

## SPLK-1001 Dumps

### Splunk Core Certified User Exam

<https://www.certleader.com/SPLK-1001-dumps.html>



**NEW QUESTION 1**

Which of the following is a Splunk search best practice?  
Splunk Core Certified User

- 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.

**Answer:** A

**NEW QUESTION 2**

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)

**Answer:** A

**NEW QUESTION 3**

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

**Answer:** A

**NEW QUESTION 4**

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.

**Answer:** A

**NEW QUESTION 5**

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.

**Answer:** C

**NEW QUESTION 6**

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

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

**Answer:** B

**NEW QUESTION 7**

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

- A. Time
- B. Fast mode
- C. Sourcetype
- D. Selected Fields

**Answer:** C

**NEW QUESTION 8**

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.

**Answer:** D

#### NEW QUESTION 9

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 “error failure”
- D. index=security NOT error NOT fail

**Answer:** B

#### NEW QUESTION 10

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.

**Answer:** B

#### NEW QUESTION 10

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.

**Answer:** A

#### NEW QUESTION 14

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.

**Answer:** C

#### NEW QUESTION 15

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.

**Answer:** D

#### NEW QUESTION 17

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

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

**Answer:** ACF

#### NEW QUESTION 20

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.

**Answer:** A

**NEW QUESTION 24**

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

- A. True
- B. False

**Answer:** A

**NEW QUESTION 26**

All components are installed and administered in Splunk Enterprise on-premise.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Explanation/Reference:

- B. False

Answer:

**NEW QUESTION 30**

You can on-board data to Splunk using following means (Choose four.):

- A. Props
- B. CLI
- C. Splunk Web
- D. savedsearches.conf
- E. Splunk apps and add-ons
- F. indexes.conf
- G. inputs.conf
- H. metadata.conf

**Answer:** BCEG

**NEW QUESTION 35**

Parsing of data can happen both in HF and UF.

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 37**

Upload option creates inputs.conf

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 41**

In monitor option you can select the following options in GUI.

- A. Only HTTP Event Collector (HEC) and TCP/UDP
- B. None of the above
- C. Only TCP/UDP
- D. Only Scripts
- E. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

**Answer:** E

**NEW QUESTION 46**

Matching search terms are highlighted.

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 49**

Splunk Parses data into individual events, extracts time, and assigns metadata.

- A. False
- B. True

**Answer:** B

**NEW QUESTION 51**

There are three different search modes in Splunk (Choose three.):

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

**Answer:** BCD

**NEW QUESTION 56**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SPLK-1001 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SPLK-1001-dumps.html>