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

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

message:

"MPC: Unable to process offense. The maximum number of offenses has been reached."

What is the reason for this message?

A. The Multi Packet Capturer cannot handle more than 2500 attacks at the same time.

B. The Magistrate Processor Core has more than 2500 active Offenses or 100000 overall Offenses.

C. The Multi Packet Capturer cannot handle more than 500 offense reports at a certain point in time.

D. The Magistrate Processor Core has reached its maximum amount of network connections at a certain time.

Correct Answer: B

QUESTION 2

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 3

An Administrator working with IBM Security QRadar SIEM V7.2.8 only needs to remove a single host

(10.1.95.142)

from the reference set with the name "Asset Reconciliation IPv4 Whitelist" from the

command line interface.

Which command would accomplish this task?

A.

./RefereceSetUtil.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142

B.

./RefereceSetUtil.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142

C.

./RefereceSetData.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142

D.

./RefereceSetData.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142

Correct Answer: B

The syntax for the command is:

ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP

QUESTION 4

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to delete a single value named

User1 from a reference set with the name "Allowed Users" from the command line interface.

Which command will accomplish this?

A. ./UtilReferenceSet.sh purge "Allowed Users" User1

B. ./ReferenceSetUtil.sh purge "Allowed Users" User1

C. ./ReferenceSetUtil.sh delete "Allowed\ Users" User1

D. ./UtilReferenceSet.sh delete "Allowed\ Users" User1

Correct Answer: B

The Referencesetutil.sh purge is the correct syntax of the command. It deletes the specific user when you mention it within the reference set.

QUESTION 5

An IBM Security QRadar SIEM V7.2.8 Administrator wants to change the reference set type. What step(s) need to be taken to accomplish this?

A. Use the CLI with the ReferenceSetUtil.sh script

B. Recreate the reference set with the new data type

C. Admin tab -> System Configuration -> Reference: Set Management -> Edit

D. Admin tab -> System Configuration -> Reference: Set Type Management -> Edit

Correct Answer: C

QUESTION 6

An Administrator working with IBM Security QRadar SIEM V7.2.8 wants to view the general statistics of all hosts in the Distributed Environment.

Where can the Administrator find this information?

A. Admin tab -> System Status -> System Health

B. Admin tab -> General Settings -> System Health

C. Admin tab -> System Configuration -> System Health

D. Admin tab -> System Configuration -> System Statistics

Correct Answer: C

QUESTION 7

Where are the IBM Security QRadar SIEM V7.2.8 log files located?

A. /var/qradar.log

B. /var/log/qradar.log

C. /opt/qradar/log/qradar.log

D. /opt/qradar/support/qradar.log

Correct Answer: B

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 8

What is a precaution an Administrator should take before beginning an upgrade of IBM Security QRadar SIEM V7.2.8?

A. Close all open offenses.

B. Purge old data and events.

C. Check and close all open messages.

D. Confirm that a backup of the data is complete.

Correct Answer: D

The first precaution listed in the IBM document states that the administrator should backup data before preparing for software upgrade. Backup of the current settings is important because if anything bad happens during the upgrade, you can always revert back to the original settings.

QUESTION 9

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 10

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

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

An Administrator working with IBM Security QRadar SIEM V7.2.8 was tasked with adding a new Microsoft Azure log source.

What protocol is supported for this?

A. FTP

B. JDBC

C. Syslog

D. WinCollect

Correct Answer: C

QUESTION 13

IBM Security QRadar SIEM V7.2.8 collects network activity information. This information represents

network activity by normalizing IP addresses, ports, byte and packet counts, as well as other details, which

effectively represent a session between two hosts.

This defines what type of information?

A. Flow Record information

B. Event Record Information

C. Data Source Information set up to a database from a server

D. A failed login action of a Virtual Private Network (VPN) session

Correct Answer: A

QUESTION 14

Where are the IBM Security QRadar SIEM V7.2.8 errors logged?

A. /var/log/qradar.error

B. /var/log/qradar/error.log

C. /opt/qradar/log/qradar.error

D. /opt/qradar/support/qradar.log

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_siem_inst_logs.html

QUESTION 15

How can an IBM Security QRadar SIEM V7.2.8 Administrator capture specific data to a reference set when QRadar receives the data from events or flow data?

A. Create or modify a report so the required data is exported to a Reference: Set.

B. On the Admin tab. create or modify the reference set to capture the required data.

C. On the Admin tab define a Custom Action to add the required data to a Reference: Set.

D. Create or modify a rule so the Rule Response will add the required data to a Reference: Set.

Correct Answer: B

You can click on the admin tab and select system configuration. The Reference: set management will be seen. Click New and configure the parameters.