



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.passapply.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

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

- A. FortiAnalyzer is in an HA cluster.
- B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
- C. ADOMs are not enabled on FortiAnalyzer.
- D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Correct Answer: C

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 2

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 additional condition Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500>

QUESTION 3

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

Correct Answer: A

[https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20\(%22Redundant%20Array%20of%20In](https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20In)



expensive,%2C%20performance%20improvement%2C%20or%20both.

QUESTION 4

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

- A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
- B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
- C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
- D. Disk logging is enabled on the FortiGate through the CLI only.
- E. Disk logging is enabled by default on the FortiGate.

Correct Answer: BCD

QUESTION 5

Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

- A. SMS
- B. Email
- C. SNMP
- D. IM

Correct Answer: BC

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

QUESTION 6

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server



Correct Answer: D

QUESTION 7

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

QUESTION 8

An administrator has configured the following settings:

```
config system global set log-checksum md5-auth end
```

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.4.6/administration-guide/410387/appendix-b-log-integrity-and-secure-log-transfer>

QUESTION 9

What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

- A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
- B. Make sure all endpoints are reachable by FortiAnalyzer.
- C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.
- D. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.



Correct Answer: AD

Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard. Ref : <https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts>

QUESTION 10

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 11

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 FortiAnalyzer 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.

QUESTION 12

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To properly correlate logs
- B. To use real-time forwarding
- C. To resolve host names
- D. To improve DNS response times

Correct Answer: A

Study Guide 7.0 page 30: Synchronize the time on FortiAnalyzer and all Registered devices with an NTP server for correct log correlation.

QUESTION 13

What can you do on FortiAnalyzer to restrict administrative access from specific locations?

- A. Configure trusted hosts for that administrator.
- B. Enable geo-location services on accessible interface.
- C. Configure two-factor authentication with a remote RADIUS server.
- D. Configure an ADOM for respective location.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/582009/system-administrator-best-practices>

QUESTION 14

Which two statements express the advantages of grouping similar reports? (Choose two.)

- A. Improve report completion time.
- B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
- C. Reduce the number of hcache tables and improve auto-hcache completion time.
- D. Provides a better summary of reports.



Correct Answer: AC

QUESTION 15

What are the operating modes of FortiAnalyzer? (Choose two)

- A. Standalone
- B. Manager
- C. Analyzer
- D. Collector

Correct Answer: CD

[Latest NSE5_FAZ-7.0 Dumps](#)

[NSE5_FAZ-7.0 VCE Dumps](#) [NSE5_FAZ-7.0 Study Guide](#)