SPLK-1003 Q&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.leads4pass.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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 2

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

QUESTION 3

When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.

B. Enable forwarder acknowledgment.

C. splunk check-integrity -index

D. index=_internal component=ACK | stats count by host

Correct Answer: A

Per the provided Splunk reference URL

"While HEC has precautions in place to prevent data loss, it\\'s impossible to completely prevent such an occurrence, especially in the event of a network failure or hardware crash.

This is where indexer acknolwedgment comes in."

Reference https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

QUESTION 4

Which of the following is a valid distributed search group?

A. [distributedSearch:Paris] default = false servers = server1, server2

B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089

C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997

D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

Correct Answer: D

QUESTION 5

Which of the following accurately describes HTTP Event Collector indexer acknowledgement?

A. It requires a separate channel provided by the client.

B. It is configured the same as indexer acknowledgement used to protect in-flight data.

C. It can be enabled at the global setting level.

D. It stores status information on the Splunk server.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/AboutHECIDXAck

Section: About channels and sending data

Sending events to HEC with indexer acknowledgment active is similar to sending them with the setting off. There is one crucial difference: when you have indexer acknowledgment turned on, you must specify a channel when you send

events. The concept of a channel was introduced in HEC primarily to prevent a fast client from impeding the performance of a slow client. When you assign one channel per client, because channels are treated equally on Splunk Enterprise,

one client can\\'t affect another. You must include a matching channel identifier both when sending data to HEC in an HTTP request and when requesting acknowledgment that events contained in the request have been indexed. If you don\\'t,

you will receive the error message, "Data channel is missing." Each request that includes a token for which indexer acknowledgment has been enabled must include a channel identifier, as shown in the following example cURL statement,

where represents the event data portion of the request