



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.



050-11-CARSANWLN01 Dumps
050-11-CARSANWLN01 Braindumps
050-11-CARSANWLN01 Real Questions
050-11-CARSANWLN01 Practice Test
050-11-CARSANWLN01 Actual Questions



RSA

050-11-CARSANWLN01

RSA NetWitness Logs & Network Administrator



Question: 11

To add an action to the right-click menu in the Investigation UI, create a

- A. Right-click action
- B. Profile
- C. Context Hub List
- D. Context Menu Action

Answer: D

Question: 12

Parsers can be enabled on which of the following?

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

Answer: B

Question: 13

Which of the following choices describes a fundamental unit of network traffic transmitted from one IP device to another?

- A. Packet
- B. Chart
- C. Session
- D. Schedule

Answer: A

Question: 14

What are the data sources available in RSA NetWitness when creating a Reporting Engine rule?

- A. Short, Long, Truncated
- B. IPDB, ODBC, FileReader
- C. Broker, Concentrator, Decoder
- D. NetWitness DB, Warehouse DB, Respond DB

Answer: D

Question: 15

Which of the following rule types relies on two or more events occurring within a specified window of time?

- A. Network Rule
- B. Application Rule
- C. Correlation Rule
- D. BPF Filter Rule

Answer: C

Question: 16

What are the two basic operations you might perform to make use of a Live resource?

- A. move and copy
- B. download and enable
- C. save and apply
- D. subscribe and deploy

Answer: D

Question: 17

Service Groups are used primarily for

- A. grouping metadata from specified hosts
- B. deploying Live resources to specified services
- C. grouping hosts for batch configuration
- D. grouping hosts for monitoring performance in the Health and Wellness view

Answer: B

Question: 18

The NetWitness Trust Model is based on

- A. User ID
- B. User Role
- C. IP address
- D. Hardware address

Answer: B

Question: 19

What are three important things to configure on a Log Decoder'?

- A. Capture Auto-Start. Service Parsers, Capture Interface
- B. Capture Settings. Aggregation Auto-Start. Profile settings

- C. Investigation Settings. Capture Settings. Service Parsers
- D. Aggregation Auto-Start. Capture Settings. Investigation Settings

Answer: A

Question: 20

Where do you define dynamic charts for real-time display in Dashboards?

- A. Default Dashboard
- B. MONITOR > Reports > Manage > Charts
- C. MONITOR > Reports > Charts > View
- D. CONFIGURE > ESA Rules

Answer: B



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version is up to date and contains actual questions and answers.***

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!