NSE5_FAZ-6.4$^{\text{Q\&As}}$

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.pass4itsure.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

QUESTION 1

Which daemon is responsible for enforcing raw log file size?

A. logfiled

B. oftpd

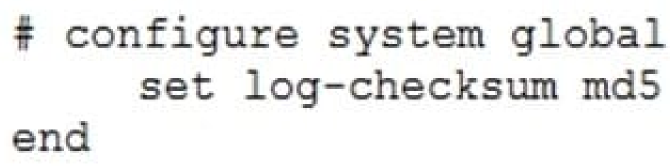
C. sqlplugind

D. miglogd

Correct Answer: A

QUESTION 2

What is the purpose of the following CLI command?



```
# configure system global
      set log-checksum md5
end
```

A. To add a log file checksum

B. To add the MD\\'s hash value and authentication code

C. To add a unique tag to each log to prove that it came from this FortiAnalyzer

D. To encrypt log communications

Correct Answer: A

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

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.

Correct Answer: BC

QUESTION 4

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs

B. Web filter logs

C. IPS logs

D. Application control logs

Correct Answer: B

Reference:

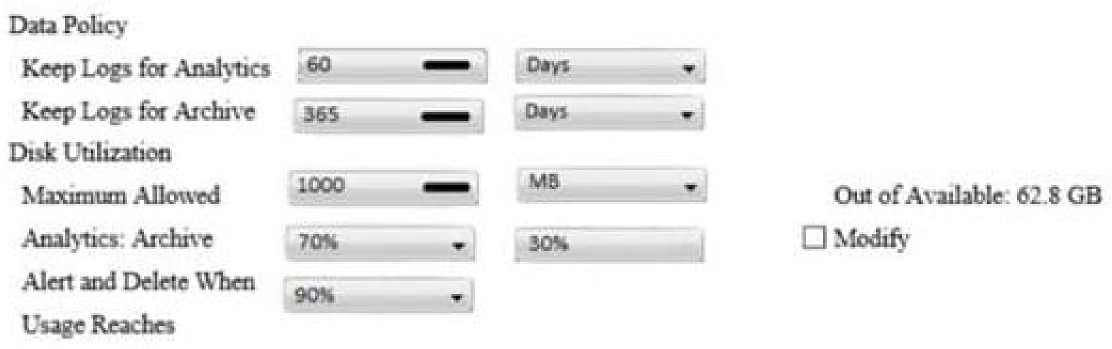
https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/

FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_

hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

QUESTION 5

View the exhibit:



Data Policy

Keep Logs for Analytics 60 Days

Keep Logs for Archive 365 Days

Disk Utilization

Maximum Allowed 1000 MB Out of Available: 62.8 GB

Analytics: Archive 70% 30% □ Modify

Alert and Delete When Usage Reaches 90%

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model

B. The disk quota for all devices in the ADOM

C. The disk quota for each device in the ADOM

D. The disk quota for the ADOM type

Correct Answer: B

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration- guide/743670/configuring-logstorage-policy