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.pass4itsure.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 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 2

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 3

An Administrator working within IBM Security QRadar SIEM V7.2.8 has created a network hierarchy that includes the following groups and subgroups: Office #1 Group

-Miscellaneous 10.10.0.0/24

-Sales 10.10.8.0/24

-Marketing 10.10.1.0/24 Office #2 Group

-Miscellaneous 10.20.0.0/16

-Sales 10.20.8.0/24

-

Marketing 10.20.1.0/24 A new subgroup is added to Office #1 having a CIDR of 10.10.50.0/24. Offenses are being triggered and during the investigation, it is noticed the rule should not fire if traffic is L2L. The offense is being triggered on traffic from 10.10.4.17 to 10.20.1.8. Is this rule using the network hierarchy correctly?

A.

This rule is parsing the network hierarchy correctly, as the 10.10.4.17 address is not contained in a group, and therefore is remote.

B.

This rule is parsing the network hierarchy correctly, as the offices are both remotely geo-located, and connecting over the Internet, it is remote traffic.

C.

This rule isn\\'t parsing the network hierarchy correctly, as the network hierarchy contains the CIDR for

10.10.4.17 and 10.20.1.0/24, therefore being L2L traffic.

D.

This rule isn\\'t parsing the network hierarchy correctly, as the network hierarchy contains both subnets, but is viewing traffic between groups to be remote instead of local.

Correct Answer: A

QUESTION 4

A retention policy allows an IBM Security QRadar SIEM V7.2.8 Administrator to define how long the system is required to keep certain types of data and what to do when data reaches a certain age. If a 3month retention policy is defined for all events, then the system will not delete event data until it\\'s on disk timestamp is 3 months in the past. Which two choices are available in the `delete data in this bucket\\'? (Choose two.)

A. When the index is full

B. Upon reboot of the system

C. When storage space is required

D. When performance is heavily affected

E. Immediately after retention period has expired

Correct Answer: CE

From the list box, select a deletion policy. Options include: ?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. Immediately after the retention period has expired ?Select this option if you want events to be deleted immediately on matching the Keep data placed in this bucket for parameter. The events or flows are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.

QUESTION 5

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.