

DUMPSBOSS.

Technical Sales Foundations for IBM QRadar for Cloud (QRoC) V1

IBM P1000-017

Version Demo

Total Demo Questions: 5

Total Premium Questions: 40

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Who has full admin access to the QRadar on cloud environment?

- A. Dev Ops
- B. All users
- C. _____ SaaS Admin
- D. QROC Admin group

ANSWER: A

QUESTION NO: 2

What type of super flow is unidirectional flow that has same source and multiple destinations?

- A. Type A superflow (Network Scans)
- B. Type B superflow (DDOS)
- C. Type C superflow (Port scans)
- D. Type D Superflow (XFE)

ANSWER: A

QUESTION NO: 3

What does log source time mean in the event detail page

- A. Time stamp created when an event arrives at Qradar
- B. Time stamp created when an event processor is started
- C. Time stamp that is extracted from the event payload
- D. Time stamp that is extracted from files when an event data is stored

ANSWER: C

QUESTION NO: 4

In the scenario where Qradar on cloud client wishes to integrate an AWS hosted data source

- A. Deploying a dedicated Qradar instance is required in AWS
- B. Deploying data gateway in AWS is required to collect data from the environmentc.
- C. Deploying a Data Gateway in event hub is required for data sources
- D. Deploying a data gateway or utilizing a TLS Connection directly from QRadar – CloudWatch and CloudTrail

ANSWER: D

QUESTION NO: 5

Which is a capabilities gap between on Prem QRadar and QRadar on Cloud

- A. Two Datacenters currently hosts QRadar on Cloud Environment
- B. QRadar on Cloud is unable to Scale beyond 100K events per second
- C. Installation of application tokens required IBM operation team interaction
- D. Investigation of the offences logs and data requires generation of support of service ticket

ANSWER: C