

PrepAwayExam

PrepAwayExam

> Contact Us

Login / Register

Search...



HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

CART (0)

Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.

Try **Online Engine** before you buy

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.

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 60 days after purchasing. And Free get any another product.



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.

<http://www.prepawayexam.com/>

High-efficient Exam Materials are the best high pass-rate Exam Dumps

Exam : **MA0-104**

Title : Intel Security Certified Product
Specialist-SIEM

Vendor : McAfee

Version : DEMO

NO.1 Which of the following are the three default users defined within the Users and Groups option in the ESM properties?

- A. NGCP, BACKUP, REPORT
- B. NGCP, SYSTEM, REPORT
- C. ADMIN, POLICY, REPORT
- D. NGCP, POLICY, REPORT

Answer: B

NO.2 When viewing the Policy Tree, what four columns are displayed within the Rules Display pane?

- A. Action, Severity, Aggregation, Copy Packet
- B. Action, Severity, Normalization, Copy Packet
- C. Action, Severity, Aggregation, Drop Packet
- D. Enable, Severity, Aggregation, Copy Packet

Answer: A

NO.3 The McAfee SIEM solution satisfies which of the following compliance requirements?

- A. Continuous monitoring, Log retention
- B. Personally Identifiable Information (PII) protection
- C. Payment Card Industry/ Data Security Standard (PCI/ DSS) protection
- D. Patch management automation

Answer: A

NO.4 When the automated system backup is configured to include events, flows and log data, the first backup

will capture all events, flows and logs

- A. in the ESM database.
- B. in the ESM database older than what is currently held in the Receivers.
- C. inserted in the ESM database on the most recent Receiver poll.
- D. in the ESM database from the current day.

Answer: D

NO.5 The Database Event Monitor (OEM) appliance prevents disclosure of Personally Identifiable Information

(PII) by employing which of the following features to those types of information?

- A. Obfuscation masks
- B. PII filter masks
- C. Sensitive data masks
- D. Filter masks

Answer: C

NO.6 A security administrator is configuring the Enterprise Security Manager (ESM) to comply with corporate

security policy and wishes to restrict access to the ESM to certain users and machines

Which of the following actions would accomplish this?

- A. Configure the Access Control List and setup user accounts
- B. Define user groups and set permissions based on IP
- C. Assign AD users to computer assignment groups

D. Setup local accounts based on IP Zones

Answer: A