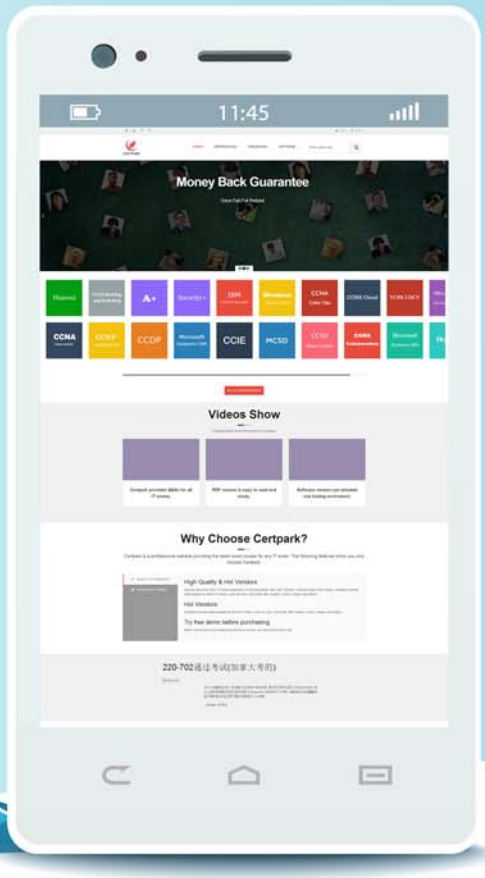
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **SPLK-1003**

Title : Splunk Enterprise Certified Admin

Version : DEMO

1.How is data handled by Splunk during the input phase of the data ingestion process?
A. Data is treated as streams.
B. Data is broken up into events.
C. Data is initially written to disk.
D. Data is measured by the license meter.
Answer: A
Explanation:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline "In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks in into 64K blocks, and annotates each block with some metadata keys."
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Deploy/Datapipeline

2.What conf file needs to be edited to set up distributed search groups?
A. props.conf
B. search.conf
C. distsearch.conf
D. distibutedsearch.conf
Answer: C
Explanation:
"You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file"
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

3.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.
Answer: D
Explanation:
https://docs.splunk.com/Documentation/Splunk/latest/Deploy/Datapipeline "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."

4.What action is required to enable forwarder management in Splunk Web?
A. Navigate to Settings > Server Settings > General Settings, and set an App server port.
B. Navigate to Settings > Forwarding and receiving, and click on Enable Forwarding.
C. Create a server class and map it to a client in SPLUNK_HOME/etc/system/local/serverclass.conf.
D. Place an app in the SPLUNK_HOME/etc/deployment-apps directory of the deployment server.
Answer: C

Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Forwardermanagementoverview
https://docs.splunk.com/Documentation/MSApp/2.0.3/MSInfra/Setupadeploymentserver
"To activate deployment server, you must place at least one app
into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. In this case, the app is the "send to indexer" app you created earlier, and the host is the indexer you set up initially.

5.Which Splunk forwarder type allows parsing of data before forwarding to an indexer?
A. Universal forwarder
B. Parsing forwarder
C. Heavy forwarder
D. Advanced forwarder
Answer: C