



## **RSA enVision® Certified Systems Engineer Certification Examination Study Guide**

### ***Introduction***

The RSA enVision® Certified Systems Engineer (CSE) examination is based on the critical job functions that an individual would typically be expected to perform with competence when working with the RSA enVision product.

A Systems Engineer is a person who works in a technical support, sales support and/or technical implementation role within RSA Security, within an RSA Security Reseller organization, or within an organization using RSA enVision.

An analysis of the major job functions expected of an RSA enVision CSE determined that there are four major areas of job role responsibility:

- General knowledge about RSA enVision technology and product capability
- Designing solutions from understanding an organization's needs and environments
- Installing solutions to meet requirements and which demonstrate RSA enVision product functionality
- Supporting solutions through troubleshooting specific implementation and system integration issues

### ***Candidate Background and Experience***

A Certified Systems Engineer candidate should have a minimum of two years of professional experience in one or more of the following technical areas and understand how these technologies relate to and integrate with the RSA enVision product. Elements of the CSE exam touch upon each of these areas.

- General knowledge of networking and network communications technology (IP, Routers, Servers) and their associated logging functions and messages
- General knowledge of hardware installation and configuration
- Some Syntactical Language exposure (C++, scripting, SQL, XML, etc)
- Awareness of business practices, compliance, and security needs served by effective data gathering, audits and reports

### ***Examination Domains***

The RSA enVision Certified Systems Engineer examination is comprised of four major Domains (subject areas). Each Domain is represented by a series of questions designed to evaluate competence and knowledge of elements relating to that domain. The following table describes the proportion of the examination that relates to each domain:

<b>Domain</b>	<b>% of Examination</b>
1.0: RSA enVision Product Knowledge	30 %
2.0: Assessment / Design Solution	30 %
3.0: Install Solution	25 %
4.0: Support	15 %
TOTAL	100 %

## **Domain 1.0: RSA enVision Product Knowledge**

The Certified Systems Engineer must have a fundamental knowledge of key features and benefits of the RSA enVision product, and understanding of available product documentation, overall theory of operation and product functionality. The CSE is expected to be able to identify business solutions that highlight the product features and benefits within customer environments and demonstrate how the product solves important issues.

### **Content Areas**

- Product documentation
  - Where and in what form user documentation exists
  - Information available within enVision and the RSA support web site relating to compliance, source devices and other application areas
- Theory of Operation
  - Event data processing and data flow through enVision's logical components
  - Operation of key elements such as Alerting, connection to external resources, and enVision services
- Architecture
  - Single/Multiple appliance configurations; connection and configuration of multiple enVision sites
  - Server, collector, and data source device configurations
- Functionality
  - Administrative GUI console functions – modules and operations to support device, queries, reports, alerts and Enterprise Dashboard functions
  - User and administrative user management

### **Domain 1.0 Sample Items**

For operations associated with the administrative GUI console, the most complete documentation can be found

- in the on-line help pages
- in the RSA enVision Configuration Guide
- in the RSA enVision Administrator's Manual
- on the RSA enVision Support web site – User Operations page

*'A' is the correct choice because the on-line help pages provide the most complete administrative documentation. 'B', 'C' and 'D' are not correct because even though information is available from these sources, the "most complete" information is in Help.*

Before being stored in the RSA enVision IPDB, data "nuggets" are processed by,

- indexing
- collecting
- replication
- scheduling

*'A' is the correct choice because data 'nuggets' are indexed as they are stored in the IPDB. 'B' is not correct because data collection occurs before nuggets are created from the incoming data; 'C' and 'D' are not correct because these functions are not involved in the data packaging (nugget creation) process.*

In an RSA enVision system a "NIC Domain" refers to,

- one or more enVision Sites
- the enVision NIC Master Site
- the set of all enVision components within a single Windows domain
- a cluster of Remote Collectors controlled by a NIC Master Site server

*'A' is the correct choice. None of the other choices fit the definition of the NIC Domain.*

## **Domain 2.0: Assessment / Design Solution**

The Certified Systems Engineer must be able to conduct an assessment of an organization's environment, an organization's business needs, and architecture. Based on this assessment, the CSE must be able to identify appropriate RSA enVision solutions that will meet these needs.

### **Content Areas**

- Customer requirements
  - Security Event/Information Management regulatory and compliance standards
  - Product data collection functions and capabilities
  - Device connections and site/domain architecture
  - Product licensing and license limits
- Source devices and logging functions
  - Configuration of source devices
  - Log data collection and collection states
- Event Explorer operations
  - Event Explorer use and capabilities
- Proof-of-Concept and Pilot considerations
  - Proof-of-Concept planning, execution and clean-up
- UDS methodology
  - Process for UDS device development
  - Use of Data Reduction and Conditional Variables

### **Domain 2.0 Sample Items**

When would log information captured by RSA enVision be different than the log information generated by a device?

- when the source IP address of the device is unknown to enVision
- when the device is configured to send only certain events to syslog
- when "Collect All Logs" is left unchecked in the Manage Devices screen
- when enVision recognizes the device events to be routine and non-critical

*'B' is the correct choice because if a device does not send all log information to syslog, enVision will not have access to it. 'A' is not correct because enVision will capture data even if the device is unknown; 'C' and 'D' are not valid statements.*

If a Device is disabled in a GUI administrative session, it will

- be disabled across the entire enVision domain
- be re-enabled when the next administrative session begins
- be re-enabled when a new event is received from that device
- require re-installation before new data can be collected from that device

*'A' is the correct choice – a device can not be disabled for only one portion of a domain. The other choices are not valid statements.*

The RSA enVision Event Explorer allows you to examine

- data nuggets prior to packaging
- data directly from device log files
- data stored in the enVision IPDB database
- raw data stored in the pre-filtered data cache

*'C' is the correct choice – the Event Explorer examines data already stored in the IPDB. The other choices are not valid statements.*

### **Domain 3.0: Install Solution**

The Certified Systems Engineer installs a solution appropriate to an organization's environment. The CSE must be able to identify the procedures and configuration issues for installing an RSA enVision system or systems and bringing the software to an appropriate operational level to meet the organization's requirements. In addition, the CSE must know how to develop a controlled rollout to end-users, assess end-user acceptance, and provide pre-deployment information and education.

#### **Content Areas**

- Appliance setup
  - Single and Multiple appliance installation and configuration
  - Planning for and using the Installation Wizard
  - Services and port configuration for communication
  - Ancillary devices, servers and services such as Authentication Server
  - enVision component connections and limits
- Source device configuration
  - Key configuration points for Windows, Check Point, Cisco, and Juniper source devices
  - enVision functions for Monitored Devices
- Services
  - Operation and function of enVision component services (NIC Locator, Logger, Collector, Packager, etc.)
- Data injector test utility
  - Operation, options and command parameters

#### **Domain 3.0 Sample Items**

When initially connecting multiple appliances of an LS series installation, a Local Collector (LC) unit

- connects directly to the A-SRV component
- connects directly to the D-SRV component
- does not require a direct connection to a server component
- must have two connections – one each to the A-SRV and D-SRV components

*'B' is the correct choice. None of the other choices are valid statements.*

Before beginning the Installation Wizard process to configure an enVision site, it is important to pre-plan and determine the site name, because

- the site name cannot be modified after the Wizard is finished
- devices must be configured to send data to a specific site before the Wizard runs
- an NSLOOKUP must be performed to assure no duplicate site name is found prior to enVision installation
- the initial administrative account used to run the Wizard will set their password to the site name to initially log on to the appliance

*'A' is the correct choice the site name cannot be changed after the Wizard completes – if a site name must be changed, the appliance first has to be re-imaged to return to the factory default state and the enVision software re-installed. None of the other choices are valid statements.*

When configuring a Juniper Networks SSL VPN device to send log data to enVision,

- you must specify the log storage location in the Juniper Syslog Servers menu
- you can select specific events to log through the Juniper Log/Monitoring console
- log data must be scheduled to export to enVision through the Juniper Log Export menu
- you can enable the Statistics function of the Juniper system menu to enable logging for all events

*'B' is the correct choice. Information for this device as well as other device configurations can be found in device configuration guides on the RSA enVision support web site. Choice 'A' is incorrect because setting the storage location is optional for the Juniper device; Choice 'C' is not true – data does not need to be scheduled; Choice 'D' is not true – enabling 'all' events cannot be performed through the Statistics menu.*

## **Domain 4.0: Support Solution**

The Certified Systems Engineer needs to provide support and troubleshoot issues throughout the installation phases and after implementation.

### **Content Areas**

- Troubleshooting
  - Data and services problems affecting enVision reports
  - Operation and settings affecting scheduled reports, alerts, and managed devices
- Correctional steps
  - Managing port conflicts
  - Removing managed devices
- RSA support
  - Supported devices
  - Resources available through the RSA Support web site

### **Domain 4.0 Sample Items**

In RSA enVision, when a View is modified, changes may not be seen in Alerts until

- the view is restarted
- the Alerter service is restarted
- the enVision appliance is re-booted
- devices are updated with the new View configuration

*'A' is the correct choice –changes in Views will be reflected in the alerting process after the view is restarted. None of the other choices are valid statements.*

To permanently remove a log source device from the RSA enVision system, you must (choose two)

- delete the device from all Views
- disconnect the device from the LAN
- delete the device from the list of monitored devices
- run the Configuration Wizard to update the list of source devices
- delete the <devicename> folder from the ..\etc\devices directory

*'C' and 'E' are the two correct steps. 'A' is not correct because changes in a View will not accomplish device deletion; 'B' is incorrect because disconnecting the device will not remove it from the enVision system; 'D' is an invalid statement.*

If an on-screen report display shows the term “No Data Available”, possible causes include which of the following? (choose three)

- a device configuration error
- a device(s) have not been discovered
- the table on which the report is run has no data
- the NIC Query Service has failed or has been disabled
- the logged-in user does not have sufficient privileges to view this data

*'A', 'B' and 'C' are correct possibilities. 'D' and 'E' are invalid statements.*

## **Examination Preparation**

### **Product Training**

Although RSA enVision product training is not a strict requirement in preparation for the RSA enVision Certified Systems Engineer Certification Examination, it is highly recommended. Statistics show that approximately 80% of the candidates who successfully pass other RSA certification exams on their first attempt have attended RSA training prior to testing.

RSA Security offers the following courses that relate to the RSA enVision product and material covered on the CSE exam:

- RSA enVision Administration and Operations
  - *This course covers the fundamental concepts and operating principles of RSA enVision technology; organization and administration; system functions; reporting.*
- RSA enVision Universal Device Support (UDS)
  - *This course covers topics involving the creation of new device support for RSA enVision to recognize the device, properly parse data, and integrate into the overall system.*

In addition, RSA SecurWorld Channel partners can avail themselves of the following courses: (note that these courses are only available to SecurWorld audiences)

- RSA enVision Product Fundamentals
  - *This course covers topics of specific interest to sales, system, and applications engineers who need to present the RSA enVision product to customers, conduct demonstrations and may be responsible for helping to set up and support an enVision system. This course covers fundamental concepts, architecture and operating principles of enVision and contains a subset of relevant topics from both the RSA enVision Administration and Operations course as well as the RSA enVision Universal Device Support (UDS) course (described below).*
- Introduction to Selling RSA enVision
  - *This course is available only in an on-line delivery format and covers topics involving the application of enVision to customer Security Information Management (SIM) and Security Event Management (SEM) as well as fulfilling compliance needs of an organization.*

For full and detailed descriptions of RSA Security course offerings and available delivery options, visit the RSA Security web site or, for RSA SecurWorld Channel partners, visit the RSA SecurWorld Partner portal.

### **Product Experience**

Many of the areas addressed by the CSE exam will be familiar to the candidate who has worked with the RSA enVision product through installation and configuration, demonstration of the product, and exploring its various modules and reporting capabilities. Candidates are strongly advised to become familiar with the modules of the administrative GUI console and how to configure system controls to monitor devices, produce reports, execute queries, set up alert functions, and configure the system dashboard. Becoming familiar with the content of the on-line Help pages is also strongly advised.

The CSE exam content areas cover a wide range of RSA enVision product capability because a Certified Systems Engineer may be called upon to install or deploy RSA enVision for a variety of requirements or solution scenarios. A candidate who has worked for a long period in one organization (under that organization's specific deployment scheme) may not have a particular advantage over a candidate who has worked for a shorter period of time installing a variety of solutions for a number of organizations. Therefore, it is difficult to quantify a time period of relevant product experience. The general recommendation is that the candidate should actively work with the RSA enVision product and components for 3 to 6 months prior to taking the exam – in addition to other preparation.

## Study and Preparation Materials

As is common with other industry certification exams, RSA enVision CSE examination questions were constructed, reviewed, edited, and refined by groups of subject matter experts. A requirement of each test item is that it be referenced to a definitive source – document, publication, product menu selection, etc. The list below defines the body of knowledge from which examination test items have been drawn.

- RSA Security Training Materials (Available only as part of an RSA Security training program)
  - *RSA enVision Administration and Operations Course Student Guide and Lab Manual*
  - *RSA enVision Universal Device Support Student Guide*
  - *RSA enVision Essentials Student Guide and Lab Manual*
- RSA enVision product documentation (Available with the purchase of an RSA enVision appliance product)
  - *RSA enVision Hardware Guide*
  - *RSA enVision Configuration Guide*
- RSA enVision Help Menus and Help Screens (These Help functions are only available as part of an installed and operating RSA enVision appliance.)

## **Examination Details**

### **Testing Centers, Locations, and Registration**

The RSA enVision Certified Systems Engineer examination is administered by the Pearson VUE organization – an internationally known examination provider. Examination centers are located worldwide. Visit the Pearson VUE web site ([www.vue.com](http://www.vue.com)) and use the [Test Center Locator](#) to find a testing facility convenient to you.

You may also use the Pearson VUE site to create a personal login account and register for an exam. The RSA enVision Certified Systems Engineer exam code is 050-v40-ENVCSE02.

### **Exam Questions**

The RSA enVision CSE exam consists of 70 questions to be completed in 90 minutes. The exam consists of multiple-choice, multiple-response, or true/false type questions. The exam is computer-based and closed book – you may not utilize any printed material, personal computers, calculators, cell phones, etc. during the test.

The minimum passing score is 70%. Test results are calculated automatically at the conclusion of the test and testing center personnel can provide you with an authorized copy of your results before you leave the testing center.

### **Exam Costs**

The fee for taking the exam is US\$ 150.00.

### **Language Availability**

The RSA enVision Certified Systems Engineer exam is available in English.

### **What to expect at the Testing Center**

You must present two forms of identification; one of which is a photo ID.

You will be required to accept the terms of an RSA Certified Security Professional Certification Non-Disclosure Agreement before beginning the examination.

### **Re-taking the Exam**

There is no limit on the number of times that you can re-take the certification exam. However, to maintain integrity and confidentiality of the test items, 60 days is the required elapsed time before retaking the test a third time. Please note that you must pay the full exam fee each time that you retake the test.