

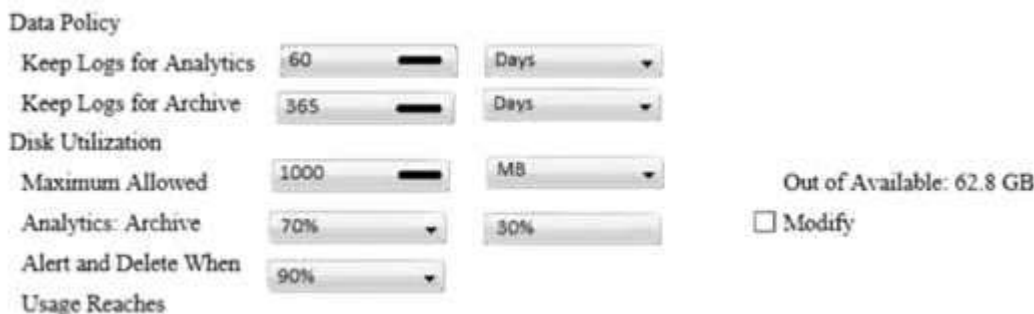
➤ **Vendor: Fortinet**➤ **Exam Code: NSE5_FAZ-7.0**➤ **Exam Name: Fortinet NSE 5 - FortiAnalyzer 7.0**➤ **New Updated Questions from [Braindump2go](#) (Updated in [October/2022](#))****Visit Braindump2go and Download Full Version NSE5_FAZ-7.0 Exam Dumps****QUESTION 1**

Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. License type
- B. Disk size
- C. Total quota
- D. RAID level

Answer: CD**Explanation:**<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>**QUESTION 2**

View the exhibit:



The screenshot shows the 'Data Policy' configuration page in FortiAnalyzer. It includes sections for 'Keep Logs for Analytics' (60 Days), 'Keep Logs for Archive' (365 Days), 'Disk Utilization' (Maximum Allowed: 1000 MB), 'Analytics: Archive' (70%), and 'Alert and Delete When Usage Reaches' (90%). A 'Modify' button is visible next to the 'Out of Available: 62.8 GB' status.

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

Answer: B**Explanation:**<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy>**[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)****[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)****<https://www.braindump2go.com/nse5-faz-7-0.html>**

QUESTION 3

You've moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

- A. FortiAnalyzer resets the disk quota of the new ADOM to default.
- B. FortiAnalyzer migrates archive logs to the new ADOM.
- C. FortiAnalyzer migrates analytics logs to the new ADOM.
- D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383>

QUESTION 4

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.

Answer: B

Explanation:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf>

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse>

QUESTION 5

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

Answer: A

Explanation:

[https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20\(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.](https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%20performance%20improvement%2C%20or%20both.)

QUESTION 6

Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

- A. Log upload
- B. Indicators of Compromise
- C. Log forwarding an aggregation mode
- D. Log fetching

Answer: D

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management>

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

QUESTION 7

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 <disk number> 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

Answer: A

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848>

QUESTION 8

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.

Answer: B

Explanation:

<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>

QUESTION 9

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom>

QUESTION 10

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

Answer: AD

QUESTION 11

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

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

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

QUESTION 12

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder>

QUESTION 13

In FortiAnalyzer's FormView, source and destination IP addresses from FortiGate devices are not resolving to a hostname. How can you resolve the source and destination IPs, without introducing any additional performance impact to FortiAnalyzer?

- A. Configure local DNS servers on FortiAnalyzer
- B. Resolve IPs on FortiGate
- C. Configure # set resolve-ip enable in the system FortiView settings
- D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Answer: B

QUESTION 14

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

- A. SFTP, FTP, or SCP server
- B. Mail server
- C. Output profile
- D. Report scheduling

Answer: AC

Explanation:

There is an option for "uploading reports to server" under configuring the output profile. The available options are: SFTP, FTP and SCP. You have to be careful on the question itself. The question tells you to "upload reports to a server (external server)". Which means, a server has been configured already in this case prior to enabling the "upload reports to server".

QUESTION 15

[NSE5_FAZ-7.0 Exam Dumps](#) [NSE5_FAZ-7.0 Exam Questions](#)

[NSE5_FAZ-7.0 PDF Dumps](#) [NSE5_FAZ-7.0 VCE Dumps](#)

<https://www.braindump2go.com/nse5-faz-7-0.html>

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

Answer: B

Explanation:

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

QUESTION 16

What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate
- D. To provide diagnostics on report generation time

Answer: AB

Explanation:

Reference: <https://docs.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/282280/enabling-autocache>

QUESTION 17

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

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

Answer: D

QUESTION 18

How does FortiAnalyzer retrieve specific log data from the database?

- A. SQL FROM statement
- B. SQL GET statement

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>

- C. SQL SELECT statement
- D. SQL EXTRACT statement

Answer: A

Explanation:

<https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b856/fortianalyzer-fortigate-sql-technote-40-mr2.pdf>

QUESTION 19

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

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts>

QUESTION 20

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

Answer: D

[NSE5_FAZ-7.0 Exam Dumps](#) **[NSE5_FAZ-7.0 Exam Questions](#)**

[NSE5_FAZ-7.0 PDF Dumps](#) **[NSE5_FAZ-7.0 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-faz-7-0.html>