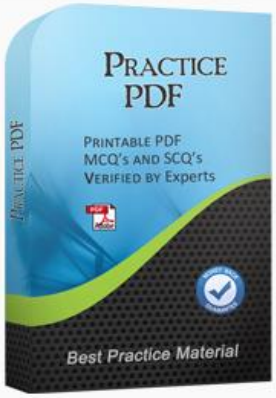
BraindumpQuiz

BraindumpQuiz

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Exam : **NSE5_FAZ-7.2**

Title : Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst

Vendor : Fortinet

Version : DEMO

NO.1 What is the main purpose of using an NTP server on FortiAnalyzer and all of its registered devices?

A. Log correlation

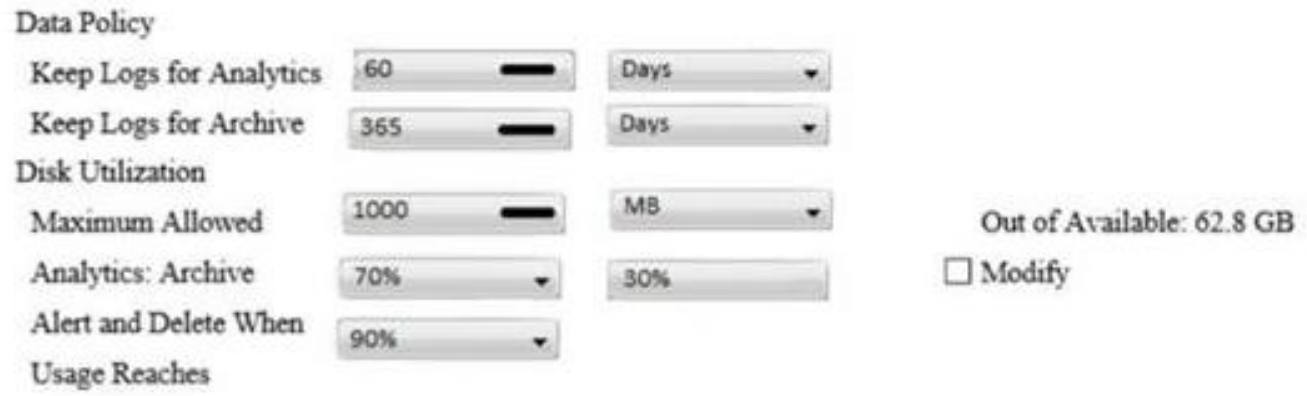
B. Host name resolution

C. Log collection

D. Real-time forwarding

Answer: A

NO.2 View the exhibit:



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

Answer: B

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-poli

NO.3 What does the disk status Degraded mean for RAID management?

A. One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.

B. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.

C. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.

D. The hard driveils no longer being used by the RAID controller

Answer: D

NO.4 Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

A. By default, Log Data Sync is disabled on all backup devise.

B. Log Data Sync provides real-time log synchronization to all backup devices.

C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its

logs with the backup device.
D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.
Answer: C D

NO.5 You crested a playbook on FortiAnalyzer that uses a FortiOS connector
When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?
A. FortiAnalyzer Event Handler
B. Incoming webhook
C. FortiOS Event Log
D. Fabric Connector event
Answer: C
Explanation:
"One possible scenario is shown on the slide:
1. Traffic flows through the FortiGate
2. FortiGate sends logs to FortiAnalyzer
3. FortiAnalyzer detects some suspicious traffic and generates an event
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
5. FortiGate runs the automation stitch with the corrective or preventive actions"
FortiAnalyzer_7.0_Study_Guide-Online page 228 In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side. FortiAnalyzer_7.0_Study Guide page no 233

NO.6 Which statement describes online logs on FortiAnalyzer?
A. Logs that reached a specific size and were rolled over
B. Logs that can be used to create reports
C. Logs that can be viewed using Log Browse
D. Logs that are saved to disk, compressed, and available in FortiView
Answer: B

NO.7 An administrator has configured the following settings:
config system global
set log-checksum md5-auth
end
What is the significance of executing this command?
A. This command records the log file MD5 hash value.
B. This command records passwords in log files and encrypts them.
C. This command encrypts log transfer between FortiAnalyzer and other devices.
D. This command records the log file MD5 hash value and authentication code.
Answer: D

NO.8 In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices

arenotresolving to a hostname.
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?
A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
B. Configure# set resolve-ip enablein the system FortiView settings
C. Configure local DNS servers on FortiAnalyzer
D. Resolve IP addresses on FortiGate
Answer: D
Explanation:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/
"As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only"

NO.9 Why run the command diagnose sql status sqlplugind?
A. To list the current SQL processes running
B. To check what is the database log insertion status
C. To display the SOL query connections and hcache status
D. To view the current hcache size
Answer: D

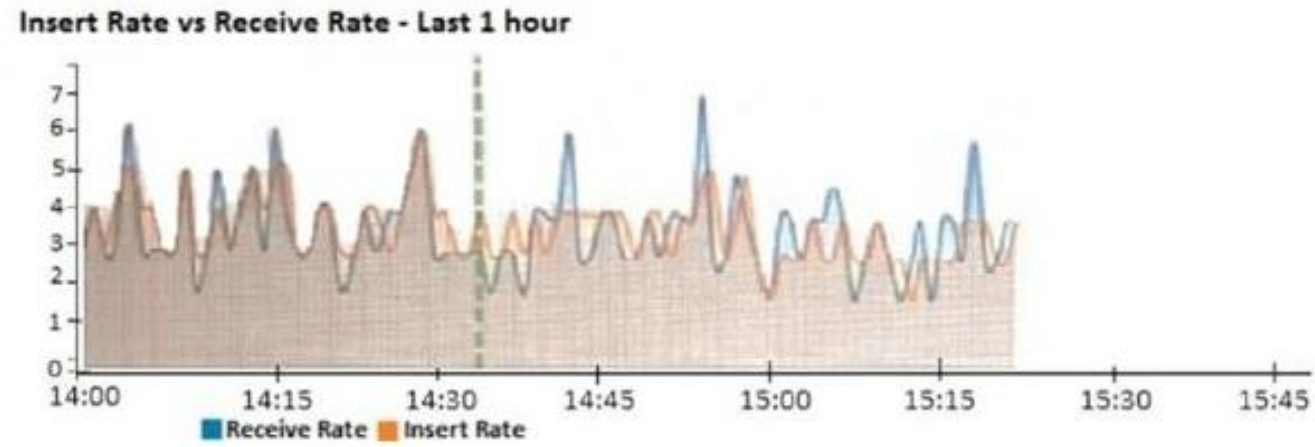
NO.10 What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?
A. The log file is stored as a raw log and is available for analytic support.
B. The log file rolls over and is archived.
C. The log file is purged from the database.
D. The log file is overwritten.
Answer: B

NO.11 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.
Answer: C
Explanation:
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

NO.12 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.
Answer: B D

NO.13 View the exhibit.



What does the data point at 14:35 tell you?
A. FortiAnalyzer is dropping logs.
B. FortiAnalyzer is indexing logs faster than logs are being received.
C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
D. The sqlplugind daemon is ahead in indexing by one log.
Answer: B
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wid

NO.14 The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?
A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.
Answer: C