Question 1

Where does QRadar display R2R events?

Options:

A- The Network Activity tab

B- The Remote Services window

C- The Tuning interface in the Use Case Manager app

D- The Testing interface in the Log Source Manager app

Answer:

C

Question 2

A QRadar deployment professional needs to transfer the configuration of a distributed environment (one Console and one EP, not using HA) onto an All-in-One (AIO) system to run some forensics against data that will be added later.

What approach should the deployment professional suggest for building the new AIO?

Options:

A- Use rsync to transfer the contents of the /store partition to the new system.

B- The configuration of the source environment should be backed up and then restored on the new AIO. After the system is up, the EP can be removed by use of the GUI.

C- Because the destination environment does not have the same number of appliances, the only option is to use the content management tool (CMT) to transfer the security configuration.

D- The configuration of the source environment should be backed up and then restored on the new AIO. After the system is up, the EP can be removed only by use of back-end PSQL commands.

Answer:

D

Question 3

Question Type: OrderList

What is the correct order of these steps to get the X-Force API Access Key and Password?

Unordered Options

| Log in to https://exchange.xforce.ibmcloud.com/ | 1 |

| Click Show User Menu | 2 |

| Click Settings | 3 |

| Click API Access | 4 |

| Enter a Name for API Key | 5 |

| Click Generate | 6 |

Ordered Options

Answer:

Click Settings for API Key
Login to https://exchange.xforce.ibmcloud.com/

Question 4

What app can be used in QRadar to visualize offenses, network data, threats, and malicious behavior provide insights and analysis about a network?

Options:

A- Threat Intelligence

B- Use Case Manager

C- Pulse

D- Vulnerability Insights

Answer:

B

Question 5

Consider this scenario and instruction.

Vulnerability assessment products launch attacks that can result in offense creation. To avoid this behavior and define vulnerability assessment products or any server that you want to ignore as a source, edit the "and when the source IP is one of the following" test to include the IP addresses of the following scanners.

VA Scanners

Authorized Scanners

What type of editable building block is described?

Options:

A- BB:HostDefinition: Authorized ScannersSource IP

B- BB:HostDefinition: VA Scanner Source IP

C- BB:NetworkDefinition: Server Networks

D- BB:HostDefinition: Proxy Servers

Answer:

C

Question 6

Question Type: **MultipleChoice**

Which of these items is updated when vulnerability scan results from third-party vulnerability scanners are imported into QRadar?

Options:

A- Assets

B- Flow sources

C- Event sources

D- Vulnerability scanner sources

Answer:

C

Question 7

Question Type: **MultipleChoice**

A deployment professional is about to add a secondary appliance to a QRadar high availability deployment. It is confirmed that both the primary and the secondary appliances are on the same QRadar version. However, the hardware configuration of both appliances is different.

What must be confirmed before adding the secondary appliance to the high availability deployment?

Options:

A- The combined size of the /store and /transient partitions on the primary host must be larger than the /store partition on the secondary host.

B- The secondary host must use a different management interface than the primary HA host.

C- The primary host must contain more physical interfaces than the secondary.

D- The combined size of the /store and /transient partitions on the secondary host must be equal to or larger than the /store partition on the primary host.

Answer:

D

Question 8

Question Type: **MultipleChoice**

The /store for a QRadar HA setup was migrated to a Fibre Channel device. High Availability is not needed on this cluster, and it needs to be disconnected.

What changes are required before disconnecting the HA cluster in this scenario?

Options:

A- Edit the /etc/fstab on only the primary HA host to remove the noauto option from /store and /storetmp.

B- Edit the /etc/fstab on only the secondary HA host to remove the noauto option from /store and /storetmp.

C- Edit the /etc/fstab on the primary HA host and secondary HA host to remove the noauto option from /store and /storetmp.

D- No changes are required before disconnecting the HA cluster.

Answer:

C

Question 9

Question Type: MultipleChoice

A QRadar deployment professional needs to add a managed host to help reduce the load on the QRadar Console.

The managed host should have local storage and also use the QRadar Custom Rule Engine.

Which managed host does the deployment professional add?

Options:

A- Event Collector

B- App Host

C- Disconnected Log Collector

D- Event Processor

Answer:

D

Question 10

Question Type: MultipleChoice

Which statement about IBM-validated QRadar content extensions is true?

Options:

A- They are only downloaded from IBM approved third-party portals.

B- They can be downloaded from IBM X-Force Fix Central.

C- They are restricted by the type of QRadar license that is acquired.

D- They are hosted on the IBM X-Force Exchange portal.

Answer:

D

Explanation:

https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-content-extensions

Question 11

Question Type: MultipleChoice

Which of these views is provided by the DSM Editor?

Options:

A- Event Mappings tab, Flow tab, Protocols

B- Workspace, Event Mappings tab, Configuration tab

C- Dashboard, Event properties, Configuration tab

D- Workspace, Flow tab, Event properties

Answer:

A