# Fortinet

## Exam Questions NSE5_FAZ-6.4

Fortinet NSE 5 - FortiAnalyzer 6.4

**NEW QUESTION 1**
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 2**
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 3**
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:** D

**NEW QUESTION 4**
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 5**
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs
B. Web filter logs
C. IPS logs
D. Application control logs

**Answer:** B

**NEW QUESTION 6**

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 7**
View the exhibit:

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model
B. The disk quota for all devices in the ADOM
C. The disk quota for each device in the ADOM
D. The disk quota for the ADOM type

**Answer:** B

**Explanation:**
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol

**NEW QUESTION 8**
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

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

**Answer:** C

**Explanation:**
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

**NEW QUESTION 9**
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 10**
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:** ACE


**NEW QUESTION 10**
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 12**
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 16**
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

**Answer:** BC


**NEW QUESTION 18**
What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation
B. Host name resolution
C. Log collection
D. Real-time forwarding

**Answer:** C


**NEW QUESTION 20**
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
B. Must establish an IPsec tunnel ID and pre-shared key.
C. IPsec cannot be enabled if SSL is enabled as well.
D. IPsec is only enabled through the CLI on FortiAnalyzer.

**Answer:** C


**NEW QUESTION 23**
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
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"


**NEW QUESTION 28**
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
D. Custom View

**Answer:** A

**Explanation:**
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder


**NEW QUESTION 33**
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:** BC


**NEW QUESTION 34**
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

A. SSL is the default setting.
B. SSL communications are auto-negotiated between the two devices.
C. SSL can send logs in real-time only.
D. SSL encryption levels are globally set on FortiAnalyzer.
E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

**Answer:** AD


**NEW QUESTION 35**
How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

A. Use static routes
B. Use administrative profiles
C. Use trusted hosts
D. Use secure protocols

**Answer:** C

**Explanation:**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts


**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 42**
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:** A


**NEW QUESTION 45**
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 48**
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 53**
What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer automatically sets the disk log quota based on the device.
C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

**Answer:** CD

**NEW QUESTION 58**
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 60**
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 61**
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.

**Answer:** BCD

**NEW QUESTION 62**
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 67**
What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.
B. When you restart FortiAnalyze
C. all stored logs are considered to be offline logs.
D. Logs that are indexed and stored in the SQL database.
E. Logs that are collected from offline devices after they boot up.

**Answer:** A

**NEW QUESTION 68**
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


**NEW QUESTION 69**
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 74**
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


**NEW QUESTION 78**
......