

# RSA

## Exam 050-ENVCSE01

CSE RSA enVision Essentials (new update)

Version: 12.0

[ Total Questions: 97 ]

**Question No : 1**

What happens if an event source device type is not immediately recognized by RSA enVision? (Check the one best answer.)

- A. It will be defined as "unknown" and for a limited time enVision will collect event data it generates
- B. Data from that device will be discarded until the device type can be defined
- C. An alert is generated by default to call an administrator's attention to the device
- D. The UDS Service will create a parsing XML file for the device and place data in the NIC Parse Cache

**Answer: A**

**Question No : 2**

When setting up a Check Point firewall device, which of the following is a good practice that should be completed first? (Check the one best answer.)

- A. Stop and restart the Check Point Firewall Service
- B. Stop and restart the enVision NIC Collector Service
- C. Verify that the CheckPoint Log Viewer is receiving events
- D. Set an 8-character key to establish an authenticated connection

**Answer: C**

**Question No : 3**

How many Remote Collectors (RC) can each Database Server (D-SRV) support? (Check the one

best answer.)

- A. Eight (8)
- B. Ten (10)
- C. Sixteen (16)
- D. Thirty two (32)

**Answer: C**

**Question No : 4**

After creating a customized Report Menu system, which RSA envision service(s) need to be restarted?

- A. Only the NIC Webserver Service
- B. The NIC Webserver and NIC Server Services
- C. The NIC Webserver, NIC Server and NIC Locator Services
- D. The NIC Webserver, NIC Server, NIC Locator, and NIC Packager Services

**Answer: A**

**Question No : 5**

When opening a connection in Event Explorer, you can define which of the following features? (Check the three correct answers.)

- A. Devices
- B. Event categories
- C. Log messages
- D. Time frame
- E. Local collector

**Answer: A,B,D**

**Question No : 6**

In the RSA enVision UDS process, what is the purpose of performing Data Reduction steps? (Check the one best answer.)

- A. Improve speed and efficiency of data processing
- B. Compress unsupported device data prior to storage
- C. Apply ISO-approved abbreviations to message text strings
- D. Decrease the rate that unsupported device data is collected

**Answer: A**

**Question No : 7**

If a customer has a specific syslog that they would like to use as part of a demonstration, you can

load it into enVision for reporting and querying using which of the following? (Check the one best

answer.)

- A. The Isdata utility to import the syslog file
- B. Copying the syslog file into the IPDB data directory
- C. Using the Data Injector utility to collect data from the syslog file
- D. Using the Custom Reports ?View External Data function of the administrative GUI

**Answer: C**

**Question No : 8**

When planning an RSA enVision installation, which statements below about the Site Name are

important considerations? (Check two answers.)

- A. The Site Name must match an enVision domain name
- B. The Site Name must be unique within an enVision domain and cannot be the same as the customer's NetBIOS domain name
- C. The Site Name must not contain any numeric or punctuation characters
- D. The Site Name must have the same suffix as the Windows domain in which it resides
- E. The Site Name must not match the name of any existing Windows domain in the network

**Answer: B,E**

**Question No : 9**

Why would the checkbox of a device type be grayed out On the Manage Device Types screen? (Check the one best answer.)

- A. It's not licensed
- B. Device is unknown but data can be collected

- C. Device is known but not compatible with enVision
- D. Device is associated with a monitored device within the NIC domain

**Answer: D**

**Question No : 10**

True or false. If a conflict exists with the default enVision collection port after appliance installation, the Collector Service can be modified to configure event collection on a different port

- A. True
- B. False

**Answer: A**

**Question No : 11**

When would you expect a difference between the log information captured by RSA enVision and the log information generated by a device? (Check the one best answer.)

- A. When the source IP address of the device is unknown to enVision.
- B. When the device is configured to send only certain events to syslog.
- C. When "Collect All Logs" is left unchecked in the Manage Devices screen.
- D. When the device is a known device and enVision recognizes the events to be non-critical.

**Answer: B**

**Question No : 12**

In RSA enVision UDS development, Value Maps, Regular Expressions, and Functions are types of which of the following? (Check the one best answer.)

- A. Data Reduction
- B. XML Parsing Rules
- C. Conditional Variables
- D. Summary Data Buckets

**Answer: C**

**Question No : 13**

Which RSA enVision module is used to configure the enVision system as well as to monitor its

health and performance? (Check the one best answer.)

- A. Overview module
- B. Alerts Module
- C. Analysis Module
- D. Reports Module

**Answer: A**

**Question No : 14**

When initially setting up a multiple appliance site, only the D-SRV unit is connected to a LAN ?all of the other units in the site then connect directly to the D-SRV.

- A. True
- B. False

**Answer: B**

**Question No : 15**

When creating a new enVision user account, which User Group is the account added to by default? (Check the one best answer.)

- A. Report-users
- B. Administrators
- C. Temporary-users
- D. All-applications-users

**Answer: D**

**Question No : 16**

What are three steps that are part of the device interpretation process using UDS? (Check the three best answers.)

- A. Configure devices to send log data to RSA enVision
- B. Device identification (i.e. vendor, device name, class, sub-class, etc.)
- C. Identification of device collection method
- D. Message definition
- E. List of known vulnerabilities
- F. Data parsing

**Answer: B,D,F**

**Question No : 17**

The administrator can use the RSA enVision's user authentication feature to complete what tasks? (Check two answers.)

- A. Use an existing Microsoft Active Directory authentication server
- B. Associate administrative users with an authentication server
- C. Require enVision users to change passwords on a periodic basis
- D. Enforce a pre-defined set of 'prohibited passwords' based on a dictionary file
- E. Utilize existing domain authenticated user accounts as the basis for enVision user accounts

**Answer: A,E**

**Question No : 18**

What two tasks does UDS complete when the command "uds reate" is executed to create a

device? (Check the two best answers.)

- A. Creates the files <devicename>.ini, <devicename>client.txt, <devicename>vendor.txt and <devicename>msg.xml
- B. Immediately starts collecting data from the new device
- C. Identifies all associated devices that have been configured
- D. Create all directory structures required for the device