



A2150-195^{Q&As}

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Pass IBM A2150-195 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/a2150-195.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which flow source is most often sampled?

- A. vFlow
- B. sFlow
- C. QFlow
- D. netflow

Correct Answer: B

QUESTION 2

How can a user cancel a running report in IBM Security QRadar V7.0 MR4?

- A. A running report cannot be canceled
- B. Select the report > Actions > Cancel Report
- C. Right-click on the report > select Cancel Report
- D. Look at the report queue, select the report to be canceled, select Delete

Correct Answer: A

QUESTION 3

Which regex should be used to capture only the domain name blackbox.computer for all future machine names based on this example?

``Computer=3 8 9.blackbox.computer\``

- A. `Computer= (. *) \s`
- B. `Computer=389. (.*)\s`
- C. `Computer=(389\..*)\s`
- D. `Computer=. *?. (.*)\s`

Correct Answer: D

QUESTION 4



Which column in the log activity displays the coalesced value?

- A. Count
- B. Raw Count
- C. Event Count
- D. Roll-up Count

Correct Answer: C

QUESTION 5

What is used to parse an event (log record) in IBM Security QRadar V7.0 MR4?

- A. CRE
- B. DSMs
- C. Qidmaps
- D. Protocols

Correct Answer: B

[A2150-195 VCE Dumps](#)

[A2150-195 Study Guide](#)

[A2150-195 Exam Questions](#)