DUMPSARENA

Fortinet NSE 6FortiAnalyzer 7.2 Administrator

Fortinet NSE6_FAZ-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment and System Configuration	6
Topic 2, Device Management	4
Topic 3, Logs and Reports	11
Topic 4, Event Management	2
Total	23

QUESTION NO: 1

Which two statements about event handlers are true? (Choose two.)

A. Event handlers can be triggered when generated events match their event filters.

B. Event filters can be used to narrow the events evaluated by an event handler.

C. Event handlers are triggered directly by every raw log received from a managed device.

D. Event handlers automatically generate a scheduled report when an event occurs.

ANSWER: A B

Explanation:

Event handlers are triggered by matching events, not directly by every incoming raw log. **Event filters define the event conditions that are evaluated by an event handler**, allowing the administrator to target relevant events before an action is performed.

Reports are generated from report definitions and schedules, not by event handlers. Enabling a handler alone also does not create events; event management must first identify events from the processed logs.

QUESTION NO: 2

A FortiGate was registered successfully with FortiAnalyzer today. The administrator now needs FortiAnalyzer to obtain historical logs that remain stored locally on the FortiGate from before the registration. Which action should the administrator use?

A. Perform a log fetch from the FortiGate.

B. Restart the FortiGate logging process.

C. Generate an on-demand report for the required time period.

D. Reauthorize the FortiGate in the Device Manager.

ANSWER: A

Explanation:

Perform a log fetch from the FortiGate. is correct because log fetching retrieves previously stored logs from a managed device and imports them into FortiAnalyzer.

Waiting for normal log forwarding only receives newly generated logs. Restarting the FortiGate logging process or generating a report does not transfer the historical logs retained on the FortiGate.