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.passapply.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

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

execute sql-local rebuild-adom

A. To reset the disk quota enforcement to default

B. To remove the analytics logs of the device from the old database

C. To migrate the archive logs to the new ADOM

D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/cli-reference/551596/sql-local

QUESTION 2

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. Remote logging must be enabled on FortiGate

B. Log encryption must be enabled

C. ADOMs must be enabled

D. FortiGate must be registered with FortiAnalyzer

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit." https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

QUESTION 3

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. License type

B. Disk size

C. Total quota

D. RAID level

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.5/administration-guide/929977/diskspaceallocation

QUESTION 4

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 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

Correct Answer: AB

To prevent the log in the store from being modified, you can add a log checksum by using the config system global command. When the log is split, archived, and the log is uploaded (if the feature is enabled), you can configure the FortiAnalyzer to log the log file hash value, timestamp, and authentication code. This can help defend against man-in-the-middle attacks when uploading log transmission data from the FortiAnalyzer to the SFTP server.