# Splunk Core Certified Power User

## What is Splunk? (eLearning)

This is discontinued.

## Intro to Splunk (Completed)

### What is Splunk?

### Using Splunk web

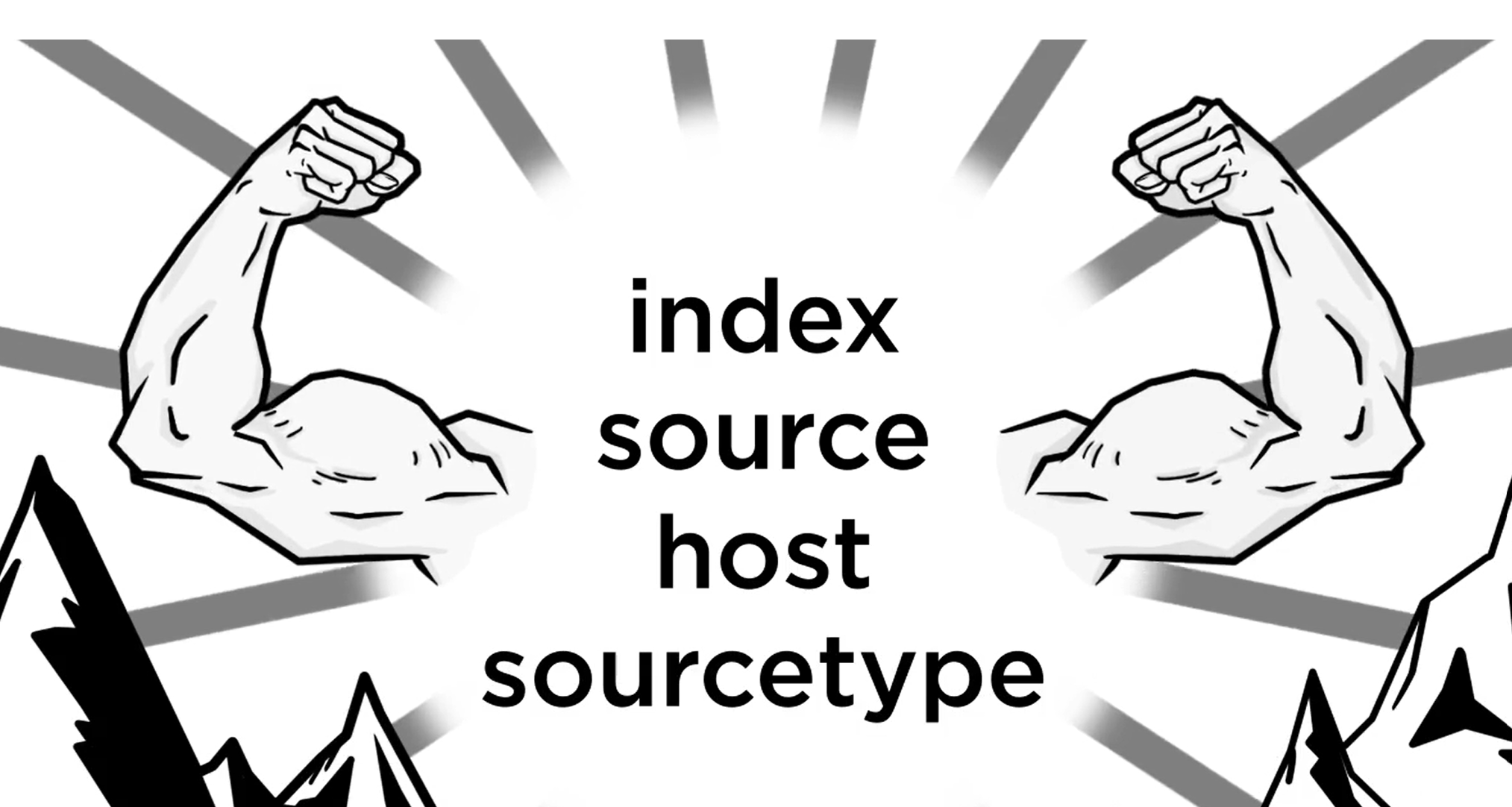
<https://splunkbase.splunk.com/>

### Using Search

### Exploring events

### Using Search term

### What are commands?



### What are Knowledge objects

### Creating Reports?

### Creating Dashboards

### Dashboard Studio

### Additional Resources

<https://www.splunk.com/en_us/training.html>

<https://www.youtube.com/channel/UCjwOFZzLPnji1EstaVyyvAw>

<https://docs.splunk.com/Documentation>

<https://lantern.splunk.com/>

### Intro to Splunk Quiz

1. Question

Which Splunk infrastructure component stores ingested data?

Select one option

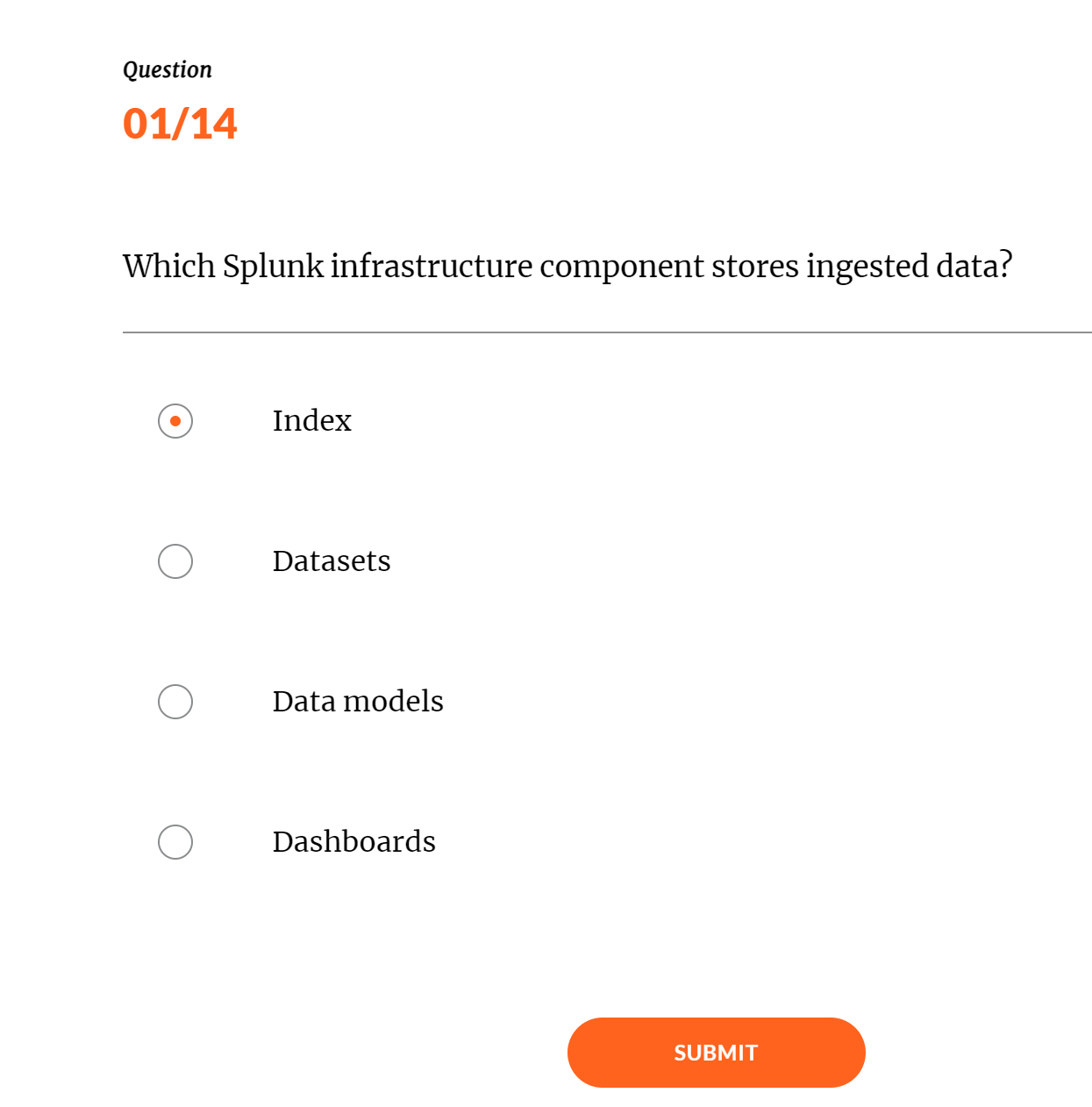
Datasets

Dashboards

Data models

Index

Answer by GPT: Index



1. Question

Which of the following searches will return results containing the words fail, failure, or failed?

Select one option

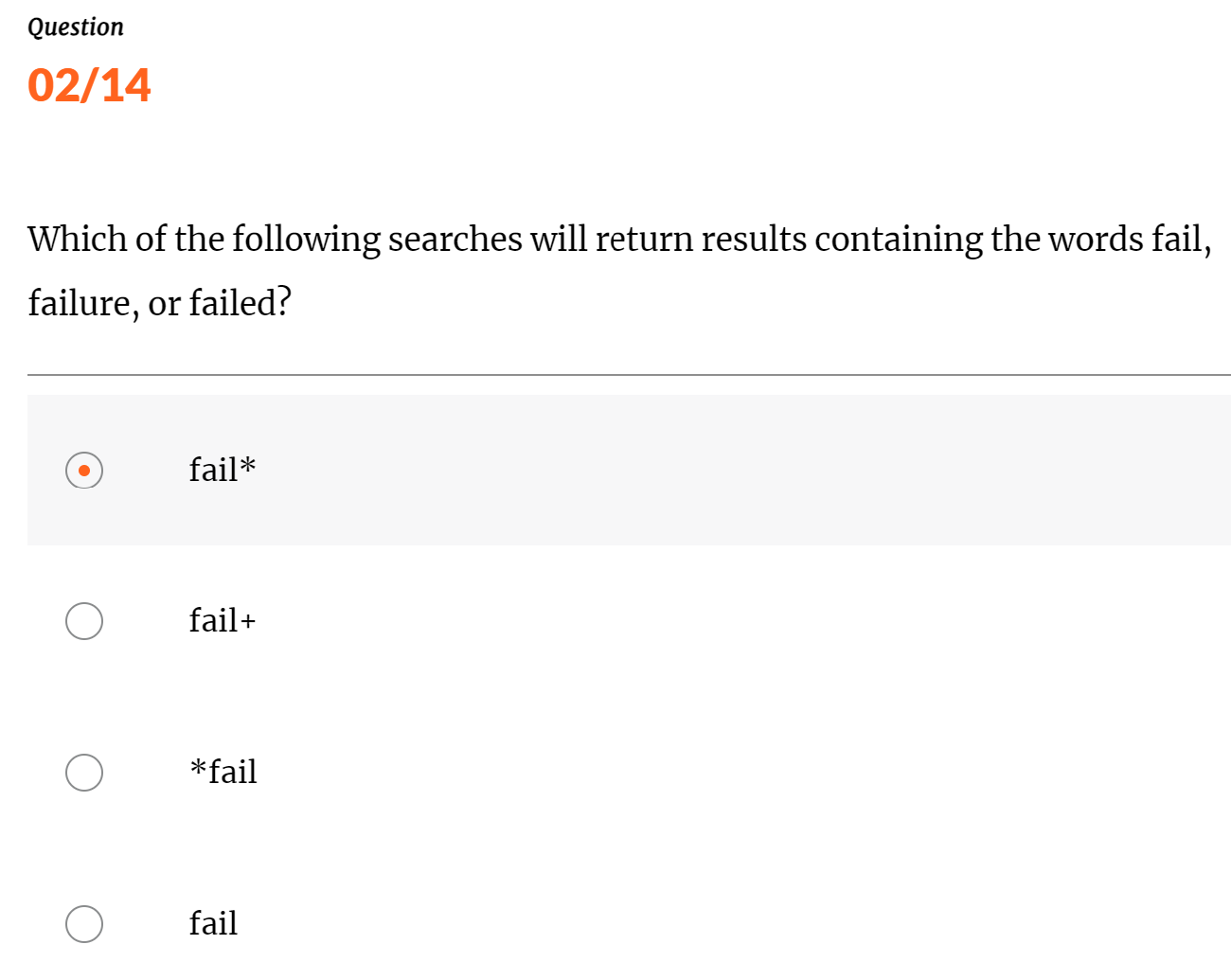
fail+

fail

fail\*

\*fail

Answer by GPT: fail\*



\

1. Question

Which command can be used to further filter results in a search?

Select one option

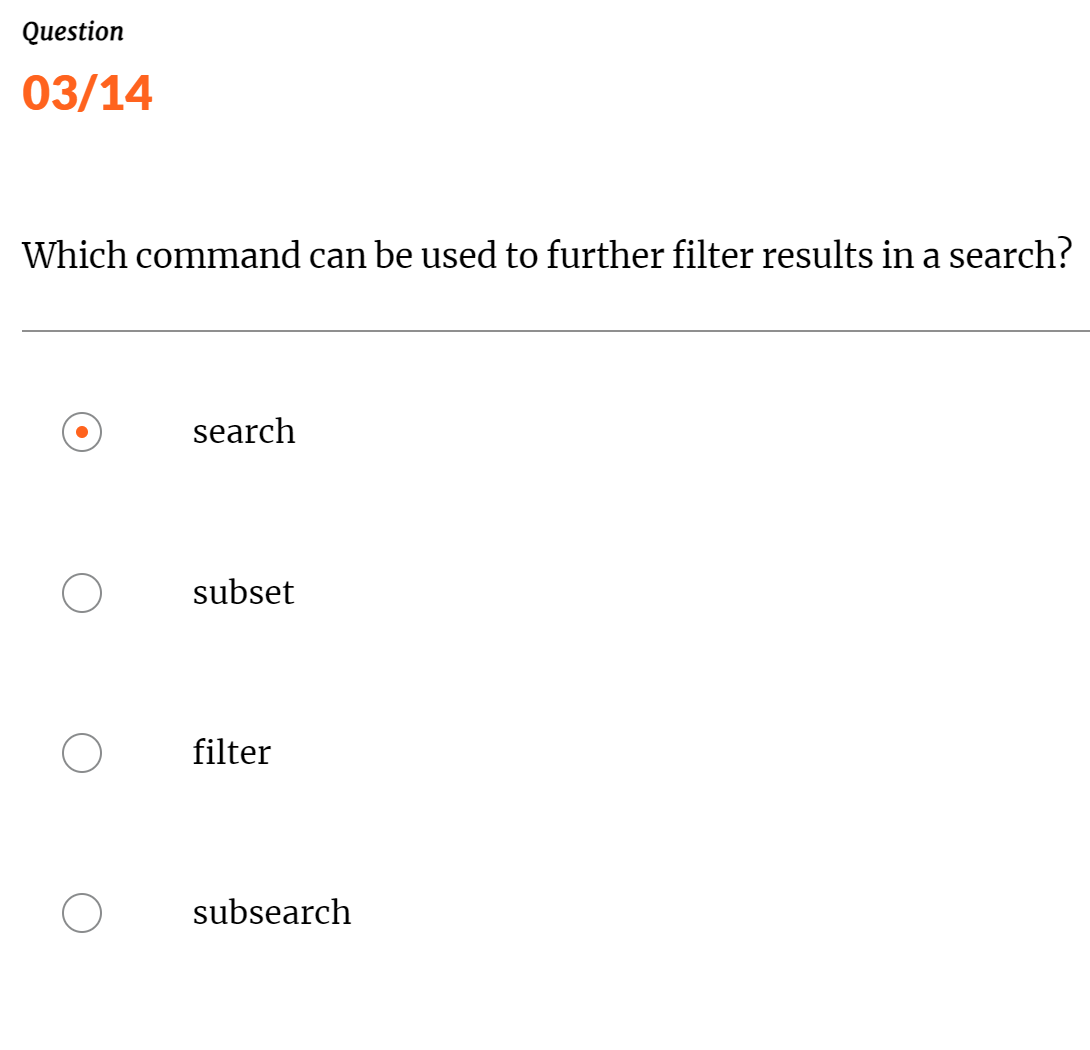
subsearch

subset

search

filter

Answer by GPT: search



4. Question

By default, how long does a search job remain active?

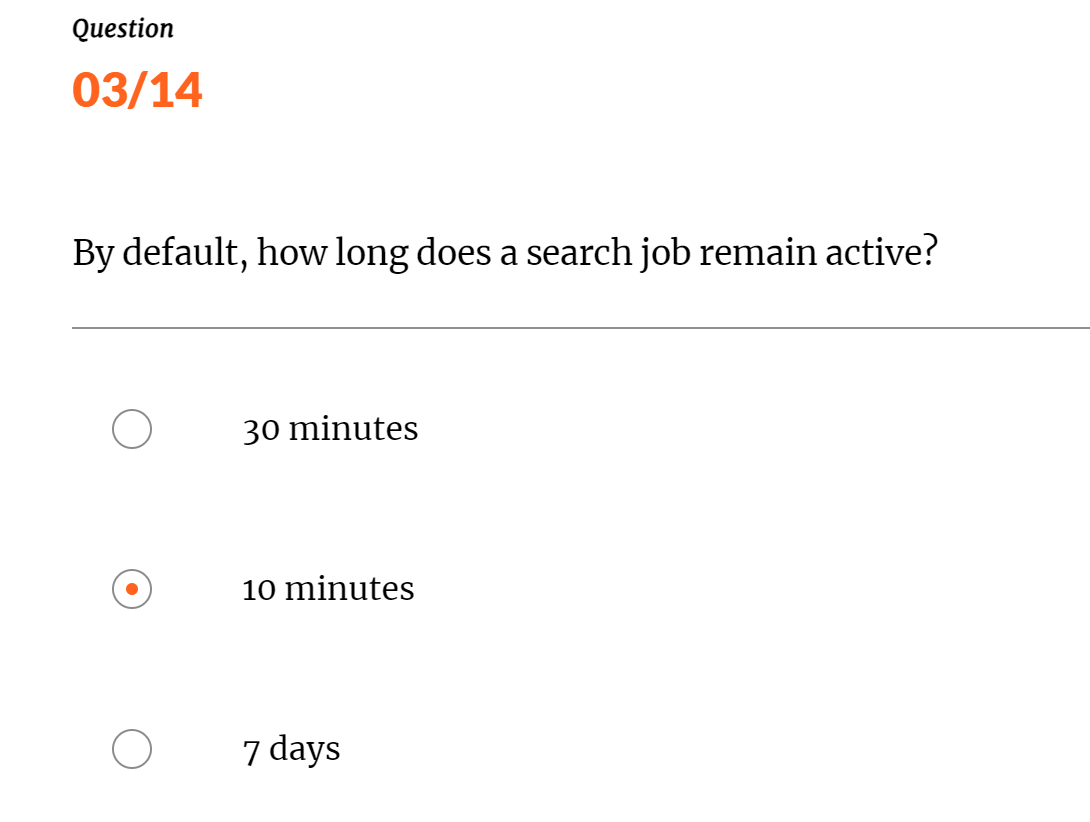
Select one option

30 minutes

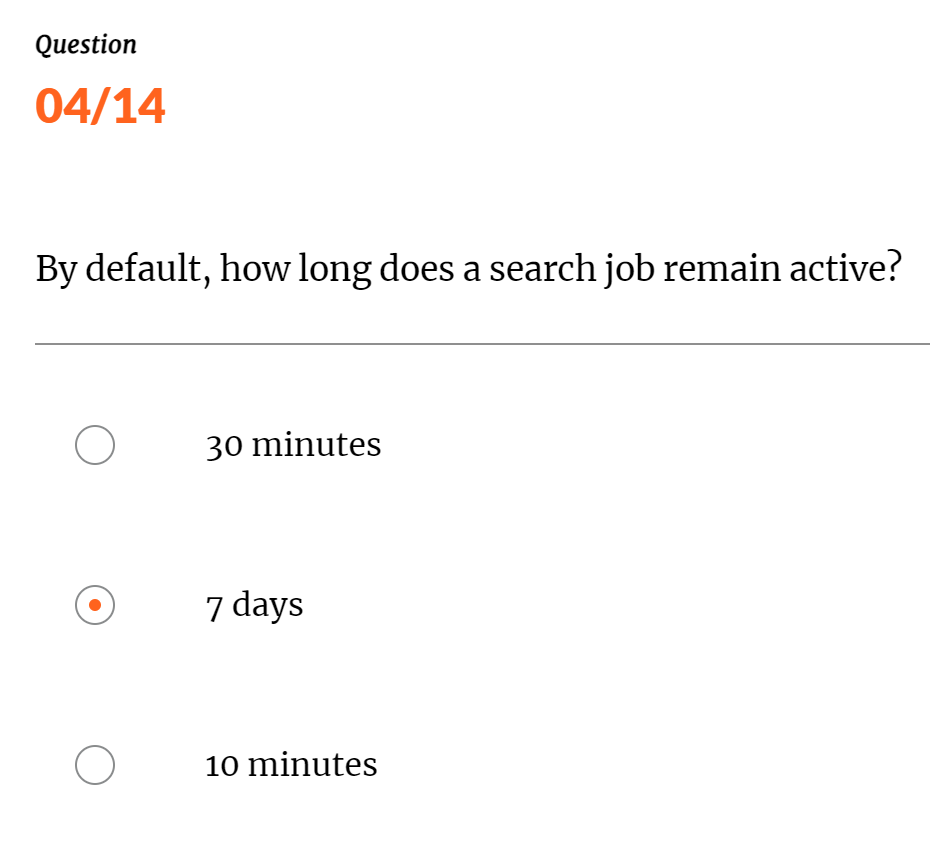
10 minutes

7 days

Answer by GPT: 10 minutes



Below screen shot may be wrong



1. Question

Which of the following searches will return results containing the terms failed, password, or failed password?

Can select multiple answers

failed password OR "failed password"

fail\*

failed OR password OR "failed password"

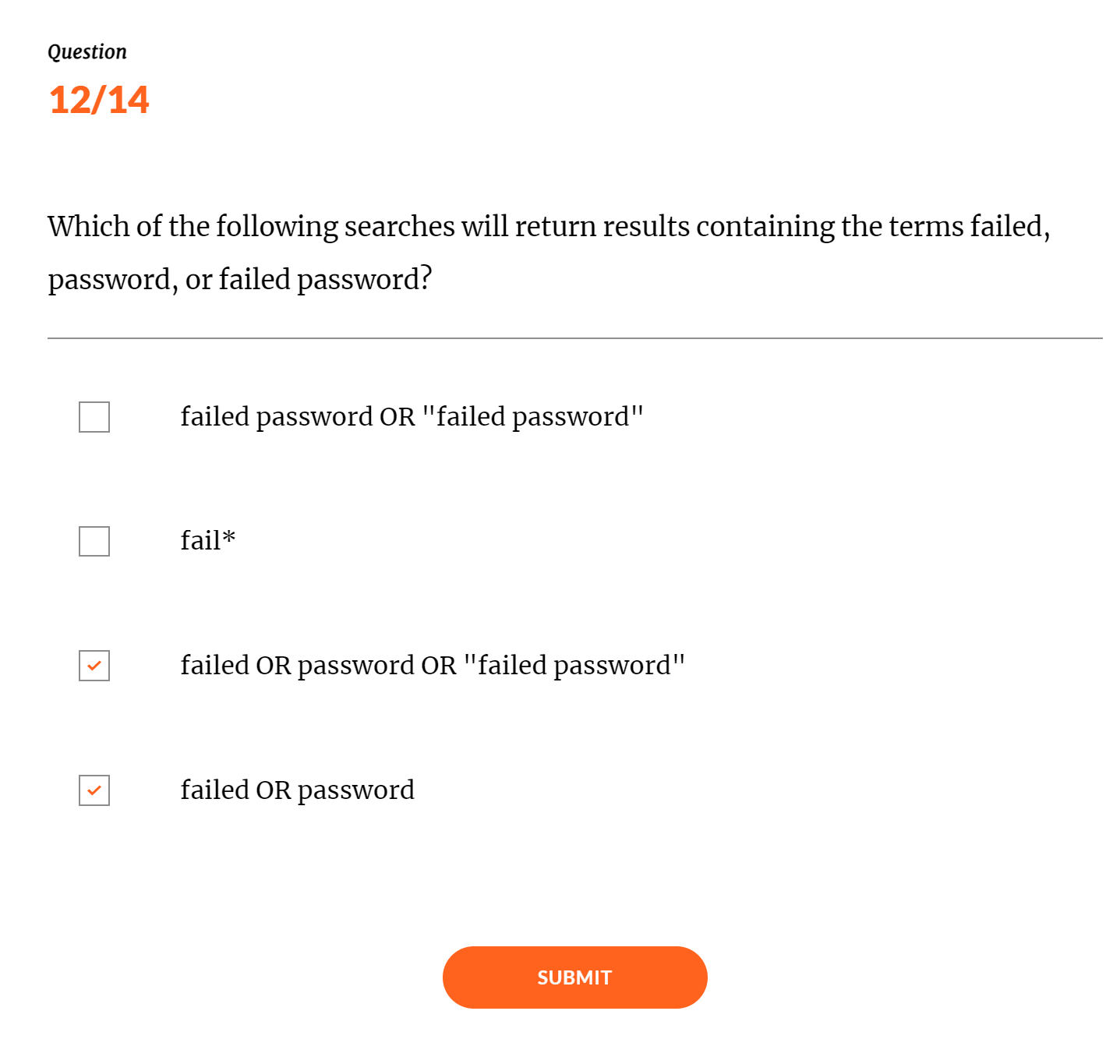
failed OR password

Answer by GPT: failed OR password OR "failed password" ,, failed OR password

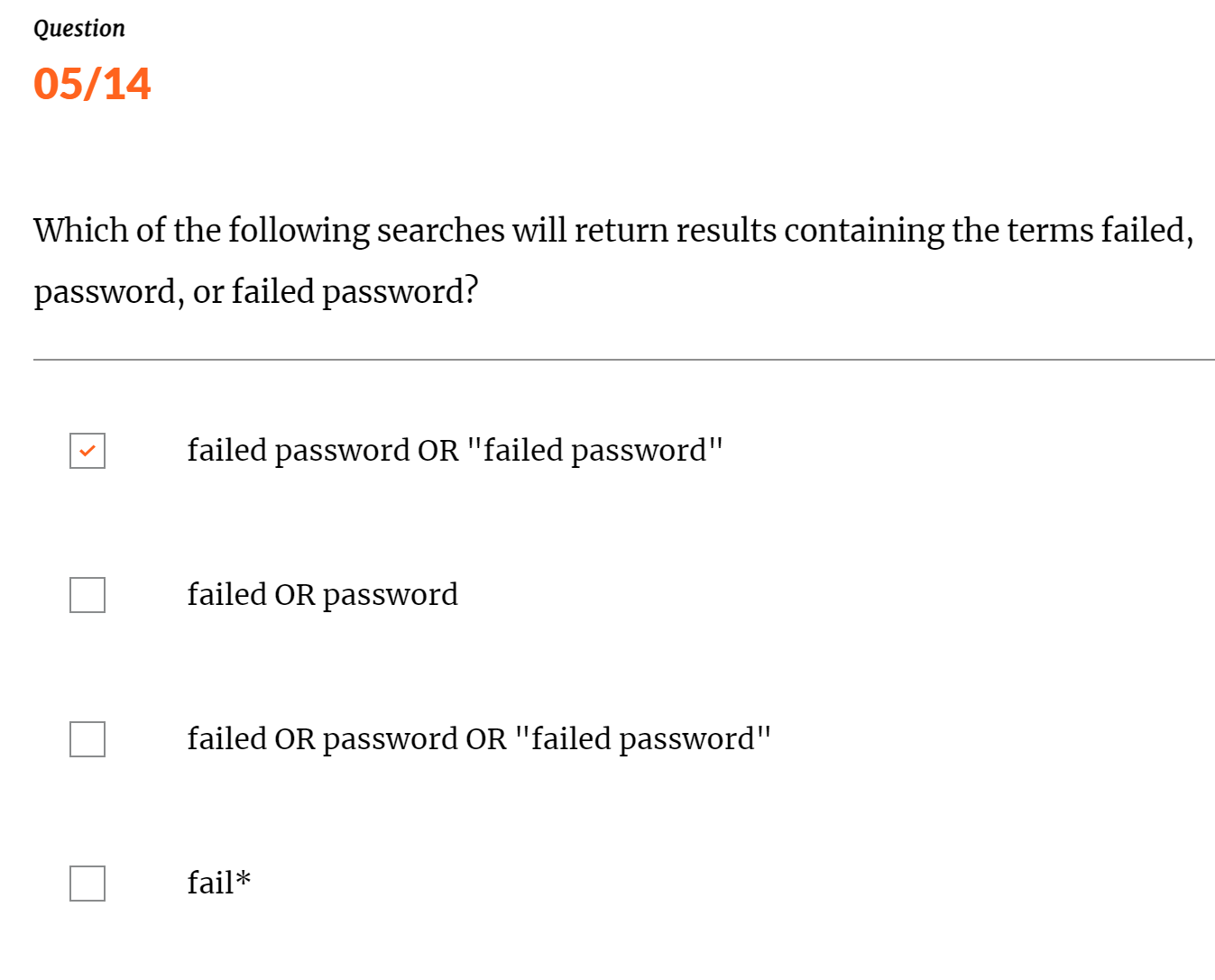
These searches will return results containing the individual terms "failed," "password," or the phrase "failed password."

failed password OR "failed password": This search would specifically look for events containing either the words "failed" and "password" separately or the exact phrase "failed password."

fail\*: This search would match terms starting with "fail," such as "failed," but it doesn't cover the term "password" or the phrase "failed password."



Below screenshot is may be wrong



6. Question

By default, who is able to view a saved report?

Select one option

The user who created it

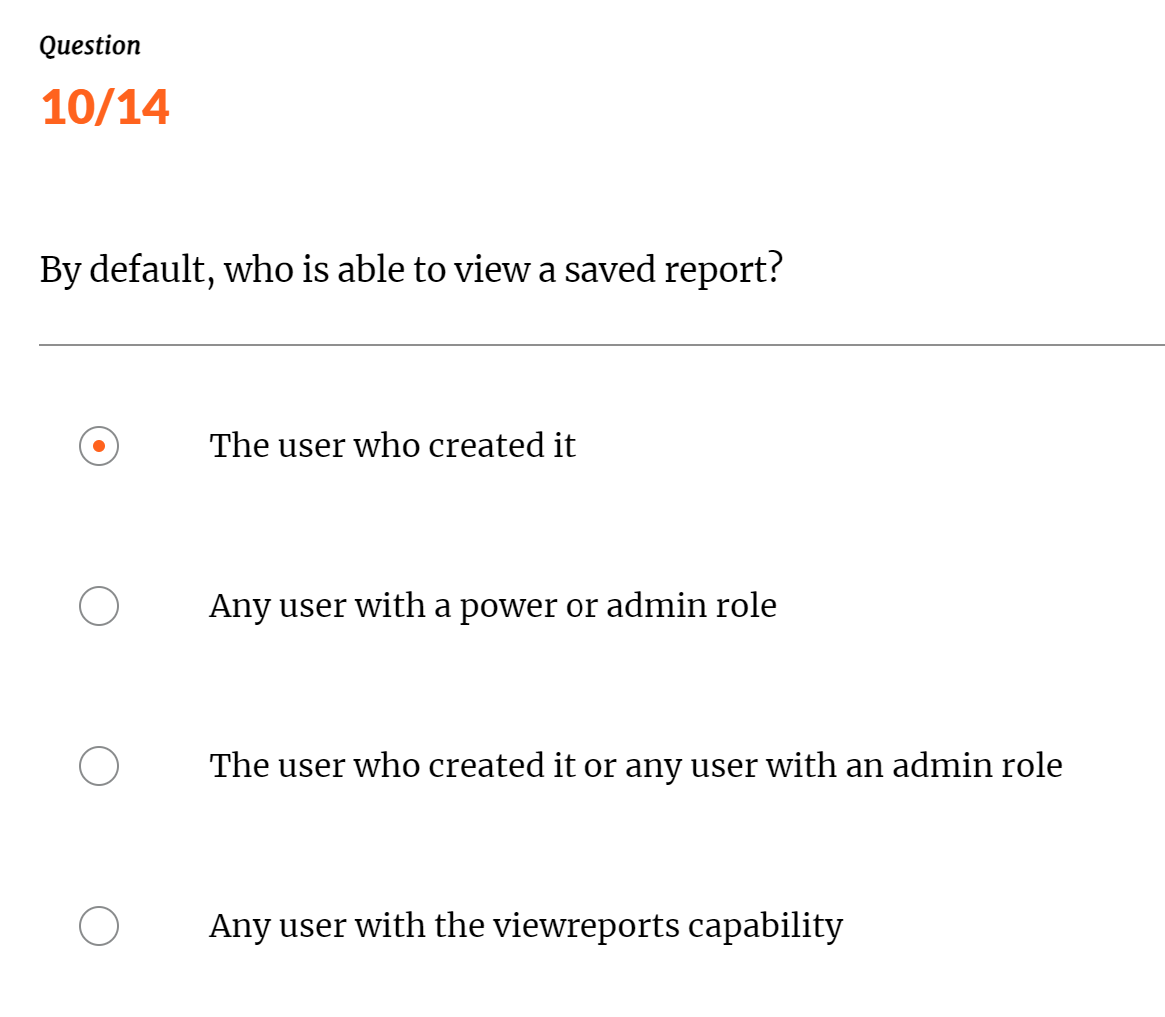
Any user with a power or admin role

The user who created it or any user with an admin role

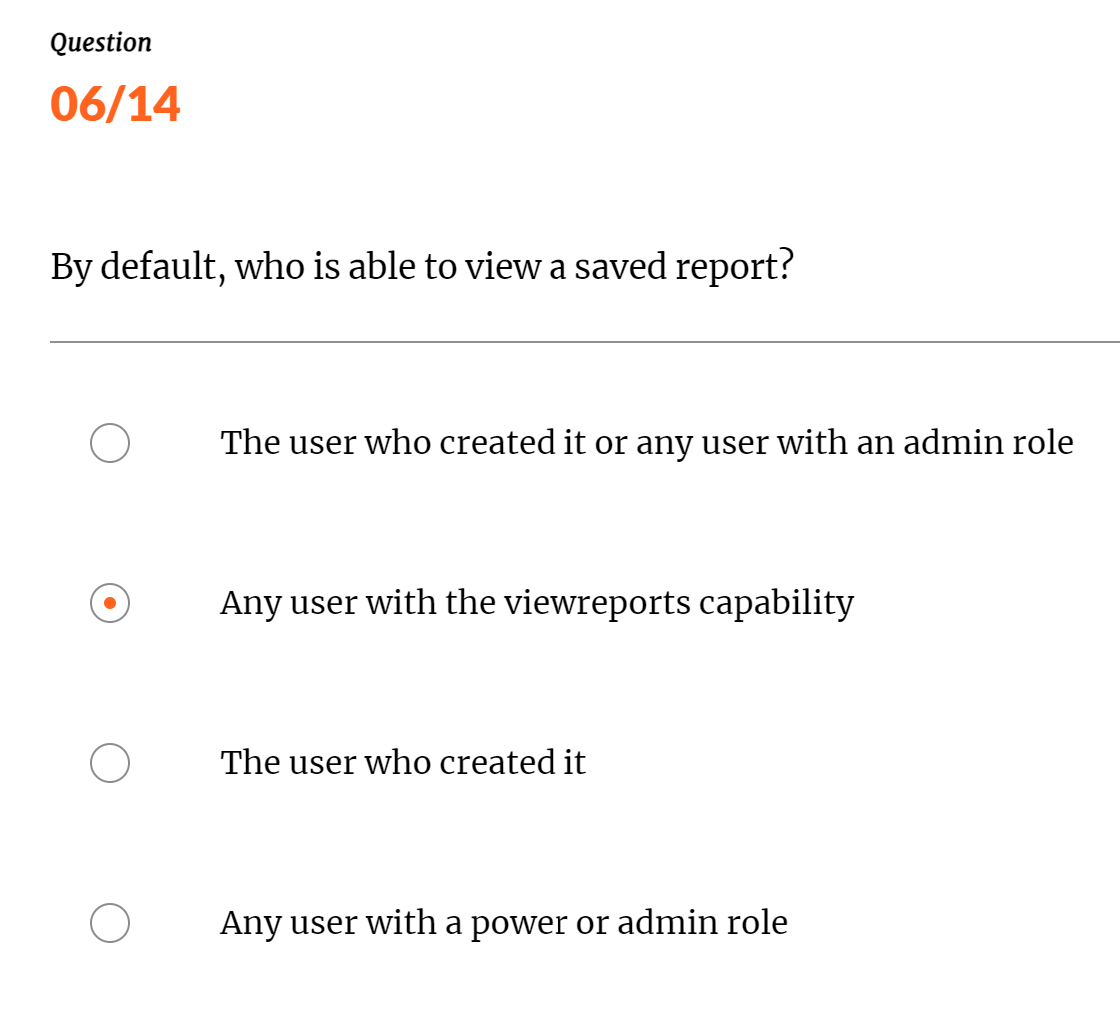
Any user with the viewreports capability

Answer by GPT: The user who created it

By default, a saved report in Splunk is private and only visible to the user who created it. The creator can choose to share it with others or make it globally accessible if needed.



Below screen shot is wrong answer



7. Question

What is the most efficient way to limit search results returned?

Select one option

index

time

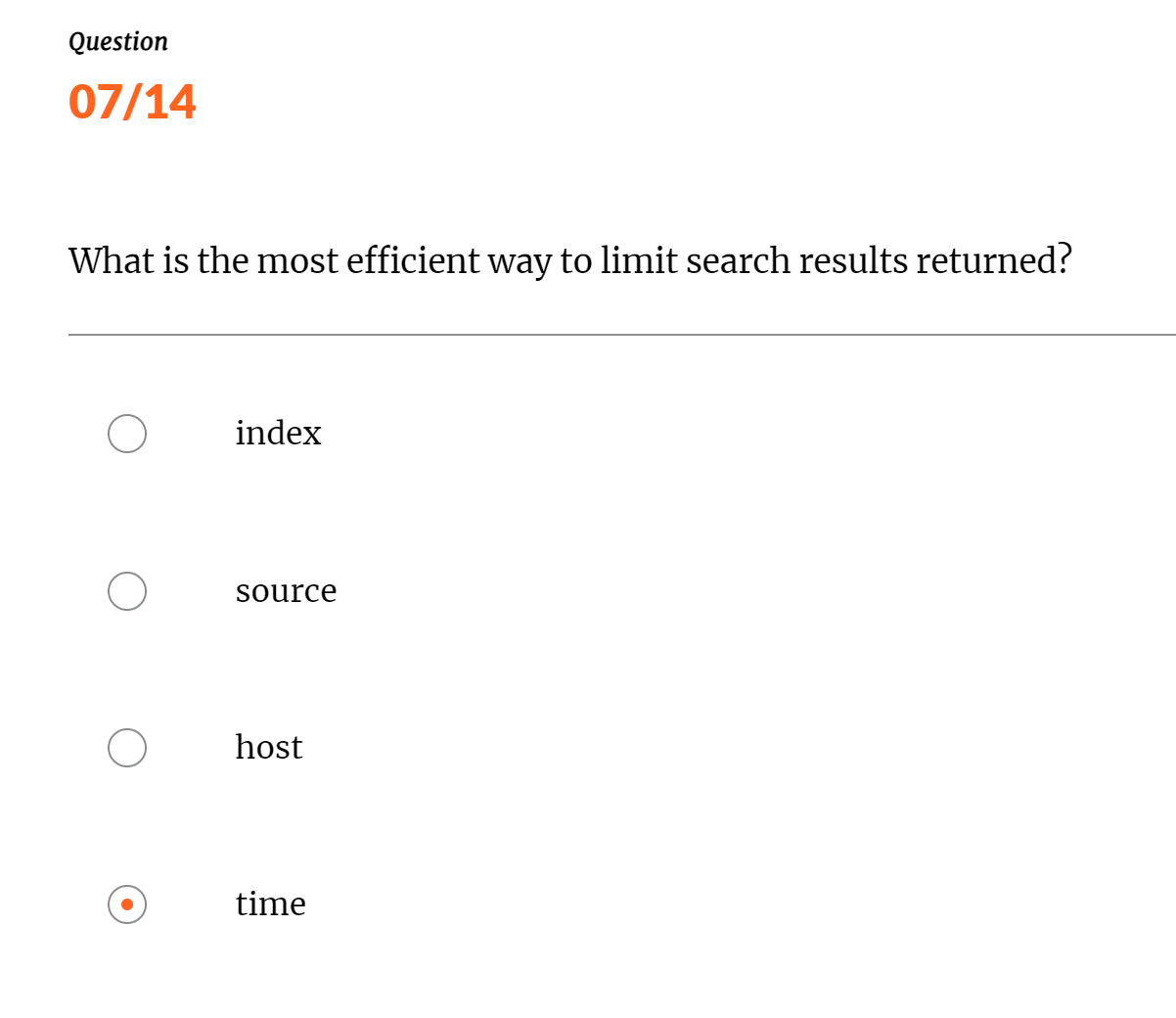
source

host

Answer by GPT: time

Limiting search results by time is the most efficient way to narrow down your results in Splunk. By specifying a time range, you reduce the volume of data that needs to be searched, which improves search performance and efficiency.

Using index, source, or host can also limit results, but applying a time filter is generally the most effective for improving search speed and relevance.



1. Question

When a search is run, in what order are events returned?

Select one option.

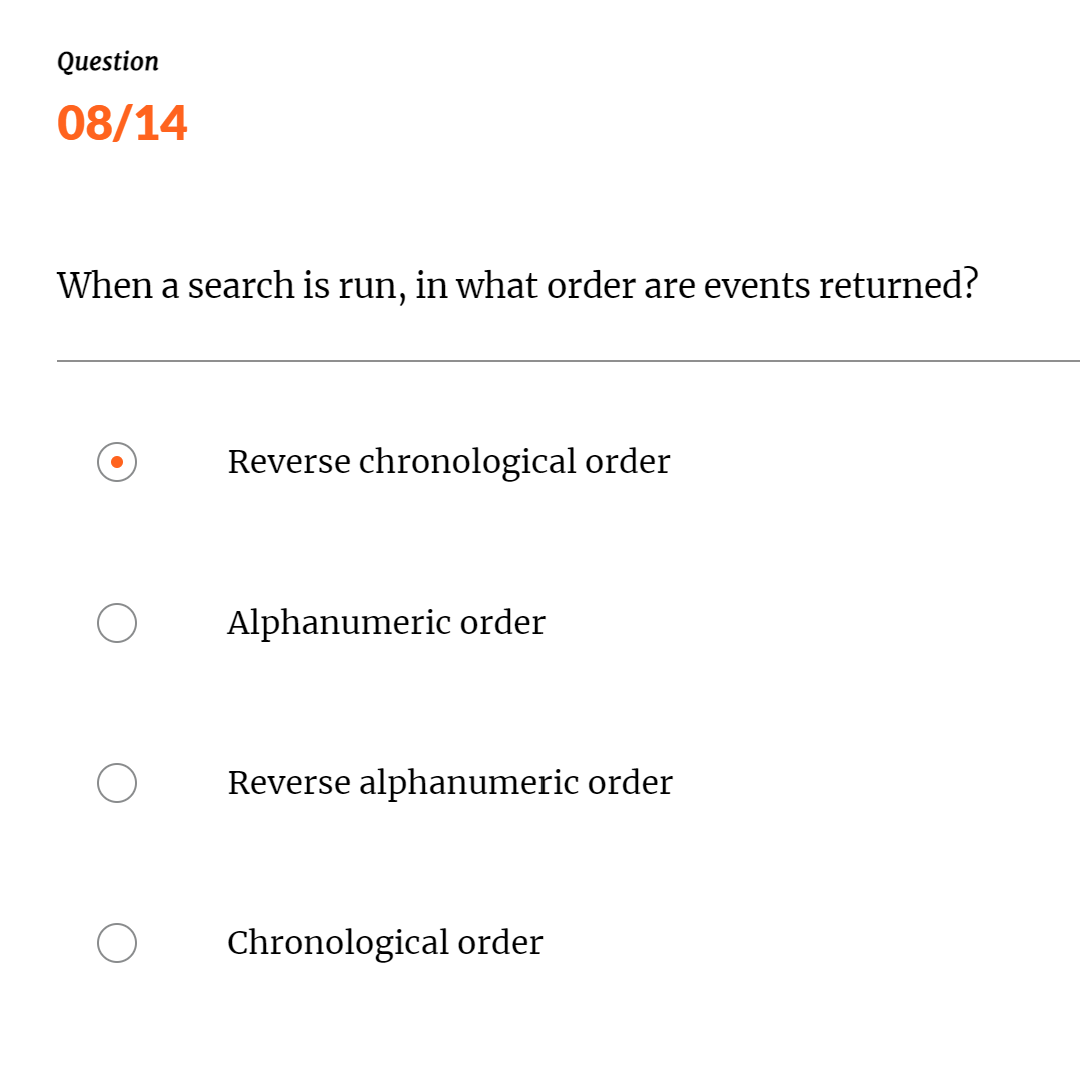
Alphanumeric order

Chronological order

Reverse alphanumeric order.

Reverse chronological order.

Answer by GPT: Reverse chronological order.



1. Question

Which search mode behaves differently depending on the type of search being run?

Select one option

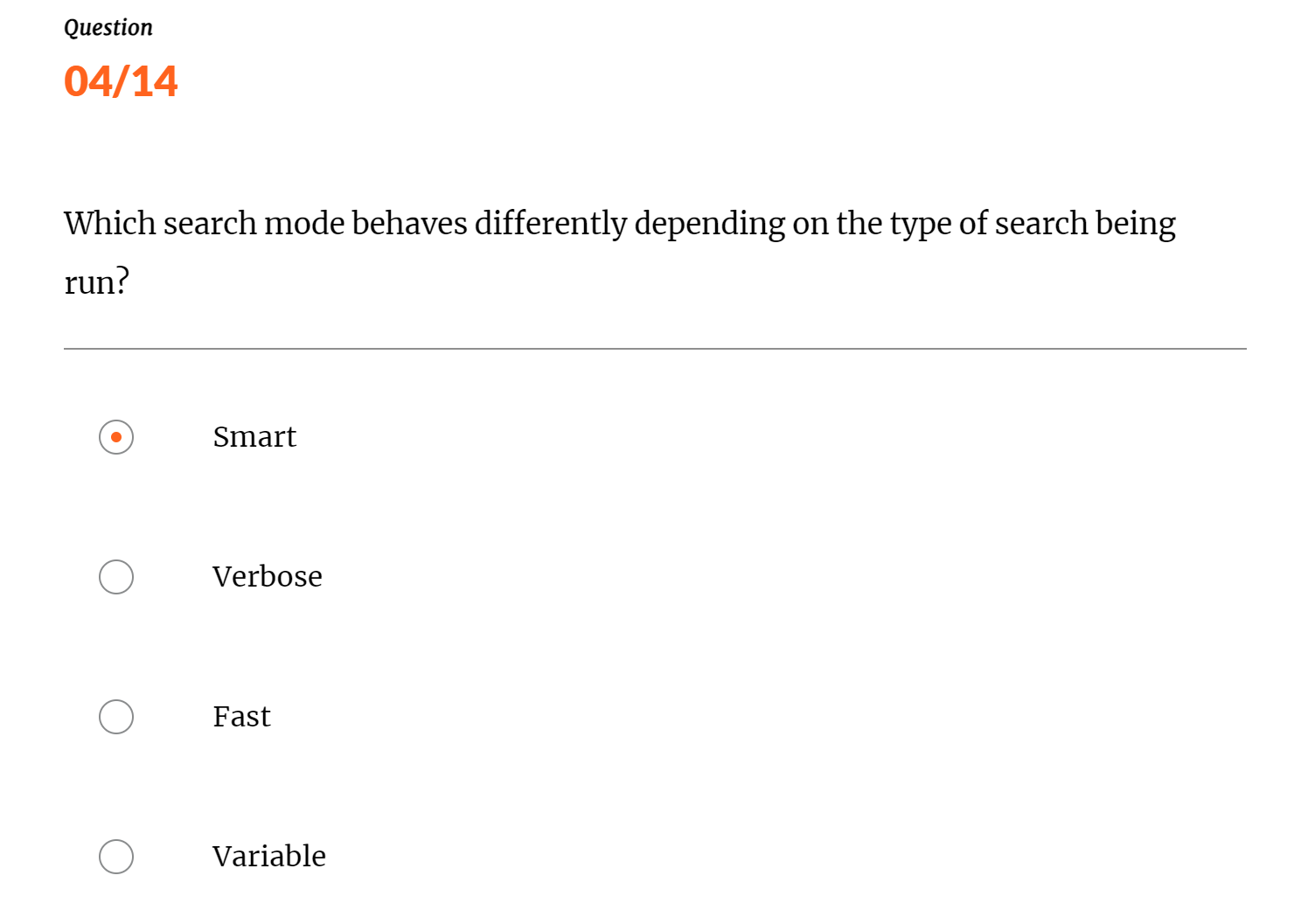
Smart

Verbose

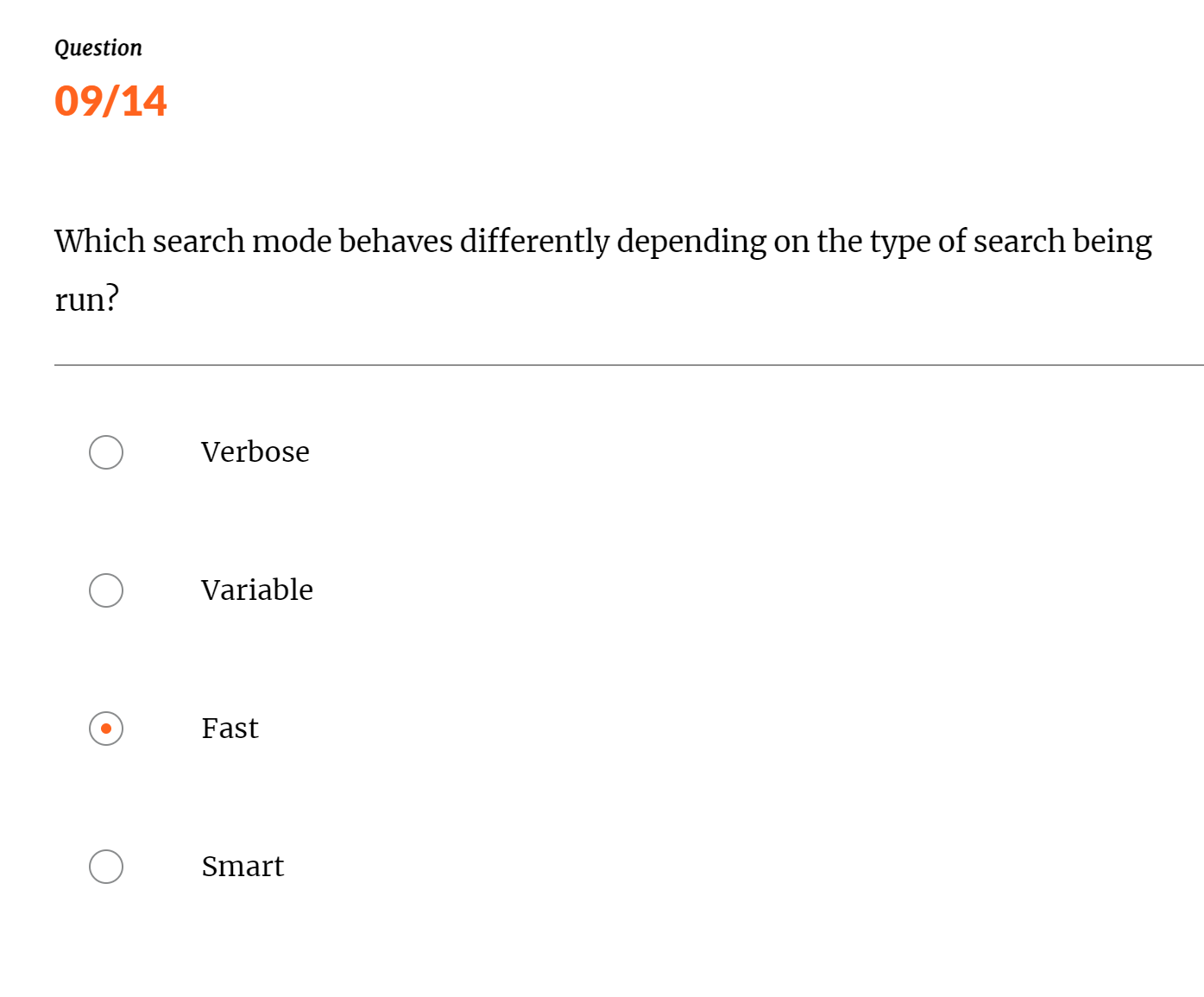
Fast

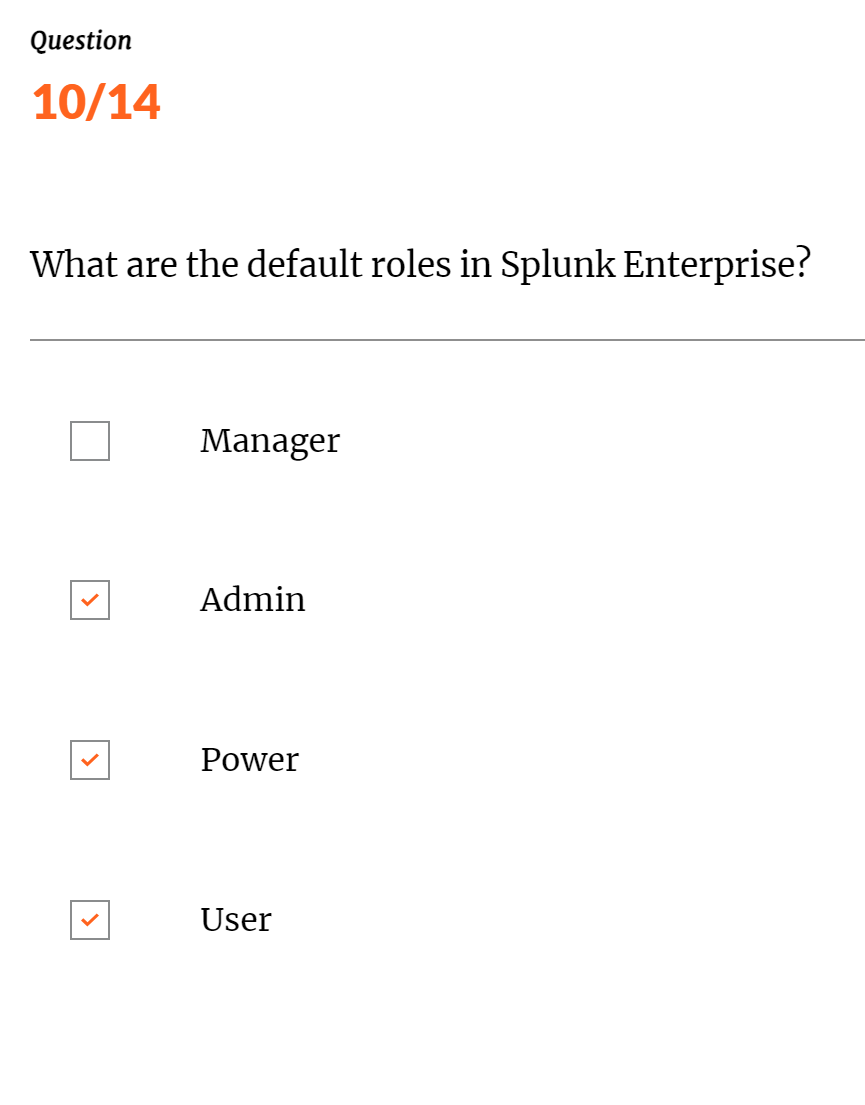
Variable

Answer by GPT: Smart



Below screenshot answer is wrong





1. Question

Which of the following booleans can be used in a search?

Can select multiple answers

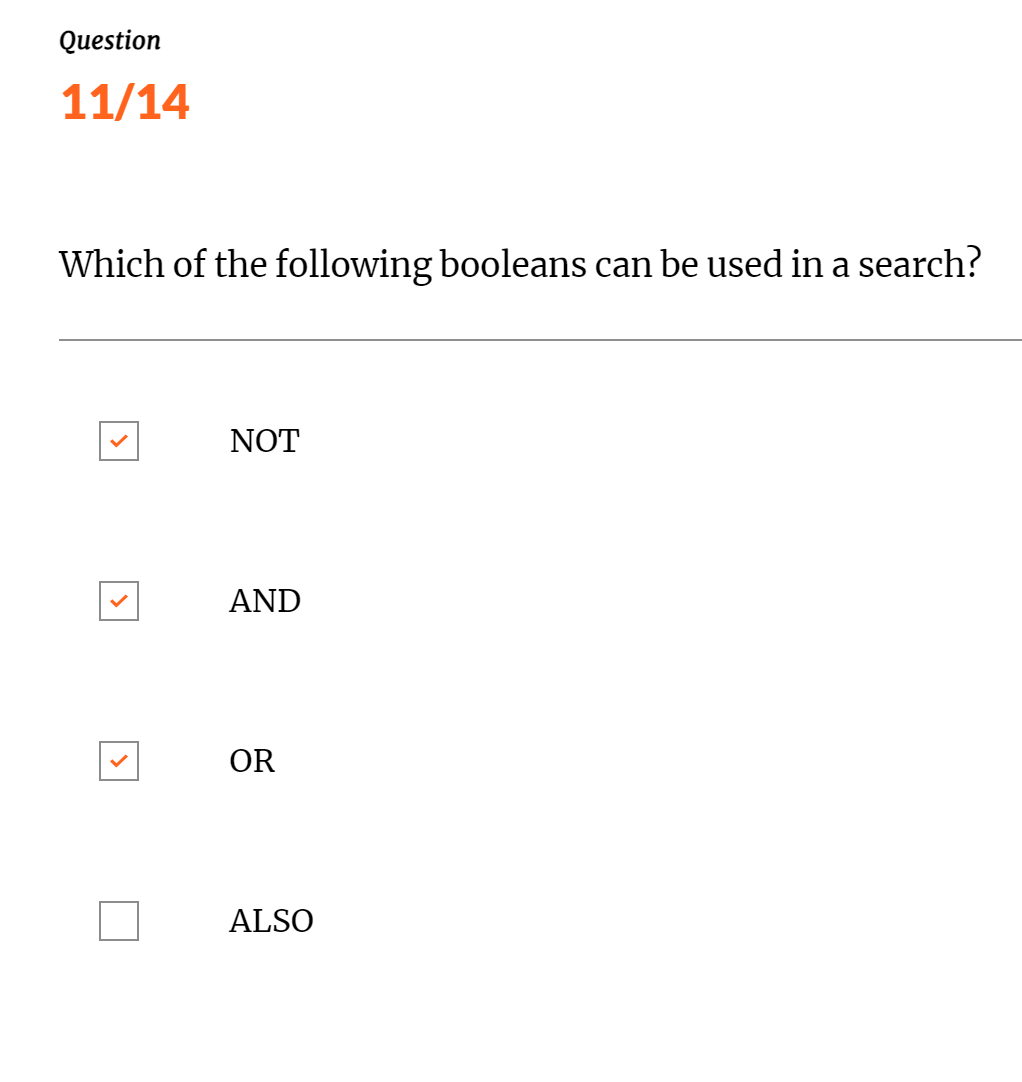
ALSO

OR

NOT

AND

Answer by GPT: OR, NOT,AND



12. Question

Which character is used in a search before a command?

Select one option

A tilde (~)

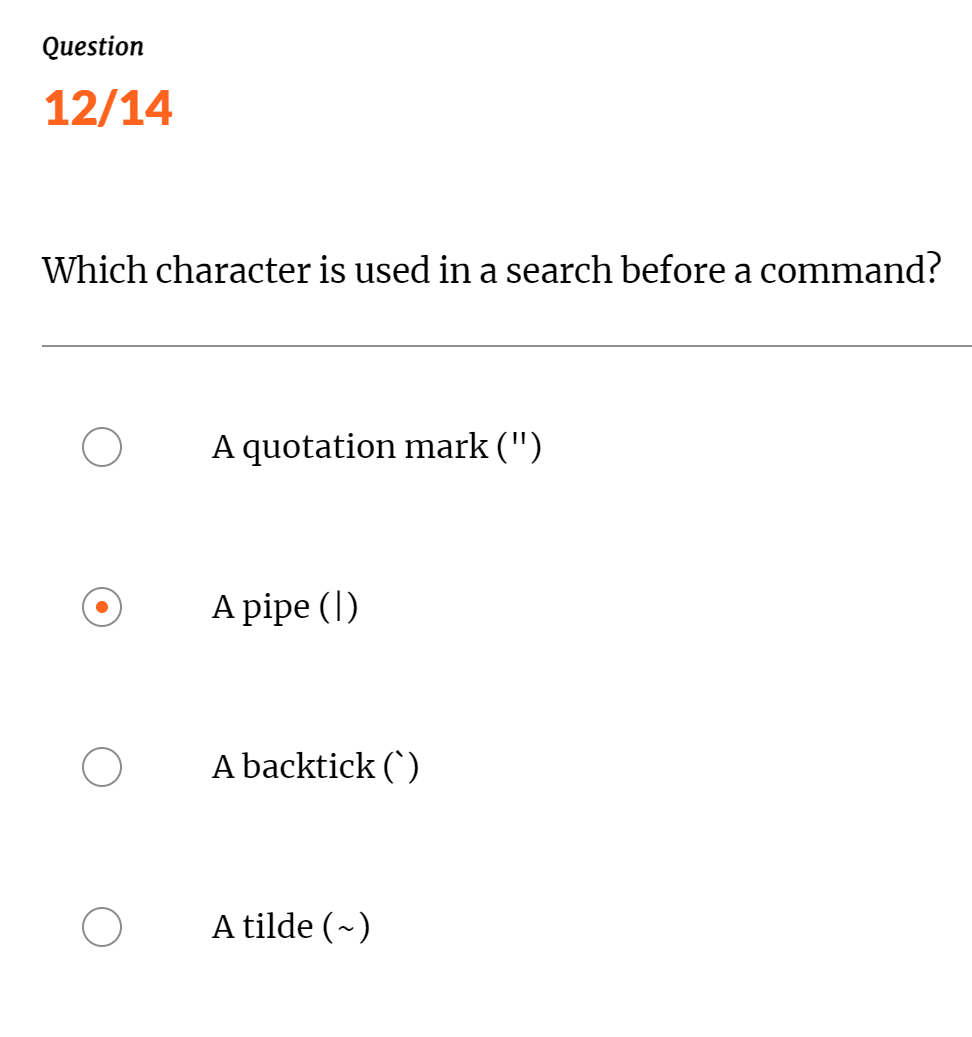
A pipe (|)

A quotation mark (")

A backtick (`)

Answer by GPT: A pipe (|).

In Splunk searches, the pipe character (|) is used before a command to pass the results of the preceding search command to the subsequent command. This is known as a pipeline and is used to chain multiple commands together for more complex queries and data processing.



13. Question

What are the default roles in Splunk Enterprise?

Can select multiple answers

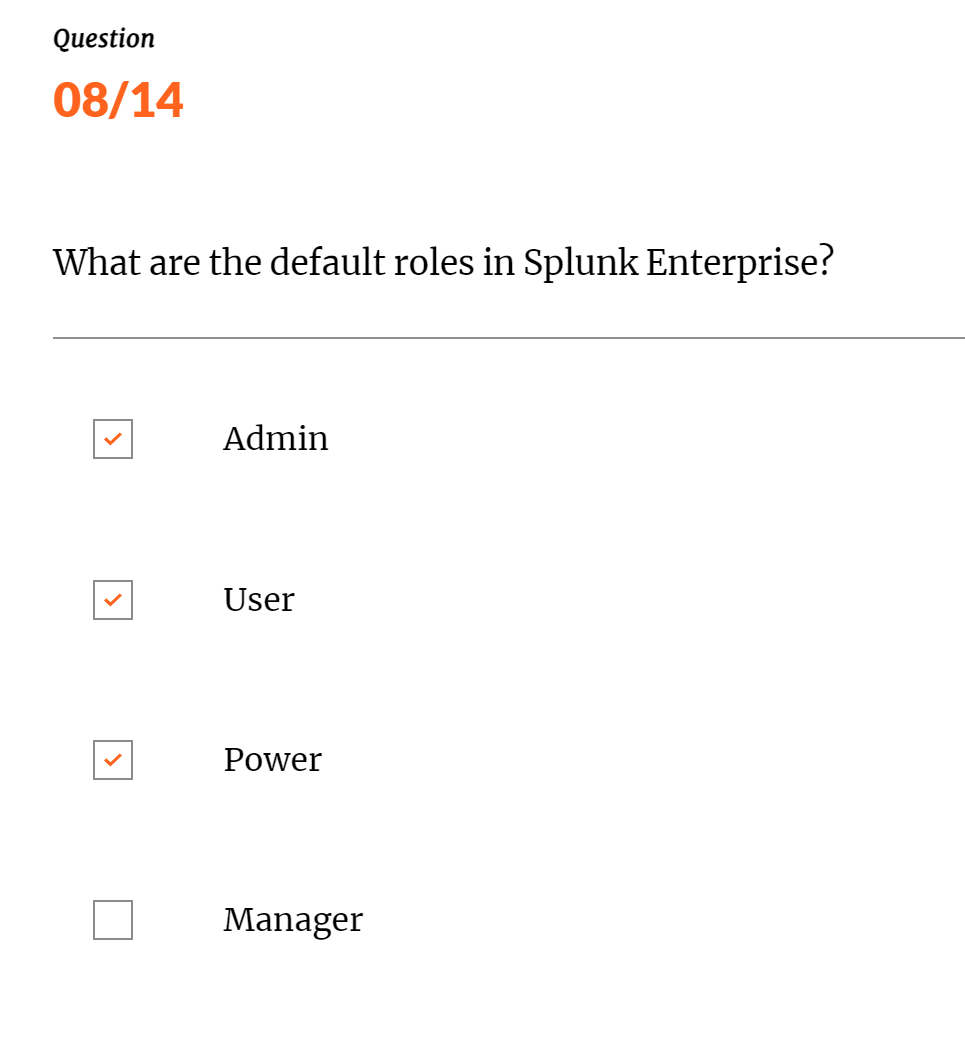
Admin

User

Power

Manager

Answer by GPT: Admin, User, Power



Question

By default, who is able to view a saved report?By default, which of the following roles are required to share knowledge objects?

Can select multiple answers

Manager

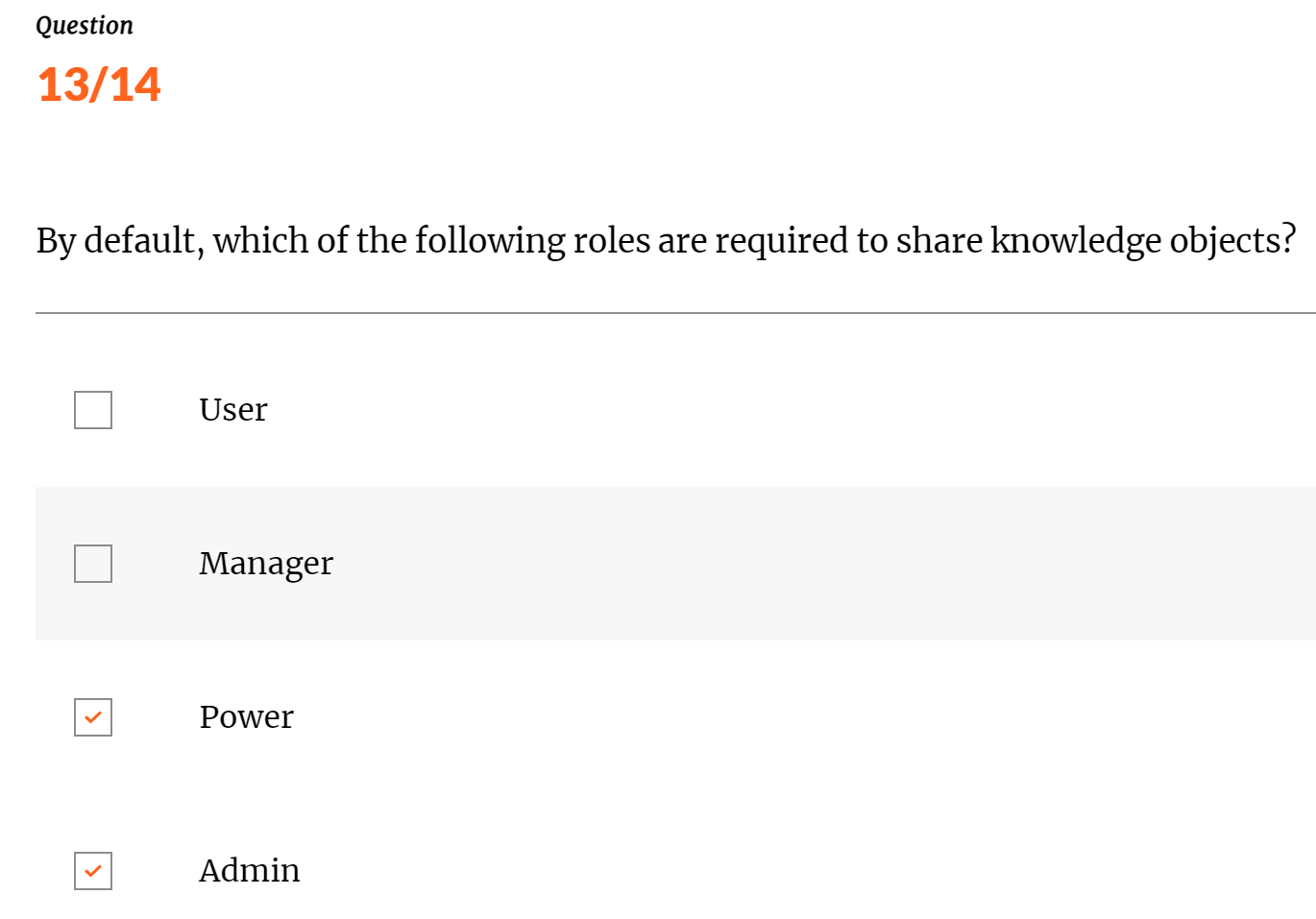
User

Power

Admin

Answer by GPT: Power , Admin

In Splunk, users with the Power or Admin roles can share knowledge objects, such as saved searches, reports, dashboards, and alerts. These roles have the necessary permissions to share and manage these objects, while the User role typically does not have sharing capabilities.



14. Question

What determines the timestamp shown on returned events in a search?

Select one option

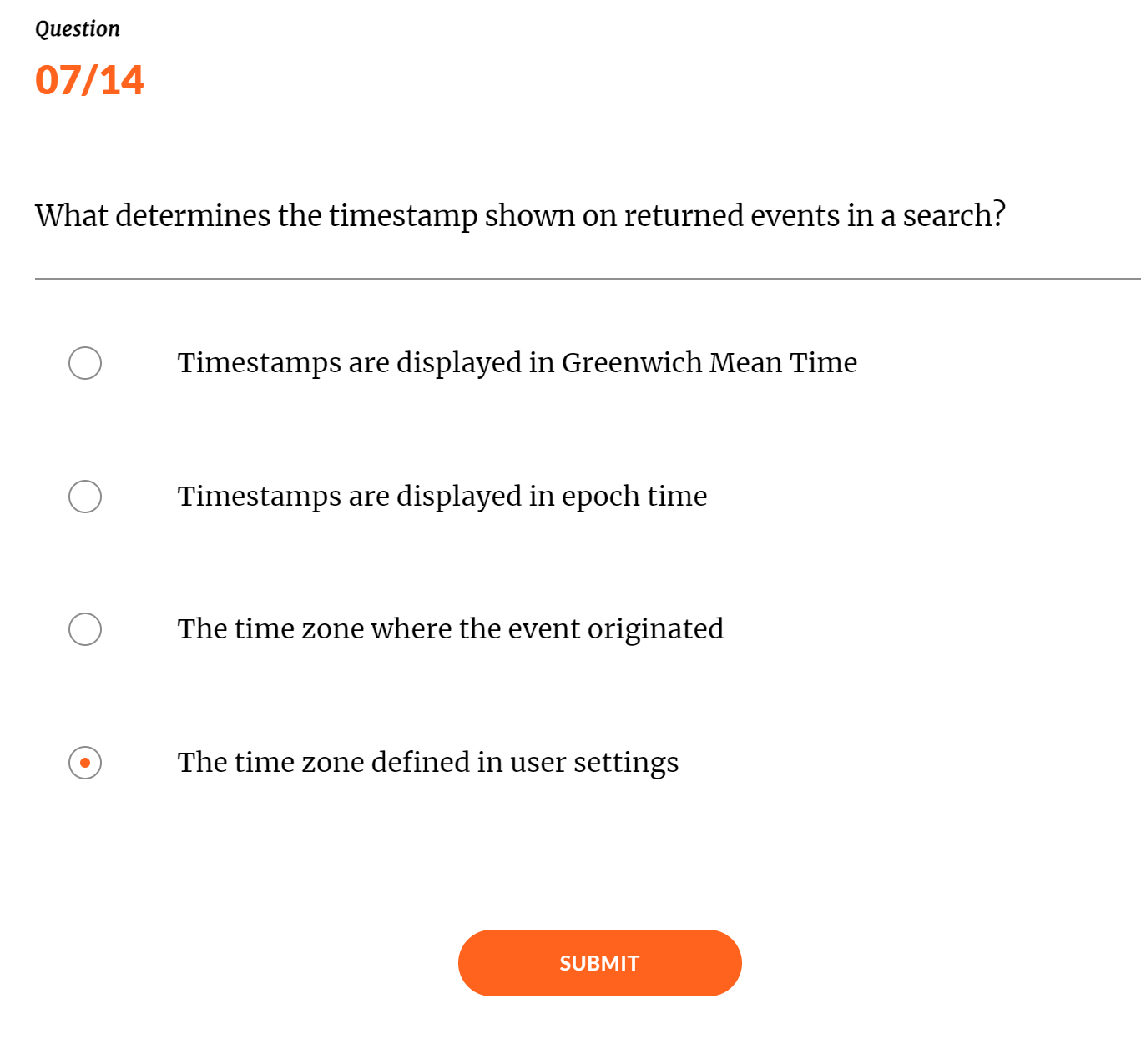
Timestamps are displayed in Greenwich Mean Time

Timestamps are displayed in epoch time

The time zone where the event originated

The time zone defined in user settings

Answer by GPT: The time zone defined in user settings



Below Scheenshot is may be wrong

