

➤ **Vendor: Fortinet**

➤ **Exam Code: NSE5_FAZ-7.0**

➤ **Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.0**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [October/2022](#))**

Visit Braindump2go and Download Full Version NSE5_FAZ-7.0 Exam Dumps

QUESTION 41

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

- A. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.
- B. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.
- C. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.
- D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer: AB

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/7.0.1/administration-guide/651442/fetcher-management>

QUESTION 42

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 43

Which two statements are true regarding ADOM modes? (Choose two.)

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

- A. You can only change ADOM modes through CLI.
- B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
- C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- D. Normal mode is the default ADOM mode.

Answer: CD

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/0400_ADOM%20Device%20Modes.htm

QUESTION 44

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

- A. In aggregation mode, you can forward logs to syslog and CEF servers as well.
- B. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
- C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
- D. Both modes, forwarding and aggregation, support encryption of logs between devices.

Answer: CD

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-difference-between-log-forward-and-log-aggregation-modes>

QUESTION 45

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.

What should the administrator do to solve this issue?

- A. Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
- B. Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.
- C. Use the execute sql-report run ADOM1 command to run a report.
- D. Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

Answer: B

Explanation:

Reference: https://help.fortinet.com/fmgr/cli/5-6-1/FortiManager_CLI_Reference/700_execute/sql-local+.htm

QUESTION 46

Which statement is true regarding Macros on FortiAnalyzer?

- A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
- B. Macros are supported only on the FortiGate ADOM.
- C. Macros are useful in generating excel log files automatically based on the reports settings.
- D. Macros are predefined templates for reports and cannot be customized.

Answer: D

Explanation:

Reference: <https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration-guide/617380/creating-macros>

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

QUESTION 47

Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

- A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
- B. Collector mode is the default operating mode.
- C. When in collector mode, FortiAnalyzer supports event management and reporting features.
- D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

Answer: AD

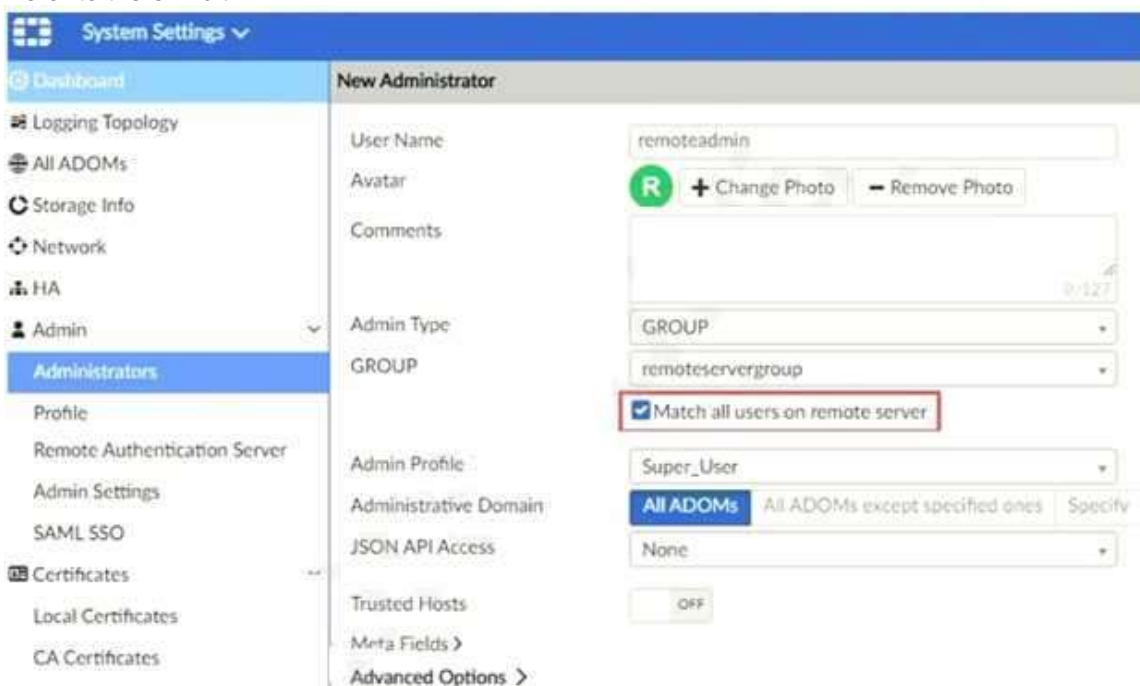
Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/227478/collector-mode>

<https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collector-collaboration>

QUESTION 48

Refer to the exhibit.



The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The left sidebar shows the 'System Settings' menu with 'Administrators' selected. The main form fields are: User Name (remoteadmin), Avatar (R icon), Comments (empty), Admin Type (GROUP), GROUP (remoteservergroup), Match all users on remote server (checked), Admin Profile (Super_User), Administrative Domain (All ADOMs), JSON API Access (None), Trusted Hosts (OFF), Meta Fields (empty), and Advanced Options (expandable). The 'Match all users on remote server' checkbox is highlighted with a red box.

The exhibit shows "remoteservergroup" is an authentication server group with LDAP and RADIUS servers.

Which two statements express the significance of enabling "Match all users on remote server" when configuring a new administrator? (Choose two.)

- A. It creates a wildcard administrator using LDAP and RADIUS servers.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- D. It allows administrators to use two-factor authentication.

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortimanager/7.0.1/administration-guide/858351/creating-administrators>

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

QUESTION 49

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.

Answer: B

Explanation:

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

QUESTION 50

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.

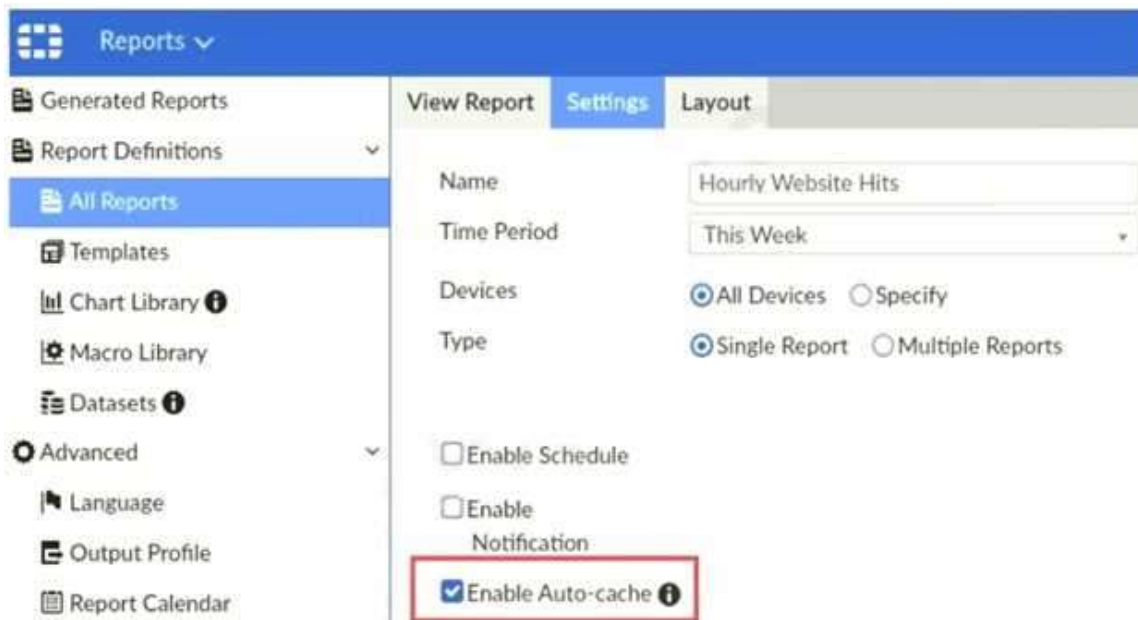
Answer: C

Explanation:

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

QUESTION 51

Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

- A. Report size will be optimized to conserve disk space on FortiAnalyzer.
- B. Reports will be cached in the memory.
- C. This feature is automatically enabled for scheduled reports.
- D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: AD

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0025_Auto-cache.htm

QUESTION 52

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

- A. FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
- B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
- D. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

Answer: BC

QUESTION 53

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: BC

Explanation:

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

QUESTION 54

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. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
- C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
- D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: AC

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts>

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

QUESTION 55

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

Explanation:

Reference: <https://community.fortinet.com/t5/FortiAnalyzer/Creating-a-Custom-report-from-FortiView-Export-to-Report-Chart/ta-p/190154?externalID=FD40483>

QUESTION 56

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.

Answer: A

Explanation:

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

QUESTION 57

What are event handlers?

- A. Threats identified by FortiGuard
- B. Specific matched conditions in the raw logs
- C. Alert notifications
- D. SNMP traps

Answer: B

QUESTION 58

Which two FortiAnalyzer features allow you to automatically build a dataset and chart based on a filtered search result? (Choose two.)

- A. Export to Report Chart (FortiView)
- B. Custom View
- C. Dataset Library
- D. Chart Builder

Answer: AD

QUESTION 59

What is the main purpose of deploying RAID with FortiAnalyzer?

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

- A. To back up your logs
- B. To make an identical copy of log data on two separate physical drives
- C. To provide redundancy of your log data
- D. To store data in chunks across multiple drives

Answer: C

QUESTION 60

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer?
(Choose two.)

- A. Virtual domains
- B. Administrative access profiles
- C. Trusted hosts
- D. Security Fabric

Answer: BC

Explanation:

Reference: <https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/219292/administrator-profiles>
<https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts>

QUESTION 61

Which daemon is responsible for enforcing raw log file size?

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

Answer: A

QUESTION 62

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.

Answer: D

Explanation:

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

QUESTION 63

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

Explanation:

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

QUESTION 64

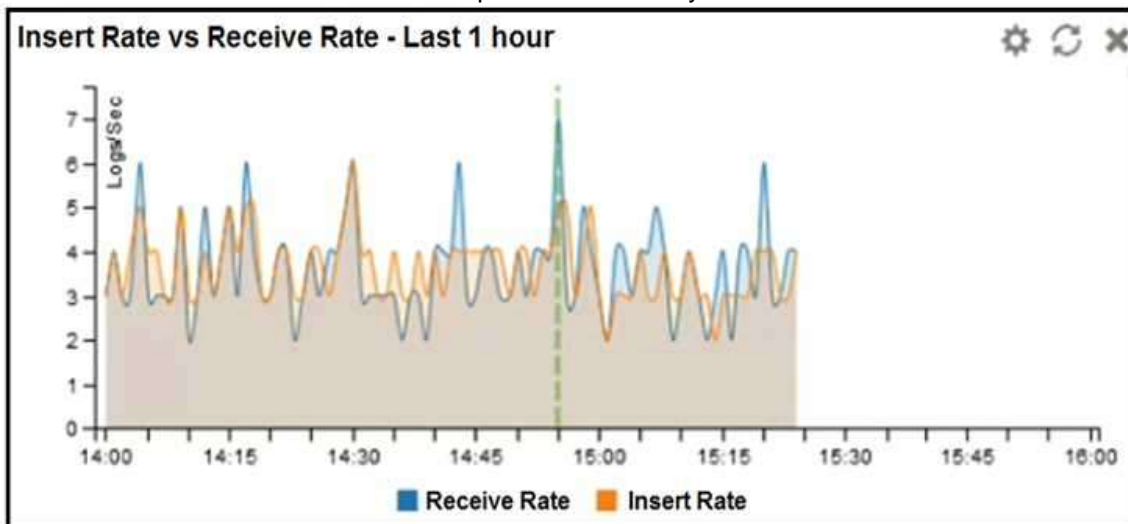
For which two purposes would you use the command set log checksum? (Choose two.)

- A. To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
- B. To prevent log modification or tampering
- C. To encrypt log communications
- D. To send an identical set of logs to a second logging server

Answer: BC

QUESTION 65

Refer to the exhibit. What does the data point at 14:55 tell you?



- A. The received rate is almost at its maximum for this device
- B. The sqlplugind daemon is behind in log indexing by two logs
- C. Logs are being dropped
- D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

QUESTION 66

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed.

What is the recommended method to replace the disk?

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

- A. Shut down FortiAnalyzer and then replace the disk
- B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
- C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
- D. Perform a hot swap

Answer: A

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

QUESTION 67

It is a best practice to upload FortiAnalyzer local logs to a remote server. Which three remote servers are supported for the upload?

(Choose three.)

- A. SFTP
- B. SCP
- C. FTP
- D. UDP
- E. TCP

Answer: ABC

QUESTION 68

Which database language does FortiAnalyzer support for the purposes of logging and reporting?

- A. LDAP
- B. SSH
- C. SQL
- D. XML

Answer: C

QUESTION 69

What should you always do after erasing the FortiAnalyzer configuration on flash?

- A. Run the execute reset all-settings command
- B. Run the execute format disk command
- C. Run the execute reboot command
- D. Perform a system backup

Answer: B

QUESTION 70

In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.

How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

- A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
- B. Configure # set resolve-ip enable in the system FortiView settings

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

- C. Configure local DNS servers on FortiAnalyzer
- D. Resolve IP addresses on FortiGate

Answer: D

Explanation:

<https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/>

As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only.

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>