



# NSE5\_FAZ-6.2<sup>Q&As</sup>

Fortinet NSE 5 - FortiAnalyzer 6.2

## Pass Fortinet NSE5\_FAZ-6.2 Exam with 100% Guarantee

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

[https://www.pass4itsure.com/nse5\\_faz-6-2.html](https://www.pass4itsure.com/nse5_faz-6-2.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

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.

Correct Answer: B

---

### QUESTION 2

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL?  
(Choose two.)

- A. SSL is the default setting.
- B. SSL communications are auto-negotiated between the two devices.
- C. SSL can send logs in real-time only.
- D. SSL encryption levels are globally set on FortiAnalyzer.
- E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Correct Answer: AD

---

### 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.

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>

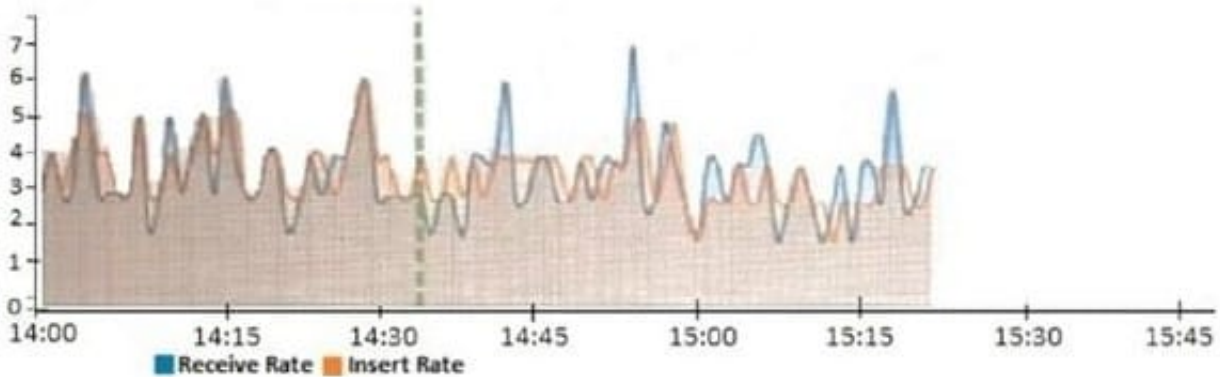
---

### QUESTION 4



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: D

Logs are received then they are indexed, no logging server in the world can index logs faster than they are received. When FAZ receives raw logs, they are inserted (indexed) by the SQL database and the sqlplugind daemon, this graph shows that FAZ received 3 logs and sqlplugind indexed 4.

## QUESTION 5

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

Correct Answer: D

[Latest NSE5\\_FAZ-6.2 Dumps](#)

[NSE5\\_FAZ-6.2 PDF Dumps](#)

[NSE5\\_FAZ-6.2 Practice Test](#)