



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.geekcert.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

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

- A. Playbooks can be exported and imported only within the same FortiAnalyzer.
- B. You can export only one playbook at a time.
- C. A playbook that was disabled when it was exported, will be disabled when it is imported.
- D. You can import a playbook even if there is another one with the same name in the destination.

Correct Answer: CD

D : If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.

C : Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

QUESTION 2

Which two statements are true regardless initial Logs sync and Log Data Sync for HA on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup device.
- B. Log Data Sync provides real-time log synchronization to all backup devices.
- C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D. When Logs Data Sync is turned on, the backup device will reboot and then rebuild the log database with the synchronized logs.

Correct Answer: CD

QUESTION 3

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

- A. Output profiles
- B. Report settings
- C. Report scheduling
- D. Custom datasets

Correct Answer: D



QUESTION 4

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy. What is the most likely problem?

- A. CPU resources are too high
- B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
- C. The total disk space is insufficient and you need to add other disk
- D. The ADOM disk quota is set too low, based on log rates

Correct Answer: D

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device%20logs.htm

QUESTION 5

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

- A. By deploying different FortiAnalyzer devices in both modes, you can improve their overall performance.
- B. When in collector mode. FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
- C. When in collector mode. FortiAnalyzer supports event management and reporting features.
- D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting
- E. Collector mode is the default operating mode.

Correct Answer: AB

FortiAnalyzer_7.0_Study_Guide-Online pag. 10

[NSE5 FAZ-7.0 VCE Dumps](#) [NSE5 FAZ-7.0 Study Guide](#) [NSE5 FAZ-7.0 Braindumps](#)