

IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

Exam : **NSE5_FAZ-7.2**

Title : Fortinet NSE 5 -
FortiAnalyzer 7.2

Version : DEMO

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>

2.Which daemon is responsible for enforcing raw log file size?

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

Answer: A

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>

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>

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

Explanation:

To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.

FortiAnalyzer_7.0_Study_Guide-Online page 149