PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 5 - FortiAnalyzer 7.2

Fortinet NSE5_FAZ-7.2

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiAnalyzer system settings	2
Topic 2, FortiAnalyzer device management	7
Topic 3, FortiAnalyzer logs and reports	8
Topic 4, FortiAnalyzer event management	3
Topic 5, FortiAnalyzer SOC features	3
Total	23

QUESTION NO: 1

What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. logfiled

B. sqlplugind

C. oftpd

D. miglogd

ANSWER: D

Explanation:

miglogd is the FortiGate daemon that manages communication with FortiAnalyzer and provides log spooling when that remote logging destination cannot be reached. Rather than immediately discarding log records during a temporary connectivity failure, it retains them in the FortiGate log cache and forwards the queued records after FortiAnalyzer connectivity is restored. This behavior helps preserve log continuity for reporting, event investigation, and compliance purposes, provided that sufficient local storage is available and the outage does not outlast the configured cache capacity. Administrators can monitor the status of logging and FortiAnalyzer connectivity from FortiGate and should ensure that reliable network connectivity and adequate disk or memory logging resources are configured for the deployment. Fortinet documentation describes FortiGate logging behavior and its integration with external FortiAnalyzer logging, while Fortinet's technical discussion specifically identifies miglogd as the process responsible for caching logs when FortiAnalyzer is unavailable. See the FortiGate 7.2 documentation and the related Fortinet technical forum reference.

QUESTION NO: 2

A weekly report is scheduled to run every Monday at 01:00. The report configuration uses the last seven days as its time period. Which logs are included when the report runs?

A. Only logs received after the previous report was generated

B. Only logs from the previous calendar week

C. All logs stored in the ADOM

D. Logs from the seven-day period preceding the scheduled run time

ANSWER: D

Explanation:

FortiAnalyzer evaluates a relative time period when the report is generated. Therefore, a report configured for the last seven days includes the logs that fall within the seven-day period immediately preceding the scheduled run time. It does not permanently use the time range that existed when the report was created.