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.certbus.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 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 2

Which appliance can run IBM Security QRadar SIEM V7.2.8 and includes a single QFlow Collector component?

A. QRadar 2100

B. QRadar 3105

C. QRadar 3124

D. QRadar 3128

Correct Answer: D

QUESTION 3

The event data collected by IBM Security QRadar SIEM V7.2.8 is being deleted after one month. The legal

department required the data be kept for two months.

What can the administrator do to accommodate this requirement?

A. Change the nightly backup Priority to "High".

B. Change the nightly backup to a monthly backup.

C. Change the Default Event Retention Policy property field "Do not delete data in this bucket" to two months.

D. Change the Default Event Retention Policy property field "Keep data placed in this bucket for" to two months.

Correct Answer: D

When storage space is required - Select this option if you want events or flows that match the Keep data placed in this bucket for parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads.

When storage is required, only events or flows that match the Keep data placed in this bucket for parameter are deleted.

QUESTION 4

How would an Administrator working with IBM Security QRadar SIEM V7.2.8 review all logs?

A. Admin Tab -> System Configuration -> Actions -> Collect Log Files

B. Admin Tab -> System Configuration -> Actions -> Collect All Log Files

C. Admin Tab -> System and License Management -> Actions -> Collect Log Files

D. Admin Tab -> System and License Management -> Actions -> Collect All Log Files

Correct Answer: B

QUESTION 5

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 6

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 7

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 8

After downloading the .sfs file from Fix Central, what is the next step to upgrade IBM Security QRadar SIEM V7.2.8?

A. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Clean SIM Model.

B. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Upgrade option.

C. Use SSH to log in to the system as the root user -> Run the patch installer with the following command: /media/updates/upgrade_qradar.

D. Use SSH to log in to the system as the root user -> Copy the patch file to the /tmp directory or to another location that has sufficient disk space.

Correct Answer: D

QUESTION 9

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

(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

What type of information is it designed to extract?

A. An IP Address

B. GPS Coordinates

C. A Telephone Number

D. A simple integer no longer than 4 digits

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 10

During the IBM Security QRadar SIEM V7.2.8 installation, which two default user roles are defined? (Choose two.)

A. All

B. Any

C. Admin

D. SuperUser

E. SuperAdmin

Correct Answer: AC

Two default user roles are listed in the left pane of the window: Admin and All. You can select a role in the left pane to view the associated role permissions in the right pane.

QUESTION 11

What procedure does a user of IBM Security QRadar SIEM V7.2.8 need to follow to delete a dashboard?

A. Click the "Dashboard" tab.From the Show Dashboard list box, select the dashboard that you want to delete.On the toolbar, click "Delete Dashboard".Click "Yes".

B. Click the "Dashboard" tab.From the Show Dashboard list box, select the dashboard that you want to delete.On the toolbar, click "Remove Dashboard".Click "Yes".

C. Click the "Dashboard" tab.On the toolbar, click "Delete a Dashboard".From the Delete Dashboard window, select the dashboard that you want to delete.Click "Yes".

D. Click the "Dashboard" tab.From the Show Dashboard list box, select the dashboard that you want to delete.On the toolbar, click "Delete Dashboard for a user".On the User selection Menu select the user you want to delete from the dashboard and click "Okay".

Correct Answer: A

QUESTION 12

An Administrator is unable to access the IBM Security QRadar SIEM V7.2.8 web GUI. What could the Administrator do to determine the reason for the issue?

A. Check the status of tomcat and httpd.

B. Check the status of ecs-ec and ecs-ep.

C. Check if the postgres database is running.

D. Check if the console is over the EPS and FPS license.

Correct Answer: A

QUESTION 13

An Administrator is creating custom rules and configuring log sources on an IBM Security QRadar SIEM

V7.2.8 console. This data needs to be retained so that it can be recovered in case of any system failure

with minimal effort.

Which option can the Administrator utilize from the Backup and Recovery Wizard to accomplish this task?

A. Data backups

B. Ariel database

C. Configuration and Data backups

D. Configuration and DB2 database

Correct Answer: A

QUESTION 14

When it comes to licensing, what is the difference between Events and Flows and how they are licensed?

A. Flows are licensed based on overall count over a minute, where Events are licensed based on overall count per second.

B. Flows are licensed based on overall count per second, where Events are licensed based on overall count over a minute.

C. Flows and Events are both licensed by overall count per minute under an Upgraded License and per second on a Basic License.

D. Flows and Events are both licensed by overall count per second under an Upgraded License and per second on a Basic License.

Correct Answer: A

A significant difference between event and flow data is that an event, which typically is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged at that time. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session. For example, a web request might download multiple files such as images, ads, video, and last for 5 to 10 seconds, or a user who watches a Netflix movie might be in a network session that lasts up to a few hours. The flow is a record of network activity between two hosts.

QUESTION 15

When upgrading IBM Security QRadar SIEM V7.2.8 in High Availability (HA) deployments, how can the upgrade be automatically applied to the associated secondary system(s)?

A. Issue the command on the primary system /media/updates/installer -HA

B. Confirm the system setting on both the primary and secondary systems are set to "Upgrade YES"

C. Make sure the primary system is the active system and the secondary system is in standby mode

D. Make sure the primary system is the active system and the secondary system is in failover mode

Correct Answer: C