

Lead1Pass

LEAD1PASS

> Contact Us

Login / Register

Search...



HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (0)



Try **PDF Demo** before you buy



Instant Download



After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates



Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

<http://www.lead1pass.com/>

Latest Exam Guide & Learning Materials

Exam : **NSE5_FAZ-6.4**

Title : Fortinet NSE 5 - FortiAnalyzer
6.4

Vendor : Fortinet

Version : DEMO

NO.1 Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

- A. In aggregation mode, you can forward logs to syslog and CEF servers as well.
- B. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
- C. Both modes, forwarding and aggregation, support encryption of logs between devices.
- D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Answer: B,D

NO.2 What is the purpose of a predefined template on the FortiAnalyzer?

- A. It can be edited and modified as required
- B. It specifies report settings which contains time period, device selection, and schedule
- C. It contains predefined data to generate mock reports
- D. It specifies the report layout which contains predefined texts, charts, and macros

Answer: D

Reference:

2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number%20of,create%20and%20for%20build%20reports.&text=A%20template%20populates%20the%20Layout,that%20is%20to%20be%20created.
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

NO.3 If you upgrade the FortiAnalyzer firmware, which report element can be affected?

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

Answer: D

Explanation:

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

NO.4 On FortiAnalyzer, what is a wildcard administrator account?

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

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts>

NO.5 Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. License type

- B. RAID level
- C. Total quota
- D. Disk size

Answer: B,D

Explanation:

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

NO.6 What are two advantages of setting up fabric ADOM? (Choose two.)

- A. It can include only FortiGate devices that are part of the same Security Fabric
- B. It can include all Fortinet devices that are part of the same Security Fabric
- C. It can be used to facilitate communication between devices in same Security Fabric
- D. It can be used for fast data processing and log correlation

Answer: B,D

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom>

NO.7 Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?

- A. To resolve host names
- B. To use real-time forwarding
- C. To properly correlate logs
- D. To improve DNS response times

Answer: C

Explanation:

- [Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for proper log correlation](#)

NO.8 For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use real-time forwarding
- B. Use DNS
- C. Use an NTP server
- D. Use host name resolution

Answer: C