SPLK-1003$^{Q\&As}$

Splunk Enterprise Certified Admin

QUESTION 1

What are the minimum required settings when creating a network input in Splunk?

A. Protocol, port number

B. Protocol, port, location

C. Protocol, username, port

D. Protocol, IP. port number

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf

[tcp://:]

*Configures the input to listen on a specific TCP network port. *If a makes a connection to this instance, the input uses this stanza to configure itself.

*If you do not specify , this stanza matches all connections on the specified port.

*Generates events with source set to "tcp:", for example: tcp:514 *If you do not specify a sourcetype, generates events with sourcetype set to "tcp-raw"

QUESTION 2

Where are license files stored?

A. $SPLUNK_HOME/etc/secure

B. $SPLUNK_HOME/etc/system

C. $SPLUNK_HOME/etc/licenses

D. $SPLUNK_HOME/etc/apps/licenses

Correct Answer: C

QUESTION 3

In which phase of the index time process does the license metering occur?

A. input phase

B. Parsing phase

C. Indexing phase

D. Licensing phase

Correct Answer: C

"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks

---

QUESTION 4

How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.

B. By rescanning active forwarders.

C. By reloading the deployment server.

D. By rebuilding the forwarder asset table.

Correct Answer: D

QUESTION 5

When running a real-time search, search results are pulled from which Splunk component?

A. Heavy forwarders and seach peers

B. Heavy forwarders

C. Search heads

D. Search peers

Correct Answer: D

Using the Splunk reference URL https://docs.splunk.com/Splexicon:Searchpeer

"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."