IBM

C1000-156 Exam

IBM Security QRadar SIEM V7.5 Administration

Thank you for Downloading C1000-156 exam PDF Demo

You can buy Latest C1000-156 Full Version Download

https://www.certkillers.net/Exam/C1000-156

Version: 4.0

Question: 1

When configuring a log source, which protocols are used when receiving data into the event ingress component?

A. SFTR HTTP Receiver, SNMP

B. Syslog, HTTP Receiver, SNMP

C. Syslog, FTP Receiver, SNMP

D. Syslog, HTTP Receiver, JDBC

Answer: B

Explanation:

When configuring a log source in IBM QRadar SIEM V7.5, the protocols used to receive data into the event ingress component are critical for ensuring proper data collection and analysis. The main protocols that are supported for this purpose are:

Syslog: A widely used protocol for message logging, supported by many network devices and servers.

HTTP Receiver: Allows QRadar to receive logs via HTTP POST requests, enabling integration with various web services and applications.

SNMP (Simple Network Management Protocol): Used for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Reference
IBM QRadar SIEM documentation and product guides confirm that these are the supported protocols for receiving data into the event ingress component. The specific details on protocol support can be found in the QRadar SIEM administration and configuration manuals.

Question: 2

Which User Management option manages the QRadar functions that the user can access?

A. Security Profile

B. Admin Role

C. Security Options

D. User Role

Answer: A

Explanation:

In IBM QRadar SIEM V7.5, managing what functions a user can access is crucial for maintaining security and ensuring that users have appropriate permissions. The Security Profile option is used to manage these access controls. Here's how it works:

Security Profile: Defines the specific permissions and roles assigned to users, dictating what actions they can perform within QRadar. This includes access to various modules, dashboards, and functionalities.

User Role: While related, user roles are more about grouping users with similar permissions rather than defining individual access.

Admin Role: Typically reserved for users with administrative privileges but does not manage the specific functions users can access.

Security Options: This is not a relevant option for managing user access to QRadar functions.

Reference
IBM QRadar SIEM V7.5 documentation details how security profiles are configured and managed, providing comprehensive steps on assigning and modifying user access based on roles and profiles.

Question: 3

Which is a benefit of a lazy search?

A. Getting results that are limited to a specific range

B. Providing every result no matter the quantity of the search results

C. Finding lOCs quickly

D. Searching across domains for any configured user

Answer: A

Explanation:

A lazy search in IBM QRadar SIEM V7.5 is designed to optimize the performance of search queries by limiting the amount of data retrieved and processed at any given time. This is particularly beneficial in environments with large datasets. Here's a detailed explanation:

Limited Results: Lazy searches limit the search results to a specific range, allowing users to get manageable chunks of data without overwhelming the system.

Performance Optimization: By reducing the amount of data processed in a single search, lazy searches improve query performance and reduce resource usage.

Incremental Data Retrieval: Users can incrementally retrieve more data as needed, making it easier to handle and analyze large datasets without performance degradation.

Reference
The functionality and benefits of lazy searches are detailed in the IBM QRadar SIEM V7.5 user guides, which explain how to configure and use lazy searches for efficient data retrieval and analysis.

Question: 4

Which profile database does the Server Discovery function use to discover several types of servers on a network?

A. Flow profile database

B. Network profile database

C. Domain profile database

D. Asset profile database

Answer: D

Explanation:

The Server Discovery function in IBM QRadar SIEM V7.5 uses the Asset Profile Database to discover various types of servers on a network. This database stores detailed information about the assets, including server types, configurations, and roles within the network. Here's how it works:

Asset Profile Database: This is the central repository that contains all the discovered asset information.

Discovery Process: During the discovery process, QRadar scans the network to identify servers and other devices, collecting information such as IP addresses, open ports, services, and operating systems.

Classification: The collected data is then analyzed and classified, updating the Asset Profile Database with the types of servers discovered.

Reference
IBM QRadar SIEM documentation specifies the use of the Asset Profile Database for server discovery functionalities and provides details on configuring and managing asset profiles.

Question: 5

Which command does an administrator run in QRadar to get a list of installed applications and their App-ID values output to the screen?

A. opt/qradar/support/deployment_info.sh

B. /opt/qradar/support/recon ps

C. /opt/qradar/support/recon connect 1005

D. /opt/qradar/support/threadTop.sh

Answer: A

Explanation:

To get a list of installed applications and their App-ID values in IBM QRadar SIEM, the administrator can run the following command:

Command: /opt/qradar/support/deployment_info.sh

Function: This command outputs detailed information about the current deployment, including a list of all installed applications and their associated App-ID values.

Usage: The administrator executes this command in the terminal, and the information is displayed on the screen.

Reference
IBM QRadar SIEM V7.5 administration guides include this command as a standard tool for retrieving deployment information, including details about installed applications and their IDs.

Thank You for trying C1000-156 PDF Demo

To try our C1000-156 Full Version Download visit link below

https://www.certkillers.net/Exam/C1000-156

Start Your C1000-156 Preparation

Use Coupon "**CKNET**" for Further discount on the purchase of Full Version Download. Test your C1000-156 preparation with actual exam questions.