## IBM

# C2150-400

*IBM Security Qradar SIEM Implementation v 7.2.1*

**QUESTION:** 166
Which character is used for naming subgroups when using the option Add Group in the Network Hierarchy editor?

A. +(plus)
B. . (period)
C. \ (Backslash)
D. /(Forward Slash)

**Answer:** B

**QUESTION:** 167
What will be restored when restoring event data or flow data for a particular period to a MH?

A. Only data sent to the console for that time period is restored to the MH.
B. Only event data or flow data for the MH being restored will be restored to that MH.
C. Only data that was accumulated for reports and searches will be restored to the MH.
D. All data for all MHs for a specific time period is restored to its respective hosts in the deployment.

**Answer:** B

**QUESTION:** 168
A customer has log files from Windows-based systems and wants to push those logs to the QRadar console. What options should the customer use in WinCollect to collect and forward these logs?

A. File Forwarder
B. Flow Forwarder
C. Event Forwarder
D. Windows-based Event Log Forwarder

**Answer:** C

**QUESTION:** 169
Which default flow source is included in the QRadar SIEM?

A. IPFIX
B. jFlow
C. QFlow
D. NetFlow

**Answer:** D

**QUESTION:** 170
What does Server discovery allow the QRadar administrator to do?

A. Discover
B. Define rules for hosts
C. Create host searches
D. Populate host definition building blocks

**Answer:** A

**QUESTION:** 171
Where is an email address from which you want to receive email alerts on QRadar SIEM located?

A. Admin > System settings > Alert Email From Address
B. Admin > Console settings > Alert Email From Address
C. Admin > System settings > Administrative Email Address
D. Admin > Console settings > Administrative Email Address

**Answer:** A

**QUESTION:** 172
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

**Answer:** B

**QUESTION:** 173
What indicates if an offense is flagged for follow-up?

A. A flag in the Flag column
B. Follow-up System Notification
C. Follow-up email notification from that offense
D. A flag in Offense Note indicating follow-up required

**Answer:** D

**QUESTION:** 174
Which view option allows you to view events as they occur?

A. Automatic
B. Live Events
C. Real Time (streaming)
D. Last Interval (auto refresh)

**Answer:** C

**QUESTION:** 175
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)

**Answer:** C, E