Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

C1000-156 MCQs
C1000-156 TestPrep
C1000-156 Study Guide
C1000-156 Practice Test
C1000-156 Exam Questions

PASS

killexams.com

IBM

C1000-156

IBM Security QRadar SIEM V7.5 Administration

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/C1000-156

Question: 1

To optimize the performance of IBM Security QRadar SIEM, which of the following actions should be taken?

A. Increasing the retention period for logs and events
B. Reducing the number of reference sets and building blocks
C. Enabling real-time indexing for all data sources
D. Disabling automatic backups

Answer: B

Explanation: To optimize the performance of QRadar SIEM V7.5, it is recommended to reduce the number of reference sets and building blocks. These components can consume significant system resources, so minimizing their usage can improve the overall performance and responsiveness of the system.

Question: 2

In IBM Security QRadar SIEM V7.5, what is the purpose of Tenants and Domains?

A. To manage user authentication and access control
B. To isolate and segregate data and system components
C. To configure high availability and failover
D. To generate compliance reports and alerts

Answer: B

Explanation: In QRadar SIEM V7.5, the purpose of Tenants and Domains is to isolate and segregate data and system components. Tenants provide logical separation of data, while Domains enable separate management and

configuration of system components, such as rules, policies, and event processing.

Question: 3

When tuning the accuracy of IBM Security QRadar SIEM V7.5, what should be considered?

A. Increasing the number of false positives
B. Decreasing the number of log sources
C. Adjusting the log source parsing order
D. Disabling event correlation rules

Answer: C

Explanation: When tuning the accuracy of QRadar SIEM V7.5, one important factor to consider is adjusting the log source parsing order. The log source parsing order determines how the system interprets and processes incoming log data. By adjusting this order, you can prioritize the parsing of more critical log sources and ensure accurate event categorization and correlation.

Question: 4

Which of the following is a valid method to configure high availability in IBM Security QRadar SIEM V7.5?

A. Configuring a primary and secondary Console with an active-active setup
B. Configuring a primary and secondary Event Collector with an active-passive setup
C. Configuring a primary and secondary Flow Processor with an active-active setup
D. Configuring a primary and secondary Data Node with an active-passive setup

Answer: A

Explanation: In QRadar SIEM V7.5, high availability can be achieved by configuring a primary and secondary Console with an active-active setup. This configuration ensures that both Consoles are active and can process events simultaneously, providing redundancy and fault tolerance.

Question: 5

When troubleshooting issues in IBM Security QRadar SIEM, which of the following actions should be performed?

A. Resetting all event retention settings to default values
B. Restarting all system services simultaneously
C. Analyzing system and application logs
D. Disabling all event notification alerts

Answer: C

Explanation: Whentroubleshooting issues in QRadar SIEM V7.5, analyzing system and application logs is an important action to perform. Logs provide valuable information about system events, errors, and potential issues. By carefully reviewing and analyzing these logs, administrators can identify the root cause of problems and take appropriate corrective actions.

Question: 6

Which feature of IBM Security QRadar SIEM enables users to create customized reports based on specific search criteria?

A. Scheduled Searches
B. Offense Analytics

C. Advanced Search
D. Search Profiles

Answer: C

Explanation: The Advanced Search feature in QRadar SIEM V7.5 enables users to create customized reports based on specific search criteria. It provides a flexible and powerful way to define search filters and parameters, allowing users to extract the desired information from the collected data.

Question: 7

Which of the following can be a potential cause of slow search performance in IBM Security QRadar SIEM V7.5?

A. Enabling real-time indexing for all data sources
B. Insufficient system memory
C. Disabling database backups
D. Increasing the number of log sources

Answer: B

Explanation: Insufficient system memory can be a potential cause of slow search performance in QRadar SIEM V7.5. When the system doesn't have enough memory resources, it may struggle to process and retrieve search results efficiently, leading to degraded performance. Allocating sufficient memory to the QRadar SIEM system can help improve search performance.

Question: 8

Which of the following data source configurations is commonly used to collect network traffic data in IBM Security QRadar SIEM?

A. Syslog event source
B. Windows event source
C. Flow source
D. Database event source

Answer: C

Explanation: To collect network traffic data in QRadar SIEM V7.5, a common data source configuration is the flow source. Flow sources capture information about network connections, such as source IP, destination IP, source port, destination port, and protocols. This data is essential for network monitoring and detecting potential security incidents.

Question: 9

Which of the following user management tasks can be performed in IBM Security QRadar SIEM?

A. Assigning specific report access to users
B. Configuring network firewall rules
C. Modifying system configuration settings
D. Managing SSL certificates

Answer: A

Explanation: In QRadar SIEM V7.5, user management tasks include assigning specific report access to users. This allows administrators to control which reports and data are accessible to different users or user groups, ensuring proper data segregation and security.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.