

**HIGHER QUALITY
BETTER SERVICE**

CERTTREE

QUESTION & ANSWER



Provide One Year
Free Update!

<https://www.certtree.com>

Exam : **NSE5_FAZ-5.4**

Title : **FortiAnalyzer 5.4 Specialist**

Version : **DEMO**

1. On FortiAnalyzer, what is a wildcard administrator account?

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

Answer: D

2. Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

- A. Log forwarding in aggregation mode
- B. Log upload
- C. Log fetching
- D. Indicators of Compromise

Answer: A

3. How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement
- C. SQL SELECT statement
- D. SQL EXTRACT statement

Answer: C

4. Logs are being deleted from one of your ADOMs earlier than the configured setting for archiving in your data policy.

What is the most likely problem?

- A. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device
- B. CPU resources are too high
- C. The ADOM disk quota is set too low based on log rates
- D. The total disk space is insufficient and you need to add other disk

Answer: D

5. How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Configure trusted hosts
- C. Assign the ADOMs to the administrator's account
- D. Assign the default Super_User administrator profile

Answer: C