EDUSUM

#1 Online Certification Guide

IBM C1000-156

IBM Security QRadar SIEM Administration Certification Questions & Answers

Exam Summary – Syllabus –Questions

C1000-156

IBM Certified Administrator - Security QRadar SIEM V7.5

62 Questions Exam – 61% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-156 Certification Well:

The C1000-156 is best suitable for candidates who want to gain knowledge in the IBM IBM Security - Not Applicable. Before you start your C1000-156 preparation you may struggle to get all the crucial Security QRadar SIEM Administration materials like C1000-156 syllabus, sample questions, study guide.

But don't worry the C1000-156 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the C1000-156 syllabus?
- How many questions are there in the C1000-156 exam?
- Which Practice test would help me to pass the C1000-156 exam at the first attempt?

Passing the C1000-156 exam makes you IBM Certified Administrator - Security QRadar SIEM V7.5. Having the Security QRadar SIEM Administration certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

IBM C1000-156 Security QRadar SIEM Administration Certification Details:

Exam Name	IBM Certified Administrator - Security QRadar SIEM V7.5
Exam Code	C1000-156
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	62
Passing Score	61%
Books / Training	**QRadar SIEM V7.5 Administration - Exam C1000-156 Preparation Guide**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM Security QRadar SIEM Administration Sample Questions**
Practice Exam	**IBM C1000-156 Certification Practice Exam**

C1000-156 Syllabus:

Topic	Details	Weights
System Configuration	- Perform license management - Administer managed hosts - Understand distributed architecture - Manage configuration and data backups - Configure custom SNMP and email templates - Manage network hierarchy - Use and manage reference data - Manage automatic update - Demonstrate the use of the asset database - Install and configure apps	20%
Performance Optimization	- Construct identity exclusions - Deal with resource restrictions - Configuring, tuning and understanding rules - Index management - Search management - Manage routing rules and event forwarding	13%
Data Source Configuration	- Manage flow sources - Manage log sources - Export event and flow data - Vulnerability information source configuration - Manage custom event and flow properties - Manage custom log source types - Manage data obfuscation	14%
Accuracy Tuning	- Understand and implement Anomaly Detection Engine rules - Manage and use building blocks - Manage content packs - Distinguish native information sources - Configure integrations	10%
User Management	- Manage users - Create and update security profiles - Create and update user roles - Manage user authentication and authorization	6%
Reporting, Searching, and Offense Management	- Manage reports - Utilize different search types - Manage offenses	13%

Topic	Details	Weights
	- Sharing content among users	
Tenants and Domains	- Differentiate network hierarchy and domain definition - Manage domains and tenants - Allocate licenses for multi-tenant - Assign users to tenants	8%
Troubleshooting	- Review and respond to system notifications - Troubleshoot common documented issues - Configure, manage and troubleshoot applications - Perform healthchecks - Basic GUI REST-API usage	16%

IBM C1000-156 Sample Questions:

Question: 1

What strategies are effective when dealing with resource restrictions for performance optimization?

(Choose two)

a) Allocating resources based on the popularity of applications
b) Ignoring resource usage warnings to maximize performance
c) Dynamically adjusting resource allocation based on usage
d) Encouraging users to perform resource-intensive tasks during peak hours

Answer: a, c

Question: 2

What are key aspects to focus on when configuring and tuning rules for performance optimization?

(Choose two)

a) Maximizing rule complexity
b) Ensuring rules are contextually relevant
c) Optimizing rule execution order
d) Designing aesthetically pleasing rule interfaces

Answer: b, c

Question: 3

In a distributed system architecture, why is it important to understand the roles of different components?

a) To create more efficient coffee breaks
b) To ensure proper data synchronization across components
c) To design better team-building activities
d) To optimize the office heating schedule

Answer: b

Question: 4

How can administrators ensure efficient data flow processing in IBM Security QRadar SIEM V7.5 during peak usage times?

a) By applying thematic visual enhancements to data flows
b) Allocating additional processing resources dynamically
c) Organizing flow data by color codes
d) Assigning musical tones to different data flow types

Answer: b

Question: 5

What is an effective method for optimizing the EPS (Events Per Second) performance in IBM Security QRadar SIEM V7.5?

a) Tuning the system based on monitored EPS trends and peak values
b) Increasing the EPS limit arbitrarily without assessing system impact
c) Assigning EPS values based on the color intensity of events
d) Setting uniform EPS thresholds for all event categories

Answer: a

Question: 6

Which configuration setting is essential for optimizing the parsing of log data in IBM Security QRadar SIEM V7.5?

a) Custom property extraction
b) Time format specification
c) Background color settings for log source identifiers
d) Animation speed for log data processing

Answer: a

Question: 7

Which practice is vital for Performance Optimization in maintaining IBM Security QRadar SIEM V7.5 system responsiveness?

a) Customizing the UI font sizes for better readability
b) Assigning unique sound effects to different alert types
c) Regularly updating desktop backgrounds on QRadar consoles
d) Defragmenting event and flow databases periodically

Answer: d

Question: 8

Why is it crucial to distinguish between different native information sources in accuracy tuning?

a) To understand the unique characteristics and reliability of each source for better data interpretation
b) To ensure that each source's data is aesthetically pleasing
c) To guarantee that data from each source is equally complicated
d) To provide more variety in the daily tasks of data analysts

Answer: a

Question: 9

When troubleshooting common documented issues, what is an important step?

a) Ignoring the issue until it becomes more significant.
b) Rebooting the system multiple times in hope the issue resolves itself.
c) Consulting the system documentation and known issue logs.
d) Guessing the solution based on your intuition.

Answer: c

Question: 10

Why is it important to use and manage reference data effectively in system configuration?

a) To streamline the office recycling program
b) To improve the company's social media presence
c) To enhance the culinary variety in the cafeteria
d) To ensure that the system uses accurate and consistent information

Answer: d

Study Guide to Crack IBM Security QRadar SIEM Administration C1000-156 Exam:

- Getting details of the C1000-156 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the C1000-156 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the IBM provided training for C1000-156 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the C1000-156 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on C1000-156 practice tests is must. Continuous practice will make you an expert in all syllabus areas.