



## Fortinet

### Exam Questions NSE5\_FAZ-6.4

Fortinet NSE 5 - FortiAnalyzer 6.4

#### NEW 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.

**Answer: C**

#### NEW QUESTION 2

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 mod
- D. FortiAnalyzer supports event management and reporting features.
- E. 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**

#### NEW QUESTION 3

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**

#### NEW QUESTION 4

What is the purpose of the following CLI command?

- A. To add a log file checksum
- B. To add the MD's hash value and authentication code
- C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- D. To encrypt log communications

**Answer: A**

#### Explanation:

<https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global>

#### NEW QUESTION 5

Refer to the exhibit.

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

- 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

#### NEW QUESTION 6

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

#### NEW QUESTION 7

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. License type
- B. Disk size
- C. Total quota
- D. RAID level

**Answer:** CD

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

#### NEW QUESTION 8

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

**Answer:** C

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383>

#### NEW QUESTION 9

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

**Answer:** C

#### NEW QUESTION 10

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

- A. It automatically updates the hcache when new logs arrive.
- B. It provides diagnostics on report generation time.
- C. It reduces the log insert lag rate.
- D. It reduces report generation time.

**Answer:** AD

#### NEW QUESTION 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:** AC

#### NEW 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.

**Answer:** A

#### NEW QUESTION 17

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super\_User administrator profile

**Answer:** B

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to>

#### NEW QUESTION 18

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

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

**Answer:** B

#### NEW QUESTION 23

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

#### NEW QUESTION 24

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

#### NEW QUESTION 28

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

- A. Custom datasets
- B. Report scheduling
- C. Report settings
- D. Output profiles

**Answer:** B

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports>

#### NEW QUESTION 30

View the exhibit.

Why is the total quota less than the total system storage?

- A. 3.6% of the system storage is already being used.
- B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
- C. The oftpd process has not archived the logs yet
- D. The logfiled process is just estimating the total quota

**Answer:** B

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

**NEW QUESTION 33**

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?

- 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:**

<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta->

**NEW QUESTION 34**

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy. What is the most likely problem?

- A. CPU resources are too high
- B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
- C. The total disk space is insufficient and you need to add other disk
- D. The ADOM disk quota is set too low, based on log rates

**Answer:** D

**NEW QUESTION 37**

Refer to the exhibit.

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

**NEW QUESTION 40**

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:** AB

**NEW QUESTION 45**

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

- A. Output profiles
- B. Report settings
- C. Report scheduling
- D. Custom datasets

**Answer:** D

**NEW QUESTION 48**

How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement
- C. SQL SELECT statement
- D. SQL EXTRACT statement

**Answer:** A

**Explanation:**

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8>

### NEW QUESTION 53

By default, what happens when a log file reaches its maximum file size?

- A. FortiAnalyzer overwrites the log files.
- B. FortiAnalyzer stops logging.
- C. FortiAnalyzer rolls the active log by renaming the file.
- D. FortiAnalyzer forwards logs to syslog.

**Answer:** C

### NEW QUESTION 54

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:** BD

### Explanation:

[https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400\\_execute/backup.htm](https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm)

### NEW QUESTION 58

What is the purpose of a predefined template on the FortiAnalyzer?

- A. It can be edited and modified as required
- B. It specifies the report layout which contains predefined texts, charts, and macros
- C. It specifies report settings which contains time period, device selection, and schedule
- D. It contains predefined data to generate mock reports

**Answer:** B

### NEW QUESTION 63

In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

- A. Configure local DNS servers on FortiAnalyzer
- B. Resolve IPs on FortiGate
- C. Configure # set resolve-ip enable in the system FortiView settings
- D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

**Answer:** B

### NEW QUESTION 66

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE5\_FAZ-6.4 Practice Exam Features:

- \* NSE5\_FAZ-6.4 Questions and Answers Updated Frequently
- \* NSE5\_FAZ-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE5\_FAZ-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE5\_FAZ-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE5\\_FAZ-6.4 Practice Test Here](#)**