"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

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.

Question: 6

From which two (2) resources can an administrator download QRadar security content?

A. QRadar Application Repository

B. IBM Applications Database

C. IBM Fix Central

D. IBM App Central

E. IBM Security App Exchange

Answer: A, E

Explanation:

Administrators can download QRadar security content from the following two resources:

QRadar Application Repository: This repository contains a wide range of applications, rules, reports, and other content specifically designed for QRadar.

IBM Security App Exchange: A platform where users can find and download security applications, including those for QRadar. It offers a variety of tools to extend and enhance the functionality of QRadar SIEM.

These resources provide curated and validated security content, ensuring that administrators have access to the latest and most effective tools for their security needs.

Reference

IBM QRadar documentation and support resources detail the QRadar Application Repository and IBM Security App Exchange as primary sources for downloading and updating QRadar security content.

Question: 7

Which authentication type in QRadar encrypts the username and password and forwards the username and password to the external server for authentication?

A. RADIUS authentication

B. Two-factor authentication

C. TACACS authentication

D. System authentication

Answer: C

Explanation:

TACACS (Terminal Access Controller Access-Control System) authentication is a protocol used in IBM QRadar SIEM V7.5 for authenticating users by forwarding their credentials to an external server. Here's how it works:

Encryption: TACACS encrypts the entire payload of the authentication packet, including the username and password, ensuring secure transmission.

Forwarding Credentials: After encryption, the credentials are forwarded to an external TACACS server, which performs the actual authentication.

Authentication Process: The external server checks the credentials against its database and sends a response back to QRadar indicating whether the authentication is successful or not.

Reference

IBM QRadar SIEM documentation explains TACACS authentication in detail, highlighting its secure encryption and external server verification process.

Question: 8

In which QRadar section can the administrator view the license giveback rate?

A. Admin tab > system settings

B. Log Activity tab > AQL query in the Advanced Search "select LicenseGiveback from license"

C. Admin tab > License pool management

D. Log Activity tab by searching for the term "giveback" in the Quick Filter

Answer: C

Explanation:

In IBM QRadar SIEM V7.5, the license giveback rate can be viewed in the License Pool Management section. Here's the step-by-step process:

Access Admin Tab: The administrator needs to navigate to the Admin tab in the QRadar GUI.

License Pool Management: Under the Admin tab, there is an option for License Pool Management.

View License Giveback Rate: Within the License Pool Management section, the administrator can view details about license usage, including the giveback rate.

Reference

The QRadar SIEM administration guide provides detailed steps on accessing and managing license information, including the giveback rate, under the Admin tab.

Question: 9

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?

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: 10

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

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: 11

Which two (2) pieces of information from the MaxMind account must be included in QRadar for geographic data updates?

A. Account/User ID

B. API key

C. License Key

D. MaxMind username

E. API password

Answer: B, C

Explanation:

To include geographic data updates from MaxMind in IBM QRadar SIEM V7.5, the following two pieces of information from the MaxMind account are required:

API Key: This key is used to authenticate and authorize access to the MaxMind services, ensuring that QRadar can request and receive geographic data updates.

License Key: This key is associated with the MaxMind account and allows QRadar to utilize the licensed geographic data for enhanced location-based analysis.

These keys ensure that the data integration is secure and that the usage complies with MaxMind's licensing agreements.

Reference

IBM QRadar SIEM documentation specifies the API key and license key as necessary credentials for integrating MaxMind geographic data, detailed in the setup and configuration sections.

Question: 12

To detect outliers, which Anomaly Detection Engine rule tests events or flows for volume changes that occur in regular patterns?

A. Behavioral rules

B. Threshold rules

C. Anomaly rules

D. Building block rules

Answer: C

Explanation:

In IBM QRadar SIEM V7.5, Anomaly Detection Engine rules that test events or flows for volume changes occurring in regular patterns are known as Anomaly Rules. Here's how they function:

Detection: Anomaly rules are designed to identify deviations from normal behavior by analyzing patterns in the data.

Volume Changes: These rules specifically look for unusual increases or decreases in event or flow volumes that might indicate potential security incidents.

Regular Patterns: By understanding regular patterns in network traffic and event logs, anomaly rules can highlight significant outliers that warrant further investigation.

Reference

The functionality and configuration of anomaly rules are covered extensively in the IBM QRadar SIEM administration guide, providing administrators with the tools to effectively detect and respond to abnormal network activities.

Question: 13

What is the default day and time setting for when QRadar generates weekly reports?

A. Sunday 01:00 AM

B. Monday 02:00 AM

C. Sunday 02:00 AM

D. Monday 01:00 AM

Answer: A

Explanation:

In IBM QRadar SIEM V7.5, the default setting for generating weekly reports is configured to occur on:

Day: Sunday

Time: 01:00 AM

This setting ensures that the reports are generated during a typical low-activity period, minimizing the impact on system performance and ensuring that the latest data from the previous week is included.

Reference

The default configuration for report generation times is specified in the IBM QRadar SIEM V7.5 administration and user documentation.

Question: 14

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

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: 15

A QRadar administrator needs to quickly check the disk space for all managed hosts. Which command does the administrator use?

A. /opt/qradar/support/all_servers.sh 'Is -ltrsh"

B. /opt/qradar/support/all_servers.sh "rra -rf /store'

C. /opt/qradar/support/all_servers.sh -C -k 'df -Th'

D. /opt/qradar/support/all_servers.sh -C -K 'watch Is'

Answer: C

Explanation:

To quickly check the disk space for all managed hosts in IBM QRadar SIEM V7.5, the administrator uses the following command:

Command: /opt/qradar/support/all_servers.sh -C -k 'df -Th'

Function: This command checks the disk space across all managed hosts, providing detailed information about the filesystem types and disk usage.

Parameters:

-C: Executes the command on all managed hosts.

-k: Keeps the output in a human-readable format.

'df -Th': The specific command to display the disk space usage in a tabular format with human- readable file sizes.

Reference

The IBM QRadar SIEM documentation provides a comprehensive list of commands for system administration, including those for checking disk space on managed hosts.

Question: 16

Which two (2) open standards does the QRadar Threat Intelligence app use for feeds?

A. TAXII

B. AQL

C. STIX

D. JSON

E. OSINT

Answer: A, C

Explanation:

The QRadar Threat Intelligence app uses open standards to integrate and utilize threat intelligence feeds effectively. The two key standards used are:

TAXII (Trusted Automated eXchange of Indicator Information): This is an application layer protocol used for exchanging cyber threat intelligence over HTTPS. It enables the sharing of threat information across different systems and organizations.

STIX (Structured Threat Information eXpression): This is a standardized language used for representing structured cyber threat information. STIX enables the consistent and machine-readable representation of threat data, facilitating the integration and analysis of threat intelligence.

These standards ensure that threat intelligence data is formatted and exchanged in a consistent and interoperable manner, enhancing the overall effectiveness of the threat intelligence processes in QRadar.

Reference

The IBM QRadar SIEM documentation and threat intelligence app configuration guides describe the use of TAXII and STIX for integrating threat intelligence feeds.

Question: 17

Which event advanced search query will check an IP address against the Spam X-Force category with a confidence greater than 3?

A. select * from events where XFORCE_IP_CONFIDENCE('Spam', sourceip>>3

B. select * from flows where XFORCE_IP_CONFIDENCE{'Spam', sourceip)<3

C. select * from flows where XF0RCE_iP_C0NFiDEKCE{*Malware',sourceip)-3

D. select * from events where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3

Answer: D

Explanation:

To check an IP address against the Spam X-Force category with a confidence greater than 3 using an advanced search query in QRadar, the correct query format is:

Query Structure: select * from events where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3

Components:

select * from events: This part of the query selects all events from the QRadar events database.

where XF0RCE_IP_C0NFIDENCE('Malware',sourceip)>3: This filter checks if the source IP address has a confidence level greater than 3 for being associated with malware according to the X-Force category.

This query is designed to filter out and display events where the source IP is identified with high confidence as being associated with malicious activity.

Reference

The syntax and usage of advanced search queries are detailed in the IBM QRadar SIEM search and analytics guides, providing specific examples for utilizing X-Force threat intelligence data.

Question: 18

When will events or flows stop contributing to an offense?

A. When the offense becomes dormant

B. When the offense becomes inactive

C. After the offense is assigned to an analyst

D. When you protect the offense

Answer: A

Explanation:

In IBM QRadar SIEM V7.5, events or flows stop contributing to an offense when the offense becomes dormant. Here's how it works:

Dormant Offense: An offense becomes dormant when there is no new activity contributing to it for a specified period. This indicates that the threat or incident has not had any further related events or flows.

Contribution Stoppage: Once an offense is marked as dormant, no additional events or flows are added to it, which helps in managing the offense lifecycle and resources within QRadar.

This behavior helps in distinguishing between active and inactive threats, allowing security analysts to focus on ongoing incidents.

Reference

The QRadar SIEM administration and user guides provide detailed explanations of offense management, including the conditions under which offenses become dormant and how this affects event and flow contributions.

Question: 19

What is the main reason for tuning a building block?

A. Increasing the performance of the ecs-ec-ingress service

B. Reducing the number of false positives

C. Properly documenting the building block for future administrators

D. Reducing EPS usage

Answer: B

Explanation:

Tuning a building block in IBM QRadar SIEM V7.5 is primarily aimed at reducing the number of false positives. This process involves adjusting the rules and logic within the building block to better differentiate between normal and suspicious activity. Here's the detailed explanation:

False Positives: High numbers of false positives can overwhelm analysts and obscure genuine threats. Tuning helps in refining detection criteria to reduce these false alarms.

Rule Adjustments: Modifying the thresholds, conditions, and filters within the building block rules to ensure they more accurately reflect the environment's typical behavior.

Improved Accuracy: Enhanced precision in detecting true security incidents, thus improving the overall effectiveness of the SIEM solution.

Reference

IBM QRadar SIEM administration guides and best practice documents emphasize the importance of tuning to minimize false positives, ensuring more actionable alerts.

Question: 20

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

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: 21

What occurs when QRadar reaches the events per second (EPS) or flows per minute (FPM) shared license pool limits?

A. Incremental Licensing removes the limits on EPS and FPM.

B. QRadar generates a notification that the limit was reached and stops processing.

C. Data accumulates in a temporary burst handing queue, but QRadar continues to process events and flows.

D. Events and flows continue to process, and the Network and Log Activity tabs remain active.

Answer: C

Explanation:

When IBM QRadar SIEM V7.5 reaches the events per second (EPS) or flows per minute (FPM) shared license pool limits, the following occurs:

Burst Handling Queue: QRadar utilizes a temporary burst handling queue to manage the overflow of events and flows. This queue temporarily holds data until the system can process it.

Continued Processing: QRadar continues to process events and flows despite reaching the license limits, ensuring no data is lost.

Efficiency: This mechanism allows QRadar to handle short-term spikes in data volume without compromising the integrity

or continuity of event and flow processing.

Reference

The handling of EPS and FPM limits is described in IBM QRadar SIEM's system administration and configuration guides, which explain how QRadar manages data when license thresholds are exceeded.

Question: 22

Which three (3) resource restriction types are available in QRadar?

A. Role-based restrictions

B. Tenant-based restrictions

C. User-based restrictions

D. Service-based restrictions

E. Event-based restrictions

F. Domain-based restrictions

Answer: A, B, F

Explanation:

IBM QRadar SIEM V7.5 provides several types of resource restriction mechanisms to manage access control and data visibility. The three main types are:

Role-based restrictions: These restrictions limit what actions users can perform based on their assigned roles. Each role has specific permissions that dictate access to different functionalities and data within QRadar.

Tenant-based restrictions: This type of restriction is used in multi-tenant environments, where different tenants (organizational units) need to have isolated views and access to their data. Tenant-based restrictions ensure that users from one tenant cannot access data from another tenant.

Domain-based restrictions: Domains in QRadar are used to segment data logically. Domain-based restrictions control which data is visible to users based on the domains they have been granted access to.

These restriction types ensure that access control is granular and adheres to organizational security policies.

Reference

IBM QRadar SIEM documentation outlines the use of role-based, tenant-based, and domain-based restrictions for managing access control and data visibility.

Question: 23

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

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: 24

An administrator receives a file with all the vital assets in the company and wants to import this file into QRadar. How

must this import file be formatted?

A. CSV file in the format: IP address. Name, Weight. Description

B. JSON file in the format: IP address. Name, Weight, Domain

C. XML file in the format: IP address. Name, Weight, Domain

D. XLS file in the format: IP address, Name. Weight, Description

Answer: A

Explanation:

When importing vital asset information into IBM QRadar SIEM V7.5, the import file must be formatted as a CSV file with the following structure:

Format: CSV (Comma-Separated Values)

Fields: The required fields are IP address, Name, Weight, and Description.

IP address: The IP address of the asset.

Name: The name of the asset.

Weight: A numerical value representing the importance or criticality of the asset.

Description: A brief description of the asset.

This format ensures that QRadar can correctly parse and import the asset information, integrating it into its asset database for further analysis and correlation.

Reference

IBM QRadar SIEM documentation provides guidelines on the required CSV format for importing asset information, detailing the necessary fields and their order.

Question: 25

When do you consider reconfiguring your QRadar environment to a distributed deployment?

A. When flow sources reach a threshold of 20 Mbps

B. When processing or storage expands beyond capacity on your single deployed appliance

C. When you need to upgrade the Log Source Manager application

D. When your combined log sources are less than 2000 events per second

Answer: B

Explanation:

Reconfiguring your IBM QRadar environment to a distributed deployment is considered under the following circumstances:

Capacity Limits: When the processing or storage requirements of your QRadar environment exceed the capacity of a single appliance, it becomes necessary to distribute the workload across multiple systems.

Performance Improvement: A distributed deployment allows for better load balancing and performance optimization by distributing event and flow processing tasks.

Scalability: As your organization's data volume grows, a distributed deployment ensures that QRadar can handle the increased load without degradation in performance.

Reference

IBM QRadar SIEM administration guides discuss the considerations and benefits of moving to a distributed deployment when scaling beyond the capacity of a single appliance.

Question: 26

What is the REST API interface to install and manage applications that are created by using the GUI Application Framework Software Development Kit?

A. /api/gui_app_framework

B. /api/data_classification

C. /api/system

D. /api/siem

Answer: A

Explanation:

The primary method used by IBM QRadar to install and manage applications created using the GUI Application Framework Software Development Kit (SDK) is through the REST API interface:

API Endpoint: /api/gui_app_framework

Functionality: This endpoint allows administrators to manage the lifecycle of applications, including installation, updates, and removal.

Integration: Provides seamless integration with the GUI Application Framework, enabling the development and deployment of custom applications within QRadar.

Reference

The IBM QRadar API documentation provides details on the /api/gui_app_framework endpoint and its usage for managing GUI applications.

Question: 27

A user reports that some data points are missing from a generated report. The logs show these notifications, which are determined to be the root

cause of the problem:

The accumulator was unable to aggregate all events/flows for this interval.

In what timeframe does this system need to complete data aggregation for it to be deemed successful?

A. 30 seconds

B. 5 seconds

C. 120 seconds

D. 60 seconds

Answer: D

Explanation:

In IBM QRadar SIEM V7.5, the accumulator process must complete data aggregation within a specific timeframe to be deemed successful:

Timeframe: 60 seconds

Aggregation Process: The accumulator aggregates events and flows for reporting and analysis. If it cannot complete this task within 60 seconds, it is considered unsuccessful.

Impact: Failure to aggregate within the specified timeframe can result in missing data points in reports and dashboards, affecting the accuracy and completeness of the information presented.

Reference

The QRadar SIEM administration guides detail the accumulator process and the importance of completing data aggregation within 60 seconds to ensure accurate reporting.

Question: 28

You want to use a quick filter search to look for certain elements: . 10.100.100.*

- BlueCoat
- TCP_REFRESH_MIS

Which string provides the correct results?

A. (10.100.100.- Bluecoat TCP_REFRESH_MIS)

B. 10.100.100.*%Bluecoat%TCP_REFRESH_MIS

C. "10.100.100.*%AND%Bluecoat%AND%TCP_REFRESH_MIS"

D. (10.100.100/ AND Bluecoat AND TCP_REFRESH_MIS)

Answer: C

Explanation:

In IBM QRadar SIEM V7.5, using a quick filter search requires the correct syntax to find specific elements within the event logs. The correct string to search for the elements 10.100.100.*, Bluecoat, and TCP_REFRESH_MIS is:

String Structure: "10.100.100.*%AND%Bluecoat%AND%TCP_REFRESH_MIS"

Elements: This string combines the IP address pattern, device type, and specific event message using %AND% to ensure

that all three elements are included in the search results.

Quotation Marks: The quotation marks are necessary to group the search terms and ensure that the search engine interprets them correctly.

Reference

IBM QRadar SIEM search documentation provides guidelines on using quick filter searches and the correct syntax for combining multiple search terms.

Question: 29

Which command in QRadar allows you to run a specific command inside of a specific container, when given an app ID. or a combination of workload, service, and container?

A. ifconfig -a

B. recon ps

C. recon connect

D. yum info

Answer: C

Explanation:

The recon connect command in IBM QRadar SIEM V7.5 allows administrators to run a specific command inside a specific container, given an app ID or a combination of workload, service, and container. Here's how it works:

Command: recon connect

Function: This command connects to a specified container and allows the execution of commands within that container.

Usage: Administrators use this command to manage and troubleshoot applications running in isolated environments (containers) within QRadar.

Reference

The QRadar administration and support guides detail the usage of the recon connect command for managing containerized applications.

Question: 30

When adjusting a custom email template, which two elements do you edit to include the customizations?

A. <heading> <text>

B. <heading> <body>

C. <subject> <text>

D. <subject> <body>

Answer: D

Explanation:

When adjusting a custom email template in IBM QRadar SIEM V7.5, the two elements that need to

be edited to include customizations are:

<subject>: This element defines the subject line of the email, which can be customized to provide a clear and relevant description of the email's content.

<body>: This element contains the main content of the email. Customizing the body allows administrators to include specific information, formatting, and messages relevant to the recipient.

Customizing these elements ensures that the email notifications are informative and tailored to the needs of the recipients.

Reference

The QRadar SIEM user and configuration guides provide instructions on customizing email templates, highlighting the <subject> and <body> elements as key areas for customization.

Question: 31

An administrator wants to export a list of events to a CSV file. Which items are in the default columns of the search result?

A. Log Source. Event Count. High Level Category. Related Offense

B. Event Name. Application, Username, Log Source

C. Username. Source Port. Event Count, Magnitude

D. Protocol. Storage Time, Destination Port, Source Port

Answer: A

Explanation:

When exporting a list of events to a CSV file in IBM QRadar SIEM V7.5, the default columns included in the search result typically are:

Log Source: The origin of the log data.

Event Count: The number of events.

High Level Category: The broad classification of the event.

Related Offense: The associated offense ID or description.

These columns provide a comprehensive overview of the events, helping analysts quickly understand the context and significance of the data.

Reference

IBM QRadar SIEM documentation provides details on the default columns included in search results and their significance in event analysis.

Question: 32

An administrator would like to optimize event and flow payload searches for log data that is stored for up to a month. What does an administrator need to do to achieve that requirement?

A. Perform a clean on the search model.

B. Configure the retention period for property indexes.

C. Configure the retention period for payload indexes.

D. Configure the retention period for search indexes.

Answer: C

Explanation:

To optimize event and flow payload searches for log data stored for up to a month, an administrator should configure the retention period for payload indexes. Here's the process:

Retention Period Configuration: Set the retention period for payload indexes to match the desired data storage duration (e.g., one month).

Improved Search Efficiency: By configuring the retention period appropriately, QRadar ensures that the indexed data is efficiently searchable, improving performance during searches.

Index Management: Regularly manage and clean up indexes to maintain optimal system performance and storage utilization.

Reference

The IBM QRadar SIEM administration guides provide instructions on configuring retention periods for various types of indexes, including payload indexes, to optimize search performance.

Question: 33

From which site can you download software updates for QRadar?

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: 34

A ORadar administrator needs to upgrade the system to patch a vulnerability. In what order does the administrator upgrade the managed hosts?

A. Any order

B. Console followed by remaining hosts

C. Flow Processor followed by remaining hosts

D. Event Processor followed by remaining hosts

Answer: B

Explanation:

When upgrading the IBM QRadar SIEM environment to patch a vulnerability, the recommended order for upgrading managed hosts is:

Console: Start by upgrading the Console, which is the central management point of the QRadar deployment.

Remaining Hosts: After the Console has been upgraded, proceed to upgrade the other managed hosts, including Event Processors, Flow Processors, and Data Nodes.

This order ensures that the management and coordination functionalities provided by the Console are updated first, minimizing the risk of compatibility issues during the upgrade process.

Reference

IBM QRadar SIEM upgrade guides specify that the Console should be upgraded first, followed by the remaining managed hosts, to ensure a smooth and coordinated upgrade process.

Question: 35

A ORadar administrator is trying to tune a rule so that it cannot send an email more than 10 times in a 24-hour period. Which method can be used to accomplish this goal?

A. Using a special rule test that limits the number of rule triggers

B. Using the "response limiter"

C. Tuning the rule conditions to make it trigger fewer times

D. Using the "execute custom action" rule response

Answer: B

Explanation:

To ensure that a rule in IBM QRadar SIEM V7.5 does not send an email more than 10 times in a 24- hour period, the "response limiter" can be used. Here's how it works:

Response Limiter: This feature limits the number of times a rule action (such as sending an email) can be executed within a specified timeframe.

Configuration: Set the response limiter to a maximum of 10 actions in 24 hours.

Implementation: Apply the response limiter to the rule, ensuring that even if the rule conditions are met multiple times, the email will only be sent up to the specified limit.

Reference

IBM QRadar SIEM documentation on rule management and tuning includes detailed instructions on using the response limiter to control the frequency of rule actions.

Question: 36

A ORadar administrator creates a new saved search in QRadar and wants to add the search to a dashboard, but the option "Include in my Dashboard" cannot be selected.

What is a possible reason it is unavailable?

A. The search is not grouped.

B. The option is valid only for searches based on events.

C. The option is valid only for searches based on flows.

D. The user does not sufficient permissions.

Answer: D

Explanation:

If the option "Include in my Dashboard" cannot be selected when creating a saved search in IBM QRadar SIEM V7.5, a possible reason is insufficient permissions. Here's why:

Permissions: The user needs appropriate permissions to add saved searches to the dashboard.

Role-Based Access Control: QRadar uses role-based access control to manage user permissions. The user's role must include the necessary privileges to modify dashboards.

Verification: Ensure that the user has the correct permissions assigned. This can be checked and adjusted in the user management settings.

Reference

IBM QRadar SIEM administration guides explain the permissions required for various actions, including adding saved searches to dashboards, and how to configure user roles and permissions.

Question: 37

What are some of the supported custom property expression types in QRadar?

A. Regex, RDBMS, LEEF

B. Regex, JSON, LEEF

C. RDBMS, JSON, HTML

D. Regex. JSON, HTML

Answer: B

Explanation:

IBM QRadar SIEM supports various types of custom property expressions to allow users to extract and parse data from logs in flexible and powerful ways. Among the supported custom property expression types, Regex, JSON, and LEEF are frequently utilized:

Regex (Regular Expressions): Regular expressions are a powerful tool used for pattern matching and extraction in text. In QRadar, regex can be used to create custom properties that parse specific patterns from log data, allowing for detailed and precise data extraction.

JSON (JavaScript Object Notation): JSON is a widely used data interchange format that is lightweight and easy to read and write. QRadar supports JSON expressions to parse and extract structured data from logs formatted in JSON.

LEEF (Log Event Extended Format): LEEF is a log format used by various devices to structure log data in a consistent manner. QRadar can utilize LEEF expressions to extract data from logs that use this format.

These types of expressions enhance QRadar's ability to handle diverse log formats and enable more accurate and efficient data analysis.

Reference
IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 38

An administrator opens the Offenses section and goes to Rules to edit the system notification rule.
What is the rule name for system notifications?

A. System: Notification

B. System: Hardware and Software monitoring

C. System: Software Notifications

D. System: Hardware Notifications

Answer: A

Explanation:

In IBM QRadar, system notifications are crucial for alerting administrators about various events and statuses that require attention. The rule name for system notifications is "System: Notification". Here is a detailed explanation of how it functions and how to find and edit this rule:

Accessing the Offenses Section: To view and manage rules related to offenses, an administrator needs to open the Offenses section in the QRadar console.

Navigating to Rules: Within the Offenses section, there is a subsection for rules. This is where all the predefined and custom rules are listed.

Editing System Notification Rules: The specific rule for system notifications is named "System: Notification". This rule is responsible for generating notifications based on system events and statuses.

Customizing the Rule: By selecting and editing this rule, administrators can adjust the conditions and actions associated with system notifications, ensuring they are tailored to the specific needs and policies of the organization.

This rule is essential for maintaining awareness of system events and ensuring that potential issues are promptly addressed.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 39

In a single domain QRadar deployment, which IP addresses are considered local?

A. Any private IP address

B. Any public IP address

C. Any IP address that is defined in the network hierarchy

D. Any IP address that is not defined in the network hierarchy

Answer: C

Explanation:

In a single domain QRadar deployment, the IP addresses considered local are those that are defined in the network hierarchy. Here is a detailed explanation:

Network Hierarchy: QRadar uses a network hierarchy to define and manage IP addresses within the organization. This hierarchy allows QRadar to understand which IP addresses are part of the internal network and which are external.

Defining Local IP Addresses: Any IP address that is specified within the network hierarchy is considered local. This includes all the subnets and IP ranges that are part of the internal network.

Purpose: By defining the network hierarchy, QRadar can effectively differentiate between internal (local) and external (non-local) traffic, enabling more accurate detection and correlation of security events.

This approach helps in identifying suspicious activities by comparing the source and destination of traffic against the defined internal network.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 40

Which is the default port for the first NetFlow flow source that is configured in QRadar?

A. 8413

B. 21

C. 2055

D. 514

Answer: C

Explanation:

The default port for the first NetFlow flow source configured in QRadar is 2055. Here's a detailed explanation:

NetFlow Flow Sources: NetFlow is a network protocol developed by Cisco for collecting IP traffic information. QRadar can be configured to receive NetFlow data to monitor and analyze network traffic.

Default Port: When setting up the first NetFlow flow source in QRadar, the system uses port 2055 by default. This is a standard port commonly used for NetFlow traffic.

Configuration: During the configuration process, this default port can be used to receive data from devices that export NetFlow data, such as routers and switches.

Using port 2055 helps standardize the setup process and ensures compatibility with most NetFlow-

enabled devices.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 41

Which user role is defined by default in QRadar?

A. Event and Logs

B. QRadar Users

C. WinCollect

D. QRadar Managers

Answer: B

Explanation:

The default user role defined in QRadar is "QRadar Users". Here's a detailed explanation:

User Roles in QRadar: QRadar has a role-based access control system to manage user permissions and access levels. This ensures that users can only access and perform actions within their assigned roles.

Default Role - QRadar Users: The "QRadar Users" role is the default role assigned to new users. This role typically includes basic permissions needed to access and use QRadar features without administrative privileges.

Permissions: Users with the "QRadar Users" role can view and analyze security data, but they might have limited access to configuration settings and administrative functions.

Assigning default roles helps streamline user management and ensures that new users have the necessary access to perform their tasks.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 42

You analyzed network flows and decided that you want to track any network bandwidth violations by any application that

comes from your network source. You want to report on all applications that create traffic and the amount of data (total bytes) from each IP. You want to store the IP address, the application, and the amount of data in the reference data collection.

What type of reference data collection must you create to support this use case?

A. Reference map

B. Reference map of maps

C. Reference set

D. Reference map of sets

Answer: A

Explanation:

To track network bandwidth violations by any application coming from your network source and report on all applications that create traffic along with the amount of data from each IP address, you need to store the IP address, the application, and the amount of data in a reference data collection. The appropriate type of reference data collection for this use case is a "Reference map." Here is why:

Reference Map: A reference map allows you to store key-value pairs where each key is unique. In this context, the key can be the combination of the IP address and the application, and the value can be the amount of data (total bytes).

Data Structure: This structure enables efficient lookups and updates, which is ideal for tracking and reporting bandwidth usage per application per IP address.

Use Case Suitability: The reference map is suitable for scenarios where you need to store and retrieve values based on a specific key, and it supports storing complex data structures efficiently.

This type of reference data collection supports the use case by allowing the storage and retrieval of detailed network traffic information per application and IP address.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 43

An administrator is evaluating domain criteria based on an event. The result of a regular expression that was defined in a custom property does not match a domain mapping, and the event was automatically assigned to the default

domain.

What is the order of precedence if the event does not match the domain definition for custom properties?

A. Log source. Log source group, App Hosts

B. Log source, Log source group, Event collector or data gateway, DDS

C. DLC. Log source, Log source group, Event collector or data gateway

D. DLS, Log source, Event collector or data gateway. Log source group

Answer: B

Explanation:

In QRadar, when evaluating domain criteria based on an event, the precedence order for domain assignment if the event does not match the domain definition for custom properties is as follows:

Log Source: The first criterion checked is the log source. Each event is associated with a log source, and the domain is determined based on this source.

Log Source Group: If the log source does not provide a domain match, the next criterion is the log source group. Log sources can be grouped together, and domain definitions can be applied at the group level.

Event Collector or Data Gateway: If neither the log source nor the log source group provides a match, QRadar checks the event collector or data gateway for a domain definition.

DDS (Data Domain Service): As the final step, if no other criteria match, the DDS is used to assign the default domain.

This order of precedence ensures that the most specific criteria are checked first before falling back to more general criteria, ensuring accurate domain assignment for events.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 44

What is the most restrictive permissions a user needs in order to see all of the events from a particular log source in the Log Activity tab?

A. The user needs access to the Networks AND Log Sources to see a particular log in the activity tab.

B. The user's security profile must include that log source, and the profile needs permission to Networks AND Log Sources.

C. A user needs access to Flow Sources Only.

D. The log source must be included in the user's security profile and the profile needs its precedence set to Log Sources Only.

Answer: B

Explanation:

To see all of the events from a particular log source in the Log Activity tab, a user must have the appropriate permissions set in their security profile. The most restrictive permissions needed are:

Security Profile Inclusion: The log source must be included in the user's security profile. This means the user must have explicit permission to access events from this log source.

Permissions to Networks and Log Sources: The user's security profile must also include permissions to both Networks and Log Sources. This ensures the user has the necessary access to view events related to the specified log source within the network context.

These permissions are crucial to control and restrict access, ensuring users can only view data they are authorized to see while maintaining security and privacy within the system.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 45

What is the Advanced Search field used for?

A. Running an Acceptable Query Language search

B. Running an Advanced Query Language search

C. Running an ArangoDB Query Language search

D. Running an Ariel Query Language search

Answer: D

Explanation:

The Advanced Search field in IBM QRadar is used for running Ariel Query Language (AQL) searches. Here's a detailed explanation:

Ariel Query Language (AQL): AQL is a query language used in QRadar to search and retrieve event and flow data from the Ariel database. It is similar to SQL but tailored for the specific needs of QRadar's data structure.

Advanced Search Field: The advanced search field provides a user interface for crafting and executing AQL queries. This allows users to perform detailed and complex searches to analyze specific patterns, behaviors, or events in their security data.

Functionality: Using AQL, users can specify criteria for selecting and filtering data, allowing for precise and comprehensive searches. This is essential for deep-dive investigations and custom reports.

The ability to run AQL searches gives analysts powerful tools to extract meaningful insights from their security data.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 46

What parameter contributes to the magnitude score of an offense?

A. Confidentiality

B. Availability

C. Integrity

D. Credibility

Answer: D

Explanation:

In IBM QRadar, the magnitude score of an offense is influenced by several parameters, one of which is credibility.

Here’s a detailed explanation:

Magnitude Score: The magnitude score represents the severity and importance of an offense in QRadar. It is a composite score that helps prioritize incidents for investigation.

Credibility Parameter: Credibility assesses the reliability of the event source and the likelihood that the event represents a real threat. Higher credibility indicates that the source is reliable and the threat is more likely to be legitimate.

Contribution to Magnitude: The credibility parameter directly influences the magnitude score by weighting the offense higher if the credibility of the event is high. This ensures that more reliable and potentially more severe incidents are prioritized.

Credibility is one of the key factors used by QRadar to assess and prioritize security incidents, ensuring effective incident management.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 47

Which command can a QRadar administrator use to connect to the QRadar app container?

A. yum info <app id>

B. recon connect <app id>

C. recon ps <app id>

D. app connect <app id>

Answer: B

Explanation:

A QRadar administrator can use the recon connect <app id> command to connect to the QRadar app container. Here is a detailed explanation:

App Container Connection: QRadar applications run in isolated containers. Administrators may need to connect to these containers for troubleshooting, management, or configuration purposes.

Recon Command: The recon command-line tool is used for managing and interacting with application containers in QRadar.

Connect Command: The specific command recon connect <app id> allows the administrator to initiate a connection to the specified application container. <app id> should be replaced with the actual application ID.

Usage: This command is typically used when an administrator needs to access the container's environment to perform tasks such as checking logs, modifying configurations, or diagnosing issues.

This command facilitates direct access to the application container, enabling efficient management and troubleshooting.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 48

A QRadar administrator creates a new saved search in QRadar.

Which option does the administrator enable to allow this search to be opened as the Log Activity tab is opened?

A. Set as Default

B. Include in my Quick Searches

C. Include in my Dashboard

D. Share with Everyone

Answer: A

Explanation:

When a QRadar administrator creates a new saved search and wants it to open by default whenever the Log Activity tab is opened, they need to enable the "Set as Default" option. Here is a detailed explanation:

Creating a Saved Search: When saving a search in QRadar, the administrator can define specific criteria and filters to create a custom search that meets their requirements.

Set as Default Option: By enabling the "Set as Default" option, the administrator ensures that this particular search will be automatically executed and displayed whenever the Log Activity tab is accessed. This saves time and provides immediate access to the most relevant data.

Benefits: Setting a default search streamlines the workflow for security analysts by presenting the most important or frequently used search results right away.

This feature enhances efficiency by ensuring that users are presented with the most pertinent data as soon as they access the Log Activity tab.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 49

A QRadar administrator creates a new saved search in QRadar.

Which option does the administrator enable to allow this search to be opened as the Log Activity tab is opened?

A. Set as Default

B. Include in my Quick Searches

C. Include in my Dashboard

D. Share with Everyone

Answer: A

Explanation:

Similar to the previous question, when a QRadar administrator creates a new saved search and wants it to be the first search displayed upon opening the Log Activity tab, the correct option to enable is "Set as Default." Here's the detailed process:

Saved Search Creation: The administrator specifies the search parameters and criteria to create a new saved search.

Enabling Default Setting: By selecting the "Set as Default" checkbox, the administrator ensures that this search will automatically run and display when the Log Activity tab is accessed.

Utility: This option is particularly useful for quickly accessing the most relevant data without needing to manually select and run the saved search each time.

Setting a default search helps maintain focus on critical security events by providing immediate access to predefined search results.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 50

Before configuring a WinCollect log source, which two ports does a QRadar administrator ensure are open?

A. 514 and 8413

B. 445 and 8413

C. 443 and 8413

D. 8080 and 8413

Answer: A

Explanation:

Before configuring a WinCollect log source in QRadar, the administrator must ensure that specific network ports are open to facilitate communication. The required ports are:

Port 514: This is the default port for syslog, a standard protocol used to send system log or event messages to a specific server. WinCollect uses this port to send logs from Windows machines to the QRadar server.

Port 8413: This port is used for communication between the WinCollect agent and the QRadar Console. It is necessary for managing the WinCollect agent and ensuring proper data transmission.

Ensuring these ports are open is crucial for the seamless operation and integration of WinCollect with QRadar, allowing the secure and efficient collection of log data from Windows environments.

Reference

IBM Security QRadar SIEM and IBM Security QRadar EDR integration.pdf

Question: 51

On which managed hosts is QRadar event data stored in the Ariel database?

A. On the Event Collector and attached Data Node

B. On the Data Gateway and attached Data Node

C. On the Event Processor and attached Data Node

D. On the App Host and attached Data Node

Answer: C

Explanation:

QRadar event data is stored in the Ariel database on the Event Processor and any attached Data Nodes. The Event Processor is responsible for processing incoming events, performing correlation, and storing the event data. The attached Data Nodes provide additional storage capacity and can be

used to extend the storage available to the Event Processor.

Reference

IBM QRadar SIEM V7.5 Administration documentation.

Question: 52

You are using the command line interface (CLI) and need to fix a storage issue. What command do you use to verify disk usage levels?

A. df -h

B. Is -laF

C. lsof -h

D. du -h

Answer: A

Explanation:

To verify disk usage levels in a Linux environment, the df -h command is used. This command provides an overview of the disk space usage, displaying the available and used space in a human- readable format.

Open the terminal or CLI on the system.

Type df -h and press Enter.

Review the output, which will show the filesystem, size, used space, available space, and usage percentage for all mounted filesystems.

Reference

IBM QRadar SIEM V7.5 Administration documentation.

Question: 53

How can an administrator configure a rule response to add event data to a reference set?

A. Write a custom script.

B. Use AQL functions.

C. Use the "add the following data to a reference set" rule test.

D. Use the "add to reference set" rule response.

Answer: D

Explanation:

Administrators can configure a rule response in QRadar to add event data to a reference set by using the "add to reference set" rule response. This is a predefined response action in QRadar that allows specific event data to be added to a reference set when the rule conditions are met.

Navigate to the "Offenses" tab in the QRadar console.

Select "Rules" from the navigation pane.

Create a new rule or edit an existing rule.

In the "Rule Response" section, add a new response.

Select the "Add to Reference Set" response.

Specify the reference set and the data to be added.

Save and deploy the rule.

Reference

IBM QRadar SIEM V7.5 Administration documentation

Question: 54

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

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: 55

An administrator is reviewing the system notifications and discovers this error:

Insufficient disk space to complete data export request.

The Export Directory property in the System Settings has the default configuration.

Which disk partition does the administrator need to check?

A. /store/ariel/events/exports

B. /var/log/exports

C. /storetmp/exports

D. /store/exports

Answer: A

Explanation:

When the error "Insufficient disk space to complete data export request" is encountered, and the Export Directory property in the System Settings has the default configuration, the disk partition that needs to be checked is /store/ariel/events/exports. This directory is typically used for exporting event data in QRadar SIEM. The error indicates that the available disk space in this partition is insufficient to handle the export operation. Administrators should check the storage usage of this partition and manage the space by either cleaning up unnecessary files or expanding the storage capacity.

Reference

QRadar SIEM V7.5 Administration Guide - Chapter on System Notifications and Disk Management

Question: 56

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

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

Question: 57

Which field is mandatory when you use the DSM Editor to map an event to a OID?

A. High-level Category

B. Low-level Category

C. Event Category

D. Event ID

Answer: D

Explanation:

When using the DSM (Device Support Module) Editor in IBM QRadar to map an event to an OID (Object Identifier), the Event ID field is mandatory. The Event ID uniquely identifies the event within QRadar and is essential for ensuring that the correct event data is associated with the appropriate OID. This mapping process allows QRadar to properly categorize and handle events based on their unique identifiers.

Reference

QRadar SIEM V7.5 Administration Guide - Chapter on DSM Editor and Event Mapping

Question: 58

When restoring backups of your apps in a QRadar environment, what information is restored?

A. The last known good version of your apps configuration, your application data, and any apps that were configured on an App Host are restored.

B. The applications that are installed on the Console are restored, and any applications that are installed on an AppHost must be backed up separately.

C. The apps configuration, the console configuration, and app data are restored.

D. The apps configuration and app data are restored.

Answer: A

Explanation:

When restoring backups of your apps in a QRadar environment, the system restores the last known good version of your apps' configuration, your application data, and any apps that were configured on an App Host. This comprehensive restoration process ensures that all critical components of your applications, including their configurations and data, are

recovered to their previous states. This is crucial for maintaining the integrity and functionality of the applications after a restoration.

Reference

QRadar SIEM V7.5 Administration Guide - Chapter on Backup and Restore Procedures

Question: 59

How many vulnerability processors can you have in your deployment?

A. 5

B. 3

C. 10

D. 1

Answer: D

Explanation:

In QRadar SIEM V7.5, the number of vulnerability processors is limited to 1.

These vulnerability processors are responsible for handling and processing vulnerability data within the system.

Having multiple vulnerability processors is not supported in this version of QRadar.

Reference:

IBM QRadar SIEM V7.5 Administration documentation.

Question: 60

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?

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: 61

Which is a valid statement about the process of restoring a backup archive?

A. A configuration restore must be performed on a console where the IP address matches the IP address of a managed host in the backup.

B. A backup archive can only be restored for the same software version, including fix pack versions.

C. When restoring all configuration items included in the backup archive, only configuration information, offense data, and asset data are restored.

D. A restoration might fail if you restore the configuration backup before the data backup.

Answer: B

Explanation:

When restoring a backup archive in QRadar, it is essential to ensure that the software version matches exactly. This includes both the base version and any fix pack versions.

Attempting to restore a backup archive from a different software version can lead to compatibility issues, data corruption, and system instability.

Always verify that the backup archive corresponds to the same QRadar version before initiating the restoration process.

Reference:

IBM QRadar SIEM V7.5 Administration documentation.

Question: 62

Which is a valid routing rule combination?

A. Drop and Bypass Correlation

B. Drop and Log Only

C. Forward and Bypass Correlation

D. Bypass Correlation and Log Only

Answer: C

Explanation:

Forward: Data is forwarded to a specified destination. It is also stored in the database and processed by the Custom Rules Engine (CRE).

Drop: Data is dropped, meaning it is not stored in the database and is not processed by the CRE. If you select the "Drop" option, any events that match this rule are credited back 100% to the license.

Bypass Correlation: Data bypasses the CRE but is stored in the database. This option allows events to be used in analytic apps and for historical correlation runs. It's useful when you want specific events to skip real-time rules.

Log Only (Exclude Analytics): Events are stored in the database and flagged as "Log Only." They bypass the CRE and are not available for historical correlation. These events contribute to neither offenses nor real-time analytics.

Now, let's look at the valid combinations:

Forward and Drop: Data is forwarded to a specified destination, but it is not stored in the database or processed by the CRE. Dropped events are credited back to the license.

Forward and Bypass Correlation: Data is forwarded to a destination and stored in the database, but CRE rules do not run on it. Useful for scenarios where you want events to bypass real-time rules but still be available for historical correlation.

Forward and Log Only (Exclude Analytics): Events are forwarded to a destination, stored as “Log Only,” and bypass the CRE. They are not available for historical correlation and are credited back to the license.