Free Questions for 050-11-CARSANWLN01 by certsinside

Shared by Guerra on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

To enable reporting alerts to be sent to the Respond interface, you would

Options:

A- set up an output action in the Report Engine configuration

B- change the capture interface in Reporting sources

C- configure forwarding of alerts in the Reporting Engine configuration

D- set up an output action in a Report

Answer:

C

Question 2

Question Type: MultipleChoice

To prevent a Meta key from being indexed on a core service, you can

Options:

A- disable the parser for the Meta key in the device configuration

B- add the value /eve/= indexNone to the key in the custom index file

C- remove the Meta key from the Manage Default Meta Keys interface

D- add the value valueMax= "000000" to the key in the custom index file

Answer:

D

Question 3

Question Type: MultipleChoice

Which RSA NetWitness host provides the web server for reporting investigation, administration, and other aspects of the user interface?

Options:

A- NetWitness Server

B- Concentrator

C- Decoder

D- Broker

Answer:

A

Question 4

Question Type: MultipleChoice

Which step happens first in the RSA NetWitness data flow on the Packet Decoder when the capture interface is set to packet_mmap_"?

Options:

A- Feeds evaluated

B- Network rules evaluated

C- Application rules evaluated

D- Berkeley Packet Filter evaluated

Answer:

D

Question 5

Question Type: MultipleChoice

What of the following components can be used to set up external authentication for RSA NetWitness?

Options:

A- AAoP

B- Broker

C- Spectrum

D- PAM

Answer:

D

Question 6

Question Type: MultipleChoice

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

Options:

A- move and copy

B- download and enable

C- save and apply

D- subscribe and deploy

Answer:

D

Question 7

Question Type: MultipleChoice

What types of data can the Archiver store?

Options:

A- Raw Log only

B- Raw Log and Log Meta

C- Raw Log, Log Meta. Packet Meta

D- Raw Log. Log Meta. Raw Packet. Packet Meta

Answer:

D

Question 8

Question Type: MultipleChoice

The NetWitness Trust Model is based on

Options:

A- User ID

B- User Role

C- IP address

D- Hardware address

Answer:

B

Question 9

Question Type: MultipleChoice

Which RSA NetWitness component indexes metadata extracted from network or log data and makes it available for querying?

Options:

A- Broker

B- Informer

C- Spectrum

D- Concentrator

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which CLI command would have the effect of starting the Ul Web Server in NetWitness 11?

Options:

A- start ---s nwappliance

B- systemctl start saserver service

C- systemctl start jetty service

D- systemctl start -s saserver

Answer:

C

Question 11

Question Type: MultipleChoice

What happens when you set the metadata associated with a parser to Transients

Options:

A- Transient means the Decoder is using the parser to parse traffic, and the generated metadata is not stored on disk

B- Transient means the Decoder is using the parser to parse traffic, and the generated metadata is retained on disk for 24 hours

C- Transient means the Decoder is using the parser only to filter out data, not to generate metadata

D- Transient means the Decoder is using the parser only for ESA

Answer:

C

Question 12

Question Type: MultipleChoice

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

Options:

A- /etc/hosts

B- /etc/pam.d

C- /opVbin/pam

D- /usr/birVconfig

Answer:

B