

# **RSA**

**050-11-CARSANWLN01 Exam**

**RSA NetWitness Logs & Network Administrator**

**[Questions & Answers Demo]**

# Version: 7.1

---

**Question: 1**

---

Application rules can be configured on

- A. Log Decoder
- B. Log Decoder and Packet Decoder
- C. Log Decoder, Packet Decoder, and Concentrator
- D. Log Decoder, Packet Decoder, Concentrator, and Broker

---

**Answer: B**

---

---

**Question: 2**

---

The RSA NetWitness Reporting Engine provides visibility into captured data via which of the following mechanisms?

- A. static and/or dynamic analysis
- B. alerts, reports and charts
- C. community and/or sandbox analysis
- D. ad hoc, schedules, and/or auto-run features

---

**Answer: C**

---

---

**Question: 3**

---

Which of the following statements about Health and Wellness Policies is false?

- A. Policies can be defined by NW administrators
- B. Out-of-the-box policies are enabled by default
- C. Out-of-the-box policies can be edited by NW administrators
- D. Out-of-the-box policies are provided for most NW services

---

**Answer: C**

---

---

**Question: 4**

---

When adding a data source to the ESA device. RSA recommends using only the

- A. Concentrator
- B. Decoder
- C. Log Collector
- D. Archiver

---

**Answer: A**

---

---

**Question: 5**

---

To run a report you need to create which of the following?

- A. View
- B. Alert
- C. Report rule
- D. Schedule

---

**Answer: C**

---

---

**Question: 6**

---

What are the two types of device index files available in RSA NetWitness?

- A. index.xml and index.orig.xml
- B. index-rsa.txt and index-custom.txt
- C. index-rsa.xml and index-custom.xml
- D. index-<device>.xml and index-<device>-custom.xml

---

**Answer: D**

---

---

**Question: 7**

---

What is the definition of an RSA NetWitness ad hoc feed?

- A. A feed that is deployed one time on one or more Decoders
- B. A feed that is deployed once on three or more Decoders
- C. A feed that is deployed on no more than three Decoders once
- D. A feed that is deployed on one or more Decoders at least three times

---

**Answer: A**

---