Latest Version: 6.0

Question: 1

What types of logs will FortiAnalyzer store?
Response:

A. Traffic/Event/Security, Data Leak Prevention (DLP) archive, Quarantine, and IPS (Intrusion Protection System) Packets.
B. Traffic/Event, Data Leak Prevention (DLP) archive, Quarantine, and IPS (Intrusion Protection System) Packets.
C. Traffic/Event/Security, Data Leak Prevention (DLP) archive, Quarantine.
D. Data Leak Prevention (DLP) archive, Quarantine, and IPS (Intrusion Protection System) Packets.

Answer: A

Question: 2

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?
Response:

A. Log fetching
B. Indicators of Compromise
C. Log upload
D. Log forwarding an aggregation mode

Answer: A

Question: 3

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec?
(Choose two.)
Response:

A. IPsec is only enabled through the CLI on FortiAnalyzer.
B. Must establish an IPsec tunnel ID and pre-shared key.
C. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.

D. IPsec cannot be enabled if SSL is enabled as well.

Answer: C,D

Question: 4

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?
Response:

A. FortiAnalyzer resets the disk quota of the new ADOM to default.
B. FortiAnalyzer migrates archive logs to the new ADOM.
C. FortiAnalyzer migrates analytics logs to the new ADOM.
D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Question: 5

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)
Response:

A. License type
B. Disk size
C. Total quota
D. RAID level

Answer: B,D

Question: 6

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days. What is the most likely problem?
Response:

A. Quota enforcement is acting on analytical data before a report is complete
B. Logs are rolling before the report is run
C. CPU resources are too high

D. Disk utilization for archive logs is set for 15 days

Answer: A

Question: 7

What FortiGate process caches logs when FortiAnalyzer is not reachable?
Response:

A. miglogd
B. oftpd
C. logfiled
D. sqlplugind

Answer: A