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 FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload

B. Indicators of Compromise

C. Log forwarding an aggregation mode

D. Log fetching

Correct Answer: D

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration- guide/651442/fetcher-management

QUESTION 2

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

A. Output profiles

B. Report settings

C. Report scheduling

D. Custom datasets

Correct Answer: D

QUESTION 3

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.

B. Log Data Sync provides real-time log synchronization to all backup devices.

C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.

D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Correct Answer: CD

QUESTION 4

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.

B. SSL communications are auto-negotiated between the two devices.

C. SSL can send logs in real-time only.

D. SSL encryption levels are globally set on FortiAnalyzer.

E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Correct Answer: AD

QUESTION 5

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

A. Both modes, forwarding and aggregation, support encryption of logs between devices.

B. In aggregation mode, you can forward logs to syslog and CEF servers as well.

C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Correct Answer: AC

Aggregation mode is only supported between two FortiAnalyer devices, so B is wrong.

Forwarding is always in real time and does not ONLY forward to other FortiAnalyzer devices. It also forwards to Syslog/CEF. D is wrong. Answer is A and C.

Latest NSE5_FAZ-7.0
Dumps   NSE5_FAZ-7.0 PDF Dumps   NSE5_FAZ-7.0 Exam
                                                                                                                    Questions