DUMPSBOSS.

IBM QRadar SIEM V7.3.2 Deployment

IBM C1000-055

Version Demo

Total Demo Questions: 8

Total Premium Questions: 60

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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: 2

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

QUESTION NO: 3

A deployment professional is redesigning the existing deployment to add a event processor due to an increased event rate. The deployment professional observes the events per second (EPS) to be a collective 30,000 EPS from two event collectors (EC1 and EC2) and sometimes exceeds the EPS capacity. EC1 and EC2 are in same network segment.

Considering there are more licenses available than needed in the license pool, which processor should the deployment professional replace the event collector(s) with?

A. Replace EC1 with one QRadar Event Processor 1648

B. Replace EC1 and EC2 with one QRadar Event Processor 1605

C. Replace EC1 and EC2 with one QRadar Event Processor 1629

D. Replace EC1 with one QRadar Event Processor 1605

ANSWER: C

QUESTION NO: 4

A deployment professional needs to install a new QRadar application downloaded from the

IBM Security App Exchange.

Which option would the deployment professional select from the QRadar Console GUI under Admin: System Configuration to install the downloaded application?

A. Customization Management.

B. Application Management. C. Extensions Management.

C. Content Management.

ANSWER: C

QUESTION NO: 5

A deployment professional needs to check which rules cause events to be dropped on the

Console with Pipeline NATIVE_To_MPC messages.

Which script would help with this task?

A. /opt/qradar/support/findExpensiveCustomProperties.sh

B. /opt/qradar/support/findExpensiveCustomRules.sh

C. /opt/qradar/support/astat.sh

D. /opt/qradar/support/findRules.sh

ANSWER: C

QUESTION NO: 6

A deployment professional configures domain definitions for events in a multi-tenant QRadar environment. The domain assignments for tenants, flows, VA scanners, reference data, network hierarchy items are already configured.

Which is the order of precedence between the incoming event's attributes when evaluating its domain assignment?

A. Custom Properties, Network Hierarchy, Log Source, Event Collector

B. Tenant, Log Source, Network Hierarchy, Log Source Group

C. Tenant, Network Hierarchy. Log Source, Event Collector

D. Custom Properties, Log Source, Log Source Group. Event Collector

ANSWER: C

QUESTION NO: 7

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: 8

A deployment professional has been asked to ensure the system can be integrated with another system which contains lists of IP addresses and CIDR ranges in an automated manner, to allow rules to target specific communication endpoints.

Which part of QRadar is designed to hold and manage this data?

A. Domain Definition

B. Network Hierarchy

C. Asset Profiles

D. Building Blocks

ANSWER: D