

DUMPSBOSS.

RSA NetWitness Logs & Network Administrator Exam

RSA 050-11-CARSANWLN01

Version Demo

Total Demo Questions: 10

Total Premium Questions: 71

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

To create a feed for all of your event sources, you could:

- A. Deploy a feed from Live
- B. Export event source data from the Manage Events Sources interface and create a custom feed
- C. Create a log parser
- D. Export event source data from the Manage Events Sources interface and create an identity feed

ANSWER: B

QUESTION NO: 2

Which of the following is a valid data source for Respond Alerts?

- A. Live Feeds
- B. Application Rules
- C. Network Rules
- D. Reporting Engine

ANSWER: D

QUESTION NO: 3

Which of the following statements about the REST interface are true? (Choose two)

- A. The REST interface is available only for Concentrators and Decoders
- B. The REST interface is available separately for each core Service on the Host
- C. The REST interface for the Broker service defaults to 50103
- D. The REST interface for the Concentrator service defaults to 51005
- E. The REST interface for the Decoder service defaults to 50014

ANSWER: B C

QUESTION NO: 4

Where is the PAM configuration file located on an RSA NetWitness appliance'?

- A. /etc/hosts
- B. /etc/pam.d
- C. /opt/bin/pam
- D. /usr/bin/config

ANSWER: B

QUESTION NO: 5

To allow for automatic email notification when your reports have run. (Choose two)

- A. create a Report Rule
- B. enable email notification in the Report rule
- C. enable email notification in the Report Schedule view
- D. create an output action in the Reporting Engine configuration
- E. add the mail server as a data source to the Reporting Engine

ANSWER: C D

QUESTION NO: 6

Which of the following are valid sources for the Context Hub? (Choose two)

- A. RSA Endpoint
- B. Respond Server
- C. Health and Wellness module
- D. Web Threat Detection

E. Reporting Engine

ANSWER: A B

QUESTION NO: 7

In order to run Reports against data stored on the Archiver you must

- A. restore data from cold storage to any hot storage device
- B. restore the Archiver data to any Concentrator
- C. add the Archiver to the Reporting Engine's list of configured data sources
- D. add the Archiver to the Concentrator's list of configured data sources

ANSWER: C

QUESTION NO: 8

If you choose "Stop Rule Processing" in your Application Rule definition, which of the following are action choices? (Choose three)

- A. Keep
- B. Filter
- C. Truncate
- D. Index
- E. Transient
- F. Remove

ANSWER: A B C

Explanation:

<https://community.rsa.com/docs/DOC-42041>

QUESTION NO: 9

Administrators can use the Profile feature to limit views with (Choose three)

- A. Meta groups
- B. Custom column groups
- C. Assigned pre-queries
- D. Automated role assignment
- E. Data privacy policies
- F. List view

ANSWER: A B C

QUESTION NO: 10

RSA NetWitness services implement what type of access control?

- A. Role-based
- B. Digital Certificate-based
- C. Access Control List (ACL)
- D. Discretionary Access Control (DAC)

ANSWER: A