

Exam : **FCP_FAZ_AN-7.4**

Title : Fortinet FCP - FortiAnalyzer
7.4 Analyst

Version : DEMO

1.Which statement about sending notifications with incident updates is true?

- A. Each connector used can have different notification settings.
- B. You must configure an output profile to send notifications by email.
- C. Each incident can send notifications to a single external platform.
- D. Notifications can be sent only when an incident is created or deleted.

Answer: A

2.What can you do on FortiAnalyzer to restrict administrative access from specific locations?

- A. Configure trusted hosts for that administrator.
- B. Enable geo-location services on accessible interface.
- C. Configure two-factor authentication with a remote RADIUS server.
- D. Configure an ADOM for respective location.

Answer: A

3.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 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

4.Which connector type is enabled by default to be used in playbooks?

- A. Fabric
- B. EMS
- C. Local connector
- D. FortiOS

Answer: C

5.Which FortiAnalyzer featuhich statement regarding macrosoach when managing your network security?

- A. FortiView Monitor
- B. Threat hunting
- C. Incidents dashboards
- D. Outbreak alert services

Answer: B