Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **SPLK-1001**

Title : Splunk Core Certified User

Version : DEMO

1.Which search string only returns events from hostWWW3?
A. host=*
B. host=WWW3
C. host=WWW*
D. Host=WWW3
Answer: B

2.By default, how long does Splunk retain a search job?
A. 10 Minutes
B. 15 Minutes
C. 1 Day
D. 7 Days
Answer: A
Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

3.What must be done before an automatic lookup can be created? (Choose all that apply.)
A. The lookup command must be used.
B. The lookup definition must be created.
C. The lookup file must be uploaded to Splunk.
D. The lookup file must be verified using the inputlookup command.
Answer: B
Explanation:
Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/DefineanautomaticlookupinSplunkWeb

4.Which of the following Splunk components typically resides on the machines where data originates?
A. Indexer
B. Forwarder
C. Search head
D. Deployment server
Answer: B

5.What determines the scope of data that appears in a scheduled report?
A. All data accessible to the User role will appear in the report.
B. All data accessible to the owner of the report will appear in the report.
C. All data accessible to all users will appear in the report until the next time the report is run.
D. The owner of the report can configure permissions so that the report uses either the User role or the owner’s profile at run time.
Answer: D
Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Managereportpermissions