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.leads4pass.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

FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server

B. To prevent log modification during backup

C. To send an identical set of logs to a second logging server

D. To encrypt log communication between devices

Correct Answer: D

QUESTION 2

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

B. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

C. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Correct Answer: CD

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.
FortiAnalyzer_7.0_Study_Guide-Online pag. 168

QUESTION 3

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 4

Which daemon is responsible for enforcing raw log file size?

A. logfiled

B. oftpd

C. sqlplugind

D. miglogd

Correct Answer: A

QUESTION 5

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation

B. Host name resolution

C. Log collection

D. Real-time forwarding

Correct Answer: A

page 27: synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation.

NSE5_FAZ-7.0 VCE Dumps NSE5_FAZ-7.0 Practice Test NSE5_FAZ-7.0 Exam Questions