# NSE5_FAZ-7.0$^{Q\&As}$

Fortinet NSE 5 - FortiAnalyzer 7.0

**QUESTION 1**

What are offline logs on FortiAnalyzer?

A. Compressed logs, which are also known as archive logs, are considered to be offline logs.

B. When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

C. Logs that are indexed and stored in the SQL database.

D. Logs that are collected from offline devices after they boot up.

Correct Answer: A

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs

and are considered offline so they don\\'t offer immediate analytic support.

Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy.

FortiAnalyzer_7.0_Study_Guide-Online page 140

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-6/Content/FortiAnalyzer_Admin_Guide/0300_Key_concepts/0600_Log_Storage/0400_Arch ive_analytics_logs.htm

**QUESTION 2**

Which SQL query is in the correct order to query the database in the FortiAnslyzer?

A. SELECT devid WHERE \\'user\\'=\\'USER1\\' FROM $log GROUP BY devid

B. FROM $log WHERE \\'user\\'=\\'USER1\\' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE \\'user\\'=\\'USER1\\' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE \\'user\\'=\\'USER1\\'

Correct Answer: C

**QUESTION 3**

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

A. Mail server

B. Output profile

C. SFTP server

D. Report scheduling

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration- guide/598322/creating-output-profiles

**QUESTION 4**

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of an 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

Correct Answer: A

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

**QUESTION 5**

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