SPLK-1001^{Q&As}

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

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

https://www.pass4itsure.com/splk-1001.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

Universal forwarder is recommended for forwarding the logs to indexers.

A. False

B. True

Correct Answer: B

QUESTION 2

In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type

B. App, Owner, Priority, and Status

C. App, Dashboard, Severity, and Type

D. App, Time Window, Type, and Severity

Correct Answer: D

QUESTION 3

Splunk apps are used for following (Choose three.):

A. Designed to cater numerous use cases and empower Splunk.

B. We can not install Splunk App.

C. Allows multiple workspaces for different use cases/user roles.

D. It is collection of different Splunk config files like data inputs, UI and Knowledge Object.

Correct Answer: ACD

QUESTION 4

Parsing of data can happen both in HF and UF.

A. Yes

B. No

Correct Answer: B

QUESTION 5

What kind of logs can Splunk Index?

A. Only A, B

B. Router and Switch Logs

C. Firewall and Web Server Logs

D. Only C

E. Database logs

F. All firewall, web server, database, router and switch logs

Correct Answer: F

<table>
<tr><td>Latest SPLK-1001 Dumps</td><td>SPLK-1001 PDF Dumps</td><td>SPLK-1001 VCE Dumps</td></tr>
</table>