

# IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

**Exam** : **NSE5\_FAZ-6.0**

**Title** : Fortinet NSE 5 -  
FortiAnalyzer 6.0

**Version** : DEMO

1.View the exhibit:

Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1000 MB

Analytics: Archive: 70%

Alert and Delete When Usage Reaches: 90%

Out of Available: 62.8 GB

Modify

What does the 1000MB maximum for disk utilization refer to?

- A. The disk quota for the FortiAnalyzer model
- B. The disk quota for all devices in the ADOM
- C. The disk quota for each device in the ADOM
- D. The disk quota for the ADOM type

**Answer: B**

2.You've moved a registered logging device out of one ADOM and into a new ADOM.

What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

**Answer: C**

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.

**Answer: B**

4.What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

**Answer: A**

5.Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

- A. Log upload
- B. Indicators of Compromise
- C. Log forwarding an aggregation mode

D. Log fetching

**Answer: D**