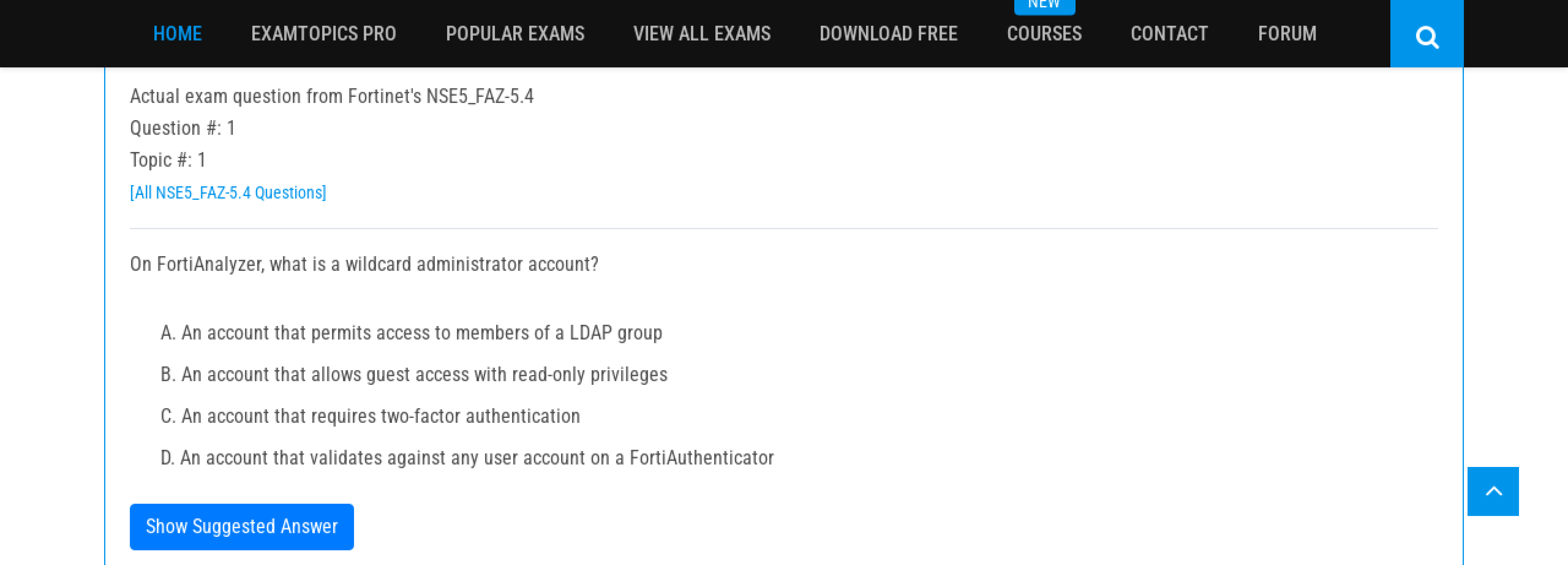


Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 1

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

On FortiAnalyzer, what is a wildcard administrator account?

A. An account that permits access to members of a 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

Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 2

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

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

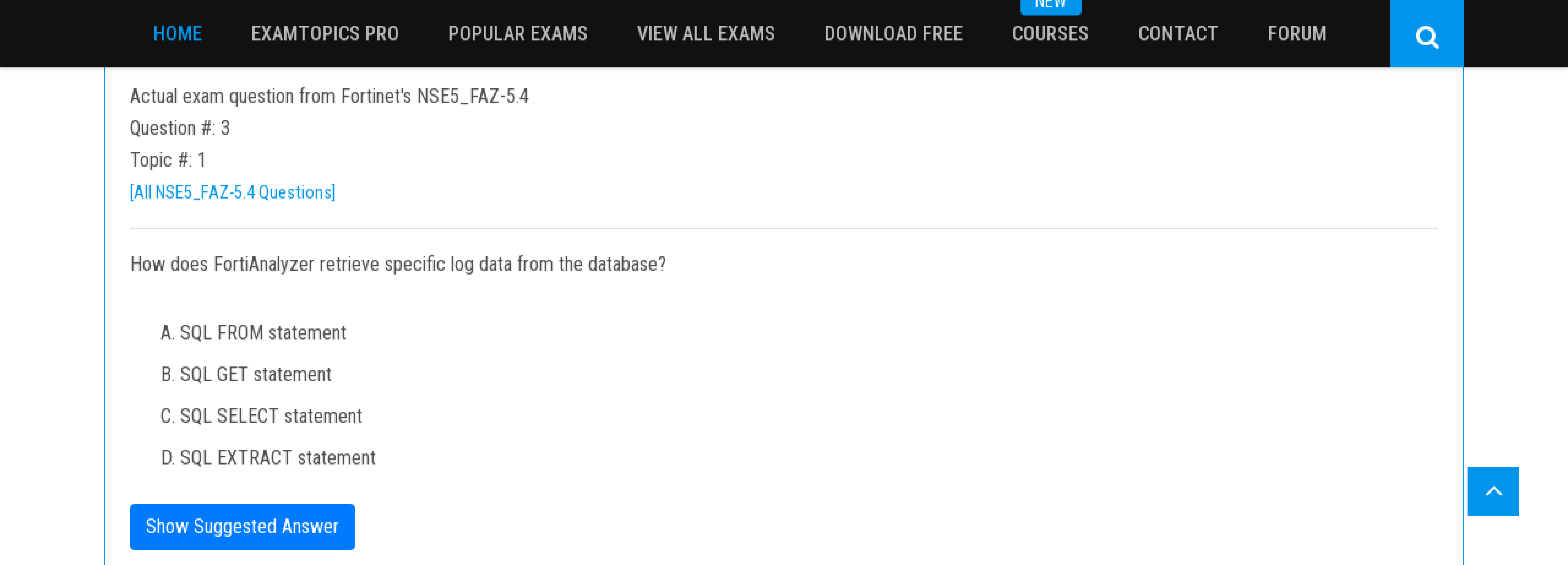
A. Log forwarding in aggregation mode

B. Log upload

C. Log fetching

D. Indicators of Compromise

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 3

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

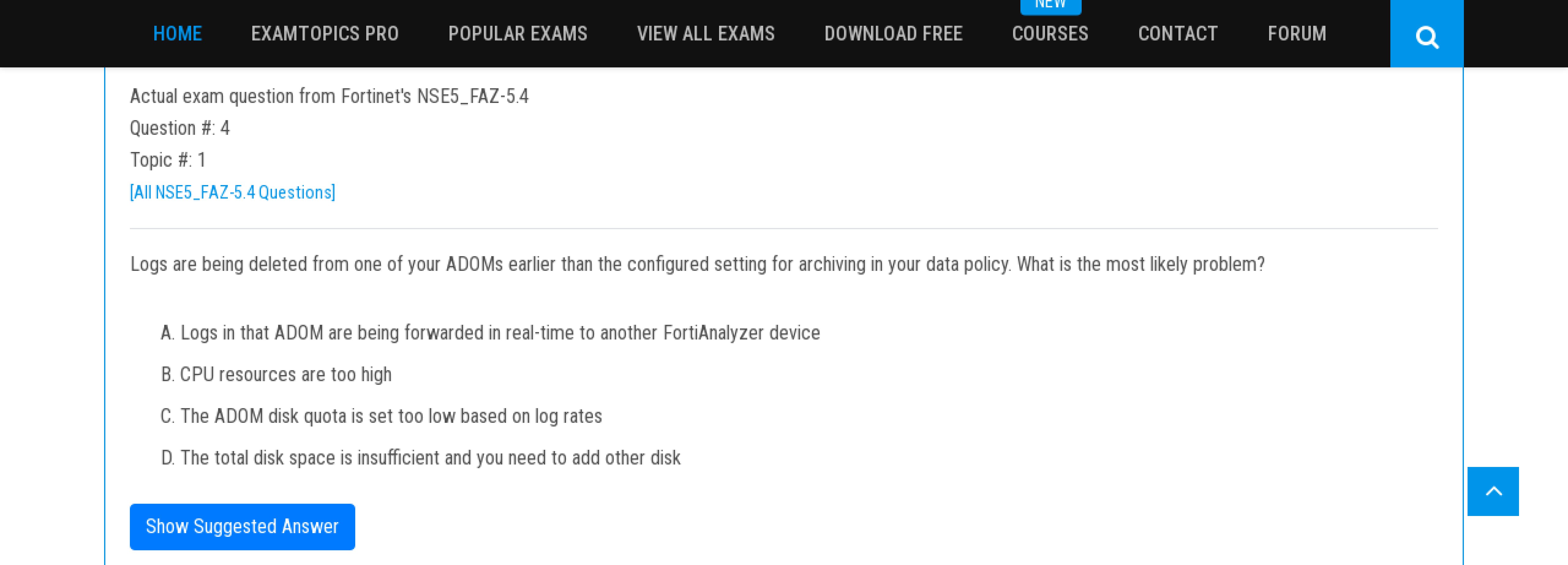
How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement

B. SQL GET statement

C. SQL SELECT statement

D. SQL EXTRACT statement



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 4

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

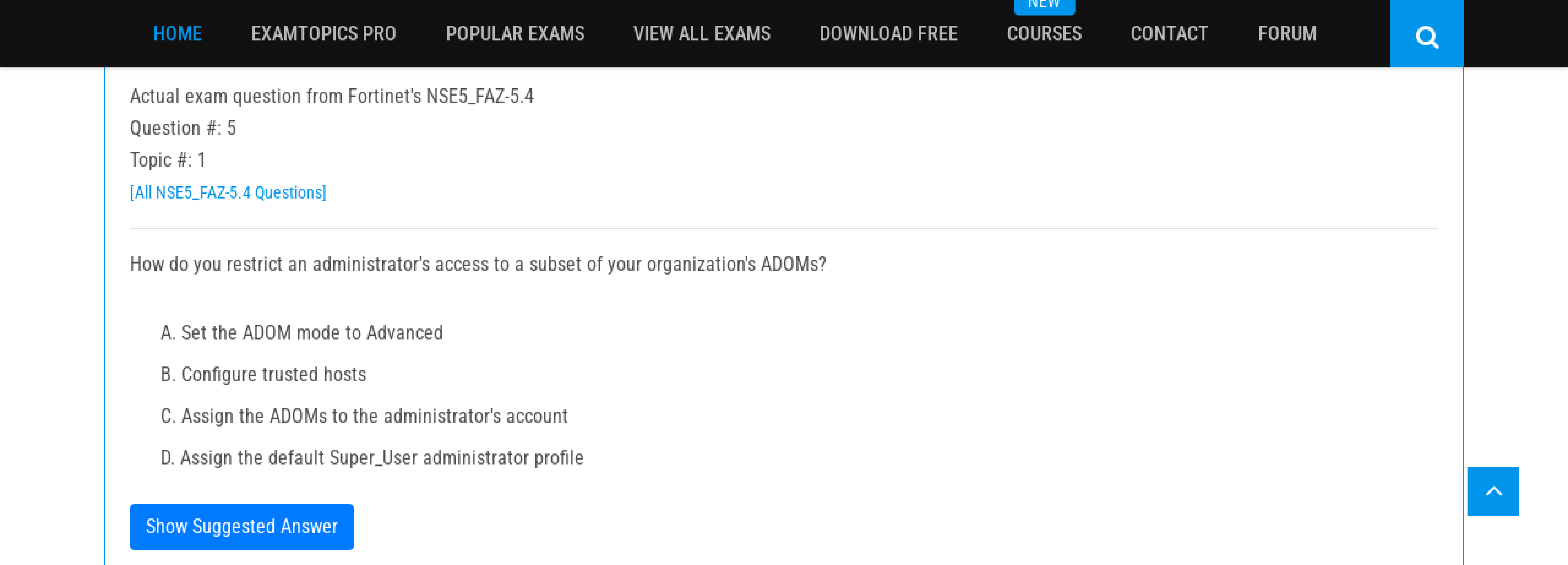
Logs are being deleted from one of your ADOMs earlier than the configured setting for archiving in your data policy. What is the most likely problem?

A. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device

B. CPU resources are too high

C. The ADOM disk quota is set too low based on log rates

D. The total disk space is insufficient and you need to add other disk



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 5

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

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

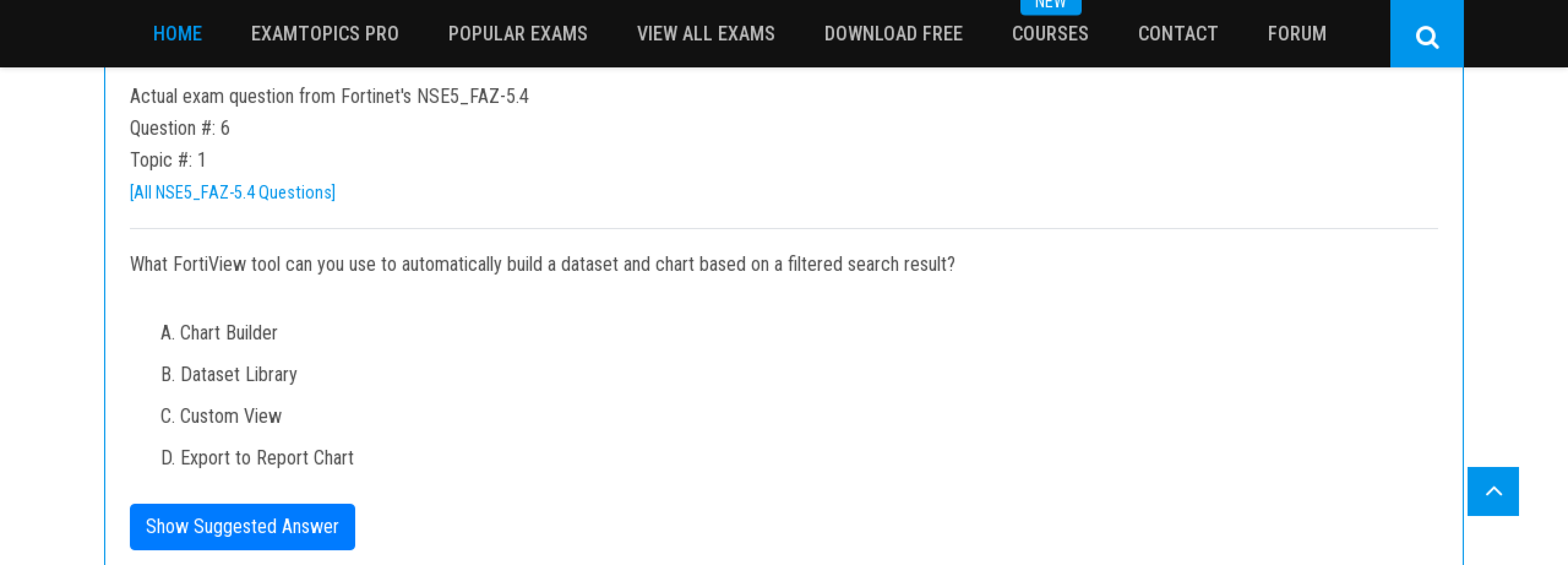
A. Set the ADOM mode to Advanced

B. Configure trusted hosts

C. Assign the ADOMs to the administrator's account

D. Assign the default Super_User administrator profile

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 6

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

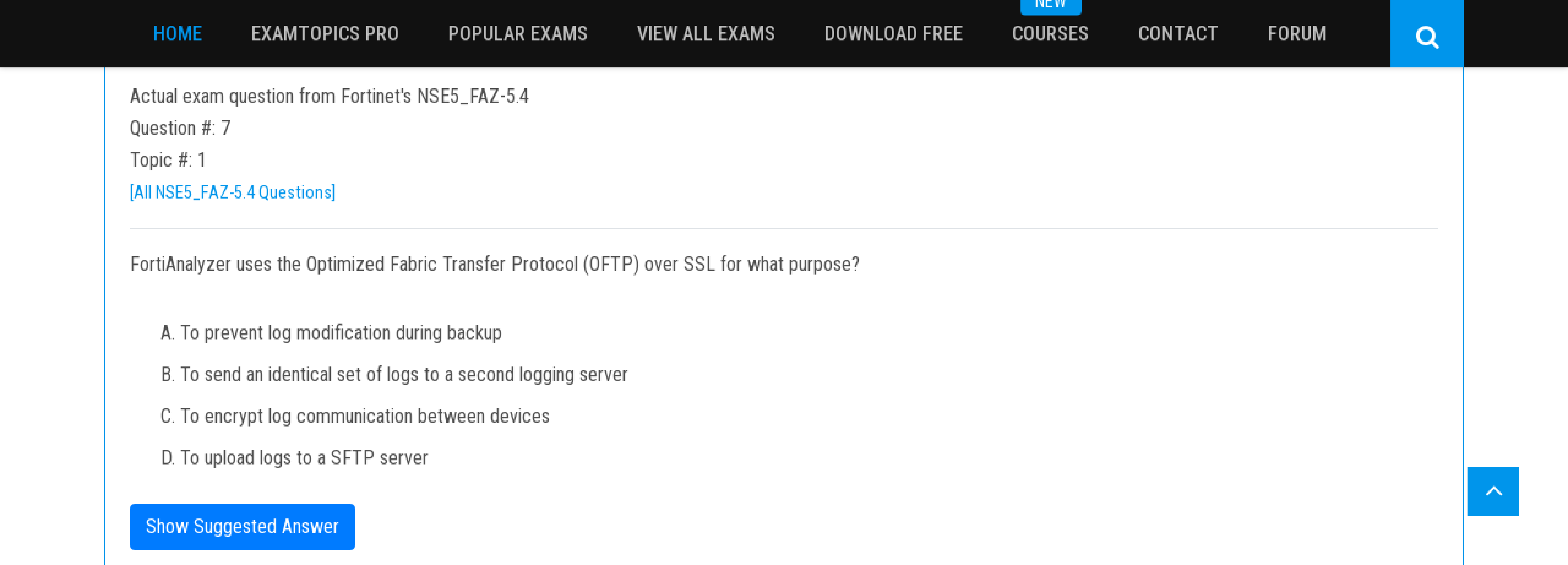
What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder

B. Dataset Library

C. Custom View

D. Export to Report Chart



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 7

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

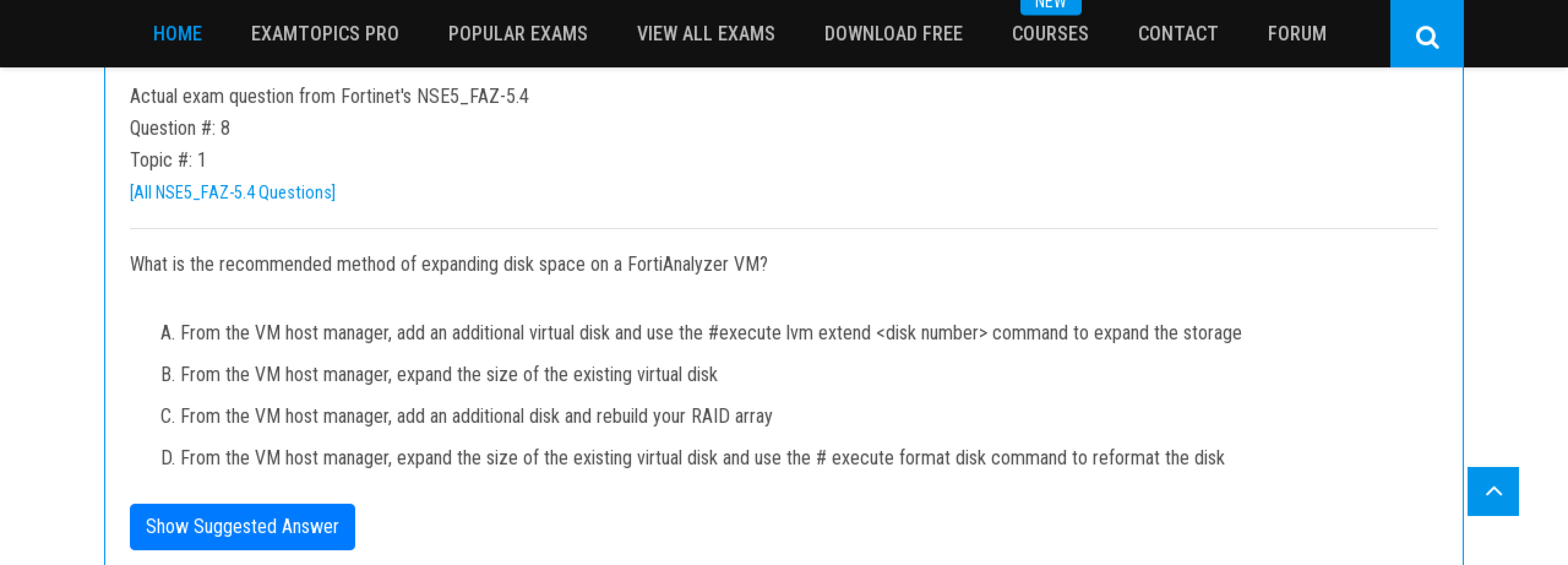
FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for what purpose?

A. To prevent log modification during backup

B. To send an identical set of logs to a second logging server

C. To encrypt log communication between devices

D. To upload logs to a SFTP server



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 8

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

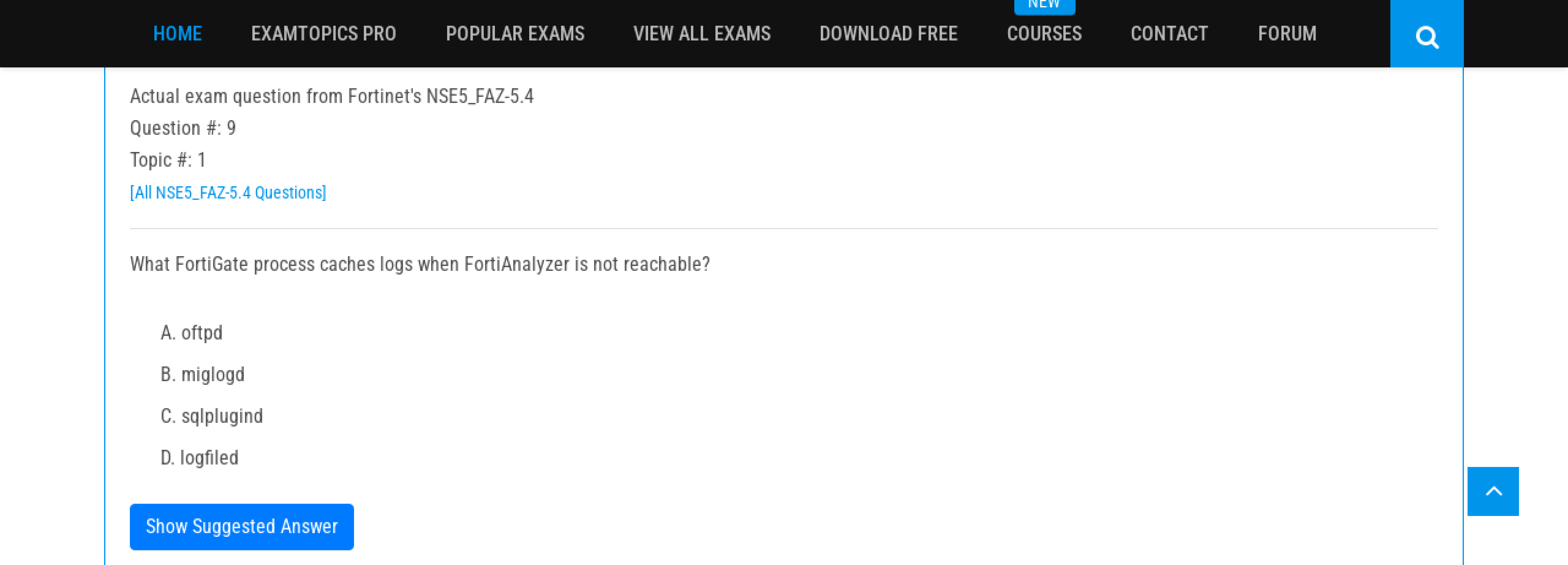
What is the recommended method of expanding disk space on a FortiAnalyzer VM?

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, add an additional disk and rebuild your RAID array

D. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 9

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

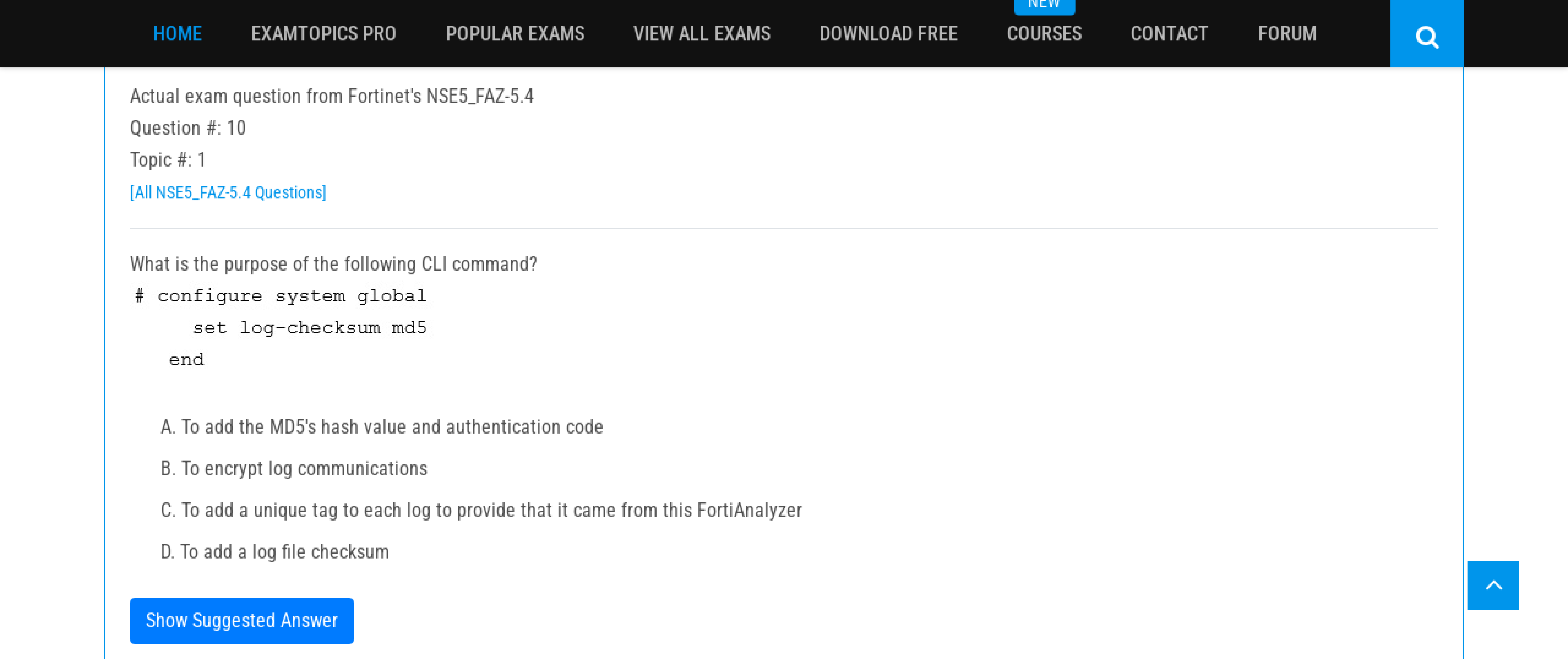
What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. oftpd

B. miglogd

C. sqlplugind

D. logfiled



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 10

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

What is the purpose of the following CLI command?

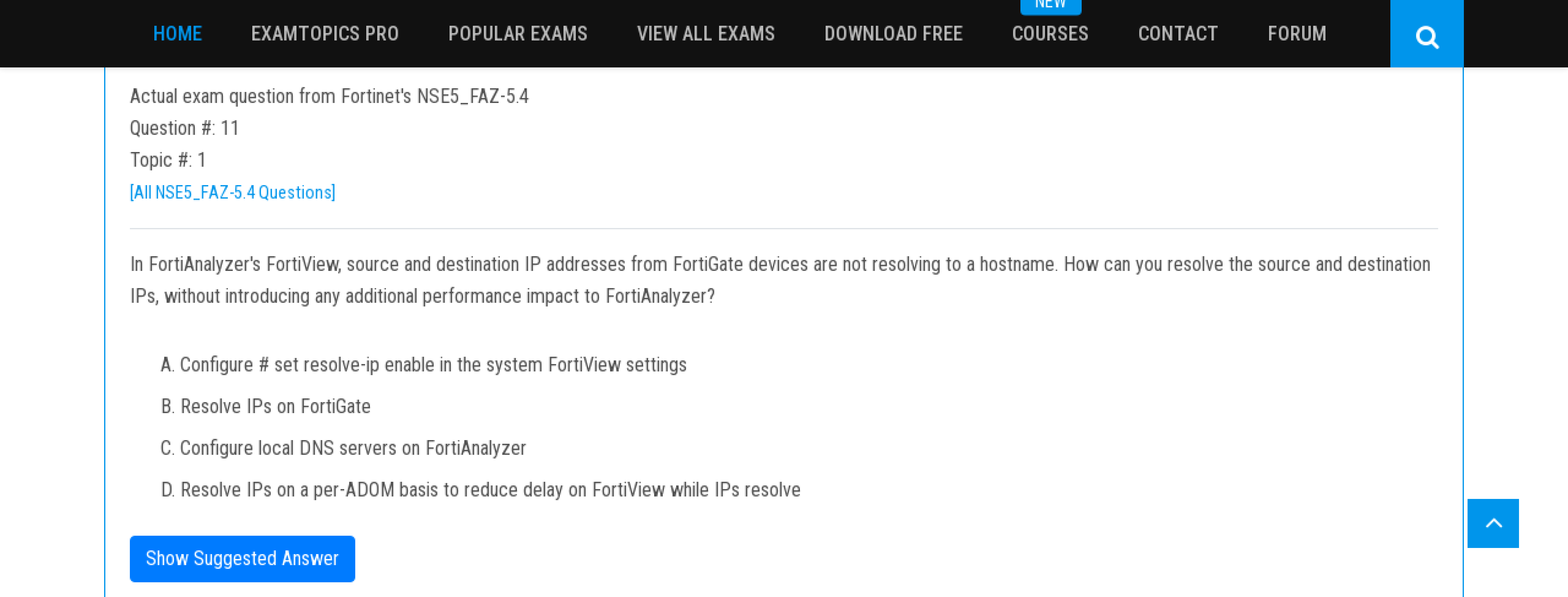
```
# configure system global
     set log-checksum md5
   end
```

A. To add the MD5's hash value and authentication code

B. To encrypt log communications

C. To add a unique tag to each log to provide that it came from this FortiAnalyzer

D. To add a log file checksum



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 11

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

In FortiAnalyzer's FortiView, 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 # set resolve-ip enable in the system FortiView settings

B. Resolve IPs on FortiGate

C. Configure local DNS servers on FortiAnalyzer

D. Resolve IPs on a per-ADOM basis to reduce delay on FortiView while IPs resolve

Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 12

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

What is the purpose of employing RAID with FortiAnalyzer?

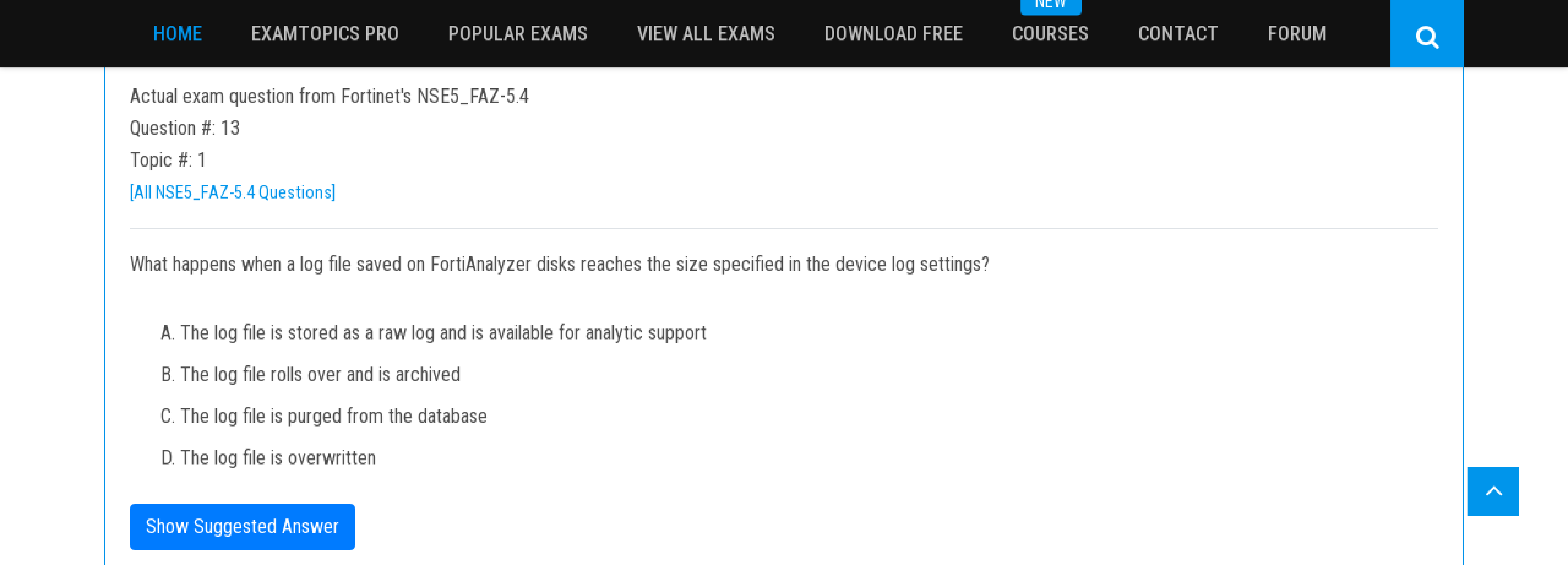
A. To provide data separation between ADOMs

B. To separate analytical and archive data

C. To back up your logs

D. To introduce redundancy to your log data

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 13

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

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

Show Suggested Answer

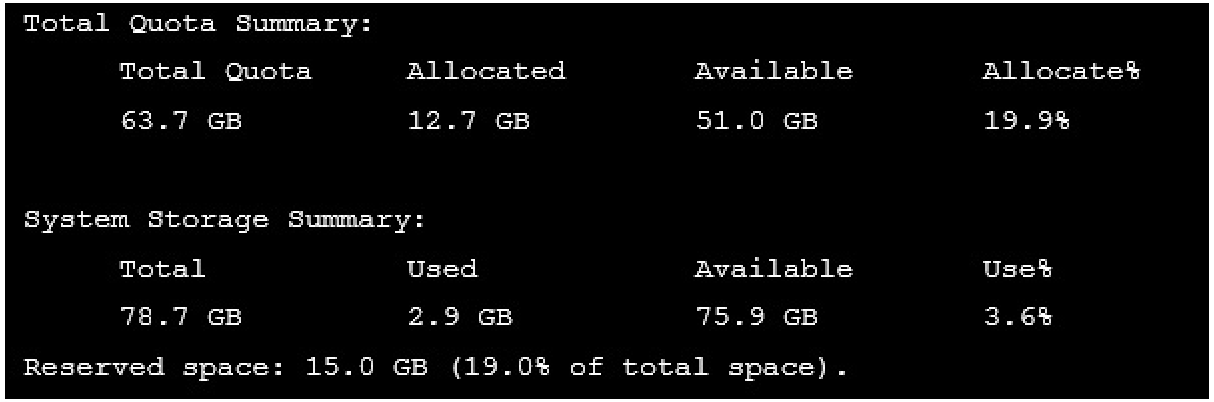
Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 14

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

View the exhibit.



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


System Storage Summary:
     Total           Used           Available      Use%
     78.7 GB         2.9 GB         75.9 GB        3.6%
Reserved space: 15.0 GB (19.0% of total space).
```

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

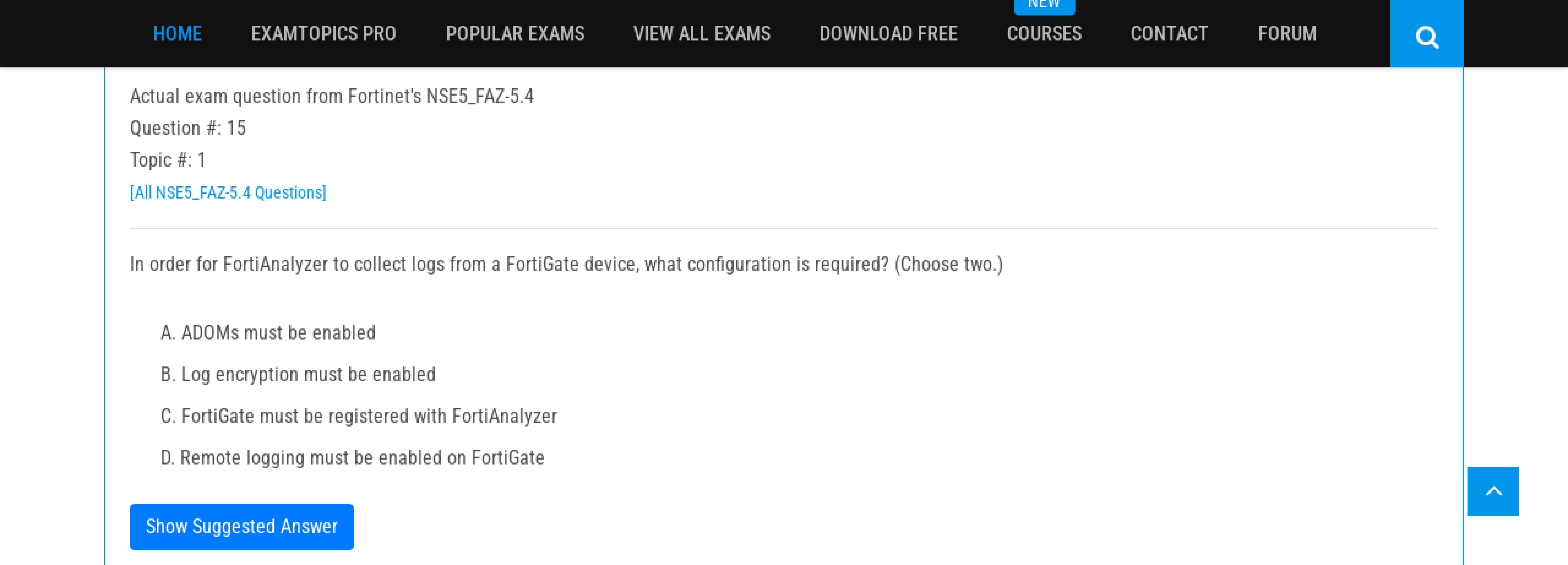
A. The oftpd process has not archived the logs yet

B. The logfiled process is just estimating the total quota

C. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

D. 3.6% of the system storage is already being used

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 15

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

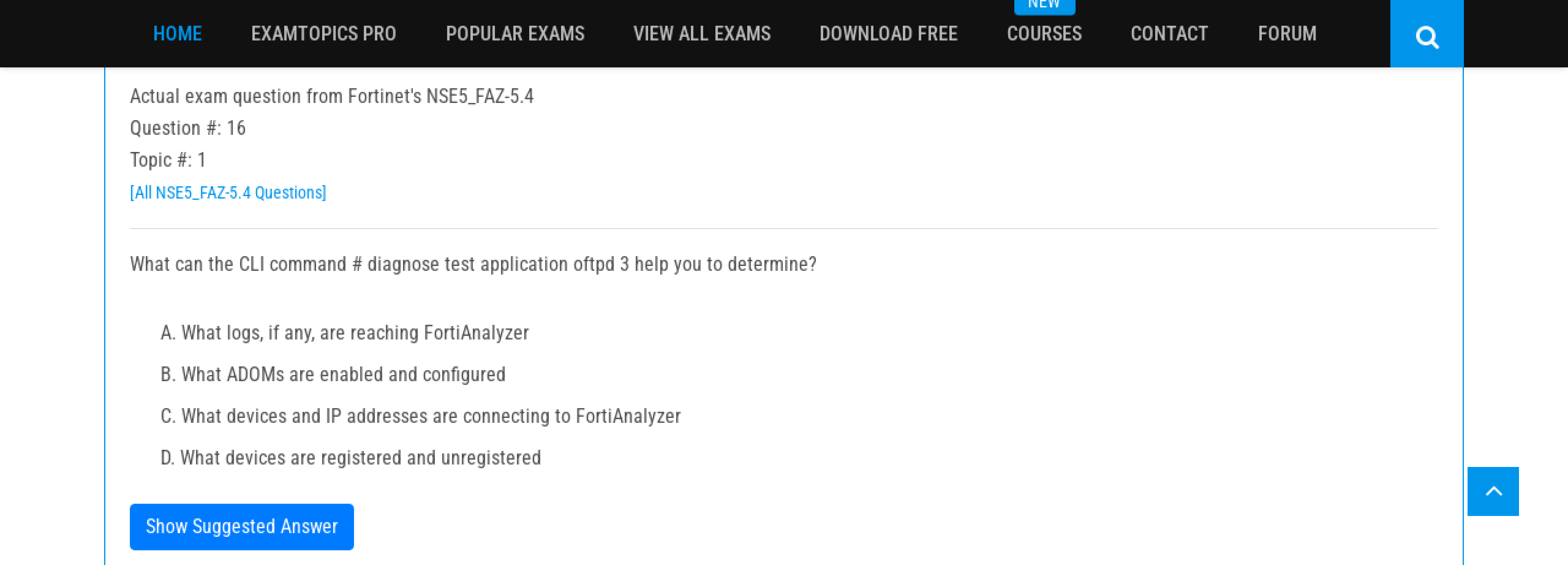
In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. ADOMs must be enabled

B. Log encryption must be enabled

C. FortiGate must be registered with FortiAnalyzer

D. Remote logging must be enabled on FortiGate



Actual exam question from Fortinet's NSE5_FAZ-5.4

Question #: 16

Topic #: 1

[All NSE5_FAZ-5.4 Questions]

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

A. What logs, if any, are reaching FortiAnalyzer

B. What ADOMs are enabled and configured

C. What devices and IP addresses are connecting to FortiAnalyzer

D. What devices are registered and unregistered

Show Suggested Answer