

Fortinet

NSE5_FAZ-7.0 Exam

Fortinet NSE 5 - FortiAnalyzer 7.0

Questions & Answers

Demo

Version: 5.0

Question: 1

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

- A. Virtual domains
- B. Administrative access profiles
- C. Trusted hosts
- D. Security Fabric

Answer: BC

Explanation:

Reference: <https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/219292/administrator-profiles>
<https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts>

Question: 2

Which daemon is responsible for enforcing raw log file size?

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

Answer: A

Explanation:

Question: 3

An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Answer: D

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-b-log-integrity-and-secure-log-transfer>

Question: 4

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally?

(Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles>

Question: 5

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

Answer: A, B
