

# NSE5\_FAZ-6.2<sup>Q&As</sup>

Fortinet NSE 5 - FortiAnalyzer 6.2

## Pass Fortinet NSE5\_FAZ-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.pass2lead.com/nse5\\_faz-6-2.html](https://www.pass2lead.com/nse5_faz-6-2.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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

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

Correct Answer: D

---

**QUESTION 2**

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?

- A. The maximum disk utilization for each device in the ADOM
- B. The maximum disk utilization for the FortiAnalyzer model
- C. The maximum disk utilization for the ADOM type
- D. The maximum disk utilization for all devices in the ADOM

Correct Answer: B

---

**QUESTION 3**

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

- 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.

Correct Answer: BC

Reference: [www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/](http://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/)

**QUESTION 4**

For which two purposes would you use the command set log checksum? (Choose two.)

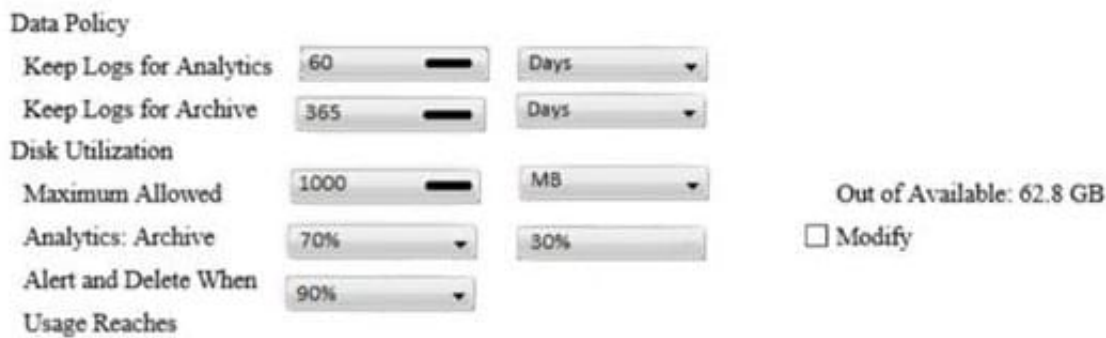
- A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
- B. To prevent log modification or tampering
- C. To encrypt log communications
- D. To send an identical set of logs to a second logging server

Correct Answer: AB

To prevent the log in the store from being modified, you can add a log checksum by using the config system global command. When the log is split, archived, and the log is uploaded (if the feature is enabled), you can configure the FortiAnalyzer to log the log file hash value, timestamp, and authentication code. This can help defend against man-in-the-middle attacks when uploading log transmission data from the FortiAnalyzer to the SFTP server.

**QUESTION 5**

View the exhibit:



What does the 1000MB maximum for disk utilization refer to?

- A. The disk quota for the FortiAnalyzer model
- B. The disk quota for all devices in the ADOM
- C. The disk quota for each device in the ADOM
- D. The disk quota for the ADOM type

Correct Answer: B