

Vendor: Fortinet

Exam Code: NSE5_FAZ-6.4

Exam Name: Fortinet NSE 5 - FortiAnalyzer 6.4

Version: DEMO

QUESTION 1

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

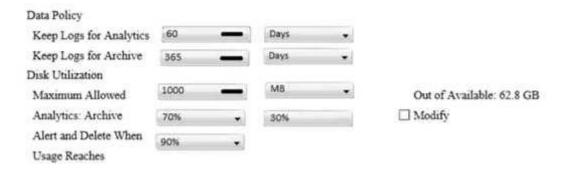
- A. License type
- B. Disk size
- C. Total quota
- D. RAID level

Answer: CD Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

QUESTION 2

View the exhibit:



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 Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

QUESTION 3

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 Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

QUESTION 4

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 Explanation:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

QUESTION 5

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 Explanation:

https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.

QUESTION 6

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 Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

QUESTION 7

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 Explanation:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

QUESTION 8

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
- B. Logs and content files are stored and uploaded at a scheduled time.
- C. Logs are forwarded as they are received.
- D. Logs and content files are forwarded as they are received.

Answer: B Explanation:

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes

QUESTION 9

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom

QUESTION 10

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

Answer: AD

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than 99,900 Satisfied Customers Worldwide.
- ★ Average 99.9% Success Rate.
- ★ Free Update to match latest and real exam scenarios.
- ★ Instant Download Access! No Setup required.
- ★ Questions & Answers are downloadable in PDF format and VCE test engine format.



- ★ Multi-Platform capabilities Windows, Laptop, Mac, Android, iPhone, iPod, iPad.
- ★ 100% Guaranteed Success or 100% Money Back Guarantee.
- ★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

























10% Discount Coupon Code: ASTR14