NSE5_FAZ-6.4 Q&As

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.geekcert.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

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

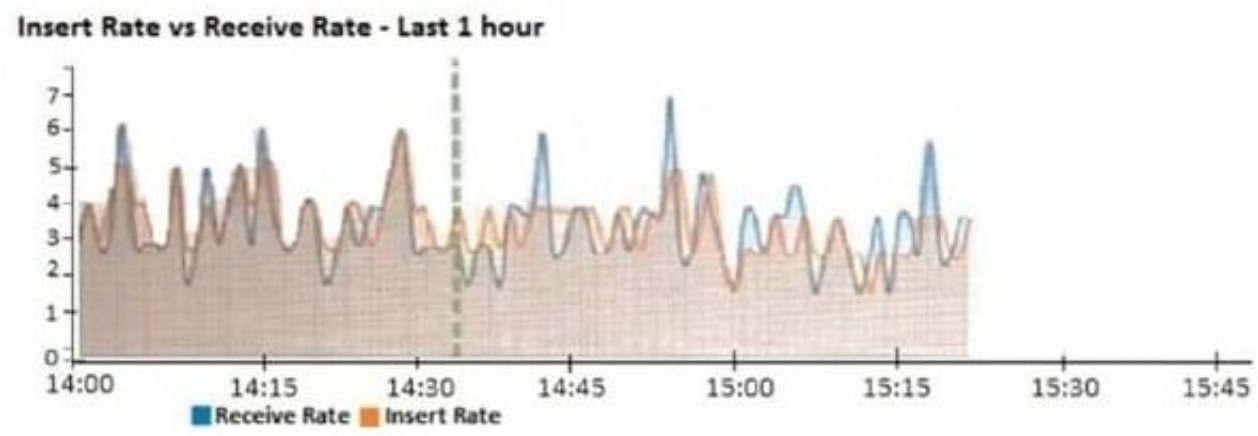
C. To resolve host names

D. To improve DNS response times

Correct Answer: A

QUESTION 2

View the exhibit.



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 3

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

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 https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-difference-between-logforward-and-log-aggregation-modes

QUESTION 4

Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.

B. Fabric connectors allow to save storage costs and improve redundancy.

C. Storage connector service does not require a separate license to send logs to cloud platform.

D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Correct Answer: AD

QUESTION 5

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.

Correct Answer: AD

Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache