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

QUESTION 1

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-and-log-aggregation-modes

---

QUESTION 2

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information

B. Logs from registered devices

C. Report information

D. Database snapshot

Correct Answer: AC

What does the System Configuration backup include?

System information, such as the device IP address and administrative user information.

Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer_7.0_Study_Guide-Online pag. 29

QUESTION 3

An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.

B. Archived logs will be moved to ADOM1 from the root ADOM automatically.

C. Logs will be presented in both ADOMs immediately after the move.

D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Correct Answer: BD

Reference: https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between- ADOMs/m-p/32683?m=158008

QUESTION 4

Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid WHERE \\'user\\'=\\'USER1\\' FROM $log GROUP BY devid

B. FROM $log WHERE \\'user\\'=\\'USER1\\' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE \\'user\\'=\\'USER1\\' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE \\'user\\'=\\'USER1\\'

Correct Answer: C

QUESTION 5

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards

B. Threat hunting

C. FortiView Monitor

D. Outbreak alert services

Correct Answer: B

FortiAnalyzer_7.0_Study_Guide-Online pag. 217

Latest NSE5_FAZ-7.0 Dumps NSE5_FAZ-7.0 PDF Dumps NSE5_FAZ-7.0 VCE Dumps