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 this example, if useACK is set to true and the maxQueueSize is set to 7MB, what is the size of the wait queue on this universal forwarder?

A. 21MB

B. 28MB

C. 14MB

D. 7MB

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/SplunkCloud/latest/Forwarding/Protectagainstlossofin-flightdata

QUESTION 2

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 3

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 4

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdat a

QUESTION 5

What options are available when creating custom roles? (select all that apply)

A. Restrict search terms

B. Whitelist search terms

C. Limit the number of concurrent search jobs

D. Allow or restrict indexes that can be searched.

Correct Answer: ACD

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits "Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."