NSE5_FAZ-6.4^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 6.4

Pass Fortinet NSE5_FAZ-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse5_faz-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. A local wildcard administrator account

B. A remote LDAP server

C. A trusted host profile that restricts access to the LDAP group

D. An administrator group

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

QUESTION 2

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

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 3

Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

A. The total disk space is insufficient and you need to add other disk.

B. CPU resources are too high.

C. The ADOM disk quota is set too low based on log rates.

D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Correct Answer: C

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device% 20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

QUESTION 4

Which two statements about log forwarding are true? (Choose two.)

A. Forwarded logs cannot be filtered to match specific criteria.

B. Logs are forwarded in real-time only.

C. The client retains a local copy of the logs after forwarding.

D. You can use aggregation mode only with another FortiAnalyzer.

Correct Answer: CD

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

QUESTION 5

Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.

B. Macros are supported only on the FortiGate ADOM.

C. Macros are useful in generating excel log files automatically based on the reports settings.

D. Macros are predefined templates for reports and cannot be customized.

Correct Answer: A

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.2.3/administration-guide/617380/creatingmacros

Latest NSE5_FAZ-6.4   NSE5_FAZ-6.4 PDF Dumps   NSE5_FAZ-6.4 Study Guide
Dumps