



# NSE5\_FAZ-6.4<sup>Q&As</sup>

Fortinet NSE 5 - FortiAnalyzer 6.4

## Pass Fortinet NSE5\_FAZ-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.passapply.com/nse5\\_faz-6-4.html](https://www.passapply.com/nse5_faz-6-4.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDMs)

Correct Answer: AC

---

### 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.

Correct Answer: B

Reference: <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a400505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf> <https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse>

---

### QUESTION 3

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

- A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
- B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
- C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
- D. Make sure all endpoints are reachable by FortiAnalyzer.

Correct Answer: BC

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewingcompromised-hosts>

---



#### QUESTION 4

What statements are true regarding disk log quota? (Choose two)

- A. The FortiAnalyzer stops logging once the disk log quota is met.
- B. The FortiAnalyzer automatically sets the disk log quota based on the device.
- C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
- D. The FortiAnalyzer disk log quota is configurable, but has a minimum of 100mb and a maximum based on the reserved system space.

Correct Answer: CD

---

#### QUESTION 5

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

Correct Answer: BCE

---

#### QUESTION 6

What are two advantages of setting up fabric ADOM? (Choose two.)

- A. It can be used for fast data processing and log correlation
- B. It can be used to facilitate communication between devices in same Security Fabric
- C. It can include all Fortinet devices that are part of the same Security Fabric
- D. It can include only FortiGate devices that are part of the same Security Fabric

Correct Answer: AC

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-securityfabric-adom>

---

#### QUESTION 7

An administrator has configured the following settings:



config system global set log-checksum md5-auth end

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Correct Answer: D

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-blog-integrity-and-secure-log-transfer>

### QUESTION 8

View the exhibit.

```
Total Quota Summary:
  Total Quota   Allocated   Available   Allocate%
    63.7GB      12.7GB      51.0GB      19.9%

System Storage Summary:
  Total      Used      Available      Use%
  78.7GB    2.9GB    75.9GB    3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?

- A. 3.6% of the system storage is already being used.
- B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
- C. The oftpd process has not archived the logs yet
- D. The logfiled process is just estimating the total quota

Correct Answer: B

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

### QUESTION 9



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

Correct Answer: A

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

### QUESTION 10

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

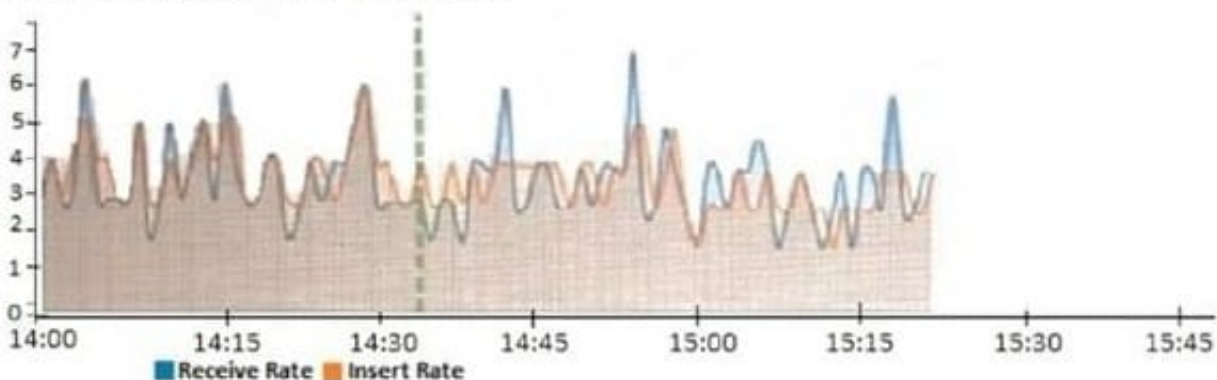
Correct Answer: AB

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567>

### QUESTION 11

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



What does the data point at 14:35 tell you?



- A. FortiAnalyzer is dropping logs.
- B. FortiAnalyzer is indexing logs faster than logs are being received.
- C. FortiAnalyzer has temporarily stopped receiving logs so older logs can be indexed.
- D. The sqlplugind daemon is ahead in indexing by one log.

Correct Answer: B

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receiverate-widget>

---

#### QUESTION 12

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

- A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
- B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
- C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
- D. Disk logging is enabled on the FortiGate through the CLI only.
- E. Disk logging is enabled by default on the FortiGate.

Correct Answer: BCD

---

#### QUESTION 13

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

Correct Answer: D

Reference: [https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100\\_Storage/0017\\_Deleted%20device%20logs.htm](https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device%20logs.htm)

---

#### QUESTION 14

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

Correct Answer: C

Reference: <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4cb0dce6-dbef-11e9-897700505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf> (40)

---

#### QUESTION 15

Which two statements are true regardless of initial Logs sync and Log Data Sync for HA on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup devices.
- B. Log Data Sync provides real-time log synchronization to all backup devices.
- C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D. When Log Data Sync is turned on, the backup device will reboot and then rebuild the log database with the synchronized logs.

Correct Answer: CD

[Latest NSE5\\_FAZ-6.4 Dumps](#)

[NSE5\\_FAZ-6.4 Study Guide](#) [NSE5\\_FAZ-6.4 Brindumps](#)