



**Vendor:** Fortinet

**Exam Code:** NSE5\_FAZ-5.4

**Exam Name:** FortiAnalyzer 5.4 Specialist

**Version:** DEMO

#### QUESTION 1

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs and content files are stored and uploaded at a scheduled time
- B. Logs and content files are forwarded as they are received
- C. Logs are forwarded as they are received
- D. Logs are forwarded as they are received and content files are uploaded at a scheduled time

**Answer:** A

#### QUESTION 2

DLP archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

- A. SNMP
- B. IPSec
- C. SMTP
- D. POP3
- E. HTTP

**Answer:** CDE

#### QUESTION 3

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.

**Answer:** BC

#### QUESTION 4

Which statement is correct? FortiAnalyzer collects and aggregates log data from:

- A. Any supported device it is configured to monitor.
- B. FortiGate devices only.
- C. FortiAnalyzer's operating in collector mode only.
- D. Any supported device it is configured to monitor, as long as it's not in the wide area network (WAN).

**Answer:** A

#### QUESTION 5

What are two of the key features of FortiAnalyzer? (Choose two)

- A. Centralized log repository

- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

**Answer:** AC

**QUESTION 6**

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

- A. FortiAnalyzer distinguishes different device 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.

**Answer:** AC

**QUESTION 7**

What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

**Answer:** B

## Thank You for Trying Our Product

### PassLeader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



**10% Discount Coupon Code: STNAR2014**