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

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?

A. $fieldname$

B. "fieldname"

C. %fieldname%

D. _fieldname_

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

QUESTION 2

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 3

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 4

Which tool Is used to update indexers In E5?

A. Index Updater

B. Distributed Configuration Management

C. indexes.conf

D. Splunk_TA_ForIndexeres. spl

Correct Answer: B

QUESTION 5

Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t

B. summaries=all

C. summariesonly=t

D. summariesonly=all

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels