Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
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 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
What can be included in the All Fields option in the sidebar?

A. Dashboards
B. Metadata only
C. Non-interesting fields
D. Field descriptions

Answer: D

NEW QUESTION 5
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 6
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.

Answer: C

NEW QUESTION 7
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

Answer: C

NEW QUESTION 8
Which component of Splunk let us write SPL query to find the required data?

A. Forwarders
B. Indexer
C. Heavy Forwarders
D. Search head

Answer: D

NEW QUESTION 9
Splunk shows data in _____ .

A. ASCII Character order.
B. Reverse chronological order.
C. Alphanumeric order.
D. Chronological order.

Answer: B

NEW QUESTION 10
Forward Option gather and forward data to indexers over a receiving port from remote machines.

A. False
B. True

Answer: B

NEW QUESTION 10
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 14
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 19
Where does Licensing meter happen?

A. Indexer
B. Parsing
C. Heavy Forwarder
D. Input

Answer: A

NEW QUESTION 23
There are three different search modes in Splunk (Choose three.):

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

Answer: BCD

NEW QUESTION 27
You can view the search result in following format (Choose three.):

A. Table
B. Raw
C. Pie Chart
D. List

Answer: ABD

NEW QUESTION 28
Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts
B. Sourcetypes
C. Sources
D. Indexes

Answer: ABC

NEW QUESTION 33
......

Relate Links

100% Pass Your SPLK-1001 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-1001-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/