



NSE5_FAZ-7.0^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse5_faz-7-0.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**

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

Correct Answer: A

QUESTION 2

What is the purpose of the following CLI command?

```
# configure system global
    set log-checksum md5
end
```

- A. To add a log file checksum
- B. To add the MD5's hash value and authentication code
- C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- D. To encrypt log communications

Correct Answer: A

<https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global>

QUESTION 3

What are offline logs on FortiAnalyzer?

- A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
- B. When you restart FortiAnalyzer, all stored logs are considered to be offline logs.
- C. Logs that are indexed and stored in the SQL database.
- D. Logs that are collected from offline devices after they boot up.

Correct Answer: A



Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs and are considered offline so they don't offer immediate analytic support.

Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy.

FortiAnalyzer_7.0_Study_Guide-Online page 140

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Archive_analytics_logs.htm

QUESTION 4

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.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/582009/system-administrator-best-practices>

QUESTION 5

An administrator has configured the following settings:

```
config system fortiview settings set resolve-ip enable end
```

What is the significance of executing this command?

- A. Use this command only if the source IP addresses are not resolved on FortiGate.
- B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
- C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
- D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Correct Answer: D

Reference: <https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in-FortiAnalyzer/m-p/95351?m=156950>



VCE & PDF

Pass4itSure.com

https://www.pass4itsure.com/nse5_faz-7-0.html

2024 Latest pass4itsure NSE5_FAZ-7.0 PDF and VCE dumps Download

[Test](#)