NSE5_FAZ-7.0$^{\text{Q\&As}}$

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

QUESTION 1

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

A. The total disk space is insufficient and you need to add other disk.

B. CPU resources are too high.

C. The ADOM disk quota is set too low based on log rates.

D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Correct Answer: C

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration- guide/87802/automatic-deletion

QUESTION 2

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation

B. Host name resolution

C. Log collection

D. Real-time forwarding

Correct Answer: A

page 27: synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation.

QUESTION 3

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed. What is the recommended method to replace the disk?

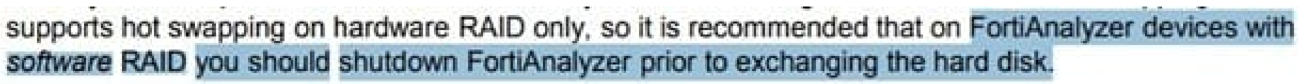
A. Shut down FortiAnalyzer and then replace the disk

B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level

C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running

D. Perform a hot swap

Correct Answer: A



supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with *software* RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on- FortiAnalyzer/ta-p/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20know n%20as%20hot%20swapping

QUESTION 4

Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid WHERE \\'user\\'=\\'USER1\\' FROM $log GROUP BY devid

B. FROM $log WHERE \\'user\\'=\\'USER1\\' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE \\'user\\'=\\'USER1\\' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE \\'user\\'=\\'USER1\\'

Correct Answer: C

QUESTION 5

What is the purpose of a dataset query in FortiAnalyzer?

A. It sorts log data into tables

B. It extracts the database schema

C. It retrieves log data from the database

D. It injects log data into the database

Correct Answer: C

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration- guide/148744/creating-datasets