DUMPSARENA

IBM QRadar SIEM V7.3.2 Deployment

IBM C1000-055

Version Demo

Total Demo Questions: 8

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A QRadar customer has a custom log source. The deployment professional has already created a custom DSM for the log source and all incoming events are correctly parsed and mapped to a QID. Now, in addition to the currently parsed properties, the customer requires that the information about the last logged in user is recorded in the asset database.

How can the deployment professional fulfill the requirement?

A. Use the DSM editor to ensure that the Identity Username property is correctly parsed.
Create an expression for any available identity property and ensure it is correctly parsed.
Also, in the DSM editor enable identity data for the login success event type.

B. Use the DSM editor to ensure that the Username property is correctly parsed. Create an expression for any available identity property and ensure it is correctly parsed. Also, in the DSM editor, enable the identity data for the login success event type.

C. Use the DSM editor to create an expression for the Username property so it is correctly parsed. Create an expression for any available identity property and make sure it is correctly parsed. It is automatically applied to all events with low level category "User login success".

D. Use the DSM editor to create an expression for the Identity Username property and make sure it parses correctly. It is automatically applied to all events with low level category "User login success".

ANSWER: D

QUESTION NO: 2

A deployment professional is asked to create QRadar deployment architecture for a company.

The company has three branch offices with WAN connection between them. The head office data center requires 14000 EPS and 200000 FPM. Each branch requires 4000 EPS and 200000 FPM.

Which deployment solution will meet the minimum requirements?

A. QRadar 3105 (Console) in head office + QRadar 1805 Event and Flow Processor in each branch office

B. QRadar 3129 (Console) in head office + QRadar 1805 Event and Flow Processor in each branch office

C. QRadar 3105 (Console) and QRadar Event and Flow Processor 1829 in head office +
QRadar 1805 Event and Flow Processor in each branch office

D. QRadar 3129 (All-in-One) in head office

ANSWER: A

QUESTION NO: 3

The client implemented a QRadar Network Insights (QNI), and is looking to add postincident investigations and threat hunting activities.

What should the deployment professional recommend?

A. An additional QRadar Incident Forensics is required.

B. An additional QRadar Network Inspector is required.

C. Existing appliances will suffice.

D. An additional QRadar Flow processor is required.

ANSWER: D

QUESTION NO: 4

A deployment professional has to decide where data will be stored in a newly configured environment to submit a plan for storage and network connectivity bandwidth.

Which QRadar components within a deployment can store raw or normalized events locally? (Choose two)

A. Event Processor

B. Event Collector

C. Data Node

D. Flow Collector

E. Data Diode

ANSWER: A C

Explanation:

:

https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_deployment.pdf

QUESTION NO: 5

IBM Security QRadar initiates a sequence of events when a primary high-availability (HA) host fails. During failover, the secondary HA host assumes the responsibilities of the primary HA host. The following actions are completed.

1.1. If configured, external shared storage devices are detected and the file systems are mounted.

2. 2. The secondary HA host connects to the console and downloads configuration files.

3. 3. A management interface network alias is created, for example, the network alias forethO is ethO:0.

4. 4. The cluster virtual IP address is assigned to the network alias.

5. 5. All QRadar services are started.

What is the order of the sequence?

A. 1,4,3,2,5

B. 1,3,4,5.2

C. 1.2,3,4,5

D. 1,4,5,3,2

ANSWER: C

QUESTION NO: 6

A deployment professional needs to find out which rules are generating most of the offenses. What should the deployment professional do? (Choose two)

A. Use search where Log source is Custom Rule Engine-8 :: and choose Grouping by Event Name

B. Offenses -> Rules -> Sort by Offense Count

C. Offenses -> By Category

D. Use search where Log source is Health Metrics-2 :: and choose Grouping by Event Name

E. Generate Report "System Summary"

ANSWER: B E

QUESTION NO: 7

A deployment professional decides to improve visibility in the network and successfully installs the Flow Collector.

What should the deployment professional connect the Flow Collector to?

A. WAN port

B. SPAN port

C. LAN port

D. SAN port

ANSWER: B

QUESTION NO: 8

A company has specific data retention policies to keep log data online for 5 years. The current QRadar storage will not handle this amount of data.

Which are possible solutions? (Choose two)

A. Migrate the QRadar /store/ariel file system to a larger off board storage device

B. Implement Data Node(s)

C. Implement Event Collector(s)

D. Implement Flow Processor(s)

E. Implement a high availability (HA) solution

ANSWER: A D