

# DUMPS ARENA

## Fortinet NSE 5 - FortiAnalyzer 6.2

Fortinet NSE5 FAZ-6.2

Version Demo

Total Demo Questions: 10

Total Premium Questions: 58

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)  
[dumpsarena.co](https://dumpsarena.co)

**QUESTION NO: 1**

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

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

**ANSWER: C****QUESTION NO: 2**

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

**ANSWER: D****QUESTION NO: 3**

FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.

What is the most likely problem?

- A. Quota enforcement is acting on analytical data before a report is complete
- B. Logs are rolling before the report is run
- C. CPU resources are too high
- D. Disk utilization for archive logs is set for 15 days

**ANSWER: A**

**QUESTION NO: 4**

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

**ANSWER: B C E**

**QUESTION NO: 5**

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

- A. RADIUS
- B. Local
- C. LDAP
- D. PKI
- E. TACACS+

**ANSWER: A C E**

**QUESTION NO: 6**

You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?

- A. The maximum disk utilization for each device in the ADOM
- B. The maximum disk utilization for the FortiAnalyzer model

- C. The maximum disk utilization for the ADOM type
- D. The maximum disk utilization for all devices in the ADOM

**ANSWER: B**

#### **QUESTION NO: 7**

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

**ANSWER: B D**

#### **QUESTION NO: 8**

Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

- A. FortiView
- B. Event Management
- C. Device Manger
- D. Reporting

**ANSWER: B**

#### **QUESTION NO: 9**

What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate

D. To provide diagnostics on report generation time

**ANSWER: A B**

**QUESTION NO: 10**

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

**ANSWER: B C**