Boost up Your Certification Score

Fortinet

FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

Exams Boost

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/fcp-faz-an-7-6

Latest Version: 9.4

Question: 1

Which log will generate an event with the status Unhandled?

A. An AV log with action=quarantine.
B. An IPS log with action=pass.
C. A WebFilter log with action=dropped.
D. An AppControl log with action=blocked.

Answer: B

Explanation:
Study Guide p.82: "Unhandled" means the security event risk is not mitigated or contained, and an IPS/AV pass action is an example.
Technical Deep Dive: The correct answer is B because an IPS log with action=pass means the traffic matched or was observed in a way that generated a security event, but the traffic was not blocked, dropped, or quarantined. FortiAnalyzer therefore treats the event as still open from a SOC workflow perspective. Option A is wrong because quarantine isolates the malicious object and maps to Contained. Options C and D are wrong because dropped or blocked actions mean enforcement already occurred, which maps to Mitigated rather than Unhandled.

Question: 2

Exhibit.

Event	Event Status	Event Type	Severity
bujyqttatbsd.findhere.org (1)	Mitigated	Web Filter	Low
Web request to suspicious destination from 10.0.3.20 blocked	Mitigated	Web Filter	Low

Which statement about the event displayed is correct?

A. The risk source is isolated.
B. The security risk was blocked or dropped.
C. The security event risk is considered open.
D. An incident was created from this event.

Answer: C

Explanation:
Study Guide p.82: "Unhandled" indicates the security event risk is considered open.

Technical Deep Dive: The displayed event is best interpreted as open/unhandled, so the correct answer is C. In FortiAnalyzer, event status is not just a label; it tells the analyst whether the risk still requires action. A risk source being isolated would map to Contained, while traffic being blocked or dropped maps to Mitigated. An incident being created from an event is a separate workflow action and cannot be concluded from the event status alone unless the exhibit explicitly shows the incident linkage.

Question: 3

Which statement describes archive logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL database
B. Logs a FortiAnalyzer administrator can access in FortiView
C. Logs compressed and saved in files with the .gz extension
D. Logs previously collected from devices that are offline

Answer: C

Explanation:
Study Guide p.39: rolled log files are compressed, receive the .gz extension, and are known as archive logs.
Technical Deep Dive: The correct answer is C. FortiAnalyzer stores received logs first as log files and also indexes them for analytics. When the log file rolls over, FortiAnalyzer renames it, timestamps it, and compresses it into a .gz file. That compressed offline file is the archive log. Option A describes analytics logs in the SQL database. Option B is wrong because FortiView uses analytics logs, not archive logs. Option D confuses archive status with device availability; a log is archived because of the storage workflow, not because the source device is offline.

Question: 4

Which statement about sending notifications with incident update is true?

A. You can send notifications to multiple external platforms.
B. Notifications can be sent only by email.
C. If you use multiple fabric connectors, all connectors must have the same settings.
D. Notifications can be sent only when an incident is updated or deleted.

Answer: A

Explanation:
Study Guide p.107: FortiAnalyzer can send incident notifications to external platforms using Fabric connectors; more than one connector can be added.

Technical Deep Dive: The correct answer is A. Incident update notifications are not restricted to email. FortiAnalyzer can use configured Fabric connectors to notify external collaboration or response platforms, and each connector can be configured for the incident activities that should trigger a notification. Option B is too narrow because email is only one possible delivery model. Option C is wrong because multiple connectors do not have to share identical settings. Option D is wrong because notification triggers are configurable for different incident activities, not only update or delete events.

Question: 5

Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate.
B. It runs as a docker container on FortiAnalyzer.
C. It requires a dedicated FortiSOAR device or VM.
D. It does not include a limited trial by default.

Answer: B

Explanation:
Official Fortinet Administration Guide: Management Extension Applications are installed and run on FortiAnalyzer; CLI options include enabling the fortisoar container.
Technical Deep Dive: The correct answer is B. FortiSOAR MEA is a management extension application hosted by FortiAnalyzer, not a separate FortiSOAR appliance requirement for this question. FortiAnalyzer uses Docker-based MEA support, and FortiSOAR MEA is one of the supported extensions. Option A is wrong because FortiManager is not required just to run the FortiSOAR MEA. Option C describes a standalone FortiSOAR deployment, not the management extension. Option D is wrong because Fortinet documents FortiSOAR MEA trial licensing behavior for evaluation use.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer