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.geekcert.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

What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer

B. What logs, if any, are reaching FortiAnalyzer

C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

Correct Answer: A

Device and ADOM Status Check

diagnose test application oftpd 3 # Devices and IPs are connecting to FortiAnalyzer diagnose test application oftpd 8 # Receiving logs in FortiAnalyzre diagnose dvm adom list # ADOMs are enabled and configured diagnose dvm device list # Devices or VDOMs are currently registed and unregistered

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli- reference/395556/test#test_application

---

QUESTION 2

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

A. Forwarded logs cannot be filtered to match specific criteria.

B. Logs are forwarded in real-time only.

C. The client retains a local copy of the logs after forwarding.

D. You can use aggregation mode only with another FortiAnalyzer.

Correct Answer: CD

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log- forwarding

---

QUESTION 3

What are analytics logs on FortiAnalyzer?

A. Log type Traffic logs.

B. Logs that roll over when the log file reaches a specific size.

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

D. Raw logs that are compressed and saved to a log file.

Correct Answer: C

QUESTION 4

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs

B. Web filter logs

C. IPS logs

D. Application control logs

Correct Answer: B

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_ hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 5

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM

B. LIMIT

C. WHERE

D. ORDER BY

Correct Answer: A

Select FROM... in any kind of database you must specify where you will get the data you are consulting, that\\'s the FROM functionality... WHERE is just an aditional condition Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500