C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

What data is purged by the SIM reset process "Hard Clean" in IBM Security QRadar SIEM V7.2.8?

A. All current and historical SIM data.

B. All historical SIM data, current SIM data is retained.

C. All SIEM data, a complete reconfiguration is required.

D. All source and destination IP addresses are purged, all offenses in the database are closed.

Correct Answer: A

Hard clean Purges all current and historical SIM data, which includes offenses, source IP addresses, and destination IP addresses.

QUESTION 2

What is needed to send the same events and flows to separate data centers or geographically separate sites and enable data redundancy in IBM Security QRadar SIEM V7.2.8?

A. A Flashcopy or GlobalMirror License.

B. A dark fibre network and proper configuration of the backup and recovery feature.

C. A load balancer or other method to deliver the same data to mirrored appliances.

D. Use the Backup and Recovery automation feature in QRadar and a dedicated fiber channel connection.

Correct Answer: C

Distribute the same event and flow data to two live sites by using a load balancer or other method to deliver the same data to mirrored appliances. Each site has a record of the log data that is sent.

QUESTION 3

Administrators on versions of IBM Security QRadar SIEM older than V7.2.4 must use a specific upgrade path to transition to newer software versions. These requirements are outlined in what technical document?

A. Fix Level Recommendation Tool

B. IBM latest firmware release notes

C. QRadar Software upgrade progress technical note

D. IBM System Security Interoperation Center (SSIC)

Correct Answer: C

Most of the upgrades of IBM products are available in technical notes. IBM security Qradar SIEM upgrade process and

information can be obtained through technical notes that IBM publishes on the web.

QUESTION 4

An Administrator has configured a customized log source extension to provide asset updates to IBM Security QRadar SIEM V7.2.8. Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name. In this situation what will QRadar report?

A. This will cause stale asset data.

B. This will cause asset growth deviations.

C. This will cause excessive authentication failure events.

D. This will cause excessive flow data to be processed by the Magistrate.

Correct Answer: B

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the

log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses

and user names.

QUESTION 5

An Administrator using IBM Security QRadar SIEM V7.2.8 is using the following RegEx:

([-+]?\d*$)

What type of information is it designed to extract?

A. Integer

B. IP address

C. Port number

D. Domain name

Correct Answer: A

Sample regular expressions:

email: (.+@[^\.].*\.[a-z]{2,}$)

URL: (http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\ S*)?$)

Domain Name: (http[s]?://(.+?)["/?:])

Floating Point Number: ([-+]?\d*\.?\d*$)

Integer: ([-+]?\d*$)

IP Address: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

For example: To match a log that resembles: SEVERITY=43 Construct the following Regular

Expression: SEVERITY=([-+]?\d*$)

QUESTION 6

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to limit the networking team to see

just the Network Flow functions.

What should the Administrator do?

A. Create a user with access to the Log Activity tab.

B. Create a user role with Network Activity -> View Flow Content.

C. Create a user role with Network Activity -> View Reference: Data.

D. Create a user role which grants access to all the functions in the Network Activity tab.

Correct Answer: B

QUESTION 7

An IBM Security QRadar SIEM V7.2.8 Administrator wants to create a security profile within the system but

receives an error upon saving.

What is a possible reason for this error?

A. The Administrator has used non alpha numeric value(s) in the name which is not allowed.

B. The Administrator has used less than 3 characters or more than 30 characters as name of the security profile.

C. The Administrator has mixed non alpha numeric value(s) and alpha numeric value(s) in the name which is not allowed.

D. The Administrator must bring the IBM Security QRadar SIEM V7.2.8 system first in edit mode before changes are allowed.

Correct Answer: B

In the Security Profile Name field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.

QUESTION 8

Where are the logs for QFlow stored on IBM Security QRadar SIEM V7.2.8?

A. /var/log/qflow.debug

B. /opt/var/log/qflow.debug

C. /opt/log/qradar/qflow.debug

D. /opt/qradar/log/qflow.debug

Correct Answer: A

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

To help you troubleshoot errors or exceptions, review the following log files.

/var/log/qradar.log

/var/log/qradar.error

If you require more information, review the following log files:

/var/log/qradar-sql.log

/opt/tomcat6/logs/catalina.out

/var/log/qflow.debug

Review all logs by selecting Admin > System and License Mgmt> Actions > Collect Log Files.

QUESTION 9

When migrating the Console after restoring from an IBM Security QRadar SIEM V7.2.8 backup, what must be manually copied?

A. The Connection data and Topology data

B. The Policy Monitor questions and event or flow data

C. TheQRadar Risk Manager device configurations and Topology data

D. The certificates, any custom generated private keys and event or flow data

Correct Answer: D

QUESTION 10

What key point should be understood about how flow information in IBM Security QRadar SIEM V7.2.8 is used?

A. Flow information generates the response that is configured in the custom rule.

B. Flow information is sent to QRadarQFlow Collector which normalizes raw log source events.

C. Flow information is actively gathered from the QRadar Event Collector and provides views, reports and alerts to the administrator.

D. Flow information is used to detect threats and other suspicious activity that might be missed if only event information were tracked.

Correct Answer: D

QUESTION 11

An Administrator working with IBM Security QRadar SIEM V7.2.8 is constantly receiving the following

message:

"SAR Sentinal: Threshold crossed."

Where will the Administrator tune the settings for these messages?

A. Admin tab -> General Settings -> Global System Notifications

B. Admin tab -> System Configuration -> Global System Notifications

C. Admin tab -> System Notifications -> System Activity Reporter Notifications

D. Admin tab -> System Configuration -> General Settings -> System Notifications

Correct Answer: B

The SAR Sentinel utility monitors QRadar for a broad number of functions, such as running processes, CPU usage, and hardware functions. The function of the SAR Sentinel is to monitor the system and provide notifications when the system load exceeds a set threshold.

QUESTION 12

What are the focus areas of the default dashboards available with IBM Security QRadar SIEM V7.2.8?

A. operating system status, network activity, system monitoring, and compliance

B. security, network activity, application activity, system monitoring, and compliance

C. errors, attack activity, network accesses, operating system status, and offense activity

D. errors, attack activity, security, network activity, application activity, system monitoring, and compliance

Correct Answer: B

QUESTION 13

An Administrator working with IBM Security QRadar SIEM V7.2.8 appliances needs to update firmware. How are the files acquired?

A. Firmware updates can be retrieved from IBM developerWorks.

B. Refer to support documents to download the firmware approved for QRadar appliances.

C. All firmware is automatically downloaded and no Administrator intervention is required.

D. All firmware updates are applied as part of the QRadar software patching process, and should not be applied independently.

Correct Answer: B

Administrators looking for the latest firmware downloads can review this page to locate firmware updates for QRadar appliances. The installation instructions include a direct download link to the firmware from IBM Fix Central.

QUESTION 14

An Administrator needs to see Events per Second (EPS) and Flows per Minute (FPM) coming to IBM Security QRadar SIEM V7.2.8 through a dashboard. How could this be accomplished?

A. Download the dashboard from IBM Security App Exchange.

B. Go to CLI and run the script /opt/qradar/bin/createdashboard.sh

C. Select any dashboard and customize it. Add a system summary item.

D. Create a new dashboard and then go to admin tab. Add item into the dashboard created.

Correct Answer: D

To determine the average EPS rate, users can click the Dashboard tab, then select the System Monitoring dashboard item. This dashboard contains and event per second and flows per minute dashboard item. To see EPS details, click the View in Log Activity link. This will give an estimate of the data size for events per day.

QUESTION 15

An IBM Security QRadar SIEM V7.2.8 Administrator needs to restore a backup archive after a hardware

failure.

The Administrator has navigated to the System Configuration tab with the Navigation menu, what are the

next steps to restore?

A. System Settings -> upload the backup file that you want to restore -> Configure the parameters >Restore -> OK

B. Backup and Recovery -> select the archive that you want to restore -> Configure -> configure the parameters -> Restore -> OK

C. System Settings -> select the archive that you want to restore -> On Demand Restoration ->Configure > Configure the parameters -> Restore -> OK -> OK

D. Backup and Recovery -> select the archive that you want to restore -> Restore, on the Restore a Backup window -> Configure the parameters -> Restore -> OK -> OK

Correct Answer: D