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.passapply.com/c2150-400.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The following message is displayed in the System Notification Widget on the Dashboard:

Jan 15 14:34:32 172.16.77.109 [ecs] [[type=com.eventgnosis.system.ThreadedEventProcessor] [parent=crssiem.crosig.group:ecs0/EP/Processor2]] com.q1labs.semsources.cre.CRE: [WARN] [NOT:0080004101][172.16.77.109/- -] [-/- -]Custom Rule Engine has sent a total of 9125354 event(s) directly to storage. 22350 event(s) were sent in the last 60 seconds. Queue is at 99 percent capacity.

Which script should be run to help determine the cause of the dropped events?

A. /opt/qradar/support/dumpGvData.sh

B. /opt/qradar/support/dumpDSMInfo.sh

C. /opt/qradar/support/cleanAssetModel.sh

D. /opt/qradar/support/findExpensiveCustomRules.sh

Correct Answer: D

QUESTION 2

A QRadar SIEM administrator wants to create a Flow Rule that includes a building block definition (BB) that includes applications that indicate communication with file sharing sites. In which group will the administrator find this specified building block?

A. Policy

B. Host Definitions

C. Network Definition

D. Category Definitions

Correct Answer: B

QUESTION 3

Which two options need to be set when adding host inside deployment editor? (Choose two.)

A. Netmask

B. IP Address

C. Root password

D. QRadar version

E. Gateway IP Address

Correct Answer: BE

QUESTION 4

How do you view an offense that is associated with an event from the Log Activity tab?

A. Double click the event

B. Click the Offense icon next to the event

C. Right click the event, select View Offenses

D. Select the event, and select Offenses from the View list box

Correct Answer: B

QUESTION 5

What are the two expected Host Statuses after HA setup if the initial synchronization is complete? (Choose two.)

A. Primary: Active

B. Primary: Offline

C. Secondary: Failed

D. Secondary: Active

E. Secondary: Standby

F. Primary: Synchronizing

Correct Answer: AE

QUESTION 6

Which two proxy options are required to be set when using a Proxy Server for Auto Updates in QRadar? (Choose two.)

A. Proxy Type

B. Proxy Name

C. Proxy Schedule

D. Proxy Server URL

E. Proxy Port number

Correct Answer: BD

QUESTION 7

Which two authentication methods for the QRadar User Interface are valid? (Choose two.)

A. SecureID

B. Client Certificates

C. System Authentication

D. Extensible Authentication Protocol (EAP)

E. Lightweight Directory Access Protocol (LDAP)

Correct Answer: CE

QUESTION 8

What does the message in the System Notification Widget on the Dashboard "Disk Sentry: Disk Usage exceeded max threshold" tell you?

A. One of your Files Systems has exceeded 92%.

B. One of your Files Systems has exceeded 95%.

C. One of your Files Systems has exceeded 98%

D. One of your Files Systems has exceeded 90%.

Correct Answer: B

QUESTION 9

What are the two support formats for exporting an Assets list from QRadar console? (Choose two.)

A. XML

B. RTF

C. PDF

D. CSV

E. HTML

Correct Answer: AE

QUESTION 10

A QRadar administrator is sizing a distributed deployment. The deployment has approximately 1.5 gigabytes of sustained throughput of traffic on a network tap. The network tap is a copper connection. Which Qflow collector should

be chosen?

A. Qflow Collector 1310

B. Qflow Collector 1202

C. Qflow Collector 1201

D. Qflow Collector 1301

Correct Answer: B

QUESTION 11

What functionalities of QRadar provide the ability to collect, understand, and properly categorize events from external sources?

A. Log sources

B. Flow sources

C. Syslog sources

D. External sources

Correct Answer: A

QUESTION 12

Which statement is true with regard to planning QRadar SIEM high availability?

A. The secondary host can be in different subnet as the primary host.

B. The secondary HA host that you want to add to the HA cluster can be a component in another HA cluster.

C. The primary HA host that you want to add to the HA cluster must be a component in another HA cluster.

D. When the IP address of the primary host is reassigned as a cluster virtual IP, the new IP address that you assign to the primary must be in the same subnet.

Correct Answer: D

QUESTION 13

Which statement is correct for patching an HAed server?

A. If the Secondary host is in an Active state, the patch should be applied to the Secondary.

B. The patch should be applied to the Primary first and the patch should be applied to the Secondary.

C. Remove Secondary, then apply the patch on Primary, and then add the Secondary again.

D. Run the patch on the Primary and the Secondary will be updated Automatically.

Correct Answer: B

QUESTION 14

What is the benefits of enabling indexes on event properties?

A. Decreased disk usage

B. Improved report accuracy

C. Improved search performance

D. Improved performance for regular expression patterns

Correct Answer: C

QUESTION 15

Which attribute is valid when defining the user roles to provide the necessary access?

A. Reports: Maintain Templates

B. Network Activity: View Custom Rules

C. Network Activity: Manage Times Series

D. Log Activity: User Defined Event Properties

Correct Answer: C