

IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

Exam : **050-V40-ENVCSE02**

Title : RSA enVision Certified
Systems Engineer 4.0 Exam

Version : Demo

1. In general, RSA enVision's security information and event management functions include which of the following? (Choose two)

- A. Storage of log data.
- B. Collection of log data.
- C. Distribution of log data.
- D. Filtering of regulatory log data.
- E. Selective rule-based log deletion.

Answer: A,B

2. Assuming that a <device>msg.xml file exists for a device and a collected log message has a match in the <device>msg.xml, which of the following statements are true? (Choose two)

- A. The device is a supported device.
- B. The LEA client service must be installed.
- C. The ODBC standard database access method is being used.
- D. The message can be parsed to the appropriate enVision database table.
- E. The device is probably producing logs in the Unix syslog or SNMP format.

Answer: A,D

3. Which of the following describes the timestamp that is shown in the Event Viewer Date/Time field?

- A. The timestamp is from the source device for that event.
- B. The timestamp is from the enVision collector that is prepended to the event.
- C. The timestamp indicates the time the event was first viewed in Event Viewer.
- D. The timestamp indicates the elapsed time between event origination and capture.

Answer: B

4. Which of the log data collection methods listed below do NOT require the configuration of a service before RSA enVision can recognize a device using that collection method? (Choose two)

- A. Syslog
- B. ODBC
- C. SNMP
- D. Log file FTP
- E. Checkpoint LEA API

Answer: A,C

5. What is the primary difference between the LC5 and LC10 local collector units?

- A. Base storage capacity.
- B. Events Per Second (EPS) capability.
- C. Physical size and weight of the units.
- D. Type of Database Server to which they may be attached.

Answer: B

6. Within the RSA enVision console, what should you reference to determine if enVision's standard reports pertain to the Sarbanes-Oxley (SOX) or the BASEL II standards?

- A. The VAM assessment control panel under the 'Compliance >> Standards' tab.

- B. The enVision administrative interface which, by default, includes both SOX and BASEL II reports.
 - C. The Best Practices tool section of the 'Overview' tab which provides an overview with links to...
 - D. The Compliance Report Filter (CRF) which can be downloaded from the RSA enVision Support...
- Answer: C

7. In RSA enVision architecture, what best defines an enVision "Domain"?

- A. One or more Sites working together.
- B. The set of servers that make up a Master site.
- C. The set of Collectors (local and remote) within one Windows domain.
- D. All network information events collected from a single Windows domain.

Answer: A

8. The exhibit shows block diagrams describing an enVision LS Site with a Database Server (D-SRV), Application Server (A-SRV), and two Local Collector (LC1 and LC2) components. Which diagram shows the correct arrangement?

- A. Diagram A
- B. Diagram
- B C. Diagram C
- D. Diagram D

Answer: B

9. The RSA enVision Event Viewer displays information from what source?

- A. Packager "nuggets".
- B. NIC Reader Service database.
- C. Report RDB relational database.
- D. Internet Protocol Database (IPDB).

Answer: D

10. Which of the following statements about the RSA enVision ES Series appliance is NOT true?

- A. The ES Series supports options for external data storage.
- B. The ES Series is designed to operate in a stand-alone non-distributed mode.
- C. The ES Series contains all three RSA enVision functional components in a single appliance.
- D. The ES Series consists of three appliances each providing collection, data management, and analysis.

Answer: D