C2150-400 Q&As

IBM Security Qradar SIEM Implementation v 7.2.1

Pass IBM C2150-400 Exam with 100% Guarantee

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

https://www.geekcert.com/c2150-400.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

A customer has developed a custom Universal Device Support Module (uDSM\\'s) for an unsupported device. The customer wants to parse Device Time field which is not in standard format.

Which parameter should an administrator define in the LSX template in this situation?

A. ext-time

B. ext-date

C. ext-data

D. ext-devicedate

Correct Answer: C

QUESTION 2

A QRadar administrator is developing custom uDSM\\'s for an unsupported device. Given this event payload:

Jan 28 12:57:23 9.77.16.19 AgentDevice=FileForwarder AgentLogFile=logger1.log Payload=January 28,2014 12:53:50 PM GMT+05:30|HOST_CREATE_ERROR|Host{1:testserver40} create failed on array {0:Abc}

Which regular expression should the administrator define for parsing the hostname "testserfvefr40"?

A. \w+\s+{.*?\\s}

B. \w+\s+{\d+\:(\.*?)\}

C. \w+\s+{\d+\:(\w+)\}

D. \w+\s+{\d+\:([a-zA-Z]+)\}

Correct Answer: D

QUESTION 3

What should be the latency between the primary and secondary HA hosts?

A. Less than 1 millisecond

B. Less than 2 milliseconds

C. Less than 3 milliseconds

D. Less than 4 milliseconds

Correct Answer: B

QUESTION 4

A customer is observing the Asset tab on the QRadar console and is getting duplicate assets in the console.

What is the reason for this asset duplication?

A. There are multiple heterogeneous assets present in environment.

B. There are multiple assets having same configuration details present in environment.

C. QRadar creates duplicate assets after a specific periodic interval without considering asset activity or inactivity.

D. Asset doesn\\'t appear in network for specific time period; when it came back QRadar detects it and created a new asset for the same.

Correct Answer: C

QUESTION 5

What is used to collect netflow and jflow traffic in a QRadar Distributed Deployment?

A. QRadar 3105 Console

B. QRadar 1705 Processor

C. QRadar 1605 Processor

D. QRadar 700 Risk Manager

Correct Answer: A