examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!
We offer free update service for one year!
http://www.examunion.com

Exam : NSE5_FAZ-6.2

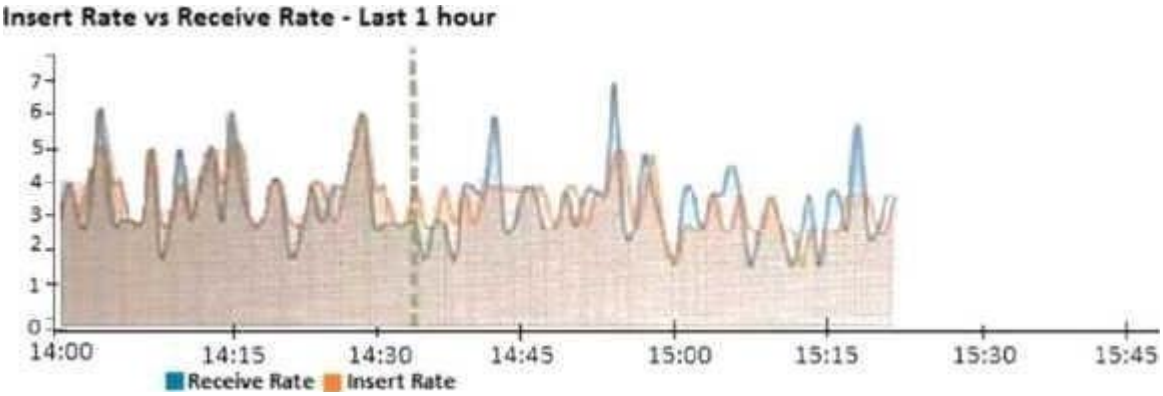
Title : Fortinet NSE 5 - FortiAnalyzer 6.2

Version : DEMO

1.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

2.Which statements are correct regarding FortiAnalyzer reports? (Choose two)
A. FortiAnalyzer provides the ability to create custom reports.
B. FortiAnalyzer glows you to schedule reports to run.
C. FortiAnalyzer includes pre-defined reports only.
D. FortiAnalyzer allows reporting for FortiGate devices only.
Answer: A,B

3.Refer to the exhibit.



What does the data point at 14:55 tell you?
A. The received rate is almost at its maximum for this device
B. The sqlplugind daemon is behind in log indexing by two logs
C. Logs are being dropped
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed
Answer: C

4.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
Answer: D

5.How does FortiAnalyzer retrieve specific log data from the database?
A. SQL FROM statement
B. SQL GET statement
C. SQL SELECT statement
D. SQL EXTRACT statement

Answer: C