

NSE5_FAZ-7.0^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_faz-7-0.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

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

Correct Answer: BCE

QUESTION 2

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: AB

QUESTION 3

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

Correct Answer: B

FortiAnalyzer_7.0_Study_Guide-Online pag. 217

QUESTION 4

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

- A. RADIUS
- B. Local
- C. LDAP
- D. PKI
- E. TACACS+

Correct Answer: ACE

QUESTION 5

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 6

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 7

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

- A. FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
- B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
- D. FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.
- E. FortiAnalyzer HA implementation is supported by all cloud providers.

Correct Answer: BC

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures. FortiAnalyzer_7.0_Study_Guide-Online pag. 60

QUESTION 8

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

- A. FortiAnalyzer is in an HA cluster.
- B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
- C. ADOMs are not enabled on FortiAnalyzer.
- D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Correct Answer: C

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

QUESTION 9

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

Correct Answer: D

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

QUESTION 10

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

Correct Answer: C

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts>

QUESTION 11

What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

- A. Log correlation
- B. Host name resolution
- C. Log collection
- D. Real-time forwarding

Correct Answer: A

page 27: synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation.

QUESTION 12

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.

Correct Answer: BD

Reference: <https://community.fortinet.com/t5/Fortinet-Forum/FW-Migration-between-ADOMs/m-p/32683?m=158008>

QUESTION 13

What does the disk status Degraded mean for RAID management?

- A. One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.
- B. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
- C. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
- D. The hard drive is no longer being used by the RAID controller

Correct Answer: D

QUESTION 14

Which two statements are true regarding fabric connectors? (Choose two.)

- A. Configuring fabric connectors to send notification to ITSM platform upon incident creation is more efficient than third-party information from the FortiAnalyzer API.
- B. Fabric connectors allow to save storage costs and improve redundancy.
- C. Storage connector service does not require a separate license to send logs to cloud platform.
- D. Cloud-Out connections allow you to send real-time logs to public cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Correct Answer: AD

QUESTION 15

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

Correct Answer: CD

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/0400_ADOM%20Device%20Modes.htm

[Latest NSE5_FAZ-7.0
Dumps](#)

[NSE5_FAZ-7.0 Practice
Test](#)

[NSE5_FAZ-7.0 Braindumps](#)