SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

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

https://www.passapply.com/splk-3001.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

Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?

A. SplunkWeb (8068), Splunk Management (8089), KV Store (8000)

B. SplunkWeb (8390), Splunk Management (8323), KV Store (8672)

C. SplunkWeb (8000), Splunk Management (8089), KV Store (8191)

D. SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

QUESTION 2

Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.

B. Removing throttling fields.

C. Increasing the throttling window.

D. Increasing threshold sensitivity.

Correct Answer: A

QUESTION 3

How is it possible to specify an alternate location for accelerated storage?

A. Configure storage optimization settings for the index.

B. Update the Home Path setting in indexes, conf

C. Use the tstatsHomePath setting in props, conf

D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C

QUESTION 4

What are adaptive responses triggered by?

A. By correlation searches and users on the incident review dashboard.

B. By correlation searches and custom tech add-ons.

C. By correlation searches and users on the threat analysis dashboard.

D. By custom tech add-ons and users on the risk analysis dashboard.

Correct Answer: D

QUESTION 5

A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.

Which of the following options is most likely to help performance?

A. Change the search heads to do local indexing of summary searches.

B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.

C. Increase memory and CPUs on the search head(s) and add additional indexers.

D. If indexed realtime search is enabled, disable it for the notable index.

Correct Answer: C