NSE5_FAZ-6.2 Q&As

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.pass4itsure.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 log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs

B. Web filter logs

C. IPS logs

D. Application control logs

Correct Answer: B

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 2

View the exhibit.

Why is the total quota less than the total system storage?

A. 3.6% of the system storage is already being used.

B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

C. The oftpd process has not archived the logs yet

D. The logfiled process is just estimating the total quota

Correct Answer: B

QUESTION 3

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.

B. The log file rolls over and is archived.

C. The log file is purged from the database.

D. The log file is overwritten.

Correct Answer: B

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a400505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf

QUESTION 4

What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone

B. Manager

C. Analyzer

D. Collector

Correct Answer: CD

QUESTION 5

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