

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : 050-11-CARSANWLN01

**Title : RSA NetWitness Logs &
Network Administrator Exam**

Version : DEMO

1.To report on matches in the NWDB against a series of fixed values, include which feature in your report definition?

- A. An Application Rule
- B. A List
- C. An Enrichment Source
- D. A Subscription

Answer: B

2.To create a custom feed, initiate the action by selecting which top-level module?

- A. Investigate
- B. Admin
- C. Monitor
- D. Configure

Answer: D

3.Which of the following choices is defined as being a delineated set of network data units that comprise a transaction from start to finish'?

- A. Frame
- B. Packet
- C. Session
- D. Token

Answer: C

4.In RSA NetWitness. viewing text or image data associated with a session is accessed through a

- A. packet level drill
- B. meta value view
- C. session reconstruction view
- D. decoder analysis view

Answer: C

5.When storage on the core devices fills to capacity, what happens?

- A. new traffic cannot be ingested
- B. the decoder leverages capacity in the concentrator, and collection continues
- C. the decoder leverages capacity in the broker, and collection continues
- D. the oldest stored sessions are deleted and collection continues

Answer: D