Question 1

Which QRadar log file contains information about the rates of EPS?

Options:

A- /var/log/eps.log

B- /var/qradar.log

C- /var/log/qradar.log

D- /var/log/qradar.old

Answer:

C

Question 2

A company plans to collect event data from two remote sites that have slow WAN links. These remote sites do not generate many events per second. The company's deployment professional wants to deploy a system that can use EPS limiters to send events to the Event Processor to overcome WAN limitations.

What type of appliance can be used to meet this requirement?

Options:

A- Packet Capture appliance

B- Data Gateway

C- Flow Collector

D- Disconnected Log Collector

Answer:

C

Question 3

Question Type: **MultipleChoice**

Which statement about the Extensions Management tool in QRadar is true?

Options:

A- The Extensions Management tool can be used to add a log source.

B- The Extensions Management tool cannot be used to export content out of QRadar.

C- QRadar can be updated by using the Extensions Management tool.

D- CSV extensions can be imported into QRadar.

Answer:

D

Question 4

Question Type: MultipleChoice

Which additional license is required to use the Am I Affected scan in the IBM Security QRadar Threat Intelligence app?

Options:

A- IBM Security QRadar Console license

B- IBM Security QRadar QVM license

C- IBM Watson license

D- IBM Advanced Threat Protection Feed license

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which two statements are prerequisites for an to upgrade of QRadar? (Choose two.)

Options:

A- Verify that scan runs and reports are complete.

B- Verify that all changes are deployed on the appliances.

C- Ensure an admin account is logged on the UI.

D- Clean up all the Offenses before any version upgrade.

E- Ensure that the ISO file is copied to all the appliances.

Answer:

A, C

Question 6

Question Type: MultipleChoice

A QRadar deployment professional wants to integrate a dynamic data set like asset information so that QRadar can use the latest information in the new data set to correlate the rules and alerts.

How can the deployment professional achieve this?

Options:

A- Use the QRadar Search to search each item in the list of imported data set.

B- Import the dynamic data in the reference set and use these reference sets in rules and building blocks.

C- Use the Threat Intelligence app.

D- Use the UCM app.

Answer:

A

Question 7

When adding a Data Node to an Event Processor, what are the minimum bandwidth and maximum latency requirements?

Options:

A- 1 Gbps link and 10 ms latency

B- 1 Gbps link and 100 ms latency

C- 10 Gbps link and 10 ms latency

D- 10 Gbps link and 100 ms latency

Answer:

C

Question 8

To increase the amount of storage for IBM Security QRadar, data is moved to an offboard storage device.

Which method for adding external storage must be used for /store/ariel?

Options:

A- /store/ariel/ cannot be moved off of a QRadar appliance.

B- Manually copy files at regular intervals.

C- Use NFS (Network File System) for external storage.

D- Use iSCSI for external storage.

Answer:

B

Question 9

For the management of applications with Qradar Assistant, which of these is not an option?

Options:

A- Pause All Instances

B- Create New Instance

C- Start All Instances

D- Delete All Instances

Answer:

A

Question 10

Where is a QRadar license obtained?

Options:

A- X-Force Exchange/license app

B- IBM Sales Representative

C- QRadar Console

D- IBMcom/qradar/licenses

Answer:

B

Question 11

What must a deployment professional select when defining a new flow source?

Options:

A- The destination port

B- The source IP address

C- The flow source type

D- The router brand

Answer:

C