Fortinet

NSE5_FAZ-6.2 Exam

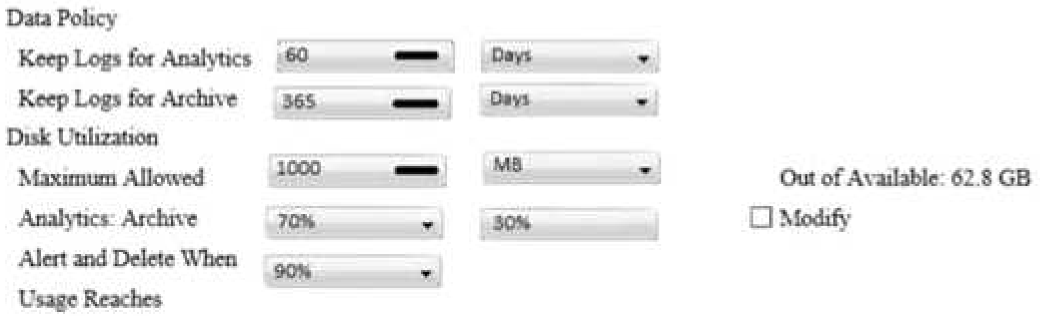
Fortinet NSE 5 - FortiAnalyzer 6.2 Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

View the exhibit:



Data Policy

Keep Logs for Analytics 60 Days

Keep Logs for Archive 365 Days

Disk Utilization

Maximum Allowed 1000 MB Out of Available: 62.8 GB

Analytics: Archive 70% 30% □ Modify

Alert and Delete When Usage Reaches 90%

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

Question: 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

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.

Answer: B

Question: 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

Question: 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

Question: 6

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
B. From the VM host manager, expand the size of the existing virtual disk
C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Answer: A