SPLK-1003Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer

B. Deployer

C. Forwarder

D. Deployment server

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Updating/Updateconfigurations

QUESTION 2

Which of the following is accurate regarding the input phase?

A. Breaks data into events with timestamps.

B. Applies event-level transformations.

C. Fine-tunes metadata.

D. Performs character encoding.

Correct Answer: D

"The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."

QUESTION 3

When using license pools, volume allocations apply to which Splunk components?

A. Indexers

B. Indexes

C. Heavy Forwarders

D. Search Heads

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/Admin/Groups,stacks,pools,andotherterminology

QUESTION 4

You update a props. conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btoo1 props list --debug. What will the output be?

A. list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props. conf configurations as they are on-disk along with a file path from which the configuration is located

D. A list of the current running props, conf configurations along with a file path from which the configuration was made

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroublesh ootconfigurations

"The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."

"The report does not necessarily represent what\\'s loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn\\'t active."

QUESTION 5

What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

A. License data

B. Metricsdata

C. Internal Splunk data

D. Internal Windows logs

Correct Answer: B