Exam Code: 050-v40-ENVCSE01

Exam Name: RSA enVision Certified Systems Engineer 4.0 Exam

Vendor: RSA

Version: DEMO

Part: A

1: Which of the following is the best architecture solution for a company distributed over a wide geographic area?
A.Multiple single-appliance sites installed at each customer location.
B.One master site and Local Collectors distributed to each collection point.
C.One master site and Remote Collectors distributed to each collection point.
D.Depends on the customer need to gather, analyze and report data at their various locations.
Correct Answers: D

2: Which of the following are valid names for user interface modules in RSA enVision? (Choose four)
A.Alerts Module
B.Reports Module
C.Analysis Module
D.Overview module
E.Collection module
F.Applications Module
G.Data Storage module
Correct Answers: A B C D

3: After logging into Event Explorer, no data is available to view until an Event Trace is opened.
A.True
B.False
Correct Answers: A

4: What is the purpose of the RSA enVision application and analysis function?
A.To collect, compress, and store raw log data.
B.To manage access and retrieval of captured events.
C.To allow messages from unsupported devices to be interpreted by enVision.
D.To interact with collected information for security and compliance related tasks.
Correct Answers: D

5: For the functions of collecting, storing, and managing event log data, RSA enVision utilizes what kind of database architecture?
A.Relational Database (RDBMS)
B.Flat File Data Structure (FFDS)
C.Internet Protocol Database (IPDB)
D.enVision Proprietary Data Management (EPDM)
Correct Answers: C

6: What is required to use the RSA enVision Event Explorer?
A.User authentication.
B.An SSL encrypted connection.

C.An Event Server installed on the user's computer.
D.Devices/Event Sources configured to send trace messages directly to Event Explorer.
Correct Answers: A

7: When running a report from the Report screen, what can cause a "No Data Available" message? (Choose three)
A.An improperly configured device.
B.The packager service is not running.
C.The SQL Query service not running.
D.A device that is not sending events to enVision.
E.A scheduled report has not been created and activated.
F.The 'Analyze' button is checked for unknown device types.
Correct Answers: A B D

8: Which of the services listed below maintains the enVision site directory information and lists the name of the site where the data was originally collected and the device or event source name?
A.Locator Service
B.Collector Service
C.Forwarder Service
D.File Reader Service
Correct Answers: A

9: In the RSA enVision system, Message Variables define what type of data?
A.Data extracted from message payloads.
B.Data used to identify unknown device types.
C.Data trying to obscure the original source IP address.
D.Data used to encrypt log traffic from secure web servers.
Correct Answers: A

10: In the Event Explorer application, an Event Trace defines
A.the specific event data you want to retrieve.
B.how you want to display different types of events.
C.a series of events that always indicates a security threat.
D.what Task Triage actions are taken when triggered by a Watchlist.
Correct Answers: A

11: Which of the following is a true statement about devices displayed in the RSA enVision Event Explorer's device tree?
A.Devices are added individually to a user's view by an administrator.
B.The device tree shows certain message types that a user has permission to see.
C.Devices the user has permission to see within enVision will be shown in a device tree.
D.All devices are shown in a device tree but only those the user has permission to see are active.
Correct Answers: C

12: When installing the Event Explorer client application it is important to use which of the following?
A.A different computer than is used to access the enVision administrative GUI.
B.A subnet mask that will allow direct connections to Remote Collector (RC) systems.
C.A Windows account that has sufficient permissions to perform a software installation.
D.A computer that has at least two network interface cards (NICs) to provide read/write access.
Correct Answers: C

13: A single RSA enVision Site can NOT contain more than one of which of the following components?
A.Local Collector (LC)
B.Remote Collector (RC)
C.Database Server (D-SRV)
D.Application Server (A-SRV)
Correct Answers: C

14: What happens when a Managed Device is disabled on the Manage Device Types screen?
A.It will be re-enabled when a new administrative session begins.
B.It will be re-enabled when a new event is received from that device.
C.It must be re-installed before new data can be collected from that device.
D.It will not be displayed in the user interface or in the Reports module menu tree.
Correct Answers: D

15: Before being stored in the RSA enVision IPDB, the packaging of data "nuggets" includes which of the following processes? (Choose two)
A.Filtering
B.Indexing
C.Scheduling
D.Replication
E.Compression
Correct Answers: B E