

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

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.

Answer: D

NEW QUESTION 3

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

- A. lookup
- B. csvlookup
- C. inputlookup
- D. outputlookup

Answer: C

NEW QUESTION 4

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.

Answer: C

NEW QUESTION 5

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.

Answer: C

NEW QUESTION 6

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 7

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 8

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.

Answer: A

NEW QUESTION 9

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

- A. dedup
- B. rename
- C. sort -
- D. fields +

Answer: A

NEW QUESTION 10

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

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 13

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 14

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 19

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 21

Which is the default app for Splunk Enterprise?

- A. Splunk Enterprise Security Suite
- B. Searching and Reporting
- C. Reporting and Searching
- D. Splunk apps for Security

Answer: B

NEW QUESTION 22

Portal for Splunk apps can be accessed through www.splunkbase.com

- A. False
- B. True

Answer: B

NEW QUESTION 25

What result will you get with following search `index=test sourcetype="The_Questionnaire_P"` ?

- A. the_questionnaire _pedia
- B. the_questionnaire pedia
- C. the_questionnaire_pedia
- D. the_questionnaire Pedia

Answer: C

NEW QUESTION 27

Forward Option gather and forward data to indexers over a receiving port from remote machines.

- A. False
- B. True

Answer: B

NEW QUESTION 30

Select the correct option that applies to Index time processing (Choose three.).

- A. Indexing
- B. Searching
- C. Parsing
- D. Settings
- E. Input

Answer: ACE

NEW QUESTION 33

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 34

Matching search terms are highlighted.

- A. Yes
- B. No

Answer: A

NEW QUESTION 36

The default host name used in Inputs general settings can not be changed.

- A. False
- B. True

Answer: A

NEW QUESTION 39

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

- A. False
- B. True

Answer: B

NEW QUESTION 41

Which symbol is used to snap the time?

- A. @
- B. &
- C. *
- D. #

Answer: A

NEW QUESTION 45

.....

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>