NSE5_FAZ-6.2^{Q&As}

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.passapply.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

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 (VDOMs)

Correct Answer: AC

QUESTION 2

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

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."
https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

QUESTION 3

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an LDAP group

B. An account that allows guest access with read-only privileges

C. An account that requires two-factor authentication

D. An account that validates against any user account on a FortiAuthenticator

Correct Answer: D

QUESTION 4

What is the purpose of the following CLI command?

```
# configure system global
      set log-checksum md5
end
```

A. To add a log file checksum

B. To add the MD\\'s hash value and authentication code

C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
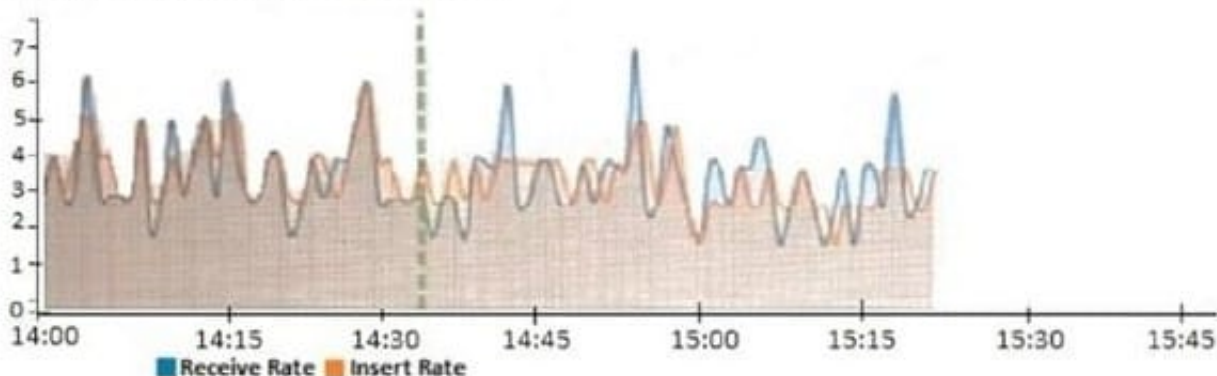
D. To encrypt log communications

Correct Answer: A

QUESTION 5

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.

NSE5_FAZ-6.2 Practice Test   **NSE5_FAZ-6.2 Study Guide**   **NSE5_FAZ-6.2 Braindumps**