



**Fortinet**

**Exam Questions NSE5\_FAZ-7.0**

Fortinet NSE 5 - FortiAnalyzer 7.0

#### NEW QUESTION 1

Consider the CLI command:

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

What is the purpose of the command?

- A. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- B. To add the MD5 hash value and authentication code
- C. To add a log file checksum
- D. To encrypt log communications

**Answer: C**

#### Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global>

#### NEW QUESTION 2

What is Log Insert Lag Time on FortiAnalyzer?

- A. The number of times in the logs where end users experienced slowness while accessing resources.
- B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
- C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
- D. The amount of time FortiAnalyzer takes to receive logs from a registered device

**Answer: C**

#### NEW QUESTION 3

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 4

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

**Answer: D**

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

#### NEW QUESTION 5

What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from d devices in a duster.
- C. FortiAnalyzer receives bgs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

**Answer: AB**

#### NEW QUESTION 6

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

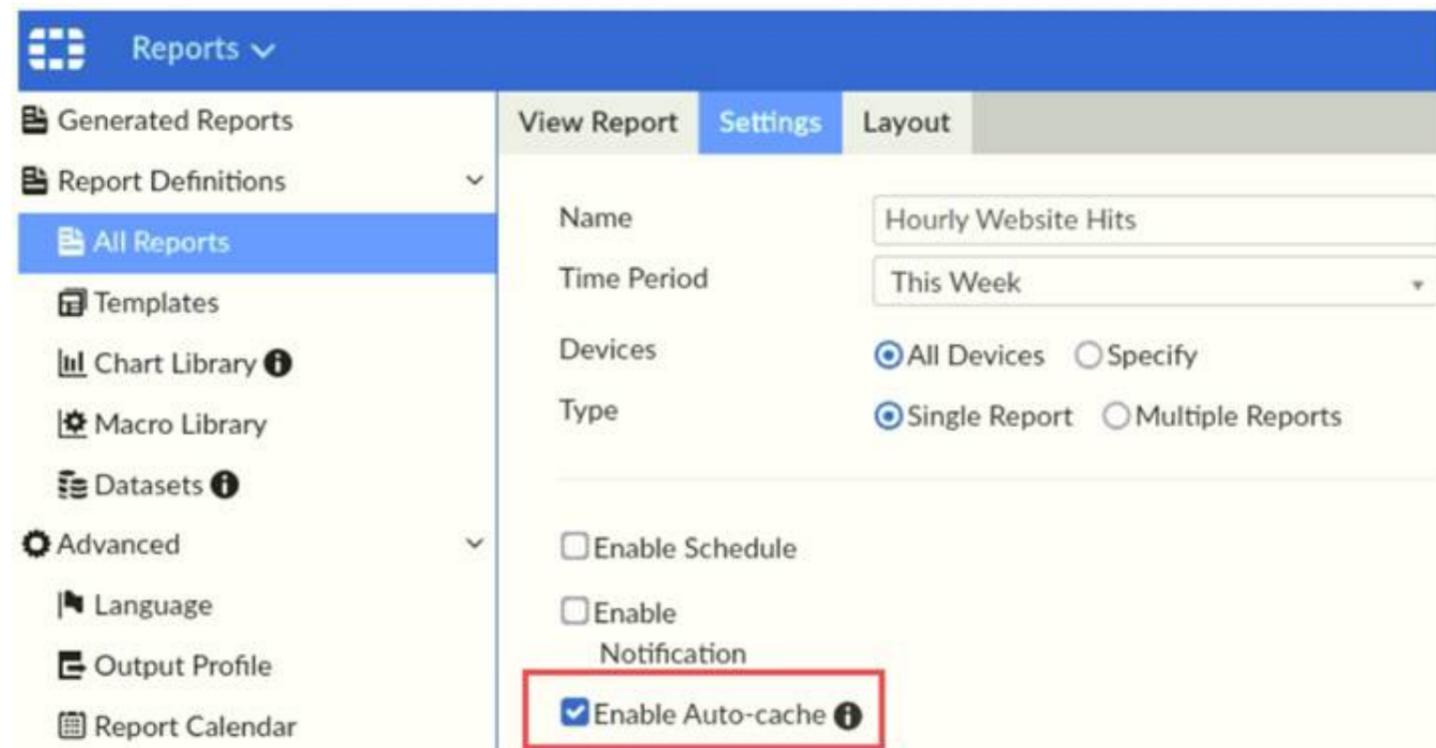
**Answer: BD**

#### Explanation:

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

**NEW QUESTION 7**

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**

**NEW QUESTION 8**

Which SQL query is in the correct order to query the database in the FortiAnalyzer?

- A. SELECT devid FROM Slog GROOP BY devid WHERE \* user' =\* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE \*user' =' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user\* =' USERI' SELECT devid GROUP BY devid

**Answer: C**

**NEW QUESTION 9**

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

**Answer: D**

**NEW QUESTION 10**

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 10**

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

- A. Log upload
- B. Indicators of Compromise
- C. Log forwarding an aggregation mode
- D. Log fetching

**Answer: D**

**Explanation:**

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management>

**NEW QUESTION 15**

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 18**

You created 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: D**

**NEW QUESTION 23**

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 27**

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

`execute sql-local rebuild-adom <new-ADOM-name>`

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM
- D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

**Answer: D**

**Explanation:**

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

**NEW QUESTION 29**

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: AB**

**NEW QUESTION 33**

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?

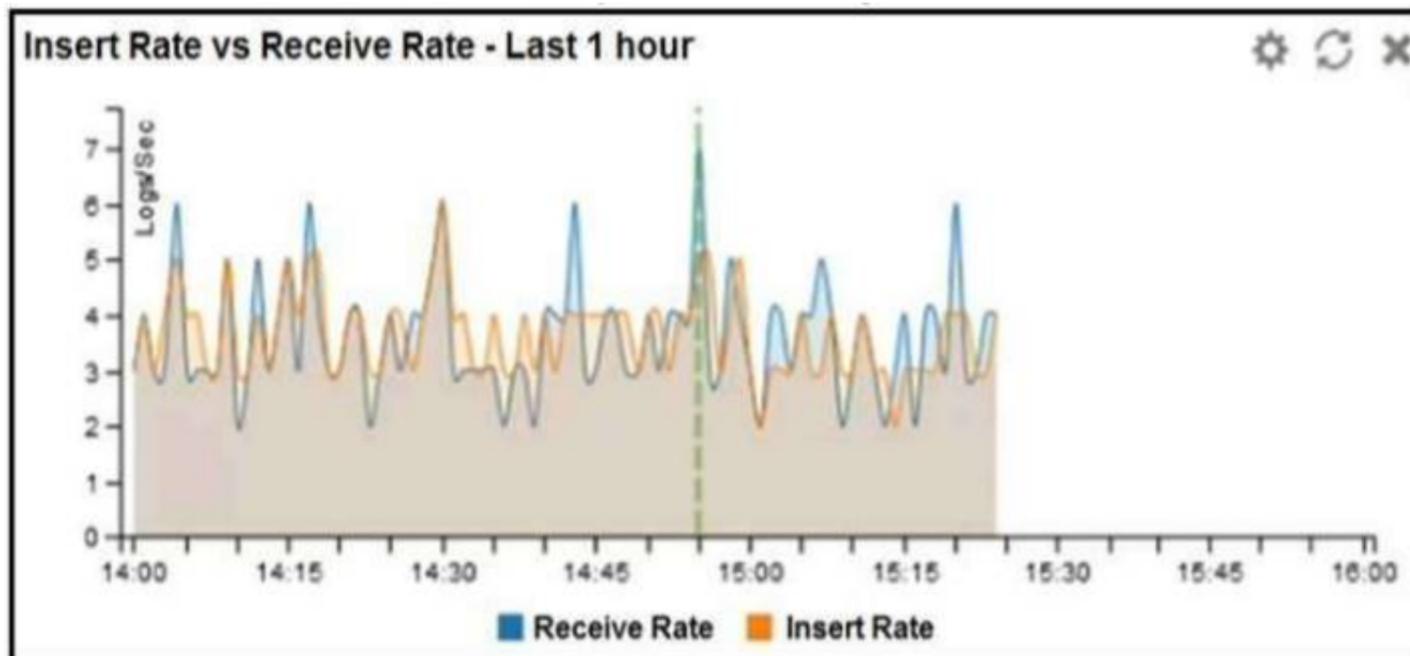
- A. The security risk was blocked or dropped.

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

Answer: A

**NEW QUESTION 37**

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 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 43**

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 44**

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

- A. First, upgrade the secondary device, and then upgrade the primary device.
- B. Both FortiAnalyzer devices will be upgraded at the same time.
- C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
- D. You can perform the firmware upgrade using only a console connection.

Answer: D

**NEW QUESTION 46**

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 ForbSIEM 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: A

#### NEW QUESTION 51

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:** C

#### NEW QUESTION 56

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 61

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 66

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 67

Which two statements are correct regarding the export and import of playbooks? (Choose two.)

- A. You can export only one playbook at a time.
- B. You can import a playbook even if there is another one with the same name in the destination.
- C. Playbooks can be exported and imported only within the same FortiAnalyzer.
- D. A playbook that was disabled when it was exported, will be disabled when it is imported.

**Answer:** BD

#### NEW QUESTION 72

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 73

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:** A

#### Explanation:

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

### NEW QUESTION 77

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 79

FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for what purpose?

- A. To upload logs to an SFTP server
- B. To prevent log modification during backup
- C. To send an identical set of logs to a second logging server
- D. To encrypt log communication between devices

**Answer:** D

### NEW QUESTION 80

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 82

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 86

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 89

Logs are being deleted from one of your ADOMs earlier than 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://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 94**

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 96**

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 97**

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:** BC

**NEW QUESTION 102**

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 107**

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 111**

.....

## 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](#)