

QUESTIONS & ANSWERS

Kill your exam at first Attempt



Fortinet

NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

https://killexams.com/pass4sure/exam-detail/NSE5_FAZ-7.0



Question: 29

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>

Question: 30

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

Answer: A,D

Explanation:

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: 31

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

Answer: D

Question: 32

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

Question: 33

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

Explanation:

Reference: <https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets>

Question: 34

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.

Answer: A,D

Question: 35

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.

Answer: C

Explanation:

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

Question: 36

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

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

Question: 37

What are analytics logs on FortiAnalyzer?

- A. Log type Traffic logs.
- B. Logs that roll over when the log file reaches a specific size.
- C. Logs that are indexed and stored in the SQL.
- D. Raw logs that are compressed and saved to a log file.

Answer: C

Question: 38

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: AB

Question: 39

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

Answer: A,B

Question: 40

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.

Answer: B,C

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FMG-FAZ/4600_HA/0000_HA.htm?TocPath=High%20Availability%7C_____0

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.