected Answer: C**

C is correct

upvoted 3 times

🗳️ 👤 **Amish0123** 1 year, 5 months ago

**Selected Answer: C**

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

upvoted 3 times

🗳️ 👤 **Sunsil** 1 year, 6 months ago

**Selected Answer: C**

C is correct option

upvoted 2 times

🗳️ 👤 **G4ct756** 1 year, 11 months ago

**Selected Answer: C**

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

upvoted 1 times

🗳️ 👤 **igweifeanyi** 1 year, 12 months ago

the answer is C for sure

upvoted 1 times

🗳️ 👤 **Joker20** 3 years, 4 months ago

C , check page 79

upvoted 2 times

🗳️ 👤 **kr57** 3 years, 7 months ago

C is correct

upvoted 4 times

🗳️ 👤 **Cameron808** 3 years, 9 months ago

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

upvoted 1 times

🗳️ 👤 **kbisht** 3 years, 10 months ago

I guess the ans is C

upvoted 3 times

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** 7 months, 1 week ago

D, page 79

upvoted 1 times

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 3 years, 7 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 3 years, 10 months ago

B. CSV, XML, JSON

upvoted 5 times

SnakeTech Most Recent 7 months, 2 weeks ago

**Selected Answer: B**

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

upvoted 1 times

viciousbeast 1 year ago

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

upvoted 1 times

igweifeanyi 1 year, 12 months ago

the sure answer is B

upvoted 1 times

Himadhar1997 2 years, 1 month 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 2 years, 4 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 3 years ago

PAGE 72 IN FUND 1 - D

upvoted 3 times

  **GDanger** 3 years, 3 months ago

72 PDF - D

upvoted 1 times

  **TeeCeeP** 3 years, 7 months ago



tested ANS = B

upvoted 4 times

  **asultan20** 3 years, 8 months ago

C is the correct answer.

upvoted 1 times

  **stallone** 3 years, 11 months 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

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 1error failure1
- 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** 6 months, 3 weeks 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** 9 months, 2 weeks ago

**Selected Answer: A**

Admin, please fix these errors  
upvoted 3 times

🗳️ **BrynnML** 12 months ago

**Selected Answer: A**

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** 1 year, 3 months ago

A because this search is not case sensitive.  
upvoted 2 times

🗳️ **Archu88** 1 year, 4 months ago

A looks correct  
upvoted 1 times

🗳️ **Sunsil** 1 year, 6 months ago

**Selected Answer: A**

A is correct  
upvoted 1 times

🗳️ **tandelmanish34** 1 year, 8 months ago

The correct answer should be A  
upvoted 2 times

🗳️ **foxx99** 1 year, 8 months ago

**Selected Answer: A**

A is correct  
upvoted 1 times

🗳️ **SlyLamp** 1 year, 9 months ago

**Selected Answer: A**

The correct answer is A  
upvoted 2 times



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*

🗨️ 👤 **A077** 8 months, 3 weeks ago

B, page 61Fun1

upvoted 1 times

🗨️ 👤 **mikelord** 2 years ago

B is Correct

upvoted 2 times

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-makerresults-stored-the.html>

  **mikelord** 1 year ago

B is correct

upvoted 1 times

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 3 years, 7 months ago

Answer is A. Page 154 in PDF

upvoted 12 times

🗲️ 👤 **SnakeTech** Most Recent 7 months, 2 weeks ago

Selected Answer: A

AAAAAAAAAAAAAAAAAAAA

upvoted 4 times

🗲️ 👤 **TheRealSplunkie** 11 months, 2 weeks ago

Selected Answer: A

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

upvoted 4 times

🗲️ 👤 **arthursabino20** 1 year, 1 month ago

Selected Answer: A

A is the correct

upvoted 1 times

🗲️ 👤 **Rider2053** 1 year, 2 months ago

Answer is A

upvoted 2 times

🗲️ 👤 **Mobyd** 1 year, 2 months ago

A but which PDF are people on about?

upvoted 4 times

🗲️ 👤 **Sunsil** 1 year, 6 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗲️ 👤 **Requete** 2 years, 1 month ago

Selected Answer: A

A is correct

upvoted 2 times

🗲️ 👤 **Avah** 3 years, 2 months ago

B is correct

upvoted 1 times

🗲️ 👤 **kr57** 3 years, 7 months ago



A is correct

upvoted 2 times

🗲️ 👤 **Glat** 3 years, 9 months ago

Answer is A

upvoted 3 times

  **oksey** 3 years, 10 months ago

Ans is A

upvoted 4 times

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 🍊 4 years, 11 months ago  
D is correct. It's always beginning of the day, not end of the day.  
upvoted 10 times

🗳️ 👤 **fa03337** Most Recent 🔍 1 year ago  
Selected Answer: D  
It's D  
upvoted 1 times

🗳️ 👤 **Lonny** 1 year, 6 months ago  
It's D  
upvoted 1 times

🗳️ 👤 **SnakeTech** 1 year, 7 months ago  
Selected Answer: D  
Correction ?  
upvoted 1 times

🗳️ 👤 **Khuli\_Dolly** 1 year, 9 months ago  
Selected Answer: D  
the @ always snaps at the beginning of the specified period  
upvoted 2 times

🗳️ 👤 **Sunsil** 2 years, 6 months ago  
Selected Answer: D  
D is correct  
upvoted 3 times

🗳️ 👤 **Requete** 3 years, 1 month ago  
Selected Answer: D  
D is correct.  
upvoted 3 times

🗳️ 👤 **ademide2** 3 years, 9 months ago  
C is correct, @d means day, so we want the day inclusive  
upvoted 1 times

🗳️ 👤 **Joker20** 4 years, 4 months ago  
D , check PDF 65  
upvoted 1 times

🗳️ 👤 **Nanila** 4 years, 6 months ago  
D is correct  
upvoted 1 times

🗨️ 👤 **labarcaremo635** 4 years, 7 months ago

D is correct, page 65 from PDF  
upvoted 2 times

🗨️ 👤 **bigmills** 4 years, 7 months ago

Who sat for this exam recently?  
upvoted 3 times

🗨️ 👤 **asultan20** 4 years, 8 months ago

D is correct.  
upvoted 2 times

🗨️ 👤 **sangramrelekar** 4 years, 11 months ago

D is correct  
upvoted 3 times

🗨️ 👤 **parelo** 5 years ago

D is right  
@month for the beginning of the month -- will be the same for day  
upvoted 3 times

🗨️ 👤 **nonee125** 5 years ago

D is correct  
upvoted 4 times



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** 10 months, 2 weeks ago

B. And is implied.

upvoted 1 times

  **saikkat7ghosh** 1 year, 4 months ago

Answer: B

upvoted 1 times


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** 7 months, 1 week ago

C, page 120

upvoted 1 times



Which is primary function of the timeline located under the search bar?

- A. To differentiate between structured and unstructured events in the data.
- B. To sort the events returned by the search command in chronological order.
- C. To zoom in and zoom out, although this does not change the scale of the chart.
- D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime.

**Suggested Answer:** *D*

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Startsearching>

  **mikelord** 1 year ago

Answer is D

upvoted 1 times

What can be configured using the Edit Job Settings menu?

- A. Export the result to CSV format.
- B. Add the Job results to a dashboard.
- C. Schedule the Job to re-run in 10 minutes.
- D. Change Job Lifetime from 10 minutes to 7 days.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

🗨️ 👤 **Hitmansd** 11 months, 1 week ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

🗨️ 👤 **MunnyStax** 1 year ago

D, p. 67

upvoted 1 times

🗨️ 👤 **marianex** 3 years, 1 month ago

D,page 69

upvoted 1 times



Which command is used to validate a lookup file?

- A. | lookup products.csv
- B. inputlookup products.csv
- C. | inputlookup products.csv
- D. | lookup\_definition products.csv

**Suggested Answer:** C

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Inputlookup>

  **Joker20** 10 months, 2 weeks ago

C , check 191

upvoted 4 times

Which statement is true about the top command?

- A. It returns the top 10 results.
- B. It displays the output in table format.
- C. It returns the count and percent columns per row.
- D. All of the above.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **fa03337** 1 year ago

**Selected Answer: D**

D,page 113

upvoted 1 times

🗳️ 👤 **SlyLamp** 2 years, 9 months ago

**Selected Answer: D**

Page 113

upvoted 2 times

🗳️ 👤 **MspI** 3 years, 1 month ago

A it's the correct answer

upvoted 1 times

🗳️ 👤 **marianex** 4 years, 1 month ago

D,page 113

upvoted 3 times


How can another user gain access to a saved report?

- A. The owner of the report can edit permissions from the Edit dropdown.
- B. Only users with an Admin or Power User role can access other users' reports.
- C. Anyone can access any reports marked as public within a shared Splunk deployment.
- D. The owner of the report must clone the original report and save it to their user account.

**Suggested Answer:** A

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/Report/Managereportpermissions>

 **marianex** 7 months, 1 week ago

A, page 139

upvoted 1 times

What is the primary use for the rare command?

- A. To sort field values in descending order.
- B. To return only fields containing five or fewer values.
- C. To find the least common values of a field in a dataset.
- D. To find the fields with the fewest number of values across a dataset.

**Suggested Answer:** *C*

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchReference/Rare>

  **mikelord** 1 year ago

C is correct

upvoted 1 times

What happens when a field is added to the Selected Fields list in the fields sidebar?

- A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
- B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
- C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
- D. The selected field and its corresponding values will appear underneath the events in the search results.

**Suggested Answer:** D

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch>

*Community vote distribution*

D (100%)

🗲️ 👤 **kiki533** 7 months, 1 week ago

**Selected Answer: D**

D correct

upvoted 1 times

🗲️ 👤 **mikelord** 2 years ago

D is Correct

upvoted 2 times

By default, which of the following is a Selected Field?

- A. action
- B. clientip
- C. categoryld
- D. sourcetype

**Suggested Answer:** *D*


Reference:

[https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch#Specify\\_additional\\_selected\\_fields](https://docs.splunk.com/Documentation/Splunk/7.3.1/SearchTutorial/Usefieldstosearch#Specify_additional_selected_fields)

  **labarcaremo635** Highly Voted 2 years, 1 month ago



Answer is D, page 79 in PDF

upvoted 9 times

  **Flavour** Highly Voted 2 years, 1 month ago



Selected Fields contain default Fields host,source and sourcetype. D is correct

upvoted 7 times

  **Iman1367** Most Recent 1 year, 2 months ago

D is correct.

upvoted 1 times

  **Robbe** 2 years, 1 month ago

The answer should be A. "Action"

upvoted 1 times

  **emlch** 7 months ago

action isn't a selected field, selected fields are by default: host, source and sourcetype. Action might be a interesting field depending or you events.

upvoted 1 times



According to Splunk best practices, which placement of the wildcard results in the most efficient search?

- A. f\*il
- B. \*fail
- C. fail\*
- D. \*fail\*

**Suggested Answer:** C

Community vote distribution

A (100%)

🗳️ 👤 **2dd1c50** 2 weeks, 1 day ago

**Selected Answer: C**

The correct answer is: C. fail\*

Explanation:

In Splunk search best practices, wildcard placement significantly affects search performance:

- fail\* is most efficient because it allows Splunk to leverage indexed terms that begin with "fail". This enables it to use index-time metadata and reduce the search scope.
- \*fail, \*fail\*, and f\*il are less efficient because they require Splunk to perform a brute-force scan across more events, as they cannot use the index as effectively. These are considered "leading wildcards" and are discouraged in large datasets.

So, C. fail\* aligns with Splunk's best practices for performance.

upvoted 1 times

🗳️ 👤 **mirko1976** 5 months, 1 week ago

**Selected Answer: C**

- Avoid using wildcards at the beginning or middle of a string
- Wildcards at beginning of string scan all events within timeframe
- Wildcards in middle of string may return inconsistent results
- So use fail\* (not \*fail or \*fail\* or f\*il)
  
- When possible, use OR instead of wildcards
- For example, use (user=admin OR user=administrator) instead of user=admin\*

upvoted 2 times

🗳️ 👤 **praveenjetty** 1 year ago

C is correct.

The best way to use a wildcard is at the end of a term

upvoted 2 times

🗳️ 👤 **mason999** 1 year ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗳️ 👤 **Asheel1** 11 months ago

How is A correct? Any documentation?

upvoted 1 times

🗳️ 👤 **mikelord** 3 years, 6 months ago

C is correct

upvoted 4 times

Which command automatically returns percent and count columns when executing searches?

- A. top
- B. stats
- C. table
- D. percent

**Suggested Answer: A**

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Aboutsubsearches>

  **Rahulgargacc** 8 months, 2 weeks ago

<https://docs.splunk.com/Documentation/SplunkCloud/9.0.2305/SearchReference/Top>

upvoted 2 times

  **mikelord** 3 years ago

A is correct

upvoted 1 times

Which of the following describes lookup files?

- A. Lookup fields cannot be used in searches.
- B. Lookups contain static data available in the index.
- C. Lookups add more fields to results returned by a search.
- D. Lookups pull data at index time and add them to search results.

**Suggested Answer: B**

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.1/Knowledge/Aboutlookupsandfieldactions>

Community vote distribution

C (100%)

🗳️ 👤 **alisyed** Highly Voted 👍 3 years, 8 months ago

C is correct, Page 185 & 186 pdf file  
upvoted 8 times

🗳️ 👤 **parelo** Highly Voted 👍 4 years ago

Lookup table data is not indexed  
Lookup table files are files that contain a lookup table. A standard lookup pulls fields out of this table and adds them to your events when corresponding fields in the table are matched in your events.  
upvoted 5 times

🗳️ 👤 **z3phyr** Most Recent 🕒 7 months ago

Selected Answer: C  
Lookup data is NOT store in the index. It is pulled from external sources.  
upvoted 3 times

🗳️ 👤 **sonishar** 1 year, 3 months ago

C  
Refer 189  
The lookup fields also appear in the field side bar.  
upvoted 1 times

🗳️ 👤 **qtygbajpesdayazko** 2 years, 1 month ago

Selected Answer: C  
C is the correnct  
upvoted 2 times

🗳️ 👤 **Requete** 2 years, 1 month ago

Selected Answer: C  
C is correct  
upvoted 2 times

🗳️ 👤 **kr57** 3 years, 7 months ago

C is correct  
upvoted 1 times

🗳️ 👤 **bigmills** 3 years, 7 months ago

C for sure  
upvoted 1 times



🗳️ 👤 **stallone** 3 years, 11 months ago

C is correct.  
upvoted 2 times

Which search string is the most efficient?

- A. `index=security&failed password&`
- B. `index=security&failed password&*`
- C. `index=*&failed password&`
- D. `index=security&failed password&`

**Suggested Answer:** *D*

  **foxx99** 8 months, 1 week ago

D is correct

upvoted 1 times

Which search string matches only events with the status\_code of 404?

- A. status\_code!=404
- B. status\_code>=400
- C. status\_code<=404
- D. status\_code>403 status\_code<405

**Suggested Answer:** D

Community vote distribution

D (89%)

11%

🗳️ **s4t4** 4 months, 2 weeks ago

**Selected Answer: D**

This is a tricky question with a tricky answer. status\_code>403 status\_code<405 will show you anything between of then...A means not equals to and B and C are just not correct answer.

upvoted 1 times

🗳️ **toony12345** 1 year ago

The answer is D. - status\_code>403 status\_code<405

query is basically saying anything between 403 and 405 , which is 404. D is correct.

upvoted 2 times

🗳️ **carnage1970** 1 year, 11 months ago

**Selected Answer: D**

status\_code=404 would have been best but wasn't an option.

upvoted 3 times

🗳️ **cagdaskarabag** 2 years, 1 month ago

**Selected Answer: D**

ppl voting for A could you please explain what you were thinking ?

:D

upvoted 4 times

🗳️ **qtygbajpesdayazko** 2 years, 1 month ago

**Selected Answer: D**

The correct is D

upvoted 1 times

🗳️ **dreese94** 2 years, 2 months ago

**Selected Answer: A**

I really think it is A

upvoted 1 times

🗳️ **wepbot** 2 years, 1 month ago

The != operator means "not equal to".

upvoted 3 times

🗳️ **crazydice0** 2 years, 1 month ago

yes != not equal too. answer is D. I just sat for the test.

upvoted 1 times

🗳️ **mikelord** 3 years ago

Answer is D

upvoted 1 times

\_\_\_\_\_ transforms raw data into events and distributes the results into an index.

- A. Index
- B. Search Head
- C. Indexer
- D. Forwarder

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **BrynnML** 12 months ago

**Selected Answer: C**

I would say C as its the indexer that normals breaks data into lines and into kvp. But i believe heavy forwarder can also do some pre-parsing of the data

upvoted 2 times

🗳️ 👤 **varan97** 2 years, 4 months ago

C is the answer , pg 24

upvoted 2 times

🗳️ 👤 **Alusine** 2 years, 5 months ago

C. Correct. Universal forwarder doesn't parse or organize data into events (unless HF). It only monitors and forwards data to the indexer.

<https://docs.splunk.com/Splexicon:Indexer#:~:text=A%20Splunk%20Enterprise%20instance%20that,data%20input%20and%20search%20management>.

upvoted 2 times

🗳️ 👤 **jake7** 2 years, 8 months ago

D IS CORRECT

upvoted 1 times

🗳️ 👤 **bmalin77** 2 years, 4 months ago

C. A Splunk Enterprise instance that indexes data, transforming raw data into events and placing the results into an index. It also searches the indexed data in response to search requests.

upvoted 1 times

🗳️ 👤 **4j1m** 2 years, 5 months ago

Page 27 Splunk Fundamental 1

Splunk Component - Forwarders

Splunk Enterprise instances that consume and send data to the index.

upvoted 1 times

🗳️ 👤 **Iman1367** 2 years, 8 months ago

C is correct

upvoted 2 times

🗳️ 👤 **splunk\_nitin** 2 years, 10 months ago

Answer is C

upvoted 2 times

🗳️ 👤 **saikkat7ghosh** 2 years, 10 months ago

Answer: D

upvoted 1 times

🗳️ 👤 **msn\_aden** 2 years, 8 months ago

why is it D?

upvoted 2 times

Documentations for Splunk can be found at docs.splunk.com

A. True

B. False

**Suggested Answer: A**

🗉 👤 **Chris\_Be** 11 months, 2 weeks ago

A is correct

upvoted 2 times

🗉 👤 **saikkat7ghosh** 1 year, 10 months ago

Answer: A

upvoted 2 times

Which component of Splunk is primarily responsible for saving data?

- A. Search Head
- B. Heavy Forwarder
- C. Indexer
- D. Universal Forwarder

**Suggested Answer:** C

  **Derag** 7 months, 2 weeks ago

Answer is C:

The indexer is responsible for parsing the data, extracting fields, creating events, compressing and storing the data, and making it available for searching. Once the data is indexed, it can be queried, analyzed, and visualized using search commands and dashboards.

upvoted 3 times

  **saikkat7ghosh** 2 years, 4 months ago

Answer: C

upvoted 1 times



Universal forwarder is recommended for forwarding the logs to indexers.

A. False

B. True

**Suggested Answer:** *B*

  **calvo** 9 months, 3 weeks ago

B. True

upvoted 1 times

Splunk apps are used for following (Choose three.):

- A. Designed to cater numerous use cases and empower Splunk.
- B. We can not install Splunk App.
- C. Allows multiple workspaces for different use cases/user roles.
- D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

**Suggested Answer:** *ACD*

  **roy88** 10 months ago

ACD - PDF page 9

upvoted 1 times

Three basic components of Splunk are (Choose three.):

- A. Forwarders
- B. Deployment Server
- C. Indexer
- D. Knowledge Objects
- E. Index
- F. Search Head

**Suggested Answer:** *ACF*

  **roy88** 10 months ago

ACF - PDF page 7

upvoted 1 times

What is Splunk?

- A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
- B. Database management tool.
- C. Security Information and Event Management (SIEM).
- D. Cloud based application that help in analyzing logs.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **oussa\_ama** 10 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 4 months ago

C is correct

upvoted 1 times

🗳️ 👤 **varan97** 3 years, 4 months ago

A is correct, pg 5

upvoted 1 times

We should use heavy forwarder for sending event-based data to Indexers.

A. False

B. True

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **Doflamingo** 1 year ago


**Selected Answer: B**

I was also thinking that Universal was the answer but now I think this answers the question directly.

The universal forwarder is the best tool for forwarding data to indexers. Its main limitation is that it forwards only unparsed data. To send event-based data to indexers, you must use a heavy forwarder.

<https://docs.splunk.com/Splexicon:Forwarder>

upvoted 3 times



  **G4ct756** 1 year, 11 months ago

**Selected Answer: B**

<https://docs.splunk.com/Splexicon:Heavyforwarder>,

"In most situations, the universal forwarder is the best way to forward data to indexers. Its main limitation is that it forwards only unparsed data, except in certain cases, such as structured data. You must use a heavy forwarder to route data based on event contents. "

upvoted 3 times

  **neledov** 2 years, 8 months ago



should we? we might use UF as well - answer is A, false

upvoted 1 times

  **JanBanan** 3 years, 3 months ago

B correct

upvoted 2 times

  **alisyed** 3 years, 8 months ago

<https://docs.splunk.com/Splexicon:Heavyforwarder>

upvoted 2 times

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True

B. False

**Suggested Answer: A**

Community vote distribution

A (50%)

B (50%)

🗳️ 👤 **SimonR2** Highly Voted 👍 3 years, 1 month ago

I disagree that its A. It says on page 8 of the PDF that Splunk Enterprise is ON PREM. Splunk Cloud is the cloud/scalable solution.

Answer is B

upvoted 6 times

🗳️ 👤 **SimonR2** 3 years, 1 month ago

Also, check Q96 - How can that question and this both be true? Its not possible.

upvoted 1 times

🗳️ 👤 **nupacniyiveli** Highly Voted 👍 3 years ago

A is the Answer - PDF pg. 8...

Splunk Enterprise as a scalable Service is Splunk Cloud.

upvoted 6 times

🗳️ 👤 **2dd1c50** Most Recent 🕒 2 weeks, 1 day ago

Selected Answer: A

The correct answer is: A. True

Explanation:

Splunk Enterprise is the core software that powers Splunk Cloud. In the cloud deployment model, Splunk Enterprise runs as a scalable, managed service in the cloud environment provided by Splunk (or via a cloud provider like AWS or GCP).

- Splunk Cloud offers the same features and capabilities as Splunk Enterprise, but it's hosted and managed by Splunk, making it scalable and easier to maintain.
- Organizations choose Splunk Cloud to avoid managing infrastructure, while still benefiting from the power of Splunk Enterprise.

So, it's correct to say:

Splunk Enterprise is used as a scalable service in Splunk Cloud – True.

upvoted 1 times

🗳️ 👤 **mirko1976** 3 months, 3 weeks ago

Selected Answer: A

Splunk Enterprise serves as the foundation for Splunk Cloud and is used as a scalable service in the cloud environment. Splunk Cloud is essentially a cloud-hosted version of Splunk Enterprise that offers the same features but is managed by Splunk.

upvoted 1 times

🗳️ 👤 **david124** 9 months, 2 weeks ago

B. False

Splunk Enterprise is the on-premises version of Splunk, designed for installation on local servers or data centers. It is not used as a scalable service in Splunk Cloud.

In Splunk Cloud, the service is provided as a Software-as-a-Service (SaaS) offering, where Splunk manages the infrastructure, maintenance, and scalability aspects for the users. Splunk Cloud is built on top of Splunk Enterprise technology but is specifically optimized for cloud deployment, offering scalability, reliability, and ease of use without the need for users to manage the underlying infrastructure.

upvoted 2 times

🗨️ 👤 **david124** 9 months, 2 weeks ago

B. False

Splunk Enterprise is the on-premises version of Splunk, designed for installation on local servers or data centers. It is not used as a scalable service in Splunk Cloud.

In Splunk Cloud, the service is provided as a Software-as-a-Service (SaaS) offering, where Splunk manages the infrastructure, maintenance, and scalability aspects for the users. Splunk Cloud is built on top of Splunk Enterprise technology but is specifically optimized for cloud deployment, offering scalability, reliability, and ease of use without the need for users to manage the underlying infrastructure.

upvoted 1 times

🗨️ 👤 **assfedassfinished** 1 year, 7 months ago

Selected Answer: A

Splunk can be deployed in various architectures, including Single Instance, Distributed, Clustered, and Cloud-based.

upvoted 1 times

🗨️ 👤 **foxx99** 1 year, 8 months ago

Selected Answer: A

A Page 8

upvoted 1 times

🗨️ 👤 **WarKarmaa** 1 year, 10 months ago

Selected Answer: B

Splunk Enterprise is ON PREM

upvoted 2 times

🗨️ 👤 **labarcaremo635** 4 years, 1 month ago

I think answer is A: Splunk Cloud is a specific Splunk Enterprise deployment. Pag 8 in PDF

upvoted 3 times

🗨️ 👤 **Flavour** 4 years, 1 month ago

Answer is A

upvoted 1 times

🗨️ 👤 **bigmills** 4 years, 1 month ago

A for Sure

upvoted 1 times

🗨️ 👤 **alisyed** 4 years, 2 months ago

Answer A: Pdf page 8

upvoted 3 times

🗨️ 👤 **AMRIT475** 4 years, 3 months ago

<https://www.datacenterknowledge.com/archives/2014/10/09/splunk-launches-enterprise-6-2-integrates-hunk-with-aws>

upvoted 1 times

🗨️ 👤 **foobar47** 4 years, 3 months ago

Answer is A , cf page 8 of PDF

upvoted 4 times

🗨️ 👤 **oksey** 4 years, 4 months ago

Ans is B Splunk Enterprise is an ON PREMISE software

upvoted 1 times

🗨️ 👤 **Noone04** 4 years, 4 months ago

Answer is A. There is no special product for the cloud. In the end, it is just Splunk enterprise but as a SaaS service which is nothing but a scalable based on your data and resource utilization.

upvoted 4 times