C2150-400 Q&As

IBM Security Qradar SIEM Implementation v 7.2.1

Pass IBM C2150-400 Exam with 100% Guarantee

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

https://www.pass4itsure.com/c2150-400.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

There is a requirement at the customer site to double the default QFlow Maximum Content Capture size. What would be the resulting packet size?

A. 64 bytes

B. 128 bytes

C. 256 bytes

D. 1024 bytes

Correct Answer: B

QUESTION 2

Which two fields are required to be filled out when adding a new network to the network hierarchy? (Choose two.)

A. Group

B. Country

C. Mail Server

D. DNS Server

E. IP and CIDR

Correct Answer: DE

QUESTION 3

What is the command to mount the Patch file 721_QRadar_patchupdate-7.2.1.679924.sfs in QRadar 7.2.1?

A. mount -o loop /media/updates 721_QRadar_patchupdate-7.2.1.679924.sfs

B. mount -o squashfs -t loop 721_QRadar_patchupdate-7.2.1.679924.sfs /media/updates

C. mount -o loop /media/updates -t squashfs 721_QRadar_patchupdate-7.2.1.67924.sfs

D. mount -o loop -t squashfs 721_QRadar_patchupdate-7.2.1.679924.sfs /media/updates/

Correct Answer: D

QUESTION 4

Which offboard storage solution provides the fastest performance?

A. AoE

B. NFS

C. iSCSI

D. Fibre Channel

Correct Answer: D

QUESTION 5

What functionalities of QRadar provide the ability to collect, understand, and properly categorize events from external sources?

A. Log sources

B. Flow sources

C. Syslog sources

D. External sources

Correct Answer: A