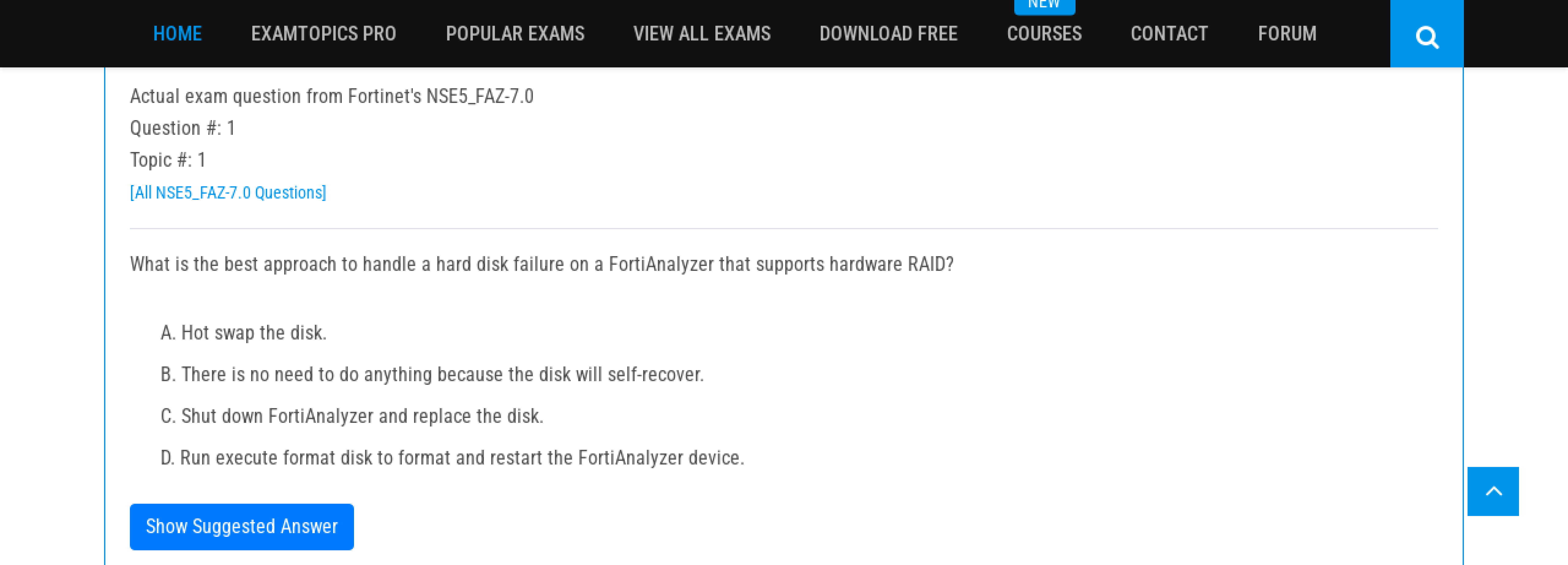


Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 1

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Hot swap the disk.

B. There is no need to do anything because the disk will self-recover.

C. Shut down FortiAnalyzer and replace the disk.

D. Run execute format disk to format and restart the FortiAnalyzer device.

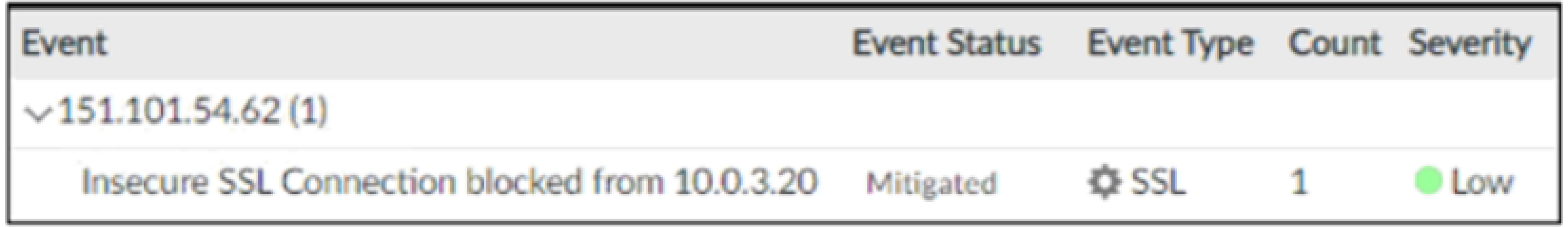
Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 2

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
∨151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙ SSL	1	● Low

Which statement is correct regarding the event displayed?

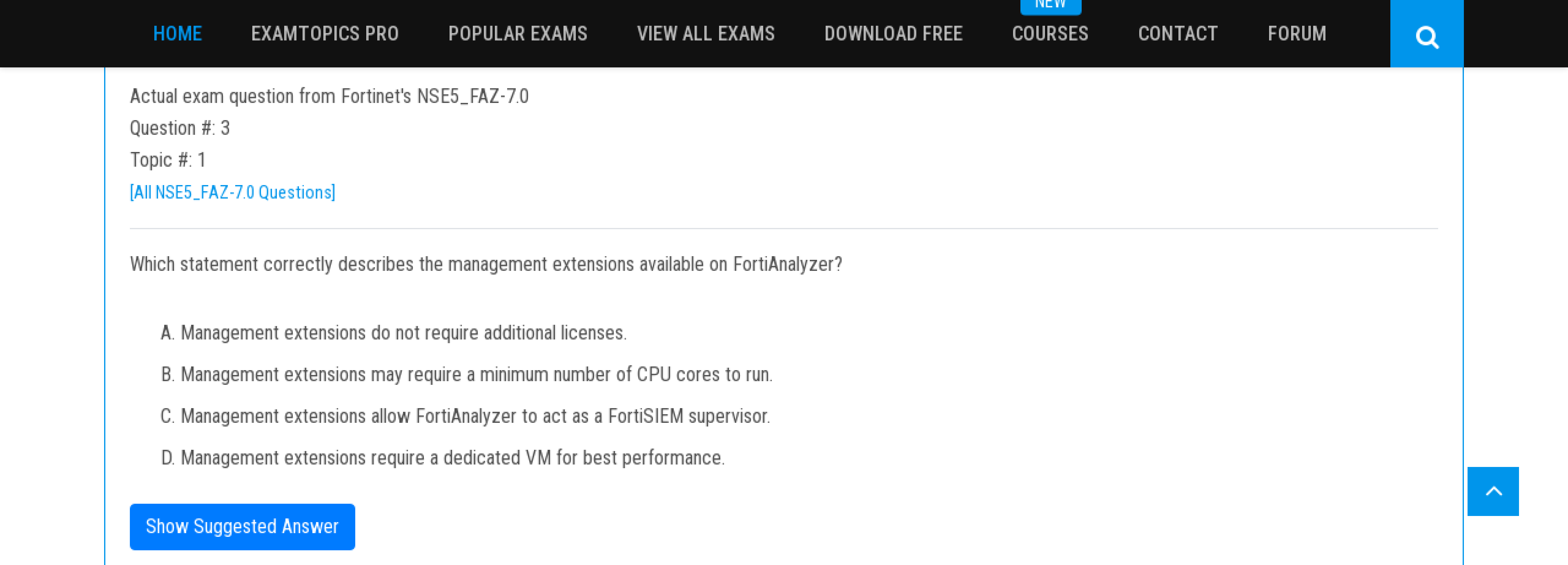
A. An incident was created from this event.

B. The security risk was blocked or dropped.

C. The security event risk is considered open.

D. The risk source is isolated.

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 3

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

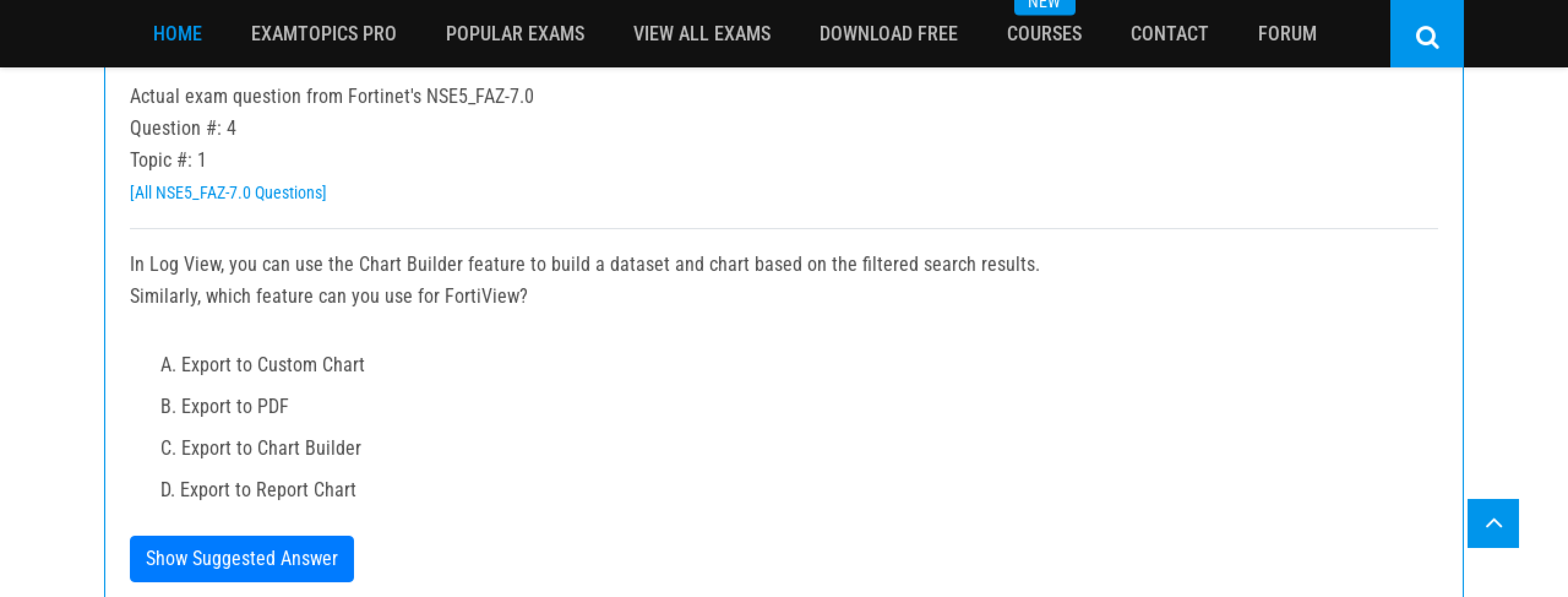
Which statement correctly describes the management extensions available on FortiAnalyzer?

A. Management extensions do not require additional licenses.

B. Management extensions may require a minimum number of CPU cores to run.

C. Management extensions allow FortiAnalyzer to act as a FortiSIEM supervisor.

D. Management extensions require a dedicated VM for best performance.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 4

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.

Similarly, which feature can you use for FortiView?

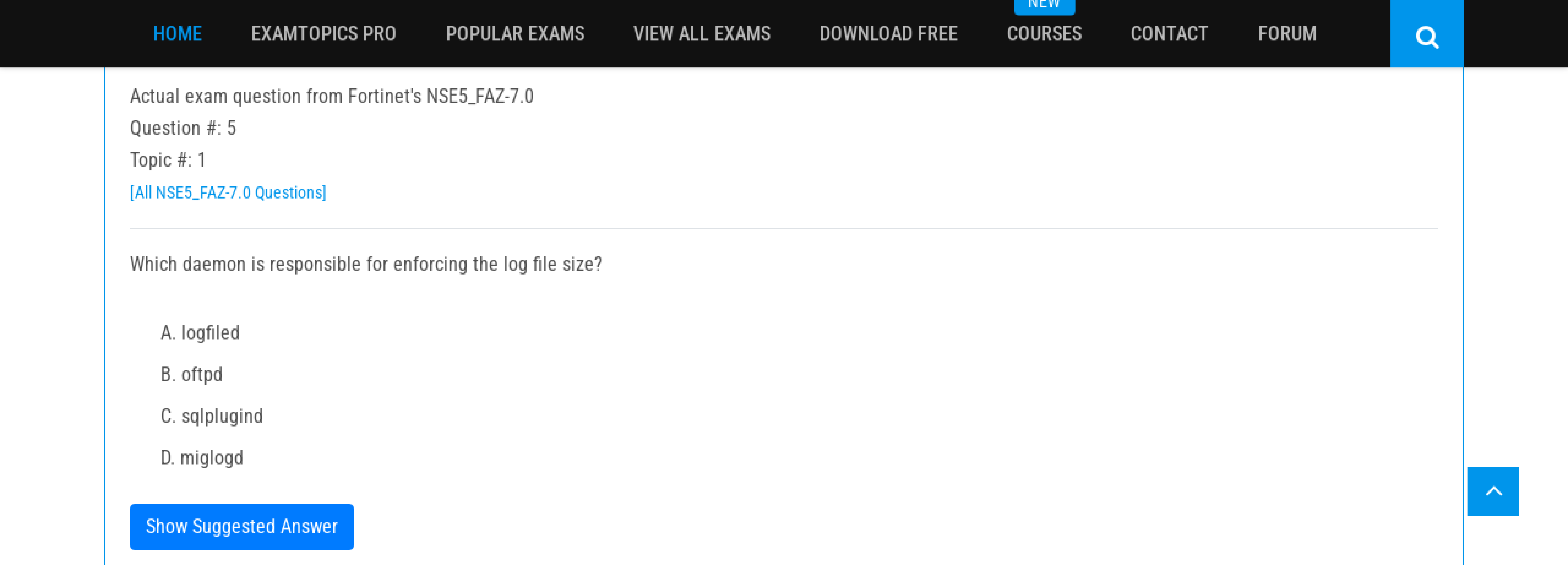
A. Export to Custom Chart

B. Export to PDF

C. Export to Chart Builder

D. Export to Report Chart

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 5

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

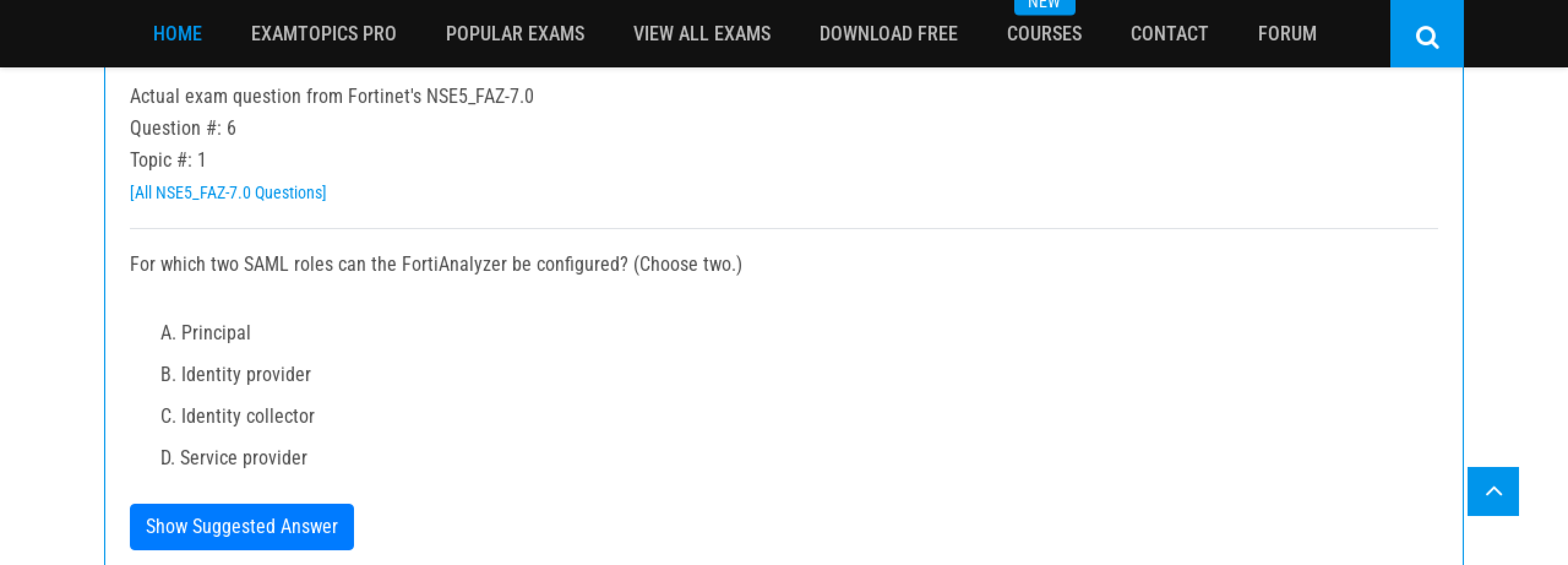
Which daemon is responsible for enforcing the log file size?

A. logfiled

B. oftpd

C. sqlplugind

D. miglogd



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 6

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

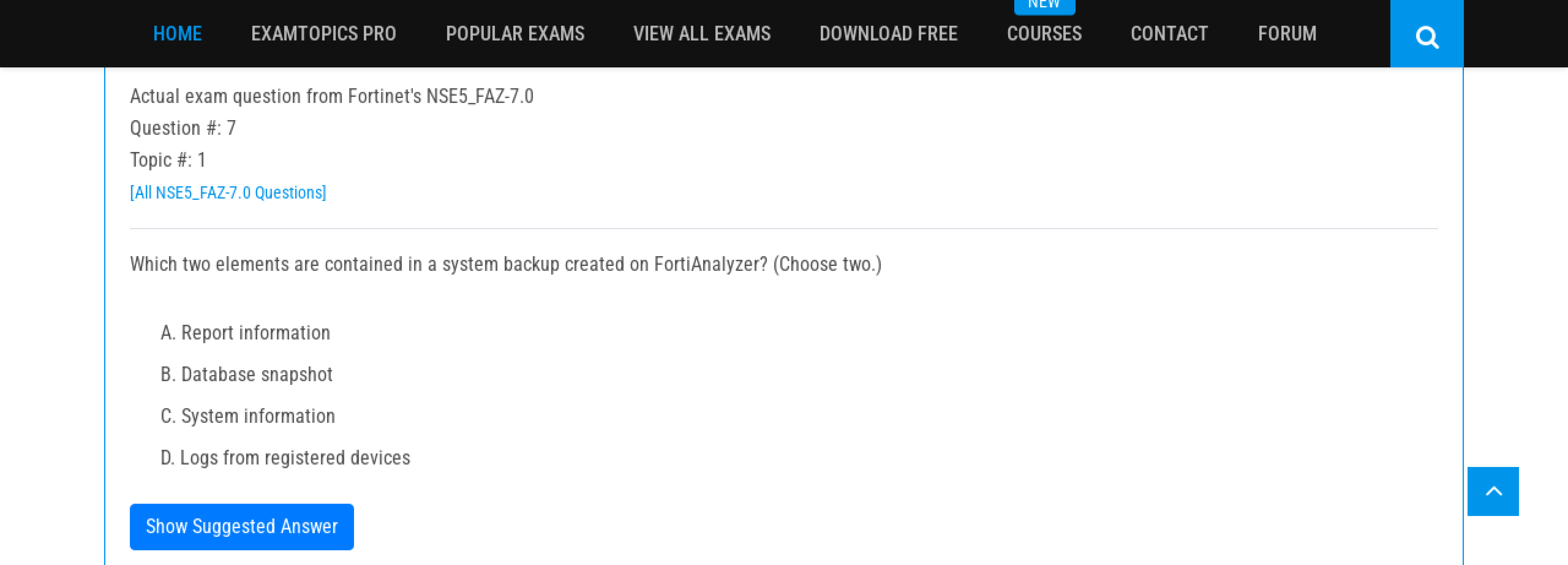
For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

A. Principal

B. Identity provider

C. Identity collector

D. Service provider



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 7

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

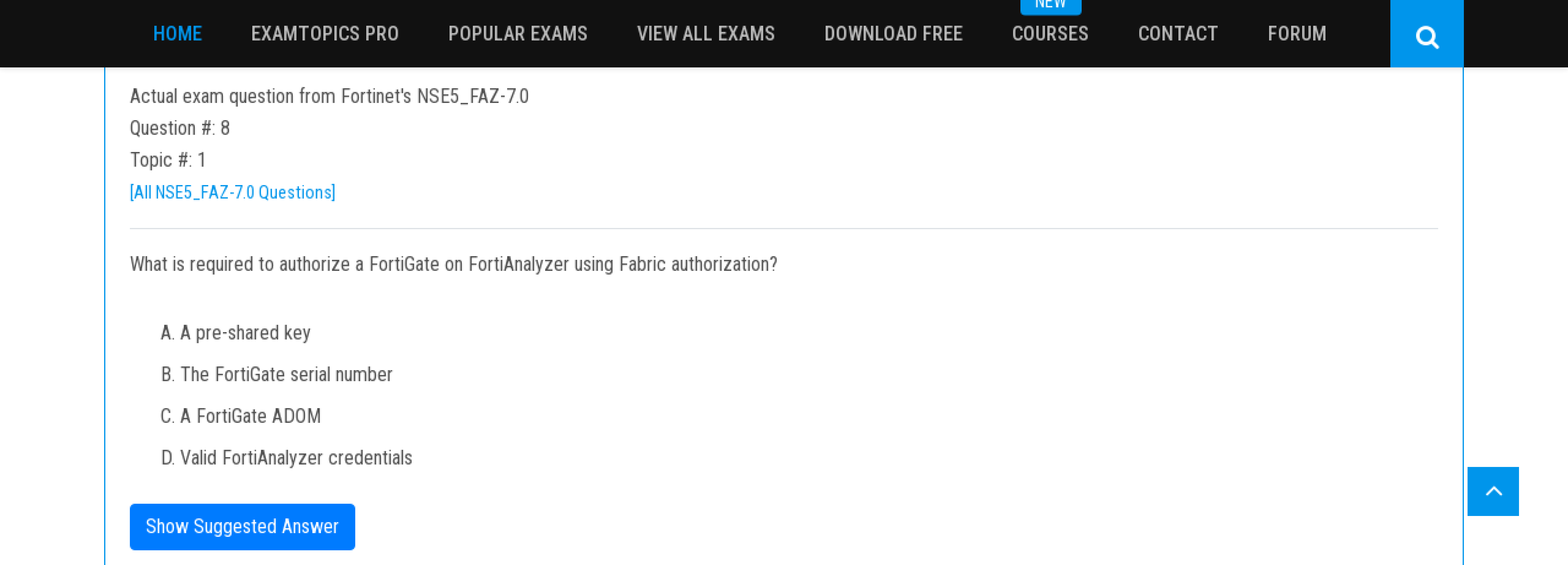
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. Report information

B. Database snapshot

C. System information

D. Logs from registered devices



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 8

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

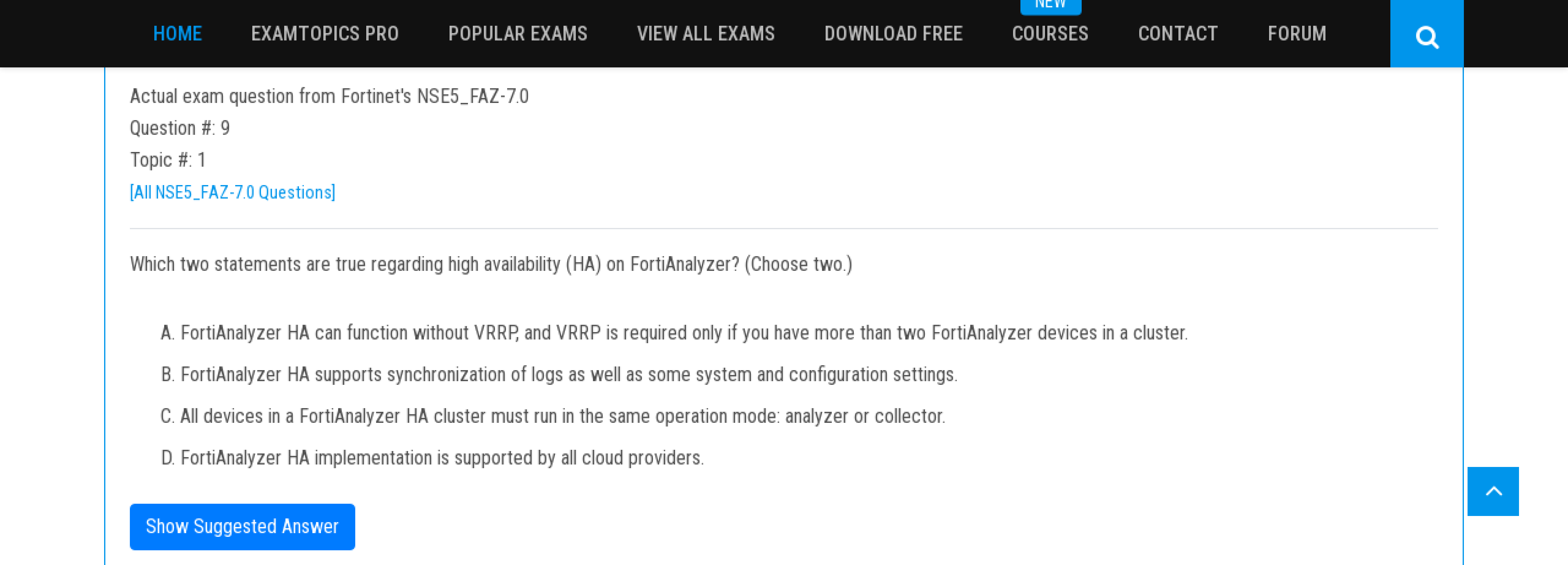
What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

A. A pre-shared key

B. The FortiGate serial number

C. A FortiGate ADOM

D. Valid FortiAnalyzer credentials



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 9

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

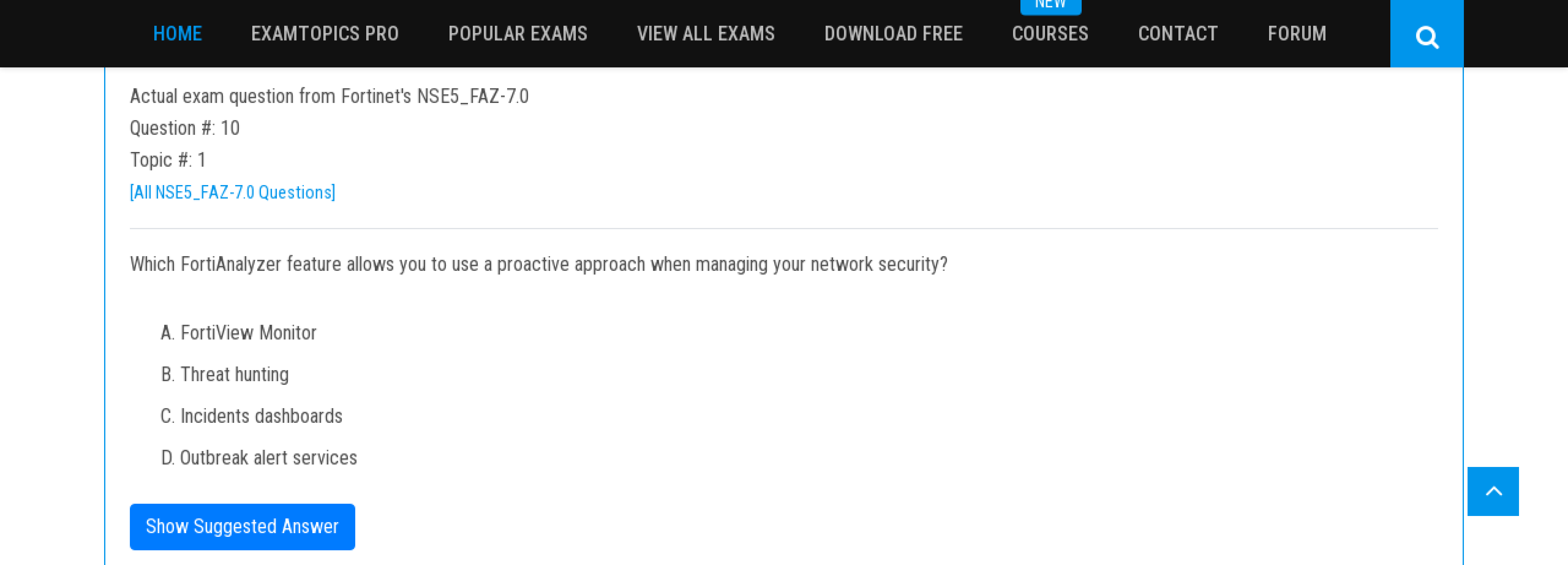
Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

A. FortiAnalyzer HA can function without VRRP, and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.

B. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.

C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.

D. FortiAnalyzer HA implementation is supported by all cloud providers.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 10

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. FortiView Monitor

B. Threat hunting

C. Incidents dashboards

D. Outbreak alert services

Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 11

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

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

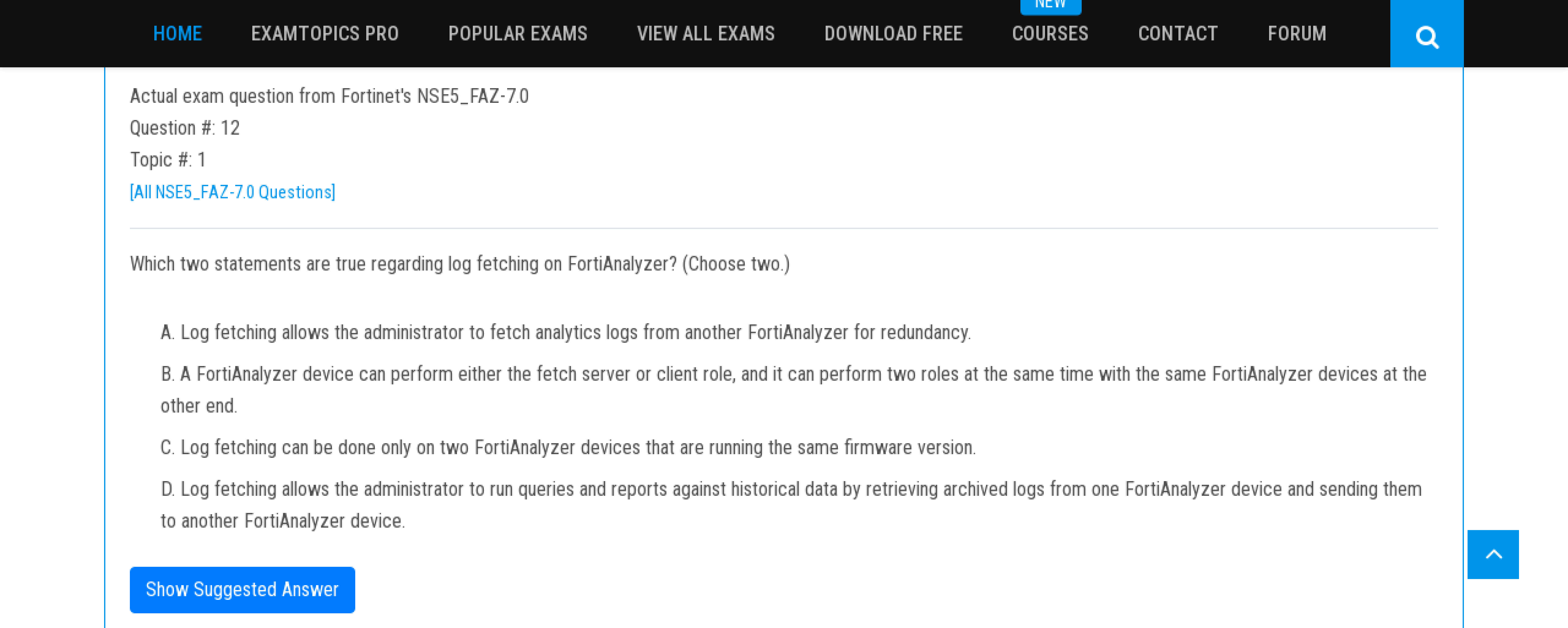
A. To set the data included in templates

B. To retrieve data from the database

C. To provide the layout used for reports

D. To define the chart type to be used

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 12

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

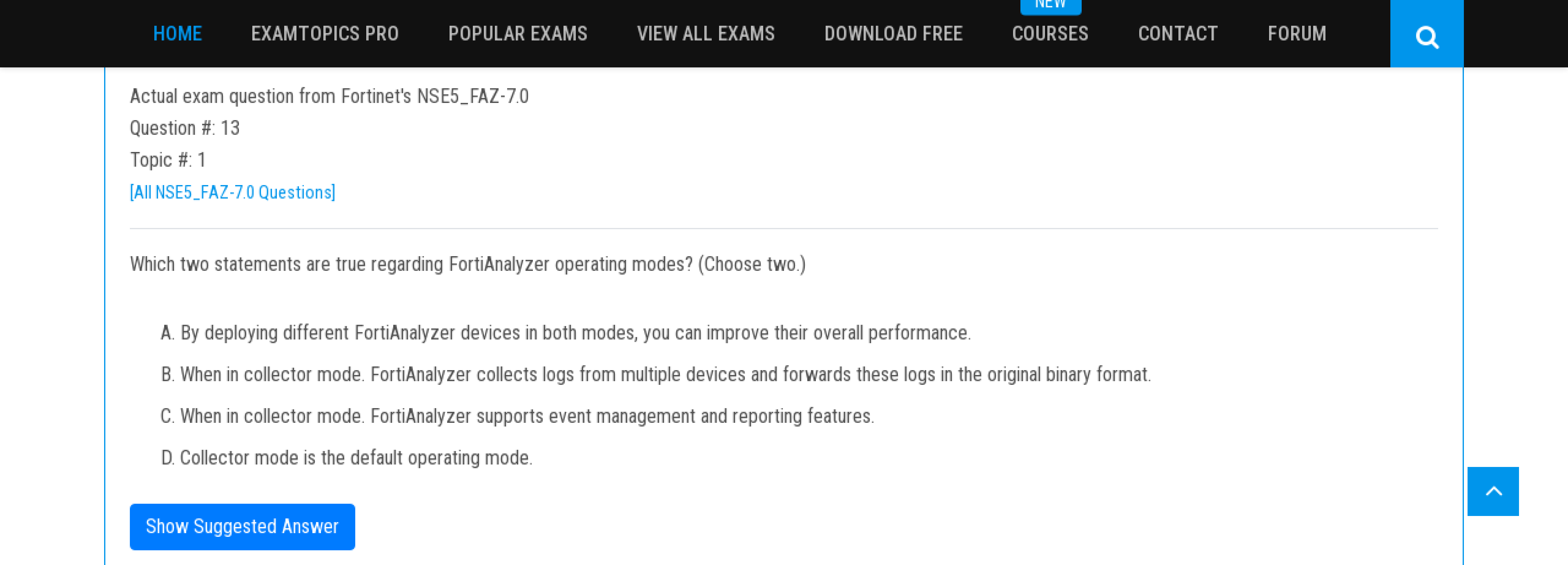
Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

A. Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

B. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

C. Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

D. Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 13

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

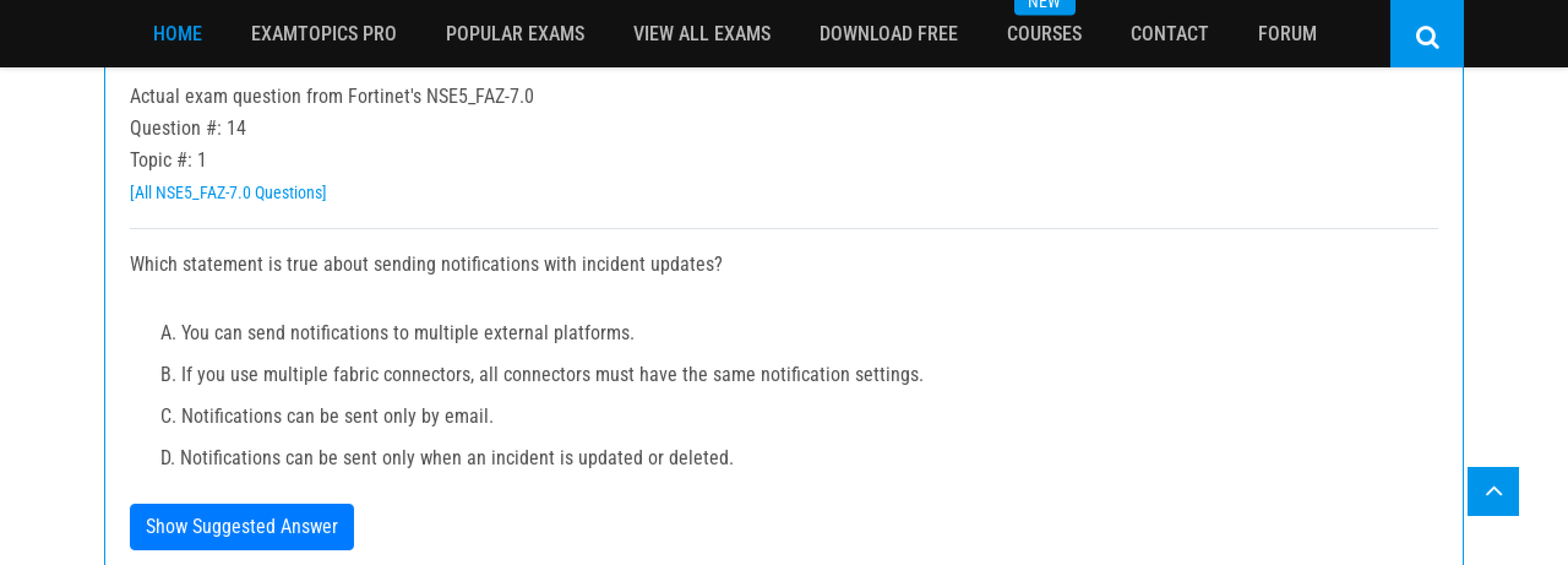
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. By deploying different FortiAnalyzer devices in both modes, you can improve their overall performance.

B. When in collector mode. FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.

C. When in collector mode. FortiAnalyzer supports event management and reporting features.

D. Collector mode is the default operating mode.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 14

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

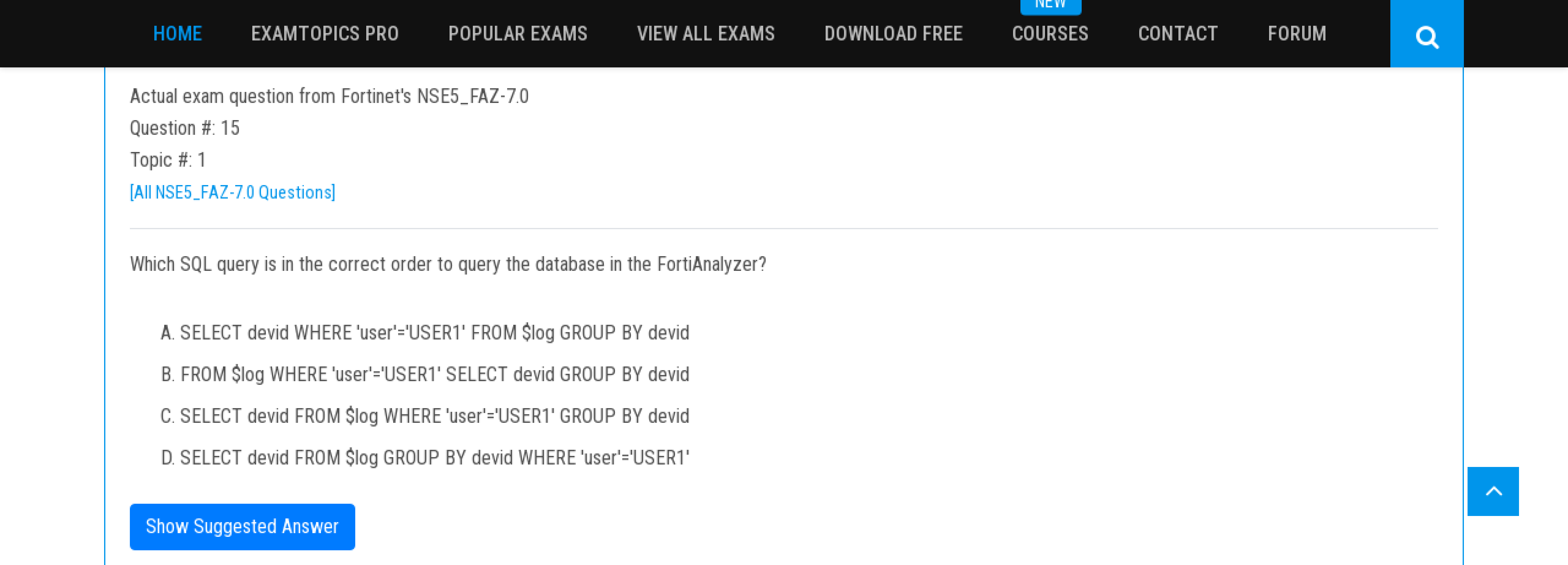
Which statement is true about sending notifications with incident updates?

A. You can send notifications to multiple external platforms.

B. If you use multiple fabric connectors, all connectors must have the same notification settings.

C. Notifications can be sent only by email.

D. Notifications can be sent only when an incident is updated or deleted.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 15

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

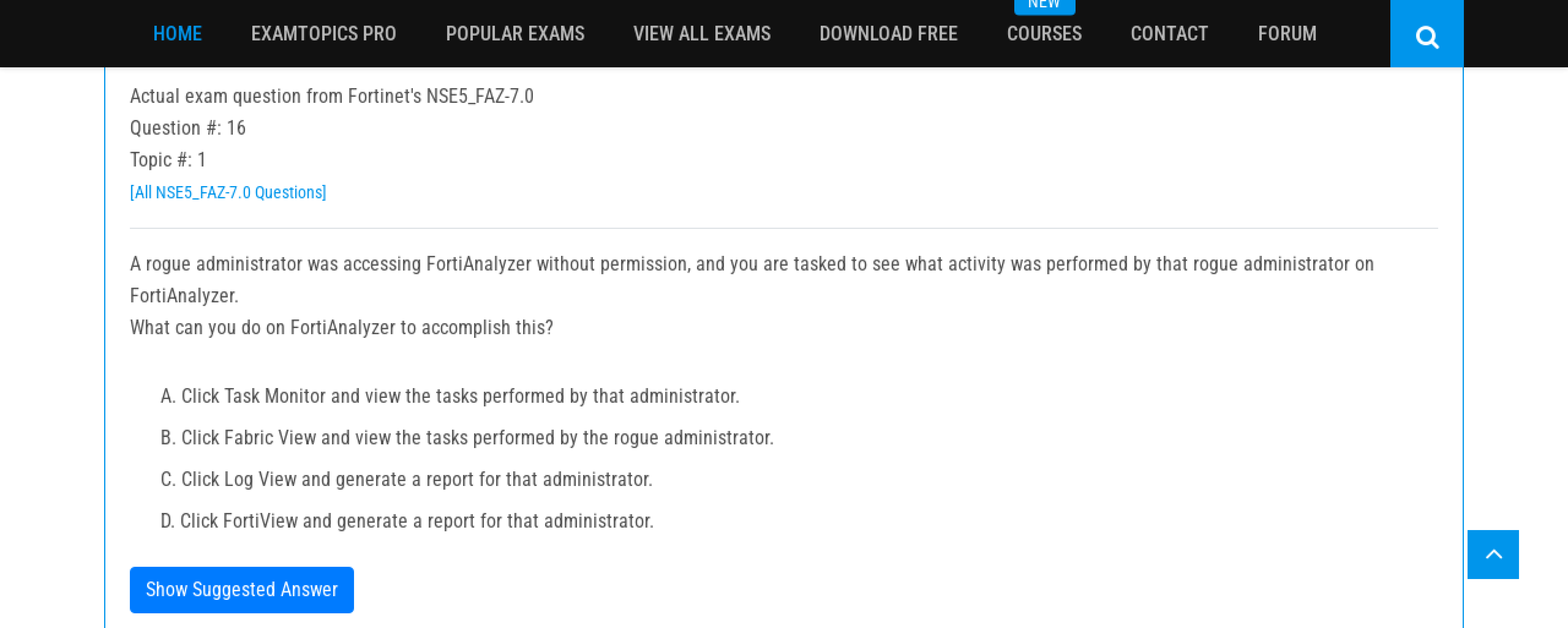
Which SQL query is in the correct order to query the database in the FortiAnalyzer?

A. SELECT devid WHERE 'user'='USER1' FROM $log GROUP BY devid

B. FROM $log WHERE 'user'='USER1' SELECT devid GROUP BY devid

C. SELECT devid FROM $log WHERE 'user'='USER1' GROUP BY devid

D. SELECT devid FROM $log GROUP BY devid WHERE 'user'='USER1'



Actual exam question from Fortinet's NSE5_FAZ-7.0
Question #: 16
Topic #: 1

[All NSE5_FAZ-7.0 Questions]

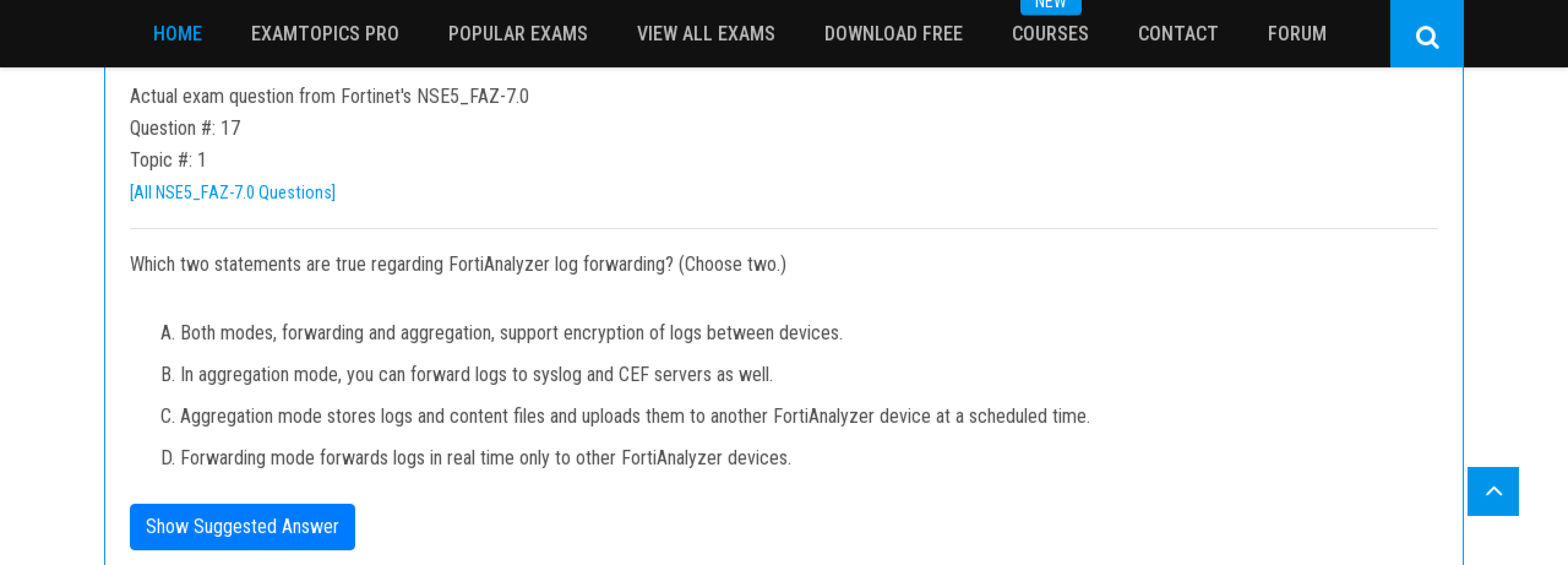
A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click Task Monitor and view the tasks performed by that administrator.

B. Click Fabric View and view the tasks performed by the rogue administrator.

C. Click Log View and generate a report for that administrator.

D. Click FortiView and generate a report for that administrator.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 17

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.

B. In aggregation mode, you can forward logs to syslog and CEF servers as well.

C. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

D. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 18

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

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 <new-ADOM-name>

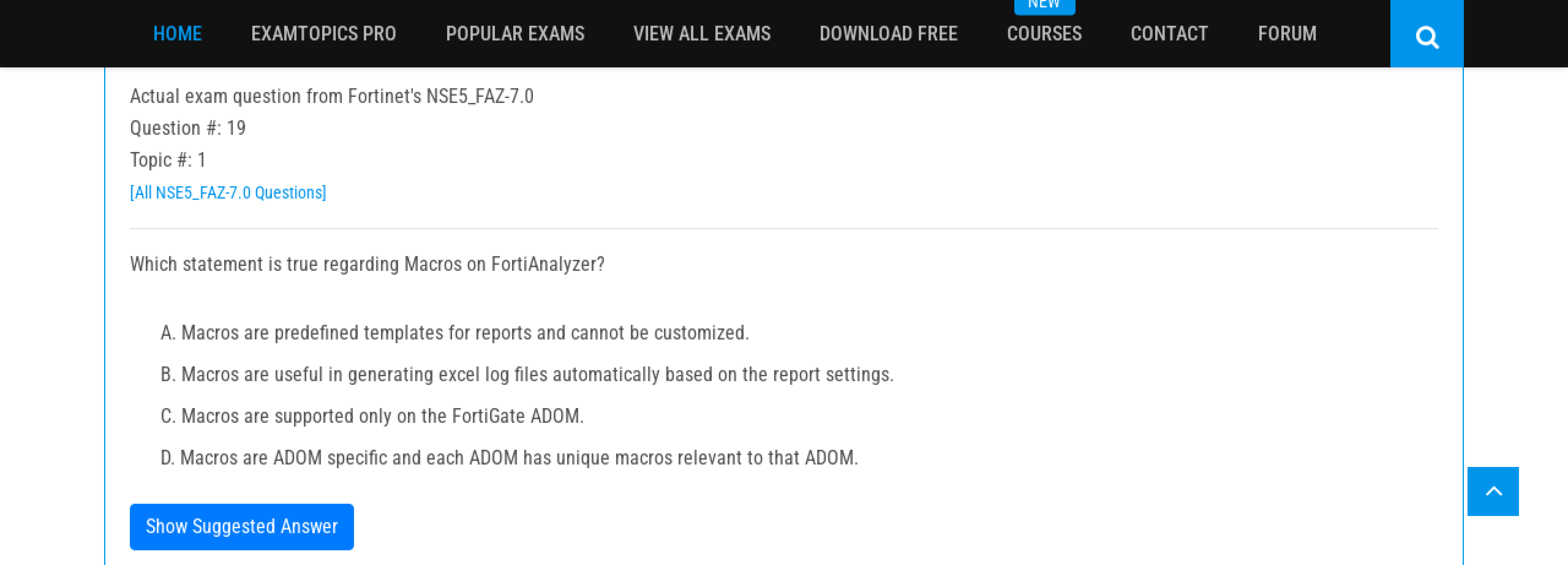
A. To reset the disk quota enforcement to default

B. To migrate the archive logs to the new ADOM

C. To remove the analytics logs of the device from the old database

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

Show Suggested Answer



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 19

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

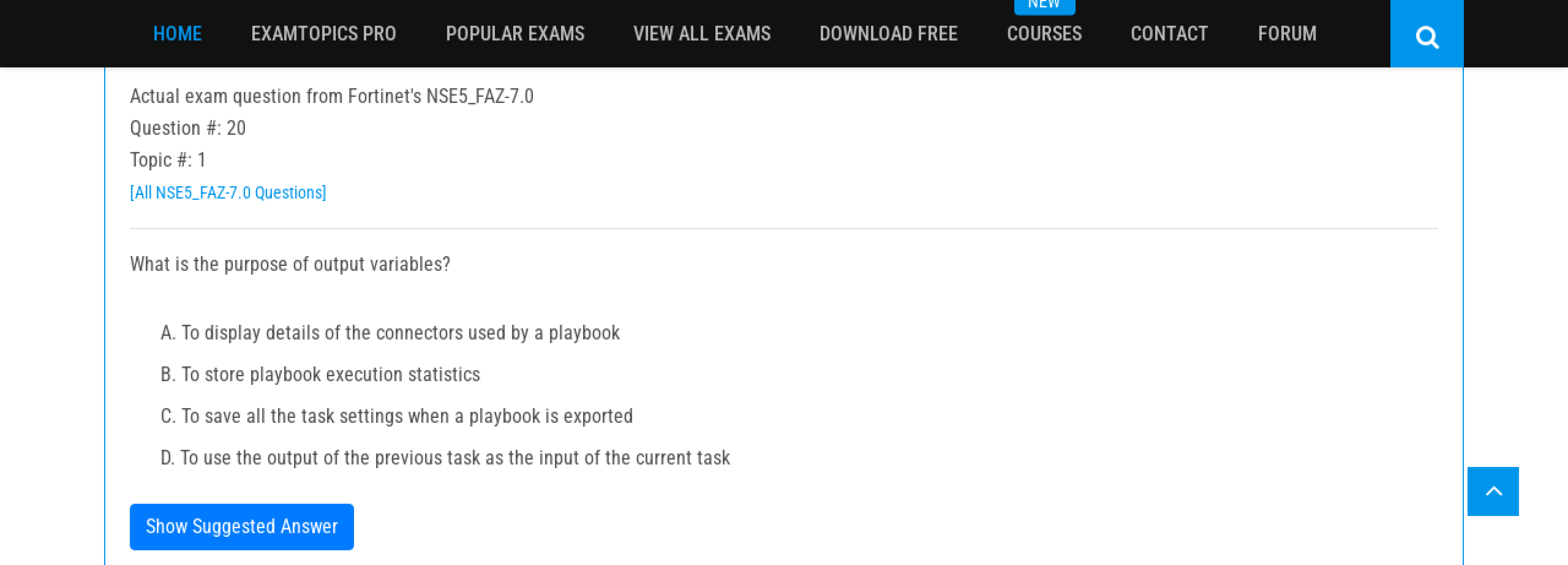
Which statement is true regarding Macros on FortiAnalyzer?

A. Macros are predefined templates for reports and cannot be customized.

B. Macros are useful in generating excel log files automatically based on the report settings.

C. Macros are supported only on the FortiGate ADOM.

D. Macros are ADOM specific and each ADOM has unique macros relevant to that ADOM.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 20

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

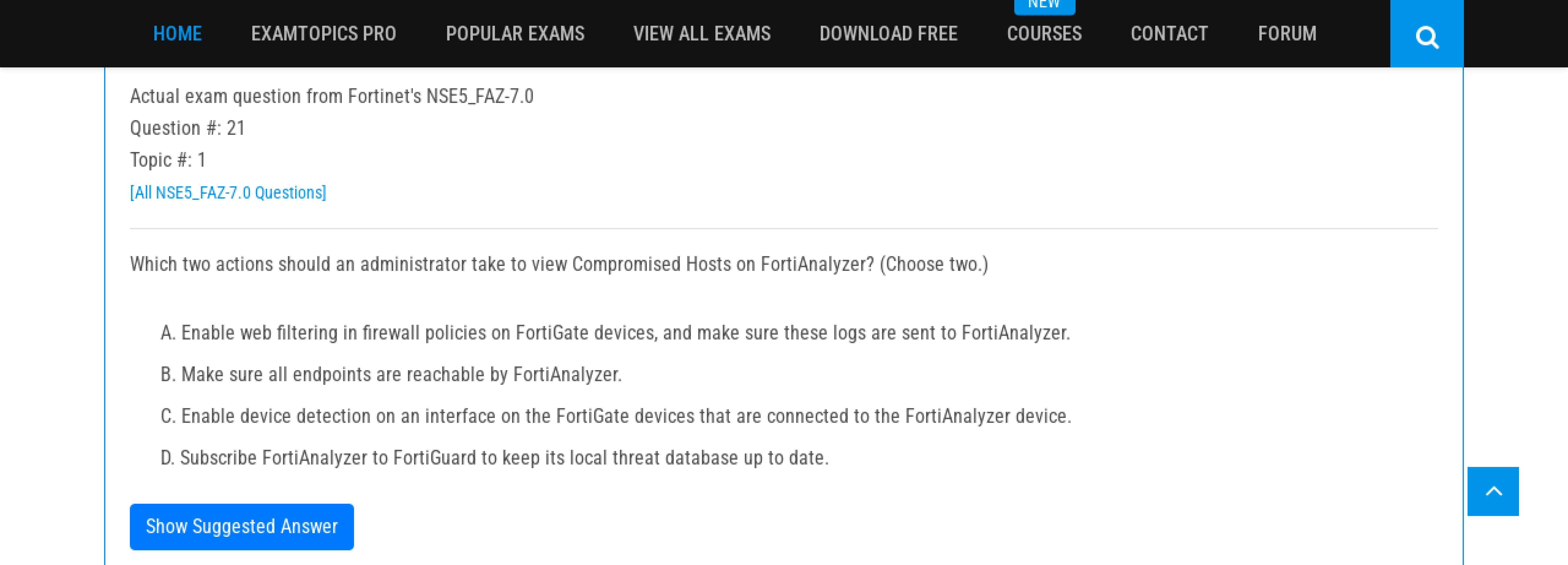
What is the purpose of output variables?

A. To display details of the connectors used by a playbook

B. To store playbook execution statistics

C. To save all the task settings when a playbook is exported

D. To use the output of the previous task as the input of the current task



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 21

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

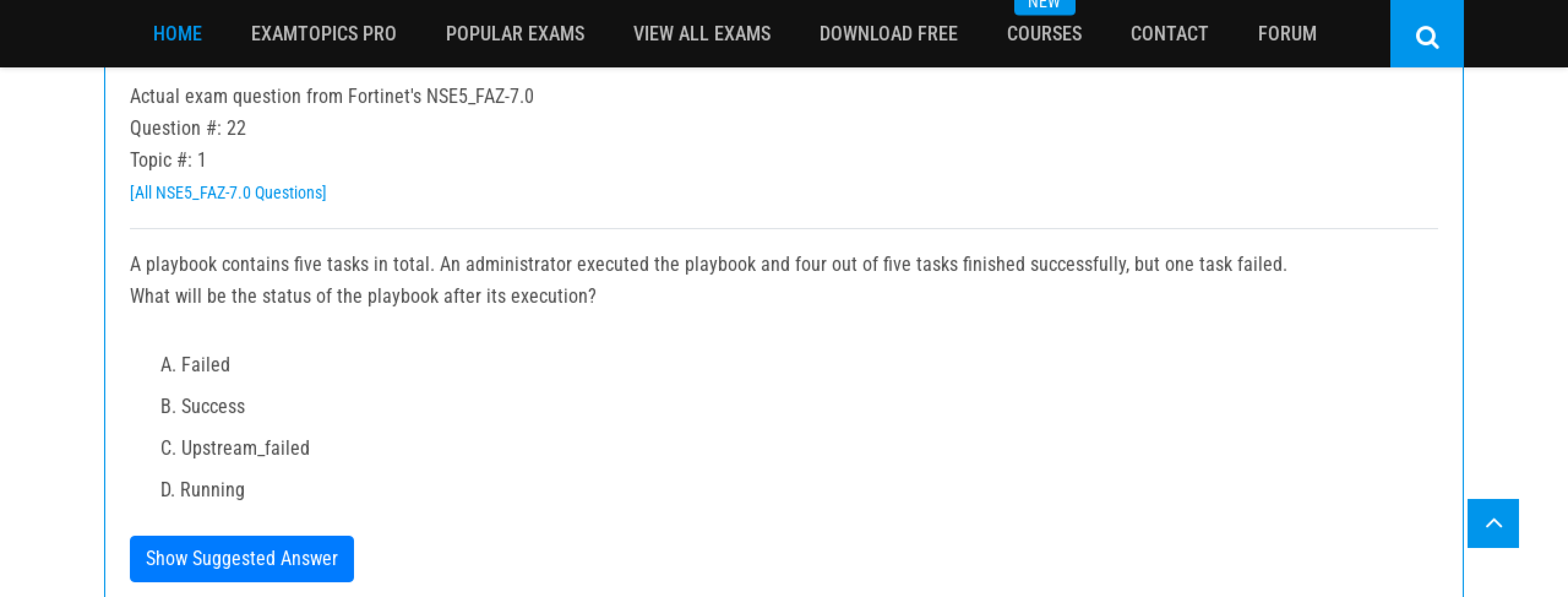
Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.

B. Make sure all endpoints are reachable by FortiAnalyzer.

C. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.

D. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.



Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 22

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

A playbook contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed.

What will be the status of the playbook after its execution?

A. Failed

B. Success

C. Upstream_failed

D. Running

Show Suggested Answer

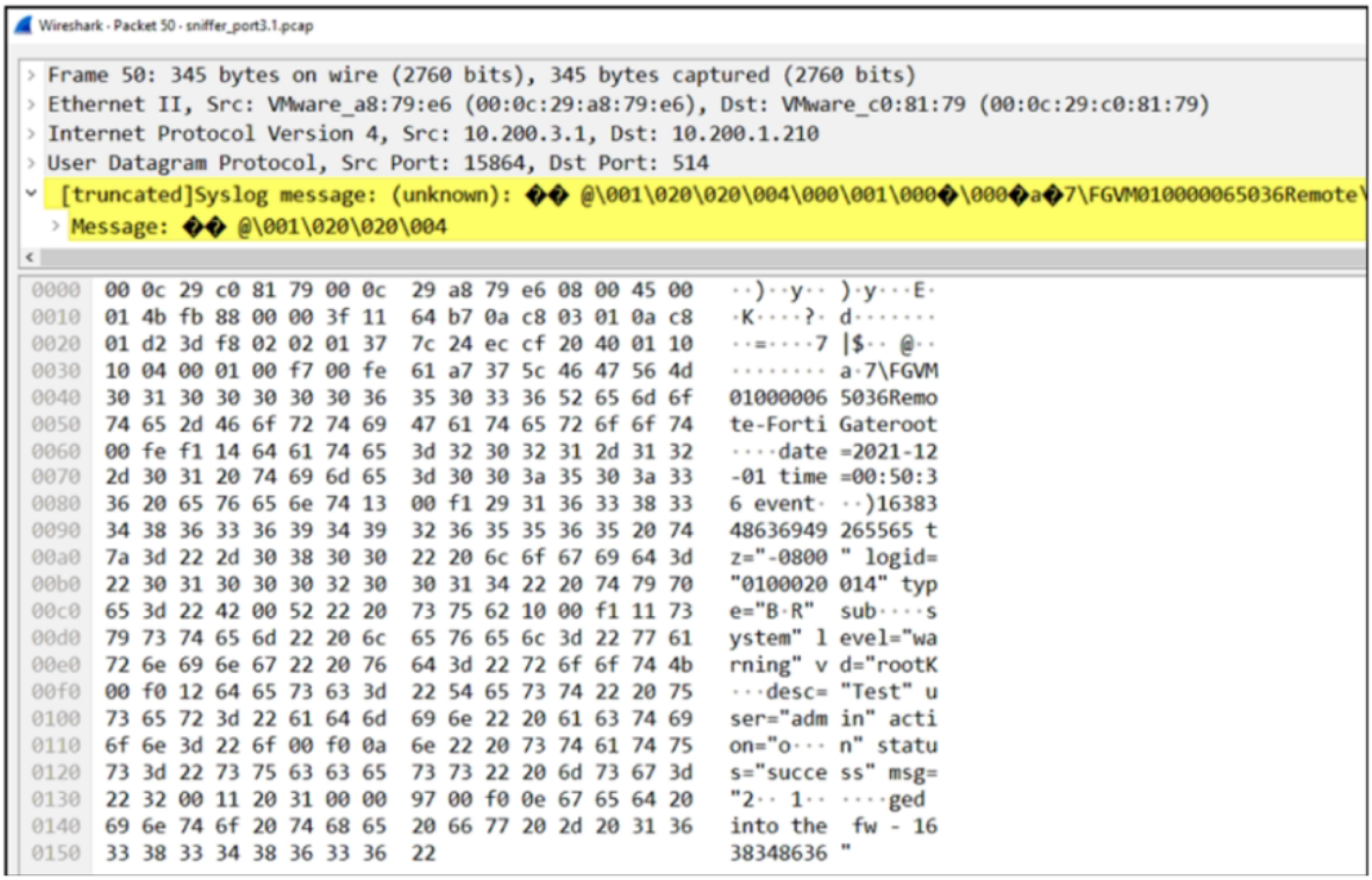
Actual exam question from Fortinet's NSE5_FAZ-7.0

Question #: 23

Topic #: 1

[All NSE5_FAZ-7.0 Questions]

Refer to the exhibit.



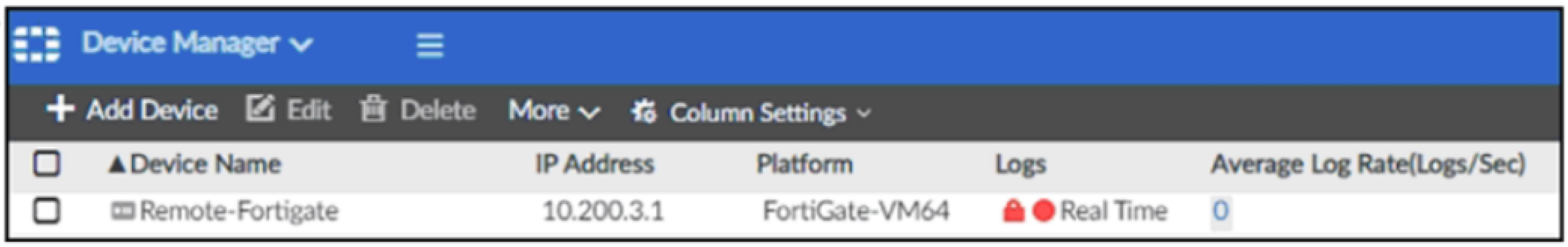
Wireshark · Packet 50 · sniffer_port3.1.pcap

```
> Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 15864, Dst Port: 514
v  [truncated]Syslog message: (unknown): �� @\001\020\020\004\000\001\000�\000�a�7\FGVM010000065036Remote\
  > Message: �� @\001\020\020\004

0000  00 0c 29 c0 81 79 00 0c  29 a8 79 e6 08 00 45 00   ··)··y·· )·y···E·
0010  01 4b fb 88 00 00 3f 11  64 b7 0a c8 03 01 0a c8   ·K····?· d·······
0020  01 d2 3d f8 02 02 01 37  7c 24 ec cf 20 40 01 10   ··=····7 |$·· @··
0030  10 04 00 01 00 f7 00 fe  61 a7 37 5c 46 47 56 4d   ········ a·7\FGVM
0040  30 31 30 30 30 30 30 36  35 30 33 36 52 65 6d 6f   01000006 5036Remo
0050  74 65 2d 46 6f 72 74 69  47 61 74 65 72 6f 6f 74   te-Forti Gateroot
0060  00 fe f1 14 64 61 74 65  3d 32 30 32 31 2d 31 32   ····date =2021-12
0070  2d 30 31 20 74 69 6d 65  3d 30 30 3a 35 30 3a 33   -01 time =00:50:3
0080  36 20 65 76 65 6e 74 13  00 f1 29 31 36 33 38 33   6 event· ··)16383
0090  34 38 36 33 36 39 34 39  32 36 35 35 36 35 20 74   48636949 265565 t
00a0  7a 3d 22 2d 30 38 30 30  22 20 6c 6f 67 69 64 3d   z="-0800 " logid=
00b0  22 30 31 30 30 30 32 30  30 31 34 22 20 74 79 70   "0100020 014" typ
00c0  65 3d 22 42 00 52 22 20  73 75 62 10 00 f1 11 73   e="B·R"  sub····s
00d0  79 73 74 65 6d 22 20 6c  65 76 65 6c 3d 22 77 61   ystem" l evel="wa
00e0  72 6e 69 6e 67 22 20 76  64 3d 22 72 6f 6f 74 4b   rning" v d="rootK
00f0  00 f0 12 64 65 73 63 3d  22 54 65 73 74 22 20 75   ···desc= "Test" u
0100  73 65 72 3d 22 61 64 6d  69 6e 22 20 61 63 74 69   ser="adm in" acti
0110  6f 6e 3d 22 6f 00 f0 0a  6e 22 20 73 74 61 74 75   on="o··· n" statu
0120  73 3d 22 73 75 63 63 65  73 73 22 20 6d 73 67 3d   s="succe ss" msg=
0130  22 32 00 11 20 31 00 00  97 00 f0 0e 67 65 64 20   "2·· 1·· ····ged
0140  69 6e 74 6f 20 74 68 65  20 66 77 20 2d 20 31 36   into the  fw - 16
0150  33 38 33 34 38 36 33 36  22                        38348636 "
```

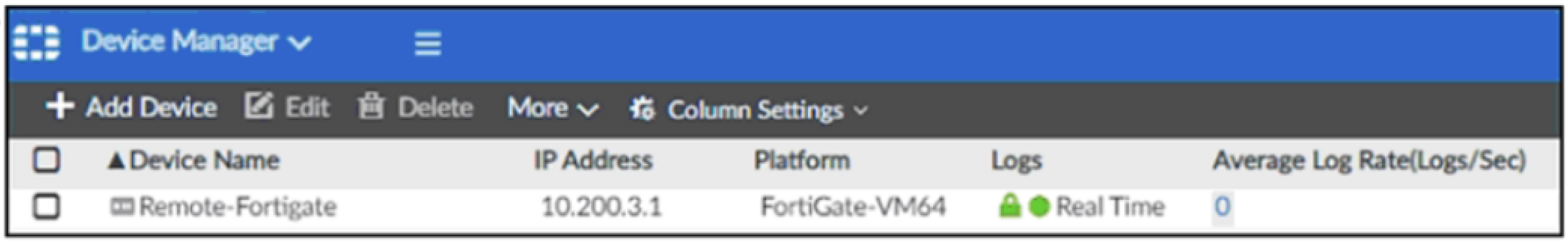
Which image corresponds to the packet capture shown in the exhibit?

A.



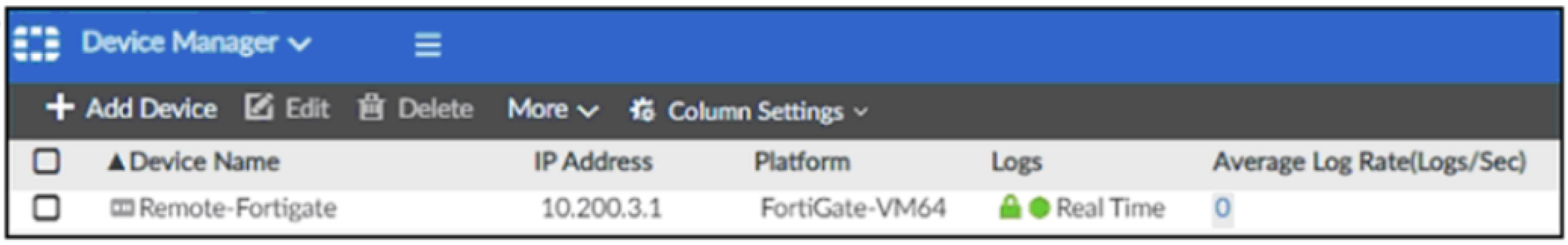
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time	0

B.



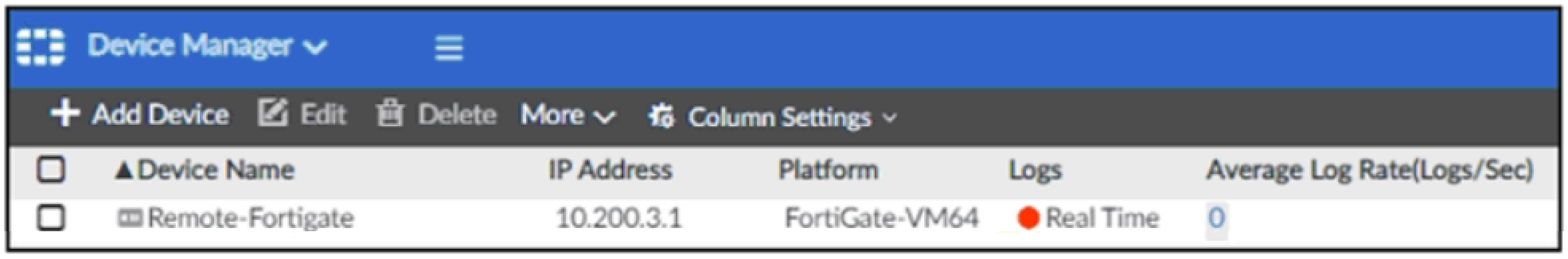
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time	0

C.



□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time	0

D.



□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	0

Show Suggested Answer