



NSE5_FAZ-6.4^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 6.4

Pass Fortinet NSE5_FAZ-6.4 Exam with 100% Guarantee

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

https://www.passapply.com/nse5_faz-6-4.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

What statements are true regarding FortiAnalyzer's treatment of high availability (HA) clusters? (Choose two)

- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from all devices in a cluster.
- C. FortiAnalyzer receives logs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know the serial number of the primary device in the cluster-it automatically discovers the other devices.

Correct Answer: AB

QUESTION 2

What is the purpose of a predefined template on the FortiAnalyzer?

- A. It can be edited and modified as required
- B. It specifies the report layout which contains predefined texts, charts, and macros
- C. It specifies report settings which contains time period, device selection, and schedule
- D. It contains predefined data to generate mock reports

Correct Answer: B

Reference:

<https://help.fortinet.com/fa/faz50hlp/56/5-6-2/>

FMGFAZ/2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%

20number%20of,create%20and%20For%20build%20reports.andtext=A%20template%20populates%20the %
20Layout,that%20is%20to%20be%20created.

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

<https://docs2.fortinet.com/document/fortianalyzer/6.0.8/administration-guide/618245/predefined-reportstemplates-charts-and-macros>

QUESTION 3

View the exhibit.



```
Total Quota Summary:
  Total Quota   Allocated   Available   Allocate%
    63.7GB      12.7GB      51.0GB      19.9%

System Storage Summary:
  Total   Used   Available   Use%
 78.7GB  2.9GB   75.9GB     3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?

- A. 3.6% of the system storage is already being used.
- B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
- C. The oftpd process has not archived the logs yet
- D. The logfiled process is just estimating the total quota

Correct Answer: B

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

QUESTION 4

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

- A. Antivirus logs
- B. Web filter logs
- C. IPS logs
- D. Application control logs

Correct Answer: B

Reference:

<https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/>

[FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6](https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6)

QUESTION 5



FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.

What is the most likely problem?

- A. Quota enforcement is acting on analytical data before a report is complete
- B. Logs are rolling before the report is run
- C. CPU resources are too high
- D. Disk utilization for archive logs is set for 15 days

Correct Answer: B

Reference: <https://forum.fortinet.com/tm.aspx?m=138806>

[NSE5 FAZ-6.4 PDF Dumps](#) [NSE5 FAZ-6.4 VCE Dumps](#)

[NSE5 FAZ-6.4 Practice Test](#)