

# Fortinet

## Exam Questions NSE5\_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0



### NEW QUESTION 1

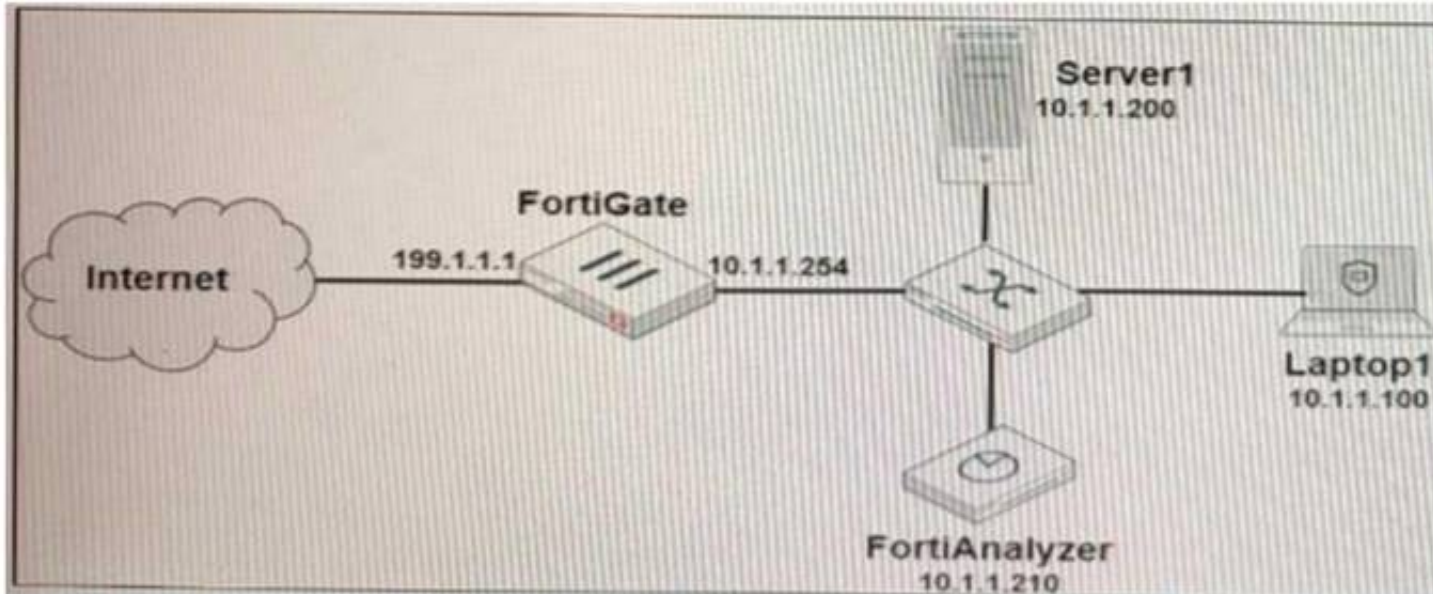
What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

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

**Answer: B**

### NEW QUESTION 2

Refer to the exhibit.



Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:  
 Which filter will achieve the desired result?

- A. operation-login & performed\_on=="GUI(10.1.1.100)" & user!=admin
- B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
- C. operation-login & dstip==10.1.1.210 & user!=admin
- D. operation-login & performed\_on=="GUI(10.1.1.210)" & user!=admin

**Answer: A**

#### Explanation:

On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed\_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

### NEW QUESTION 3

What are two benefits of using fabric connectors? (Choose two.)

- A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
- B. You do not need an additional license to send logs to the cloud platform.
- C. Fabric connectors allow you to improve redundancy.
- D. Using fabric connectors is more efficient than using third-party polling with API.

**Answer: AC**

### NEW QUESTION 4

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: AB**

#### Explanation:

To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.

FortiAnalyzer\_7.0\_Study\_Guide-Online page 149

### NEW QUESTION 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:** AC

**Explanation:**

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

#### NEW QUESTION 6

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 7

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:** BD

#### NEW QUESTION 8

Which statement about sending notifications with incident updates is true?

- A. Notifications can be sent only when an incident is created or deleted.
- B. You must configure an output profile to send notifications by email.
- C. Each incident can send notifications to a single external platform.
- D. Each connector used can have different notification settings.

**Answer:** D

#### NEW QUESTION 9

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 10

Which two statements are true regarding the outbreak detection service? (Choose two.)

- A. New alerts are received by email.
- B. Outbreak alerts are available on the root ADOM only.
- C. An additional license is required.
- D. It automatically downloads new event handlers and reports.

**Answer:** CD

#### NEW QUESTION 10

After generating a report, you notice the information you were expecting to see is not included in it. What are two possible reasons for this scenario? (Choose two.)

- A. You enabled auto-cache with extended log filtering.
- B. The logfile service has not indexed all the expected logs.
- C. The logs were overwritten by the data retention policy.
- D. The time frame selected in the report is wrong.

**Answer:** BC

#### NEW QUESTION 11

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

#### NEW QUESTION 12

What are two advantages of setting up fabric ADOM? (Choose two.)

- A. It can be used for fast data processing and log correlation
- B. It can be used to facilitate communication between devices in same Security Fabric
- C. It can include all Fortinet devices that are part of the same Security Fabric
- D. It can include only FortiGate devices that are part of the same Security Fabric

**Answer:** AC

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a>

#### NEW QUESTION 17

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

- A. The log file is stored as a raw log and is available for analytic support.
- B. The log file rolls over and is archived.
- C. The log file is purged from the database.
- D. The log file is overwritten.

**Answer:** B

#### NEW QUESTION 21

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

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

**Answer:** AC

#### Explanation:

- A) FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. "Real time" and "aggregation" is about the "moment" when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / different config).
- C) FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

#### NEW QUESTION 24

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

- 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 ADO
- D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- E. Normal mode is the default ADOM mode.

**Answer:** CD

#### NEW QUESTION 28

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 30

How can you attach a report to an incident?

- A. By attaching it to an event handler alert
- B. By editing the settings of the desired report
- C. From the properties of an existing incident
- D. Saving it in JSON format, and then importing it

**Answer:** C

**NEW QUESTION 32**

What is the purpose of trigger variables?

- A. To display statistics about the playbook runtime
- B. To use information from the trigger to filter the action in a task
- C. To provide the trigger information to make the playbook start running
- D. To store the start times of playbooks with On\_Schedule triggers

**Answer:** B

**NEW QUESTION 33**

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 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 35**

What are the operating modes of FortiAnalyzer? (Choose two)

- A. Standalone
- B. Manager
- C. Analyzer
- D. Collector

**Answer:** CD

**NEW QUESTION 40**

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:** BD

**NEW QUESTION 45**

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:**

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.

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

**NEW QUESTION 47**

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 52

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To properly correlate logs
- B. To use real-time forwarding
- C. To resolve host names
- D. To improve DNS response times

**Answer:** A

**Explanation:**

- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation

#### NEW QUESTION 56

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

**Answer:** AB

#### NEW QUESTION 59

A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

- A. Running
- B. Failed
- C. Upstream\_failed
- D. Success

**Answer:** B

#### NEW QUESTION 62

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

- A. System information
- B. Logs from registered devices
- C. Report information
- D. Database snapshot

**Answer:** AC

**Explanation:**

What does the System Configuration backup include?

System information, such as the device IP address and administrative user information. Device list, such as any devices you configured to allow log access.

Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

FortiAnalyzer\_7.0\_Study\_Guide-Online pag. 29

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 29: What does the System Configuration backup include?

- System information, such as the device IP address and administrative user information
- Device list, such as any devices you configured to allow log access
- Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

#### NEW QUESTION 65

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

- A. The size of newly generated reports is optimized to conserve disk space.
- B. FortiAnalyzer local cache is used to store generated reports.
- C. When new logs are received, the hard-cache data is updated automatically.
- D. The generation time for reports is decreased.

**Answer:** CD

#### NEW QUESTION 66

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

#### NEW QUESTION 70

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 72

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 75

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
✓ 151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙ SSL	1	● Low

Which statement is correct regarding the event displayed?

- A. The security risk was blocked or dropped.
- B. The security event risk is considered open.
- C. An incident was created from this event.
- D. The risk source is isolated.

**Answer:** A

#### Explanation:

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not. The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open. Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped. (Blank): Other scenarios.

FortiAnalyzer\_7.0\_Study\_Guide-Online pag. 206

#### NEW QUESTION 80

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer glows you to schedule reports to run.
- C. FortiAnalyzer includes pre-defined reports only.
- D. FortiAnalyzer allows reporting for FortiGate devices only.

**Answer:** AB

#### NEW QUESTION 84

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:** AC

#### NEW QUESTION 89

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

**Answer:** B

#### Explanation:

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task.  
"Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer\_7.0\_Study\_Guide-Online page 242

#### NEW QUESTION 94

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 99

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 102

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

#### NEW QUESTION 104

What is the purpose of the following CLI command?

```
# configure system global
  set log-checksum md5
end
```

- 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 108

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

- A. Incidents dashboards
- B. Threat hunting
- C. FortiView Monitor
- D. Outbreak alert services

**Answer:** B



**Explanation:**

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

**NEW QUESTION 109**

If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?

- A. The configured IP address is checked first.
- B. The active port number is checked first.
- C. The firmware version is checked first.
- D. The configured priority is checked first

**Answer:** D

**Explanation:**

In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:

- All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.
- If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.
- If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.

FortiAnalyzer\_7.0\_Study\_Guide-Online page 62

**NEW QUESTION 113**

.....

## 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-7.0 Practice Exam Features:

- \* NSE5\_FAZ-7.0 Questions and Answers Updated Frequently
- \* NSE5\_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE5\_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE5\_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE5\\_FAZ-7.0 Practice Test Here](#)**