



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 is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

Correct Answer: A

QUESTION 2

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.
- B. Management extensions may require a minimum number of CPU cores to run.
- C. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.
- D. Management extensions require a dedicated VM for best performance.

Correct Answer: B

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

QUESTION 3

A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer. What can you do on FortiAnalyzer to accomplish this?

- A. Click FortiView and generate a report for that administrator.
- B. Click Task Monitor and view the tasks performed by that administrator.



- C. Click Log View and generate a report for that administrator.
- D. View the tasks performed by the rogue administrator in Fabric View.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortimanager/6.4.1/administration-guide/792943/task-monitor>

QUESTION 4

What is the purpose of a dataset query in FortiAnalyzer?

- A. It sorts log data into tables
- B. It extracts the database schema
- C. It retrieves log data from the database
- D. It injects log data into the database

Correct Answer: C

Reference: <https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets>

QUESTION 5

Which daemon is responsible for enforcing the log file size?

- A. sqlplugind
- B. logfiled
- C. miglogd
- D. ofrpd

Correct Answer: B

Disk quota enforcement is performed by different processes:

The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

FortiAnalyzer_7.0_Study_Guide-Online pag. 121

[NSE5_FAZ-7.0 PDF Dumps](#)

[NSE5_FAZ-7.0 Practice
Test](#)

[NSE5_FAZ-7.0 Study Guide](#)