RSA Security Analytics Certified Administrator (CA) Certification Examination Study Guide

Introduction

The RSA Security Analytics Certified Administrator (CA) examination is based on the critical job functions that an individual would typically be expected to perform with competence when administering the RSA Security Analytics product.

An RSA Security Analytics CA is a person who has an IT administrator, IS Analyst, or Security Operations role within an organization.

An analysis of the major job functions expected of an RSA Security Analytics CA determined that there are three major areas of job role responsibility:

- General awareness of the functions and capabilities of the product
- Configuration and management of the product
- Monitoring and troubleshooting product operation

Candidate Background and Experience

An RSA Security Analytics CA candidate should have a minimum of two years of experience in one or more of the following technical areas and understand how these technologies relate to and integrate with the RSA Security Analytics product. Elements of the CA exam touch upon these areas:

- Previous experience in computer and network operations, information security, system administration, or another related area.
- Familiarity with most basic system administration tools and processes.
- Experience in user management, managing reports, and security-related tasks.
- Experience using the Windows operating system and a web browser.
- Troubleshooting and problem determination skills.

Examination Domains

The RSA Security Analytics CA is comprised of three 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:

Domain	% of Examination
1. General product knowledge – features, functions and capabilities	50 %
2. System configurations	35 %
3. Monitoring and Troubleshooting	15 %
TOTAL	100 %

Domain 1.0: General product knowledge – features, functions and capabilities

The RSA Security Analytics CA must have a fundamental knowledge of key features and benefits of the RSA Security Analytics product. The RSA Security Analytics CA is expected to be able to identify the functions that highlight the product features and capabilities within a customer's environment and understand how the product can be used to identify security concerns.

Content Areas

- Architecture
  - *Deployment scenarios*
  - *Virtual environment*
  - *User interface*
- Data collection
  - *Packet capture*
  - *Log collection*
- User management
  - *Device users*
  - *Roles and Groups*

Domain 1.0 Sample Items

Which of the following is processed last for log traffic within RSA Security Analytics?

☐ Network Rules
☒ Event Correlation Rules
☐ Berkley Packet Filtration
☐ Feeds

'B' is the correct choice.

Which statement is correct concerning the external storage options for RSA Security Analytics?

☐ DAS typically costs twice as much as SAN
☐ SAN is typically deployed in environments with very short retention periods
☐ DAS typically scales much higher than SAN
☒ SAN typically scales much higher than DAS

'D' is the correct choice

Which of the following alerting mechanisms is **NOT** supported by RSA Security Analytics?

☐ Syslog
☐ SMTP
☐ SNMP
☒ POP3

'D' is the correct choice..

Domain 2.0: System configurations

The RSA Security Analytics CA must have a fundamental knowledge of the key configurations of the RSA Security Analytics product and how to effect system changes to help gather data and provide consolidated metadata for analysis.

Content Areas

- Configurations
  - *Device configuration*
  - *Configuring Live*
  - *Custom Feeds*
  - *Warehouse and Warehouse Connector configuration*
  - *Archiver configuration*
  - *Configuring Malware Analysis*
- Rules
  - *Rule data flow*
  - *Network rules*
  - *Application rules*
  - *Correlation rules*

Domain 2.0 Sample Items

An RSA Security Analytics Rule is associated with which of the following actions? (choose two)

☒ Retaining data for analysis
☐ Distributing data among RSA Security Analytics appliances
☒ Filtering data for analysis
☐ Adding contextual content to network traffic
☐ Deleting data that is too old for analysis

'A' and 'C' are the correct choices.

RSA Security Analytics can leverage intelligence from the global security community through

☒ Live
☐ Investigation
☐ Alerter
☐ Warehouse

'A' is the correct choice.

Which of the following components is responsible for indexing metadata in the RSA Security Analytics system?

☐ Decoder
☒ Concentrator
☐ Broker
☐ Warehouse

'B' is the correct choice.

Domain 3.0:Monitoring and Troubleshooting

The RSA Security Analytics CA must have a fundamental knowledge of key monitoring and reporting features in the RSA Security Analytics product, understand what may indicate improper operation, and understand approaches for problem resolution or for seeking further technical assistance.

Content Areas

- Monitoring the environment
  - *Device and system statistics*
  - *Concentrator aggregation*
- Performance
  - *Query performance*
  - *Tuning the Index*
  - *REST API*
- Troubleshooting
  - *Resetting the databases*
  - *Viewing logs*
  - *Log collection*
  - *Crash Reporter*

Domain 3.0 Sample Items

Which of the following is an RSA Security Analytics decoder index file that should never be modified?

☐ index-rsa-.xml
☒ index-decoder.xml
☐ index-default.xml
☐ index-system.xml

'B' is the correct choice.

When testing rules, reports and charts, which of the following statements is most accurate?

☒ a smaller time window is better for testing
☐ at least 256 data points are needed for testing – regardless of time period
☐ larger time windows yield more accurate results
☐ the length of time is irrelevant to testing

'A' is the correct choice.

The slowest Concentrator device in a system will limit the speed of which of the following?

☐ alerts and notifications
☐ data warehousing
☒ query results
☐ log data collection

'C' is the correct choice.

Examination Preparation

Product Training

Although RSA Security Analytics product training is not a strict requirement in preparation for the examination, it is highly recommended. Statistics show that approximately 83% of the candidates who successfully pass the exam on their first attempt have attended RSA training prior to testing. RSA Education Services offers the following courses that relate to the RSA Security Analytics product and material covered on the exam:

- RSA Security Analytics Administration
  - *The course provides an overview of the RSA Security Analytics product, hands-on configuration of components, managing users, and creating filters and rules. Additionally, the course covers integration with RSA enVision and monitoring capabilities.*

For full and detailed descriptions of RSA Security course offerings, visit: ***www.emc.com/rsa-training***.

Product Experience

Many of the areas addressed by the exam will be familiar to the candidate who has worked with the product through administrative operations. The exam content areas cover a wide range of product functions because an RSA Security Analytics CA may be called upon to assist with deployments, work closely with and educate end users, and maintain the day-to-day operation of the product across a variety of scenarios.

Study and Preparation Materials

As is common with other industry certification exams, RSA Security Analytics CA 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. Therefore, a finite set of preparation materials can be recommended for study and exam preparation. Although not all of the materials listed below are available in the public domain, the list does constitute a body of knowledge from which examination test items have been drawn.

- RSA Security Analytics Training Materials (Available only as part of an RSA Security Analytics training course)
  - *RSA Security Analytics Administration Course Student Guide*
- RSA Security Analytics product documentation (Available with the product or through RSA SecurCare Online)
- RSA Security Analytics Help Menus and Help Screens

Examination Details

Testing Centers, Locations, and Registration

The 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***) 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 Security Analytics Certified Administrator exam code is 050-103-CARSASA01.

Exam Questions

The exam consists of 71 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 usually 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 Security Analytics Certified Administrator 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, 14 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.

Last Revised March 21, 2014