Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

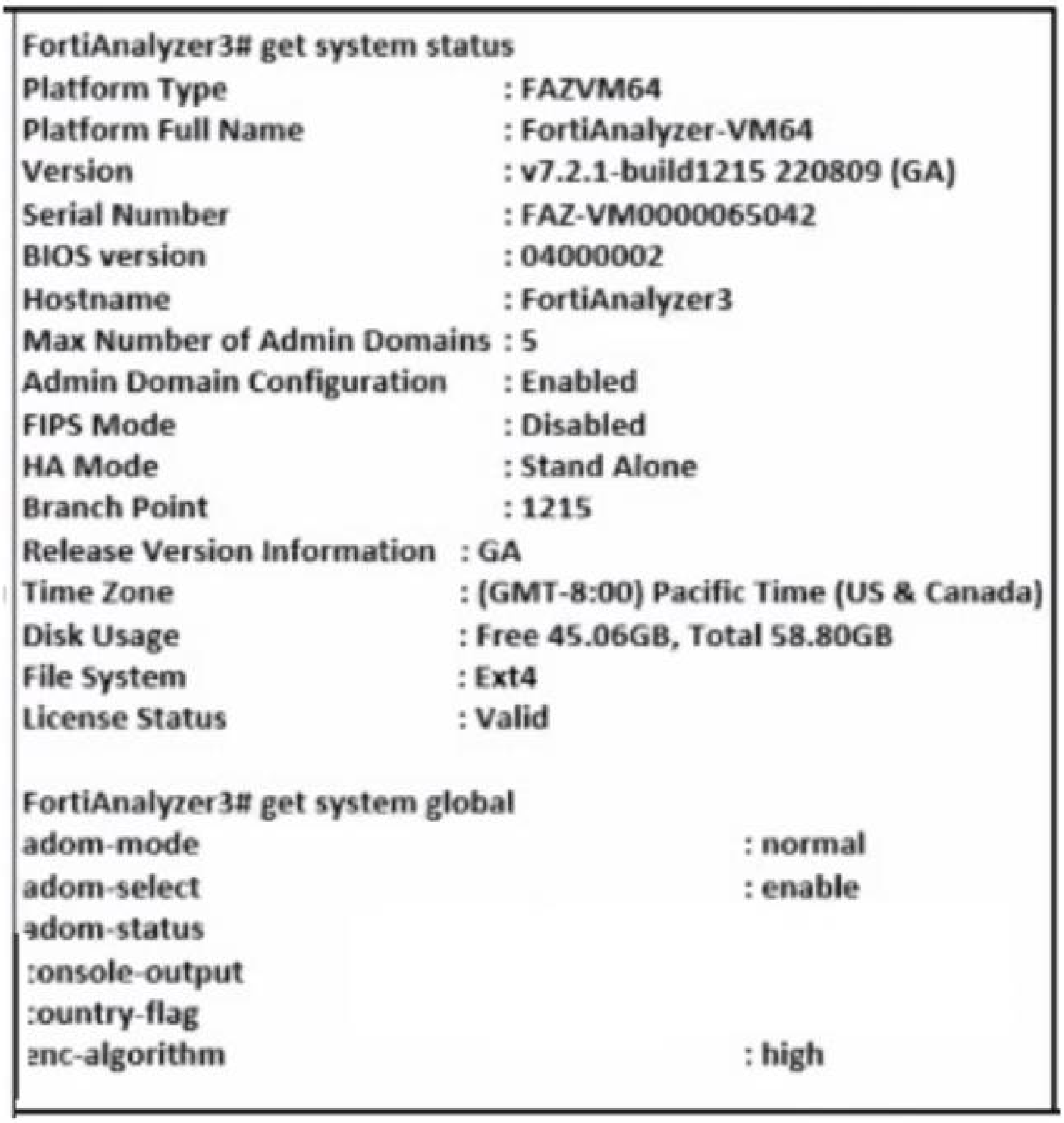
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.



```
FortiAnalyzer3# get system status
Platform Type                  : FAZVM64
Platform Full Name             : FortiAnalyzer-VM64
Version                        : v7.2.1-build1215 220809 (GA)
Serial Number                  : FAZ-VM0000065042
BIOS version                   : 04000002
Hostname                       : FortiAnalyzer3
Max Number of Admin Domains    : 5
Admin Domain Configuration     : Enabled
FIPS Mode                      : Disabled
HA Mode                        : Stand Alone
Branch Point                   : 1215
Release Version Information  : GA
Time Zone                    : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                   : Free 45.06GB, Total 58.80GB
File System                  : Ext4
License Status               : Valid

FortiAnalyzer3# get system global
adom-mode                                        : normal
adom-select                                      : enable
adom-status
console-output
country-flag
enc-algorithm                                    : high
```

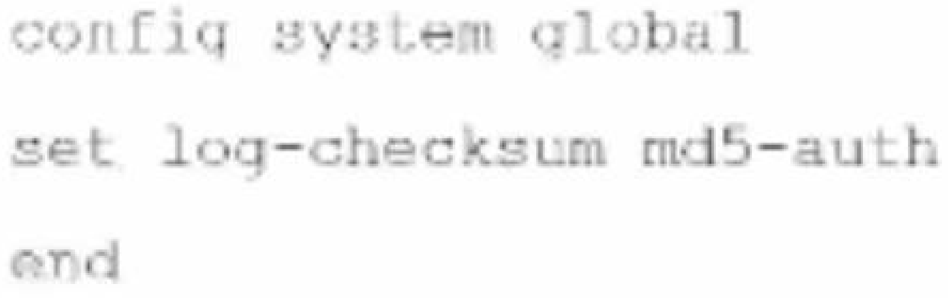
Based on the partial outputs displayed in the exhibit, which devices are ready to be configured as peers in an HA cluster?

A. FortiAnalyzer1 and FortiAnalyzer3
B. FortiAnalyzer1 and FortiAnalyzer2
C. These devices cannot participate in the same cluster.
D. FortiAnalyzer2 and FortiAnalyzer3

Answer: C

Explanation:
Based on the provided exhibit, which shows partial outputs of the system status and global settings for FortiAnalyzer devices, the devices cannot be configured as peers in an HA (High Availability) cluster. This is indicated by the HA Mode status being set to 'Stand Alone' for the displayed FortiAnalyzer device. For devices to be part of an HA cluster, they would need to havecompatible HA configurations, and usually, they should not be in 'Stand Alone' mode. Additionally, the exhibit only shows information for one FortiAnalyzer, so it cannot be determined if there is another device ready to form an HA cluster with it.

NEW QUESTION 2
An administrator has configured the following settings:



```
config system global

set log-checksum md5-auth

end
```

What is the purpose of executing these commands?

A. To record the hash value and authentication code of log files.
B. To encrypt log transfer between FortiAnalyzer and other devices.
C. To verify the integrity of the log files received.
D. To create the secure channel used by the OFTP process.

Answer: C

Explanation:
The purpose of executing the provided CLI commands, which include setting thelog-checksumtomd5-auth, is to ensure the integrity of the log files. This setting is used to record the MD5 hash value of log files, which is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. By using MD5 authentication, FortiAnalyzer ensures that the log files have not been altered or tampered with during transit, thereby verifying their integrity upon receipt.This is not related to encrypting log transfers, scheduling reports, or creating secure channels for OFTP (Over-the-FortiGate Protocol) processes.

NEW QUESTION 3
A rogue administrator was accessing FortiAnalyzer without permission.
Where can you view the activities that the rogue administrator performed on FortiAnalyzer?

A. FortiView
B. Fabric View
C. Log View
D. System Settings

Answer: A

Explanation:
To monitor the activities performed by any administrator, including a rogue one, on the FortiAnalyzer, you
should use the FortiView feature. FortiView provides a comprehensive overview of the activities and events happening within the FortiAnalyzer environment, including administrator actions, making it the appropriate tool for tracking unauthorized or suspicious activities.References:FortiAnalyzer 7.4.1 Administration Guide, "System Settings > Fabric Management" section.

NEW QUESTION 4
What is true about FortiAnalyzer reports?

A. When you enable auto-cache, reports are scheduled by default.
B. Reports can be saved in a CSV format.
C. You require an output profile before reports are generated.
D. The reports from one ADOM are available for all ADOMs.

Answer: C

Explanation:
For FortiAnalyzer reports, an output profile must be configured before reports can be generated and sent to an external server or system. This output profile determines how the reports are distributed, whether by email, uploaded to a server, or any other supported method. The options such as auto-cache, saving reports in CSV format, or reports availability across different ADOMs are separate features/settings and not directly related to the requirement of having an output profile for report generation.

NEW QUESTION 5
Which two statements are true regarding fabric connectors? (Choose two.)

A. Using fabric connectors is more efficient than third-party polling information from the FortiAnalyzer API
B. Cloud-out connectors allow you to send real-time logs to public cloud accounts like Amazon S3.
C. Fabric connectors allow you to save storage costs and improve redundancy.
D. The storage connector service does not require a separate license to send logs to the cloud platform.

Answer: AD

Explanation:
Fabric connectors in FortiAnalyzer, such as security fabric connectors (e.g., FortiClient EMS, FortiMail, FortiCASB) and storage connectors (e.g., Amazon S3, Azure Blob Container, Google Cloud Storage), provide efficient integration and data sharing capabilities.
Using fabric connectors for direct integration with FortiAnalyzer is more efficient and reliable than relying on third-party applications to poll information through the FortiAnalyzer API. Additionally, the ability to send logs to cloud storage platforms like Amazon S3, Azure Blob, and Google Cloud directly through storage connectors is a built-in feature that does not require an additional license, thus saving on storage costs and improving redundancy without incurring extra licensing fees. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Fabric Connectors' and 'Storage connectors' sections.

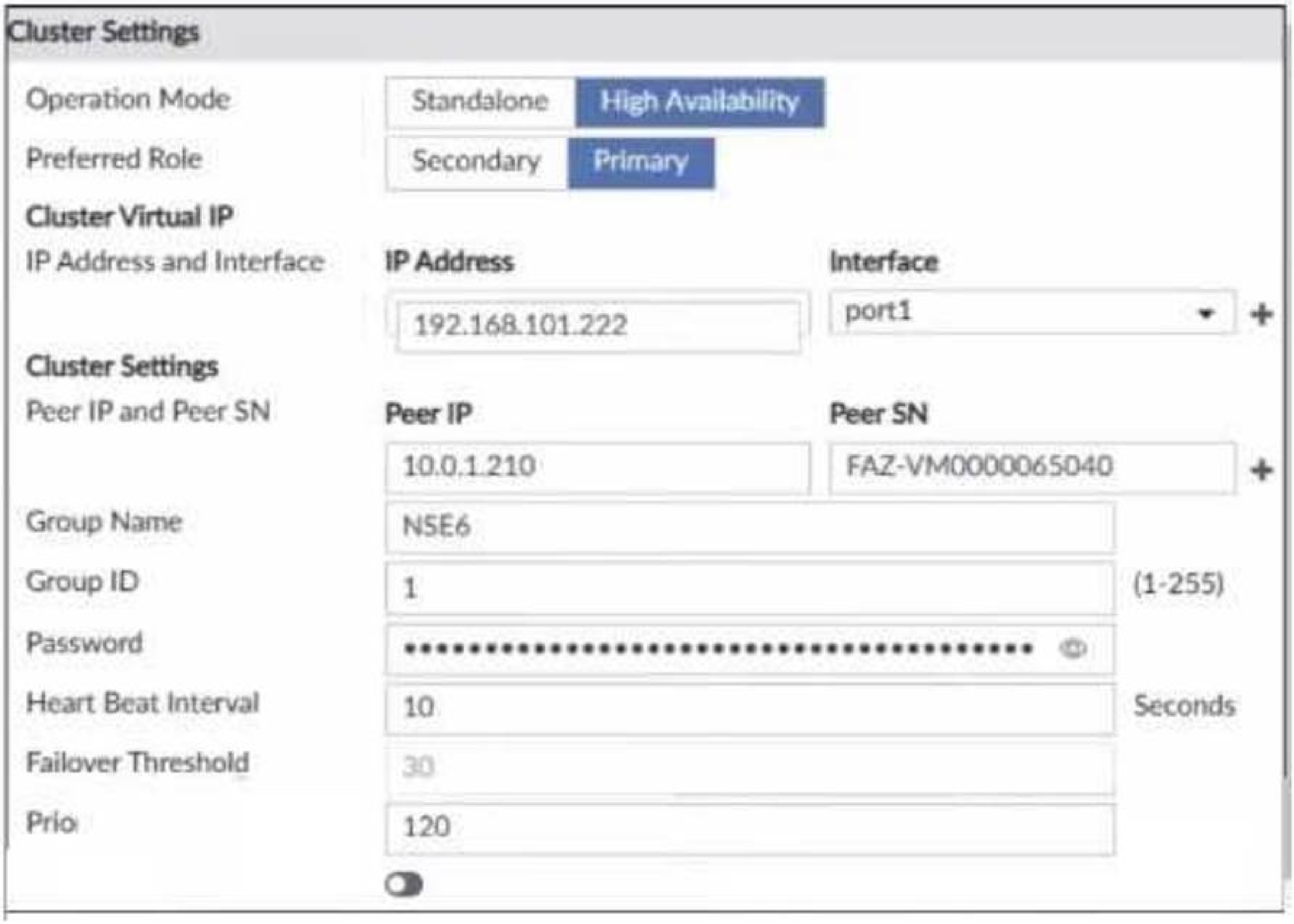
NEW QUESTION 6
Which two of the available registration methods place the device automatically in its assigned ADOM? (Choose two.)

A. Request from the device
B. Serial number
C. Fabric Authorization
D. Pre-shared key

Answer: BC

Explanation:
The registration methods that automatically place a device in its assigned ADOM are using the serial number and fabric authorization. When devices are added to FortiAnalyzer using these methods, they are automatically placed in the appropriate ADOM, which could be a default ADOM based on the device type or a predefined ADOM based on the serial number or fabric authorization. This simplifies the management of devices and their logs by organizing them into their respective ADOMs from the moment they are registered. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Default device type ADOMs' and 'Assigning devices to an ADOM' sections.

NEW QUESTION 7
Refer to the exhibit.



Cluster Settings

Operation Mode: Standalone | **High Availability**

Preferred Role: Secondary | **Primary**

Cluster Virtual IP

IP Address and Interface — IP Address: 192.168.101.222 — Interface: port1

Cluster Settings

Peer IP and Peer SN — Peer IP: 10.0.1.210 — Peer SN: FAZ-VM0000065040

Group Name: NSE6

Group ID: 1 (1-255)

Password: ••••••••••••••••••••••••••••••••••••••

Heart Beat Interval: 10 Seconds

Failover Threshold: 30

Prio: 120

The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.
What can you conclude from the configuration displayed?

A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
C. This FortiAnalyzer will join to the existing HA cluster as the primary.
D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: D

Explanation:
The configuration displayed in the exhibit indicates that the FortiAnalyzer is set up with a cluster virtual IP address of 192.168.101.222 assigned to interface port1. This setup is typically used for the FortiAnalyzer to receive logs on that interface when operating in a High Availability (HA) configuration. The exhibit does not provide enough information to conclude whether this FortiAnalyzer will be the primary unit in the HA cluster or the duration for the failover trigger; it only confirms the interface configuration for log reception.References:Based on the FortiAnalyzer 7.4.1 Administration Guide, the similar configurations for HA and log reception are discussed, which would be relevant for understanding the settings in FortiAnalyzer 7.2.

NEW QUESTION 8
What is true about a FortiAnalyzer Fabric?

A. Supervisors support HA.
B. Members events can be raised from the supervisor.
C. The supervisor and members cannot be in different time zones
D. The members send their logs to the supervisor.

Answer: D

Explanation:
In a FortiAnalyzer Fabric, the FortiAnalyzer can recognize a Security Fabric group of devices, and it supports the Security Fabric by storing and analyzing logs from these units as if they were from a single device. The members of the Security Fabric group send their logs to the FortiAnalyzer, which acts as a supervisor for log storage and analysis, providing a centralized point of visibility and control over the logs.References:FortiAnalyzer 7.4.1 Administration Guide, "Security Fabric" section.

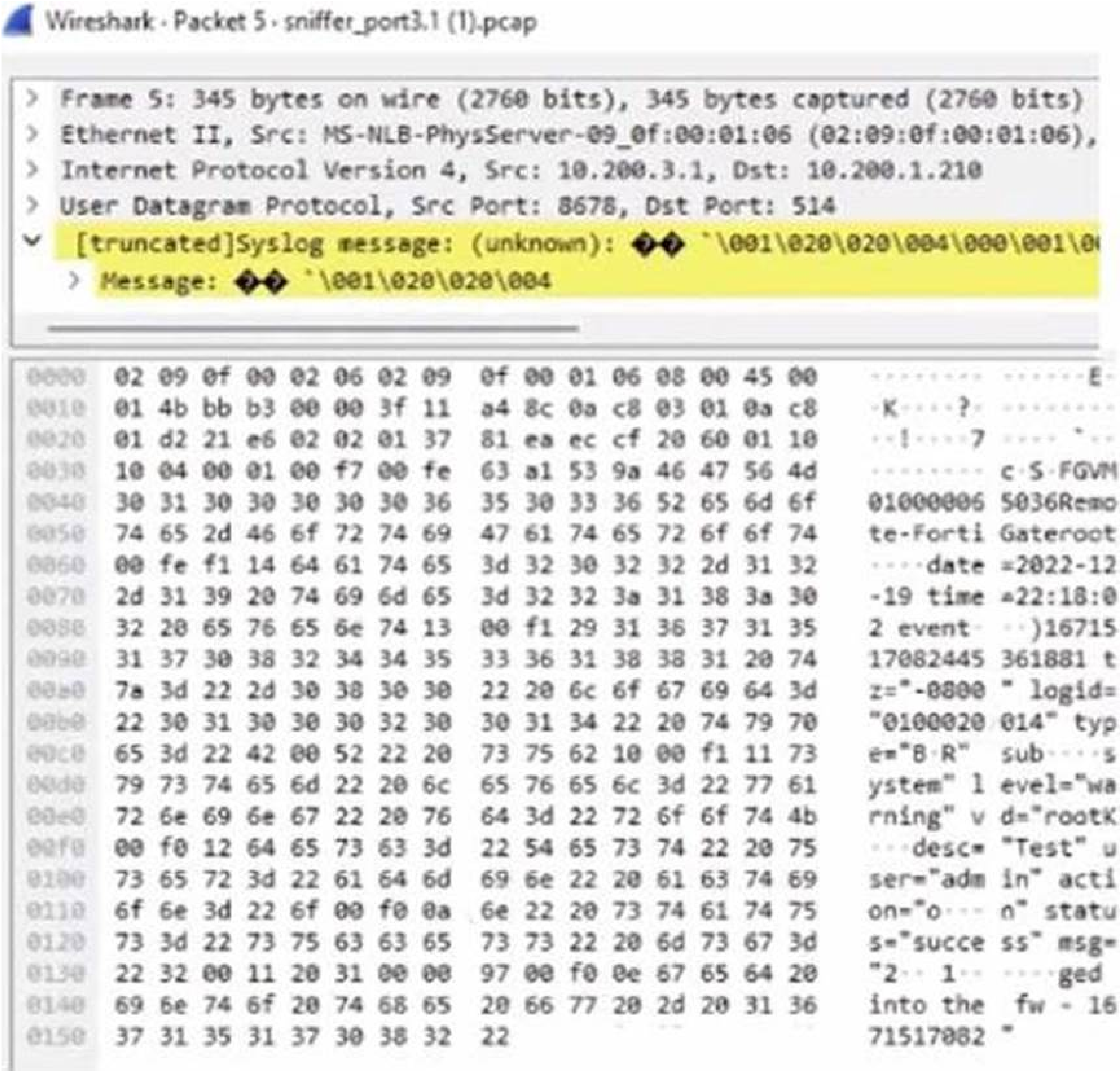
NEW QUESTION 9
Which items must you configure on FortiAnalyzer to send its reports to an external server?

A. Report schedule
B. Mail server
C. Fabric connector
D. Output profile

Answer: D

Explanation:
To send reports from FortiAnalyzer to an external server, you must configure the output profile. This involves specifying the method (FTP, SFTP, or SCP), server IP, username, password, and the directory where the report will be saved. Additionally, you have the option to delete the report after it has been uploaded to the server.
Reference: FortiAnalyzer 7.2 Administrator Guide, "Enable uploading of generated reports to a server" section.

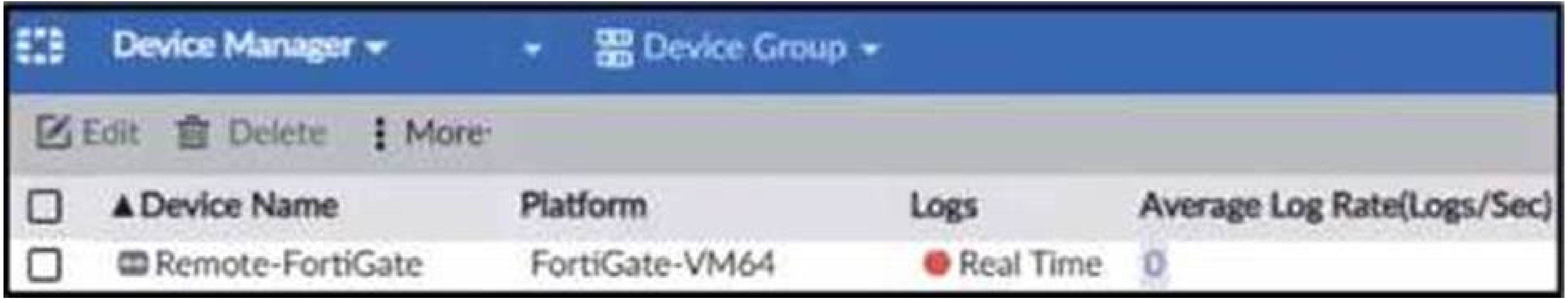
NEW QUESTION 10
Refer to the exhibit.



Wireshark · Packet 5 · sniffer_port3.1 (1).pcap

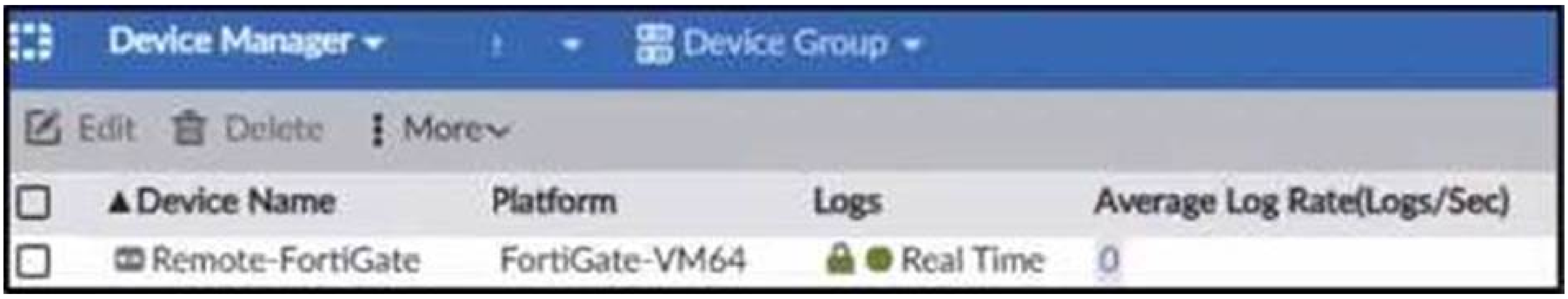
```
> Frame 5: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06),
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 8678, Dst Port: 514
v  [truncated]Syslog message: (unknown): ◆◆ `\001\020\020\004\000\001\0
   > Message: ◆◆ `\001\020\020\004

0000  02 09 0f 00 02 06 02 09  0f 00 01 06 08 00 45 00   ········ ······E·
0010  01 4b bb b3 00 00 3f 11  a4 8c 0a c8 03 01 0a c8   ·K····?· ········
0020  01 d2 21 e6 02 02 01 37  81 ea ec cf 20 60 01 10   ··!····7 ···· `··
0030  10 04 00 01 00 f7 00 fe  63 a1 53 9a 46 47 56 4d   ········ c·S·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 32 2d 31 32   ····date =2022-12
0070  2d 31 39 20 74 69 6d 65  3d 32 32 3a 31 38 3a 30   -19 time =22:18:0
0080  32 20 65 76 65 6e 74 13  00 f1 29 31 36 37 31 35   2 event· ··)16715
0090  31 37 30 38 32 34 34 35  33 36 31 38 38 31 20 74   17082445 361881 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  37 31 35 31 37 30 38 32  22                        71517082 "
```

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



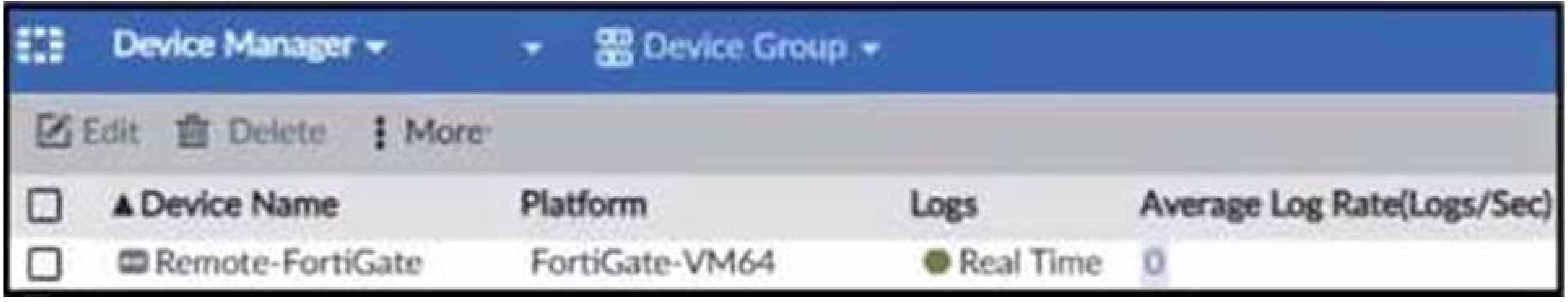
□	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-FortiGate	FortiGate-VM64	● Real Time	0

B)



☐	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
☐	Remote-FortiGate	FortiGate-VM64	🔒 ● Real Time	0

C)



☐	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
☐	Remote-FortiGate	FortiGate-VM64	● Real Time	0

A. Option A
B. Option B
C. Option A

Answer: D

Explanation:
The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions "real-time". Therefore, Option A is the correct answer because it shows logs with "Real Time" status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture.
Reference: Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

NEW QUESTION 10
......

Relate Links

100% Pass Your NSE6_FAZ-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE6_FAZ-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/