

# **Fortinet**

**Exam NSE5\_FAZ-5.4**

**FortiAnalyzer 5.4 Specialist**

**Version: 7.0**

**[ Total Questions: 25 ]**

**Question No : 22**

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs and content files are stored and uploaded at a scheduled time
- B. Logs and content files are forwarded as they are received
- C. Logs are forwarded as they are received
- D. Logs are forwarded as they are received and content files are uploaded at a scheduled time

**Answer: A**

**Question No : 23**

How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

- A. Use trusted hosts
- B. Use administrative profiles
- C. Use secure protocols
- D. Use static routes

**Answer: A**

**Question No : 24**

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

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

**Answer: A**

**Question No : 25**

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?

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

**Answer: C**