

NSE5_FAZ-6.2^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 6.2





Pass Fortinet NSE5_FAZ-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse5_faz-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

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

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

Correct Answer: D

QUESTION 2

On FortiAnalyzer, what is a wildcard administrator account?

- A. An account that permits access to members of an LDAP group
- B. An account that allows guest access with read-only privileges
- C. An account that requires two-factor authentication
- D. An account that validates against any user account on a FortiAuthenticator

Correct Answer: D

QUESTION 3

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

Correct Answer: C

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48500>

QUESTION 4

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

Correct Answer: D

Reference: https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1100_Storage/0017_Deleted%20device%20logs.htm

QUESTION 5

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

- A. Forwarded logs cannot be filtered to match specific criteria.
- B. Logs are forwarded in real-time only.
- C. The client retains a local copy of the logs after forwarding.
- D. You can use aggregation mode only with another FortiAnalyzer.

Correct Answer: BC

Reference: www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/

QUESTION 6

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

Correct Answer: BC

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

QUESTION 7

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

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

Correct Answer: CD

QUESTION 8

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

Correct Answer: C

QUESTION 9

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

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

Correct Answer: A

QUESTION 10

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.

Correct Answer: C

QUESTION 11

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.

Correct Answer: C

QUESTION 12

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

Correct Answer: BD

QUESTION 13

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

Correct Answer: D

Reference: <https://www.fortinetguru.com/2016/04/system-settings/6/>

QUESTION 14

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

Correct Answer: A

QUESTION 15

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Correct Answer: D

Reference: <https://forum.fortinet.com/tm.aspx?m=143106>

[NSE5_FAZ-6.2 VCE Dumps](#)

[NSE5_FAZ-6.2 Practice
Test](#)

[NSE5_FAZ-6.2 Exam
Questions](#)