



IBM C1000-156 Practice Questions

Shared by Petersen on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

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

Options:

- 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.

Question 2

Question Type: MultipleChoice

How can you configure a log source to provide events to different domains?

Options:

- A- Create a saved search on the Network Activity tab to view events in specific domains.
- B- Use the Assistant app to update the domain information for the log source.
- C- Use custom properties to assign events from a single log source to different domains.
- D- Use the Use Case Manager app to update building blocks to support multi domain events.

Answer:

C

Explanation:

To configure a log source in IBM QRadar SIEM V7.5 to provide events to different domains, administrators can use custom properties. Here's how it works:

Custom Properties: Create and configure custom properties to tag events with specific domain information.

Assigning Events: When events are ingested from a log source, these custom properties can be used to dynamically assign events to different domains based on predefined criteria.

Domain Management: This approach allows flexibility in managing and segregating data from a single log source across multiple domains, ensuring that each domain receives the relevant events.

Reference The configuration of custom properties for domain assignment is detailed in the QRadar SIEM administration guides, providing step-by-step instructions for setting up and using custom properties for domain management.

Question 3

Question Type: MultipleChoice

What is the primary method used by QRadar to alert users to problems?

Options:

- A- System Notifications
- B- System Summary
- C- Use Case Manager
- D- QRadar Assistant

Answer:

A

Explanation:

The primary method used by IBM QRadar SIEM V7.5 to alert users to problems is through System Notifications. Here's how it works:

System Notifications: These are alerts generated by QRadar to inform users of various issues, such as system performance problems, license issues, or security incidents.

Visibility: Notifications are prominently displayed in the QRadar GUI, ensuring that administrators and users can quickly identify and respond to any problems.

Customization: Users can configure notification settings to receive alerts for specific types of issues, ensuring they stay informed about critical aspects of the system's health and performance.

Reference IBM QRadar SIEM documentation outlines the use of System Notifications as the primary method for alerting users to issues, detailing how to configure and manage these alerts.

Question 4

Question Type: MultipleChoice

When creating an identity exclusion search, what time range do you Choose?

Options:

- A- Previous 7 days
- B- Real time (streaming)
- C- Previous 30 days
- D- Previous 5 minutes

Answer:

B

Explanation:

When creating an identity exclusion search in IBM QRadar SIEM V7.5, the time range selected

is 'Real time (streaming).' This setting ensures that the search continuously monitors and excludes identities in real-time as data is ingested. Here's the process:

Real-time Monitoring: Continuously updates the search results based on incoming data, providing immediate exclusion of specified identities.

Streaming Data: Processes data in a live stream, ensuring that the exclusion criteria are applied instantaneously as new events occur.

Reference The setup and configuration of identity exclusion searches are detailed in the QRadar SIEM administration guides, highlighting the importance of real-time streaming for effective identity management.



Question 5

Question Type: MultipleChoice

What two things are required for an administrator to deobfuscate data in QRadar?

Options:

- A- Public key and the password for the key that is used to obfuscate data
- B- Private key and the password for the key that is used to obfuscate data
- C- Private key and public key that is used to obfuscate data
- D- Public key and the password for the private key that is used to obfuscate data

Answer:

B

Explanation:

In IBM QRadar SIEM V7.5, to deobfuscate data, an administrator requires two critical components:

Private Key: This key is used to decrypt the data that was originally obfuscated. The private key must match the public key used during the obfuscation process.

Password for the Private Key: This password is necessary to unlock the private key, allowing the decryption process to proceed.

The process involves using the private key in conjunction with its password to reverse the obfuscation, ensuring that the data is securely accessed only by authorized personnel.

Reference The requirement for the private key and its password for deobfuscating data is detailed in the IBM QRadar SIEM administration and security guides, ensuring that the process adheres to best practices for data security.

Question 6

Question Type: MultipleChoice

Domain assignments take precedence over the settings of which other elements from a security profile?

Options:

- A- Security profiles, Networks, and Log Sources tabs
- B- Security profiles. Networks, and Domains
- C- Permission Precedence, and Log Sources tabs
- D- Permission Precedence. Networks, and Log Sources tabs

Answer:

D

Explanation:

In IBM QRadar SIEM, domain assignments take precedence over the settings of other elements from a security profile, specifically Permission Precedence, Networks, and Log Sources tabs. This hierarchical precedence ensures that the domain settings are enforced across different security configurations. The domain settings effectively override other configurations to maintain consistency and security across the environment. This structure helps in managing access and permissions more effectively by ensuring that the domain-level policies are the primary controlling factor.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on Domain Management and Security Profiles

Question 7

Question Type: MultipleChoice

The Report wizard provides a step-by-step guide to design, schedule, and generate reports. Which three (3) key elements does the report wizard use to help you create a report?

Options:

- A- Content
- B- Format
- C- Container
- D- Display
- E- Banner
- F- Layout

Answer:

A, B, F

Explanation:

The Report wizard in IBM QRadar SIEM provides a structured approach to designing, scheduling, and generating reports. The three key elements used by the Report wizard to help you create a report are:

Content: This element involves selecting the specific data and metrics you want to include in the report. It can include various log sources, events, and other relevant security data.

Format: This element defines how the data will be presented in the report. It includes selecting the type of report (e.g., tabular, graphical) and the specific visualizations that will best represent the data.

Layout: This element refers to the overall structure and design of the report, including the arrangement of content and visual elements to ensure the report is easily readable and professionally formatted.

These elements together ensure that the reports generated are comprehensive, visually appealing, and tailored to the specific needs of the organization.

Reference IBM QRadar SIEM documentation

Question 8

Question Type: MultipleChoice

In the QRadar GUI, you notice that no new offenses were generated today. A review of the notifications shows:

MPC: Unable to create new offense. The maximum number of active offenses has been reached.

What is the default value of the maximum number?

Options:

A- 3500

B- 1500

C- 5000

D- 2500



Answer:

D

Explanation:

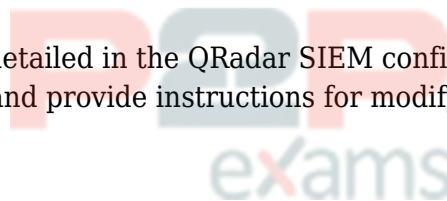
In IBM QRadar SIEM V7.5, the default value for the maximum number of active offenses is set to 2500. This limit is in place to manage system performance and ensure efficient processing of security incidents. Here's the detailed information:

Default Setting: The default setting for the maximum number of active offenses is 2500.

Impact: If this limit is reached, QRadar will not generate new offenses until some of the existing offenses are closed or archived.

Configuration: Administrators can adjust this setting based on their organizational needs, but the default value is 2500.

Reference This information is detailed in the QRadar SIEM configuration and tuning guides, which specify default settings and provide instructions for modifying the maximum number of active offenses if necessary.



Question 9

Question Type: MultipleChoice

From which site can you download software updates for QRadar?

Options:

- A- IBM Fix Central
- B- IBM X-Force Exchange
- C- IBM Passport Advantage Online
- D- QRadar 101

Answer:

A

Explanation:

The primary site for downloading software updates for IBM QRadar is IBM Fix Central. Here's how it works:

IBM Fix Central: A centralized platform for downloading fixes, updates, and patches for IBM software products.

Accessing Updates: Administrators can log in to IBM Fix Central, select QRadar from the list of products, and download the necessary updates.

Regular Updates: Keeping QRadar updated with the latest fixes and patches ensures optimal performance and security.

Reference IBM QRadar SIEM documentation and support resources direct users to IBM Fix Central for downloading and applying software updates.

Question 10

Question Type: MultipleChoice

Which two (2) data sources can be assigned to a domain in the Domain Management function?

Options:

- A- Users
- B- Rules
- C- Flow collectors
- D- Log sources
- E- X-Force Integration Feed

Answer:

C, D

Explanation:

In the Domain Management function of IBM QRadar SIEM, two key data sources that can be assigned to a domain are Flow Collectors and Log Sources. Flow collectors capture and analyze network flow data, while log sources refer to various devices and applications that send log data to QRadar for analysis. By assigning these data sources to a domain, administrators can segment and manage the data more effectively, ensuring that the correct flow and log data are processed and analyzed within the designated domain. This segmentation enhances security and performance by isolating data handling according to domain-specific policies.

Reference QRadar SIEM V7.5 Administration Guide - Chapter on Domain Management and Data Source Assignment

To Get Premium Files for C1000-156 Visit

<https://www.p2pexams.com/products/c1000-156>

For More Free Questions Visit

<https://www.p2pexams.com/ibm/pdf/c1000-156>

20%
DISCOUNT

P2P
exams