Question 1

What are two advantages of setting up fabric ADOM? (Choose two.)

Options:

A- It can be used for fast data processing and log correlation

B- It can be used to facilitate communication between devices in same Security Fabric

C- It can include all Fortinet devices that are part of the same Security Fabric

D- It can include only FortiGate devices that are part of the same Security Fabric

Answer:

A, C

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

Question 2

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

Options:

A- Log correlation

B- Host name resolution

C- Log collection

D- Real-time forwarding

Answer:

A

Question 3

Consider the CLI command:

```
# configure system global
    set log-checksum md5
  end
```

What is the purpose of the command?

Options:

A- To add a unique tag to each log to prove that it came from this FortiAnalyzer

B- To add the MD5 hash value and authentication code

C- To add a log file checksum

D- To encrypt log communications

Answer:

C

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

Question 4

Which two methods can you use to send event notifications when an event occurs that matches a configured

event handler? (Choose two.)

Options:

A- SMS

B- Email

C- SNMP

D- IM

Answer:

B, C

Explanation:

Question 5

Question Type: MultipleChoice

Which two statements about log forwarding are true? (Choose two.)

Options:

A- Forwarded logs cannot be filtered to match specific criteria.

B- Logs are forwarded in real-time only.

C- The client retains a local copy of the logs after forwarding.

D- You can use aggregation mode only with another FortiAnalyzer.

Answer:

C, D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

Question 6

Question Type: **MultipleChoice**

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

Options:

A- Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.

B- Must establish an IPsec tunnel ID and pre-shared key.

C- IPsec cannot be enabled if SSL is enabled as well.

D- IPsec is only enabled through the CLI on FortiAnalyzer.

Answer:

B, D

Explanation:

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.

Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

Question 7

Question Type: **MultipleChoice**

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

Options:

A- All FortiGates can send logs to FortiAnalyzer using the store and upload option.

B- Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.

C- Both secure communications methods (SSL and IPsec) allow the store and upload option.

D- Disk logging is enabled on the FortiGate through the CLI only.

E- Disk logging is enabled by default on the FortiGate.

Answer:

B, C, D

Question 8

Question Type: MultipleChoice

What are two of the key features of FortiAnalyzer? (Choose two.)

Options:

A- Centralized log repository

B- Cloud-based management

C- Reports

D- Virtual domains (VDOMs)

Answer:

A, C