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

What type of users can view all reports that are created by other users?

A. Auditors

B. Analysts

C. Managers

D. Administrators

Correct Answer: D

QUESTION 2

Which two IP Addresses are required to Add a HA host? (Choose two.)

A. Public IP Address

B. Private IP Address

C. Cluster IP Address

D. Remote IP Address

E. IP Address of Secondary Host

Correct Answer: CE

QUESTION 3

What is used to collect netflow and jflow traffic in a QRadar Distributed Deployment?

A. QRadar 3105 Console

B. QRadar 1705 Processor

C. QRadar 1605 Processor

D. QRadar 700 Risk Manager

Correct Answer: A

QUESTION 4

A flow is sequence of packets that have which common characteristics?

A. Same source, MAC address, flow source and destination IP address

B. Same source IP address, flow source and transport layer port information

C. Same source and destination IP address and transport layer port information

D. Same destination IP address, source bytes and transport layer port information

Correct Answer: D

QUESTION 5

Which offboard storage solution provides the fastest performance?

A. AoE

B. NFS

C. iSCSI

D. Fibre Channel

Correct Answer: D

QUESTION 6

Which statement is correct for patching an HAed server?

A. If the Secondary host is in an Active state, the patch should be applied to the Secondary.

B. The patch should be applied to the Primary first and the patch should be applied to the Secondary.

C. Remove Secondary, then apply the patch on Primary, and then add the Secondary again.

D. Run the patch on the Primary and the Secondary will be updated Automatically.

Correct Answer: B

QUESTION 7

A QRadar administrator is sizing a distributed deployment. The deployment has approximately 1.5 gigabytes of sustained throughput of traffic on a network tap. The network tap is a copper connection. Which Qflow collector should be chosen?

A. Qflow Collector 1310

B. Qflow Collector 1202

C. Qflow Collector 1201

D. Qflow Collector 1301

Correct Answer: B

QUESTION 8

A QRadar administrator is sizing a distributed deployment. The deployment has approximately 25,000 events per second and needs at least 7 terabytes of storage.

Which architecture is correct?

A. One 1605 event processor

B. One 1624 event processor

C. Two 1605 event processors

D. Two 1624 event processors

Correct Answer: C

QUESTION 9

Which two proxy options are required to be set when using a Proxy Server for Auto Updates in QRadar? (Choose two.)

A. Proxy Type

B. Proxy Name

C. Proxy Schedule

D. Proxy Server URL

E. Proxy Port number

Correct Answer: BD

QUESTION 10

What are the two expected Host Statuses after HA setup if the initial synchronization is complete? (Choose two.)

A. Primary: Active

B. Primary: Offline

C. Secondary: Failed

D. Secondary: Active

E. Secondary: Standby

F. Primary: Synchronizing

Correct Answer: AE

QUESTION 11

Which two options are available for Override parameter when an administrator views the Asset Profile Summary page? (Choose two.)

A. Forever

B. Until Next Scan

C. After Next Scan

D. Before Next Scan

E. After Specified Time

Correct Answer: AB

QUESTION 12

Which string creates a network hierarchy group called WebServers inside a group called DMZ?

A. DMZ/WebServers

B. DMZ_WebServers

C. DMZWebServers

D. DMZ+WebServers

Correct Answer: A

QUESTION 13

In QRadar SIEM, customer wants to tune one of the firewall deny event which shows firewall deny for all events coming from a Syslog Server and has been identified as false positive. The customer clicked on the "false positive" button to tune the specific event.

What are the traffic directions that will be available during declaring this event as a false positive? (Choose two.)

A. SourceIP to Local Network

B. SourceIP to Any Destination

C. Any source to Any Destination

D. Destination IP to Local Network

E. Source IP to Destination Network

Correct Answer: BE

QUESTION 14

Which scanners report vulnerabilities on all ports? (Choose two.)

A. Axis

B. NMap

C. Qualys

D. tcpdump

E. nCircle IP360

Correct Answer: BC

QUESTION 15

Which tab in the QRadar web console allows events to be monitored and investigated?

A. Admin

B. Offenses

C. Forensics

D. Log Activity

Correct Answer: D