

# Fortinet

## Exam Questions NSE5\_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2



#### 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

When working with FortiAnalyzer reports, what is the purpose of a dataset?

- A. To provide the layout used for reports
- B. To define the chart type to be used
- C. To retrieve data from the database
- D. To set the data included in templates

**Answer: C**

#### NEW QUESTION 3

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 4

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 5

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 6

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 7

Which statement describes online logs on FortiAnalyzer?

- A. Logs that reached a specific size and were rolled over
- B. Logs that can be used to create reports
- C. Logs that can be viewed using Log Browse
- D. Logs that are saved to disk, compressed, and available in FortiView

**Answer: C**

#### NEW QUESTION 8

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 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

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 10

Why run the command `diagnose sql status sqlplugind`?

- A. To list the current SQL processes running
- B. To check what is the database log insertion status
- C. To display the SOL query connections and hcache status
- D. To view the current hcache size

**Answer:** C

#### NEW QUESTION 13

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

**Answer:** A

#### Explanation:

[https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20\(%22Redundant%20Array%20of%20Inexpensive,%2C%](https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%)

#### NEW QUESTION 18

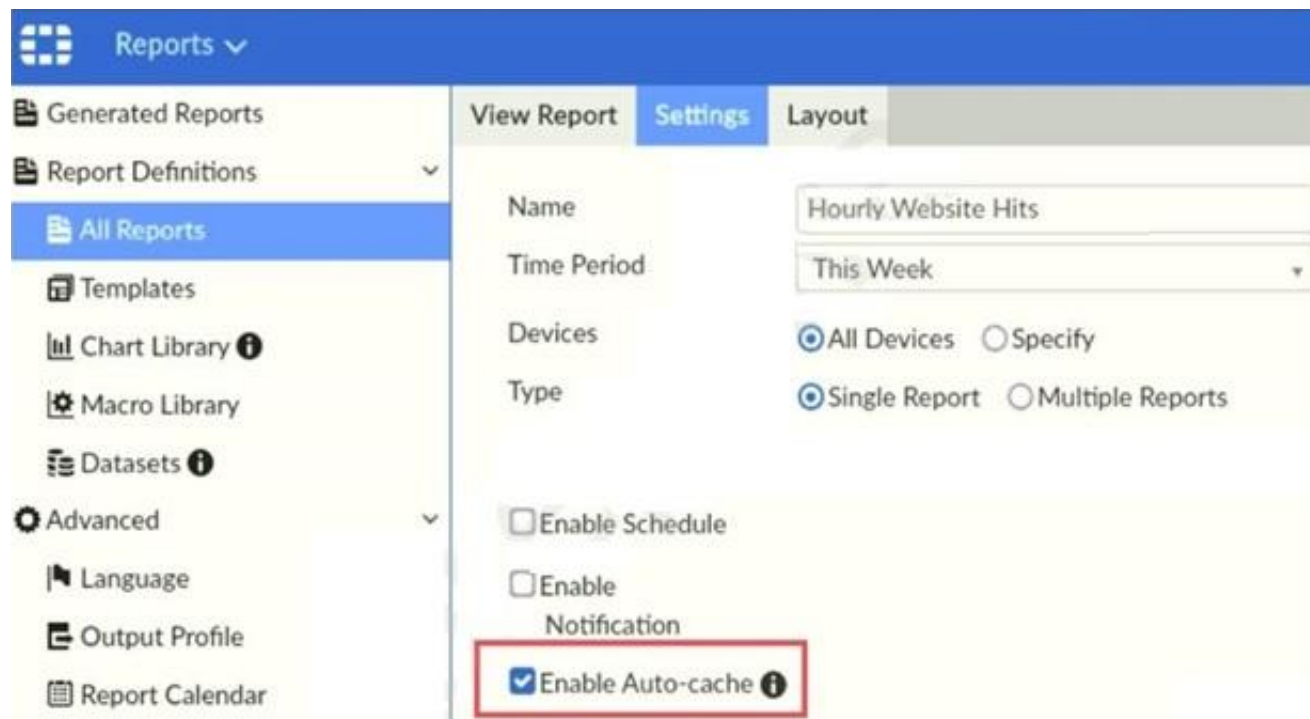
What is the purpose of a predefined template on the FortiAnalyzer?

- 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 22

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:** CD

**Explanation:**

"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."

FortiAnalyzer\_7.0\_Study\_Guide-Online page 306

**NEW QUESTION 26**

Which statement correctly describes the management extensions available on FortiAnalyzer?

- A. Management extensions do not require additional licenses.
- B. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.
- C. Management extensions require a dedicated VM for best performance.
- D. Management extensions may require a minimum number of CPU cores to run.

**Answer:** D

**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. 189.

FortiAnalyzer\_7.0\_Study\_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

**NEW QUESTION 28**

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:** BD

**Explanation:**

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

**NEW QUESTION 31**

Refer to the exhibit.

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster. What can you conclude from the configuration displayed?

- A. This FortiAnalyzer will join to the existing HA cluster as the primary.
- B. This FortiAnalyzer is configured to receive logs in its port1.
- C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

**Answer:** B

**Explanation:**

"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit." (<https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104>)

**NEW QUESTION 32**

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 33**

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. FortiOS Event Log
- D. Fabric Connector event

**Answer:** B

**Explanation:**

"One possible scenario is shown on the slide:

- \* 1. Traffic flows through the FortiGate
- \* 2. FortiGate sends logs to FortiAnalyzer
- \* 3. FortiAnalyzer detects some suspicious traffic and generates an event
- \* 4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
- \* 5. FortiGate runs the automation stitch with the corrective or preventive actions" FortiAnalyzer\_7.0\_Study\_Guide-Online page 228

In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side. FortiAnalyzer\_7.0\_Study Guide page no 233

**NEW QUESTION 37**

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 39**

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 40**

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

**Answer:** D

**NEW QUESTION 44**

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

**Answer:** D

**NEW QUESTION 49**

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

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer allows 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 53**

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 54**

Refer to the exhibit.



What does the data point at 12:20 indicate?

- A. The performance of FortiAnalyzer is below the baseline.
- B. FortiAnalyzer is using its cache to avoid dropping logs.
- C. The log insert lag time is increasing.
- D. The sqlplugind service is caught up with new logs.

**Answer: C**

#### NEW QUESTION 58

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 59

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 60

.....

## 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-7.2 Practice Exam Features:

- \* NSE5\_FAZ-7.2 Questions and Answers Updated Frequently
- \* NSE5\_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE5\_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE5\_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE5\\_FAZ-7.2 Practice Test Here](#)**