



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.pass4itsure.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**

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

- A. Remote logging must be enabled on FortiGate
- B. Log encryption must be enabled
- C. ADOMs must be enabled
- D. FortiGate must be registered with FortiAnalyzer

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."

<https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf> Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

QUESTION 2

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

Correct Answer: B

QUESTION 3

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

Correct Answer: C

**QUESTION 4**

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 5

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.

Correct Answer: AB

QUESTION 6

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.

Correct Answer: BC

QUESTION 7

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 8

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

Correct Answer: B

QUESTION 9

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

Correct Answer: AB

To prevent the log in the store from being modified, you can add a log checksum by using the config system global command. When the log is split, archived, and the log is uploaded (if the feature is enabled), you can configure the FortiAnalyzer to log the log file hash value, timestamp, and authentication code. This can help defend against man-in-the-middle attacks when uploading log transmission data from the FortiAnalyzer to the SFTP server.

QUESTION 10

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



- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from all devices in a cluster.
- C. FortiAnalyzer receives logs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know the serial number of the primary device in the cluster-it automatically discovers the other devices.

Correct Answer: AB

QUESTION 11

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 12

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

Correct Answer: D

QUESTION 13

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What devices and IP addresses are connecting to FortiAnalyzer
- B. What logs, if any, are reaching FortiAnalyzer



- C. What ADOMs are enabled and configured
- D. What devices are registered and unregistered

Correct Answer: A

QUESTION 14

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

Correct Answer: A

QUESTION 15

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

Correct Answer: AB

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enablingautocache>

[NSE5_FAZ-6.2 PDF Dumps](#) [NSE5_FAZ-6.2 Study Guide](#) [NSE5_FAZ-6.2 Braindumps](#)