

NSE5_FAZ-6.4 Dumps

Fortinet NSE 5 - FortiAnalyzer 6.4

https://www.certleader.com/NSE5_FAZ-6.4-dumps.html



NEW QUESTION 1

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used. What does the disk quota refer to?

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

Answer: D

NEW QUESTION 2

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

NEW QUESTION 3

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

NEW QUESTION 4

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

Answer: BC

NEW QUESTION 5

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>

NEW QUESTION 6

Which two purposes does the auto cache setting on reports serve? (Choose two.)

- A. It automatically updates the hcache when new logs arrive.
- B. It provides diagnostics on report generation time.
- C. It reduces the log insert lag rate.
- D. It reduces report generation time.

Answer: AD

NEW QUESTION 7

Logs are being deleted from one of your ADOMs earlier than 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.

Answer: C

Explanation:

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>

NEW QUESTION 8

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

Answer: BCE

NEW QUESTION 9

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To properly correlate logs
- B. To use real-time forwarding
- C. To resolve host names
- D. To improve DNS response times

Answer: A

Explanation:**NEW QUESTION 10**

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>

NEW QUESTION 10

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.

What can you do on FortiAnalyzer to accomplish this?

- A. Click FortiView and generate a report for that administrator.
- B. Click Task Monitor and view the tasks performed by that administrator.
- C. Click Log View and generate a report for that administrator.
- D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

NEW QUESTION 14

Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

- A. SMS

- B. Email
- C. SNMP
- D. IM

Answer: BC

NEW QUESTION 16

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder>

NEW QUESTION 18

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

NEW QUESTION 21

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NEW QUESTION 25

Which two statements are true regarding ADOM modes? (Choose two.)

- A. You can only change ADOM modes through CLI.
- B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
- C. In an advanced mode ADO
- D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- E. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 27

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

Answer: A

Explanation:

<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta->

NEW QUESTION 32

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

- A. CPU resources are too high
- B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
- C. The total disk space is insufficient and you need to add other disk
- D. The ADOM disk quota is set too low, based on log rates

Answer: D

NEW QUESTION 35

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

NEW QUESTION 40

What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate
- D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 42

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

Answer: BD

NEW QUESTION 43

On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

- A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
- B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
- C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
- D. FortiAnalyzer is functioning normally

Answer: C

NEW QUESTION 47

By default, what happens when a log file reaches its maximum file size?

- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

Answer: C

NEW QUESTION 52

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

Answer: D

NEW QUESTION 55

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE5_FAZ-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FAZ-6.4-dumps.html