

## NSE5\_FAZ-6.2<sup>Q&As</sup>

Fortinet NSE 5 - FortiAnalyzer 6.2

### Pass Fortinet NSE5\_FAZ-6.2 Exam with 100% Guarantee

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

[https://www.leads4pass.com/nse5\\_faz-6-2.html](https://www.leads4pass.com/nse5_faz-6-2.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**

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

---

**QUESTION 2**

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

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

Correct Answer: AB

---

**QUESTION 3**

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

Correct Answer: AC

---

#### QUESTION 4

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What devices and IP addresses are connecting to FortiAnalyzer
- B. What logs, if any, are reaching FortiAnalyzer
- C. What ADOMs are enabled and configured
- D. What devices are registered and unregistered

Correct Answer: A

---

#### QUESTION 5

What are the operating modes of FortiAnalyzer? (Choose two)

- A. Standalone
- B. Manager
- C. Analyzer
- D. Collector

Correct Answer: CD

---

#### QUESTION 6

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?

execute sql-local rebuild-adom

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM

D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Correct Answer: B

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.0.2/cli-reference/551596/sql-local>

---

### QUESTION 7

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

- A. The log file is stored as a raw log and is available for analytic support.
- B. The log file rolls over and is archived.
- C. The log file is purged from the database.
- D. The log file is overwritten.

Correct Answer: B

Reference: <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a400505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf>

---

### QUESTION 8

On FortiAnalyzer, what is a wildcard administrator account?

- A. An account that permits access to members of an LDAP group
- B. An account that allows guest access with read-only privileges
- C. An account that requires two-factor authentication
- D. An account that validates against any user account on a FortiAuthenticator

Correct Answer: D

---

### QUESTION 9

Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

- A. ADOMs are enabled by default.
- B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
- C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
- D. All administrators can create ADOMs--not just the admin administrator.

Correct Answer: BC

---

**QUESTION 10**

View the exhibit:

Data Policy

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

Disk Utilization

Maximum Allowed: 1000 MB

Analytics: Archive: 70%

Alert and Delete When Usage Reaches: 90%

Out of Available: 62.8 GB

Modify

What does the 1000MB maximum for disk utilization refer to?

- A. The disk quota for the FortiAnalyzer model
- B. The disk quota for all devices in the ADOM
- C. The disk quota for each device in the ADOM
- D. The disk quota for the ADOM type

Correct Answer: B

---

**QUESTION 11**

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend command to expand the storage
- B. From the VM host manager, expand the size of the existing virtual disk
- C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Correct Answer: A

---

**QUESTION 12**

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

Correct Answer: B

---

### QUESTION 13

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

- A. Principal
- B. Service provider
- C. Identity collector
- D. Identity provider

Correct Answer: BD

Reference: [https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/samladminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%20the%20identity%20provider%20\(IdP,external%20identity%20provider%20is%20available](https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/957811/samladminauthentication#:~:text=for%20the%20administrator.-,FortiAnalyzer%20can%20play%20the%20role%20of%20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available)

---

### QUESTION 14

If you upgrade the FortiAnalyzer firmware, which report element can be affected?

- A. Custom datasets
- B. Report scheduling
- C. Report settings
- D. Output profiles

Correct Answer: A

---

### QUESTION 15

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

- A. Remote logging must be enabled on FortiGate

- B. Log encryption must be enabled
- C. ADOMs must be enabled
- D. FortiGate must be registered with FortiAnalyzer

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."

<https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf> Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

[Latest NSE5\\_FAZ-6.2 Dumps](#)

[NSE5\\_FAZ-6.2 Practice Test](#)

[NSE5\\_FAZ-6.2 Braindumps](#)