




# New SPLK-1002 Study Materials Exam Pass Certify | SPLK-1002: Splunk Core Certified Power User Exam



THE INSTITUTE OF  
CHARTERED ACCOUNTANTS  
OF SRI LANKA



**APPLICATIONS NOW ACCEPTED FOR  
ON-DEMAND EXAMS FOR BUSINESS LEVEL I & II  
- JUNE 2025 -**

Dear Students,

CA Sri Lanka is now accepting applications for on-demand examinations for Business Level I & II which will be held from 12th June 2025 onwards.

This is a computer-based exam and will be held at the following CA Sri Lanka locations:

- Head Office in Colombo 7
- Anuradhapura Branch
- Jaffna Branch
- Kalmunai Branch
- Kandy Branch
- Kurunegala Branch
- Matara Branch
- Ratnapura Branch

The on-demand exams will be held during the below time slots from the above date:

- 09:00 AM to 11:00 AM
- 12:00 Noon to 02:00 PM
- 03:00 PM to 05:00 PM

You can select a time slot of your choice when applying for the on-demand exam at a location of your preference. However, please note that time slots will be available on a first come first served basis.

The same exam will be held virtually only for students living overseas.

Students who wish to sit for the on-demand exams can register by clicking the link below **on or before 15th May 2025**, based on the availability of the time slots.

Please note that you should not apply for the same subject if you have already applied for the respective subject for the **May 2025 Business Level exam**.

Before submitting the exam application, it is mandatory for students to renew their studentship for 2025 and purchase the relevant study packs. Further, before registering for the on-demand exam, students must also pay the exam fee.

[CLICK HERE TO REGISTER ONLINE](#)

Director Examinations  
CA Sri Lanka

[www.casrilanka.com](http://www.casrilanka.com)

What's more, part of that Prep4away SPLK-1002 dumps now are free: [https://drive.google.com/open?id=1HE\\_EU1RnhU3eJJSzbxJfIdRL6VAiCUVZ2](https://drive.google.com/open?id=1HE_EU1RnhU3eJJSzbxJfIdRL6VAiCUVZ2)

Our Splunk Core Certified Power User Exam (SPLK-1002) exam questions are being offered in three easy-to-use and compatible formats. This SPLK-1002 exam dumps formats offer a user-friendly interface and are compatible with all devices, operating systems, and browsers. The Prep4away Splunk Core Certified Power User Exam (SPLK-1002) PDF questions file contains real and valid Splunk SPLK-1002 exam questions that assist you in SPLK-1002 exam dumps preparation and boost the candidate's confidence to pass the challenging Splunk Core Certified Power User Exam (SPLK-1002) exam easily.

Splunk is a data analytics tool that allows organizations to collect, analyze, and visualize large amounts of data from various sources. The SPLK-1002 Certification Exam tests the candidate's ability to use Splunk to extract meaningful insights from this data and make informed business decisions based on the results.

>> **New SPLK-1002 Study Materials** <<

## 2026 Authoritative 100% Free SPLK-1002 – 100% Free New Study Materials | Valid Splunk Core Certified Power User Exam Exam Tips

Our SPLK-1002 Exam Dumps with the highest quality which consists of all of the key points required for the SPLK-1002 exam can really be considered as the royal road to learning. Prep4away has already become a famous brand all over the world in this field since we have engaged in compiling the SPLK-1002 practice materials for more than ten years and have got a fruitful outcome. You are welcome to download the free demos to have a general idea about our SPLK-1002 training materials.

Splunk SPLK-1002 Certification Exam is a highly sought-after certification for IT professionals who are interested in mastering the core concepts of Splunk. SPLK-1002 exam is designed to test the knowledge and skills of the candidates in using Splunk to collect, analyze, and visualize data from various sources. Splunk Core Certified Power User Exam certification is the second level of certification in the Splunk certification program, following the Splunk SPLK-1001 certification.

## Splunk Core Certified Power User Exam Sample Questions (Q221-Q226):

### NEW QUESTION # 221

How is an event type created from the search window? (select all that apply)

- A. In an event's detail dropdown, click Event Actions > Build Event Type.
- B. In the top right corner, click Save As > Event Type.
- C. Edit `eventtypes.conf` and add a new stanza.
- D. Add `| eventtype` to the SPL and execute the search.

**Answer: B,C**

Explanation:

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type<sup>1</sup>. This opens the Save as Event Type dialog, where you can provide the event type name and optionally apply tags to it<sup>1</sup>.

You can also create an event type by editing the `eventtypes.conf` file and adding a new stanza<sup>1</sup>. Each stanza in the `eventtypes.conf` file represents an event type<sup>1</sup>. The stanza name is the name of the event type, and the search attribute specifies the search string that defines the event type<sup>1</sup>.

It's important to note that while you can use the `eventtype` command in a search to find events associated with a specific event type, adding `| eventtype` to the SPL and executing the search does not create a new event type<sup>1</sup>. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create a new event type<sup>1</sup>.

### NEW QUESTION # 222

Selected fields are displayed \_\_\_\_\_ each event in the search results.

- A. below
- B. interesting fields
- C. above
- D. other fields

**Answer: A**

Explanation:

Explanation

Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the `fields` command<sup>2</sup>. Selected fields are displayed below each event in the search results, along with their values<sup>2</sup>. Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

### NEW QUESTION # 223

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Verbose
- B. Smart
- C. Fast

**Answer: A**

Explanation:

The search modes determine how Splunk processes your search and displays your results<sup>2</sup>. There are three search modes: Fast, Smart and Verbose<sup>2</sup>. The search mode that automatically returns all extracted fields in the fields sidebar is Verbose<sup>2</sup>. The Verbose mode shows all the fields that are extracted from your events, including default fields, indexed fields and search-time extracted fields<sup>2</sup>. The fields sidebar is a panel that

shows the fields that are present in your search results<sup>2</sup>. Therefore, option C is correct, while options A and B are incorrect because they are not search modes that automatically return all extracted fields in the fields sidebar.

#### NEW QUESTION # 224

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

- A. tag=Priv\*
- B. tag=priv\*
- C. tag=Priv
- D. tag=privileged

**Answer: A**

Explanation:

Explanation/Reference: <https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity>

#### NEW QUESTION # 225

Two separate results tables are being combined using the |join command. The outer table has the following values:  
Refer to following Tables

email	employeeNumber <sup>®</sup>
jsmith@acme.com	1
mcarpenter@acme.com	2
jrogers@acme.com	3
bsparrow@acme.com	4
eripper@acme.com	5

The inner table has the following values:

employeeNumber	firstName	lastName
1	John	Smith
2	Mary	Carpenter
3	Jeff	Rogers

The line of SPL used to join the tables is: |join employeeNumber type=outer How many rows are returned in the new table?

- A. Three
- B. Five
- C. Zero
- D. Eight

**Answer: D**

Explanation:

When performing an outer join in Splunk using the |join employeeNumber type=outer command, it combines the rows from both tables based on the employeeNumber field. An outer join returns all rows from both tables, with matching rows from both sides where available. If there is no match, the result is NULL on the side of the join where there is no match.

In the provided tables, there are five rows in the first table and three in the second. Since it's an outer join, all rows from both tables will be returned. This means the new table will have a total of eight rows, combining the matched rows and the unmatched rows from both tables.

References:

\* Splunk Documentation on the join command.

\* Splunk Community discussions on the usage of join and types of joins.

### NEW QUESTION # 226

• • • • •

**Valid SPLK-1002 Exam Tips:** <https://www.prep4away.com/Splunk-certification/braindumps.SPLK-1002.etc.file.html>

- [illegible]

BONUS!!! Download part of Prep4away SPLK-1002 dumps for free: [https://drive.google.com/open?id=1HE\\_EU1RnhU3eJJSzbxfjdRL6VAiCUVZ2](https://drive.google.com/open?id=1HE_EU1RnhU3eJJSzbxfjdRL6VAiCUVZ2)