NSE5_FAZ-7.0 Q&As

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse5_faz-7-0.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

Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.

B. Macros are supported only on the FortiGate ADOM.

C. Macros are useful in generating excel log files automatically based on the reports settings.

D. Macros are predefined templates for reports and cannot be customized.

Correct Answer: A

FortiAnalyzer 7.0 Study Guide online page no: 283 Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration- guide/617380/creating-macros

QUESTION 2

What is the purpose of a predefined template on the FortiAnalyzer?

A. It can be edited and modified as required

B. It specifies the report layout which contains predefined texts, charts, and macros

C. It specifies report settings which contains time period, device selection, and schedule

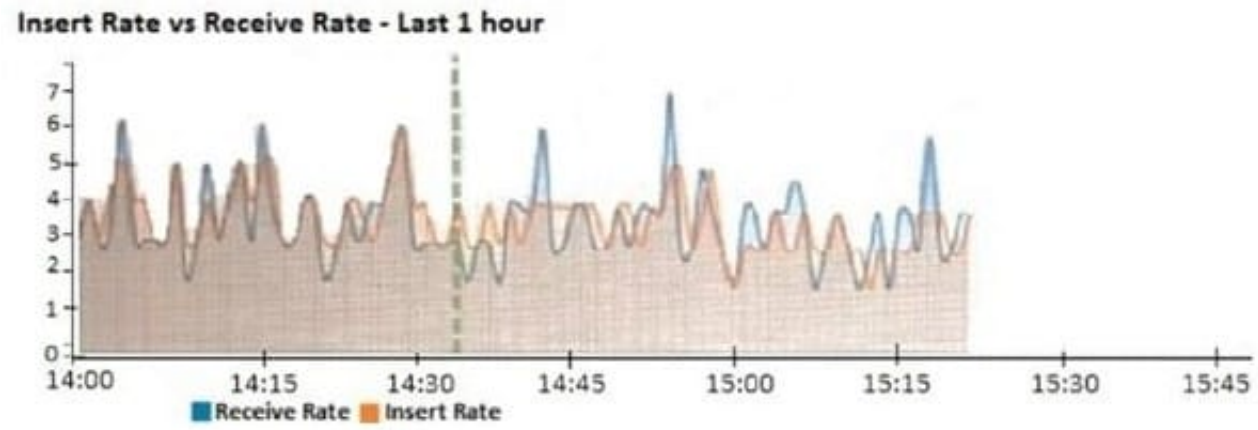
D. It contains predefined data to generate mock reports

Correct Answer: B

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administration- guide/618245/predefined-reports-templates-charts-and-macros

QUESTION 3

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

Raw logs are received and then that log is indexed. So indexing can never be ahead of logs received. But it can be that at a certain point in time logs are being indexed faster than they are received.

If you look at the study guide you will notice that there is something called Insert Lag Time. And in this example it\\'s between 30-50 seconds. The point is the indexing of the logs can\\'t be ahead if it gets processed a few seconds later.

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

QUESTION 4

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.

B. When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

C. Logs that are indexed and stored in the SQL database.

D. Logs that are collected from offline devices after they boot up.

Correct Answer: A

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs

and are considered offline so they don\\'t offer immediate analytic support.

Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data

policy.

FortiAnalyzer_7.0_Study_Guide-Online page 140

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Arch ive_analytics_logs.htm

QUESTION 5

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView

B. Event Management

C. Device Manger

D. Reporting

Correct Answer: AD