

NSE5_FAZ-7.0^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse5_faz-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

How can you configure FortiAnalyzer to permit administrator logins from only specific locations?

- A. Use static routes
- B. Use administrative profiles
- C. Use trusted hosts
- D. Use secure protocols

Correct Answer: C

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/186508/trusted-hosts>

QUESTION 2

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
- B. Logs and content files are stored and uploaded at a scheduled time.
- C. Logs are forwarded as they are received.
- D. Logs and content files are forwarded as they are received.

Correct Answer: B

<https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/>
<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes> Reference:
<https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is-the-difference-between-log-forward-and-log-aggregation-modes>

QUESTION 3

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

Correct Answer: D

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnaly>

zer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running ?known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

Reference: <https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/tap/194997?externalID=FD41397#:~:text=If%20a%20hard%20disk%20on,process%20know n%20as%20hot%20swapping>

QUESTION 4

When working with FortiAnalyzer reports, what is the purpose of a dataset?

- A. To provide the layout used for reports
- B. To define the chart type to be used
- C. To retrieve data from the database
- D. To set the data included in templates

Correct Answer: C

FortiAnalyzer_7.0_Study_Guide-Online pag. 257 Reference:
<https://docs2.fortinet.com/document/fortianalyzer/6.0.4/administration-guide/148744/creating-datasets>

QUESTION 5

You crested a playbook on FortiAnalyzer that uses a FortiOS connector

When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

- A. FortiAnalyzer Event Handler
- B. Incoming webhook
- C. FortiOS Event Log
- D. Fabric Connector event

Correct Answer: B

"One possible scenario is shown on the slide:

1.

Traffic flows through the FortiGate

2.

FortiGate sends logs to FortiAnalyzer

3.

FortiAnalyzer detects some suspicious traffic and generates an event

4.

The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch

5.

FortiGate runs the automation stitch with the corrective or preventive actions"

[NSE5_FAZ-7.0 PDF Dumps](#)

[NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 Braindumps](#)