

# DUMPSBOSS.

## Fortinet NSE 5 - FortiAnalyzer 7.0

Fortinet NSE5 FAZ-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 114

Buy Premium PDF

<https://dumpsboss.co>

[support@dumpsboss.co](mailto:support@dumpsboss.co)

support@dumpsboss.co  
dumpsboss.co

## QUESTION NO: 1

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: B**

**Explanation:**

Reference: <https://forum.fortinet.com/tm.aspx?m=138806>

## QUESTION NO: 2

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.

**ANSWER: B D**

**Explanation:**

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

## QUESTION NO: 3

Which statement is true about sending notifications with incident updates?

- A. Notifications can be sent only when an incident is updated or deleted.

- B. If you use multiple fabric connectors, all connectors must have the same notification settings
- C. Notifications can be sent only by email.
- D. You can send notifications to multiple external platforms

**ANSWER: D**

**Explanation:**

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

## QUESTION NO: 4

An administrator has configured the following settings:

```
config system fortiview settings
```

```
set resolve-ip enable
```

```
end
```

What is the significance of executing this command?

- A. Use this command only if the source IP addresses are not resolved on FortiGate.
- B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
- C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
- D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

**ANSWER: D**

**Explanation:**

Reference: <https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in-FortiAnalyzer/m-p/95351?m=156950>

## QUESTION NO: 5

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?

(Choose two.)

- A. SFTP, FTP, or SCP server
- B. Mail server
- C. Output profile

D. Report scheduling

**ANSWER: A C**

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles>

## QUESTION NO: 6

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.

**ANSWER: A C**

## QUESTION NO: 7

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**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enabling-autocache>

## QUESTION NO: 8

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

D)

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
Remote-Fortigate	10.200.3.1	FortiGate-VM64	Real Time	0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**ANSWER: C**

## QUESTION NO: 10

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

**ANSWER: A C**