Exam Number/Code: C2150-196

Exam Name: IBM Security QRadar SIEM V7.1 Implementation

Version: Demo

QUESTION:1

What is the result of modifying a saved search?

A. The original search criteria is not changed.
B. The user will be prompted to save the new search criteria as a new saved search.
C. The original search criteria is automatically saved and updated with the new criteria.
D. The user will be prompted to update the search criteria to that of the modified criteria.

Answer: A

QUESTION:2

To overwrite an IBM Security QRadar SIEM V7.1 system, what must be typed in when prompted during the re-imaging process?

A. OK
B. FLATTEN
C. REFRESH
D. REINSTALL

Answer: B

QUESTION:3

Where does IBM SecurityQRadar SIEM V7.1 get the severity of an event?

A. from the QIDmap
B. from the event payload
C. from the Tomcat server
D. from the user's definition

Answer: A

QUESTION:4

IBM Security QRadar SIEM V7.1 can be forced to run an instant backup by selecting which option?

A. Backup Now
B. On Demand Backup
C. Launch On Demand Backup
D. Configure On Demand Backup

Answer: B

QUESTION:5

An IBM Security QRadar SIEM V7.1 (QRadar) ALE agent should be installed on which system to collect Windows logs?

A. the QRadar Console
B. a QRadar Event Processor
C. any Windows 2000 or newer server
D. any Linux server with SMB installed

Answer: C

QUESTION:6

Which statement best describes the supported external storage options in IBM Security QRadar SIEM V7.1(QRadar)?

A. While QRadar supports NES for external storage, NES is recommended for backups, not for storing active data
B. QRadar data is located in the /store file system. An off board storage solution can be used to migrate the entire /store file system to an external system for faster performance.
C. The /store/ariel directory is the most commonly off boarded file system. Subsequently, collected event logs and flow records data can be relocated to external storage using protocols such as SMB.
D. Any subdirectory in the /store file system can be used as a mount point for external storage device. By creating multiple volumes and mounting /store/ariel/logs and /store/ariel/qflow, storage capabilities can be extended past the 64TB file system limit currently supported by QRadar

Answer: A

QUESTION:7

By default how often are events forwarded from an event collector to an event processor?

A. every hour
B. continuously
C. every 2 hours
D. it does not forward until the forwarding schedule is set

Answer: B

QUESTION:8

What is required to configure users for successful external authentication?

A. A configured External Authentication type
B. Users with no account on the IBM Security QRadar SIEM V7.1 (QRadar) appliance
C. Users with existing accounts onQRadar and a configured External Authentication type
D. Select which users require external authentication and select the correct authentication type

Answer: C

QUESTION:9

What are the main functions of the Report wizard within IBM Security QRadar SIEM V7.1?

A. to enable branding of reports with a customer's logo or local identification information
B. to specify the schedule, layout, report content, output format, and distribution channels
C. to create new report groups which are placed in the existing hierarchy of reporting groups
D. to select from compliance, executive, log source, network management, and security' reports

Answer: B

QUESTION:10

Where is the optimal location for IBM Security QRadar QFlow appliances to monitor Internettraffic?

A. in the datacenter
B. at the workstation switches
C. at the wireless access points
D. at an ingress/egress point in the network

Answer: D