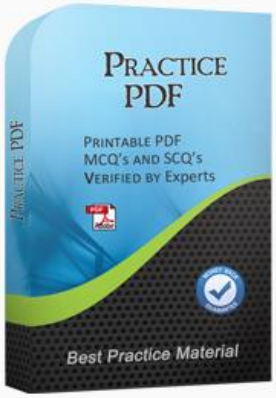
SurePassExams

SurePassExams

- 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.

http://www.surepassexams.com/

Legal & authoritative company offering the highest pass-rate Exam Torrent materials and helping use pass for sure.

Exam : **NSE5_FAZ-7.0**

Title : Fortinet NSE 5 - FortiAnalyzer 7.0

Vendor : Fortinet

Version : DEMO

NO.1 On the RAID management page, the disk status is listed as Initializing.
What does the status Initializing indicate about what the FortiAnalyzer is currently doing?
A. FortiAnalyzer is functioning normally
B. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
C. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
D. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
Answer: D
Reference:
8977-00505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

NO.2 An administrator has moved FortiGate A from the root ADOM to ADOM1.
Which two statements are true regarding logs? (Choose two.)
A. Logs will be presented in both ADOMs immediately after the move.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.
D. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
Answer: B,C

NO.3 View the exhibit.

```
Total Quota Summary:
     Total Quota    Allocated   Available   Allocate%
        63.7GB        12.7GB      51.0GB       19.9%

System Storage Summary:
     Total      Used       Available      Use%
    78.7GB     2.9GB        75.9GB       3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?
A. 3.6% of the system storage is already being used.
B. The logfiled process is just estimating the total quota
C. The oftpd process has not archived the logs yet
D. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
Answer: D
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

NO.4 How does FortiAnalyzer retrieve specific log data from the database?
A. SQL EXTRACT statement
B. SQL SELECT statement
C. SQL FROM statement

D. SQL GET statement

Answer: C

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b856/fortianalyzer-fortigate-sql-technote-40-mr2.pdf

NO.5 Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains

B. Security Fabric

C. Administrative access profiles

D. Trusted hosts

Answer: C,D

Reference:
https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts

NO.6 You need to upgrade your FortiAnalyzer firmware.
What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

A. The logfiled process stores logs in offline mode

B. FortiAnalyzer uses log fetching to retrieve the logs when back online

C. FortiGate uses the miglogd process to cache the logs

D. Logs are dropped

Answer: C

NO.7 Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are supported only on the FortiGate ADOM.

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

Answer: B

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

NO.8 Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

A. IM

B. Email

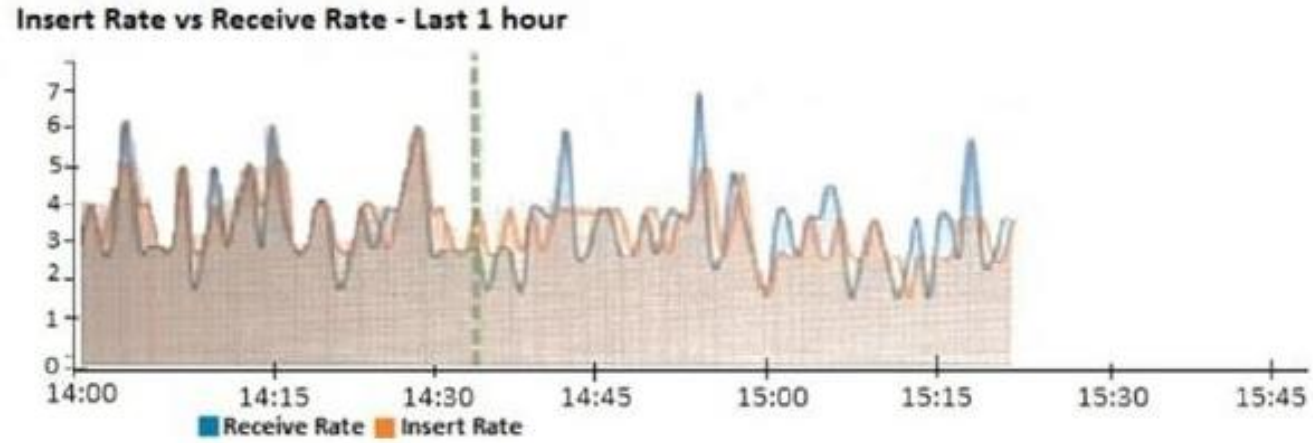
C. SNMP

D. SMS

Answer: B,C

Reference:
FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

NO.9 View the exhibit.



What does the data point at 14:35 tell you?

A. FortiAnalyzer is dropping logs.

B. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.

C. FortiAnalyzer is indexing logs faster than logs are being received.

D. The sqlplugind daemon is ahead in indexing by one log.

Answer: C

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-widget

NO.10 What are offline logs on FortiAnalyzer?

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

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

Answer: D

Reference:

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