Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

NEW QUESTION 1
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. There is no need to do anything because the disk will self-recover.
B. Run execute format disk to format and restart the FortiAnalyzer device.
C. Perform a hot swap of the disk.
D. Shut down FortiAnalyzer and replace the disk.

Answer: C

Explanation:
In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

NEW QUESTION 2
Which process is responsible for enforcing the log file size?

A. oftpd
B. miglogd
C. sqlplugind
D. logfiled

Answer: D

Explanation:
The logfiled process is responsible for enforcing log file size and managing log rotation on FortiAnalyzer. It ensures that log files do not exceed the configured size limits and handles the creation and rotation of new log files when necessary.

NEW QUESTION 3
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

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

Answer: C

Explanation:
RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.
Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.
The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 4
Refer to the exhibit.

```
FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:31  total-so-far:4642589
global log dev statistics:
faz=180191781, faz_cloud=0, fds_log=0
faz 0: sent=180189698, failed=4507, cached=0, dropped=0
```

Based on the output, what can you conclude about the FortiAnalyzer logging status?

A. The connection between FortiGate and FortiAnalyzer is overloaded.
B. FortiGate has logs to send, but FortiAnalyzer is unavailable.
C. FortiGate is configured to send logs in batches.
D. FortiGate is sending logs again after it performed a reboot.

Answer: B

Explanation:
The output shows that FortiGate has sent a large number of logs (sent=180189698), but some logs have failed to be sent (failed=4507). This suggests that FortiAnalyzer was temporarily unavailable or had an issue receiving logs, leading to the failure count. There are no logs cached or dropped, indicating FortiGate is still attempting to send logs but with some failures.

NEW QUESTION 5
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

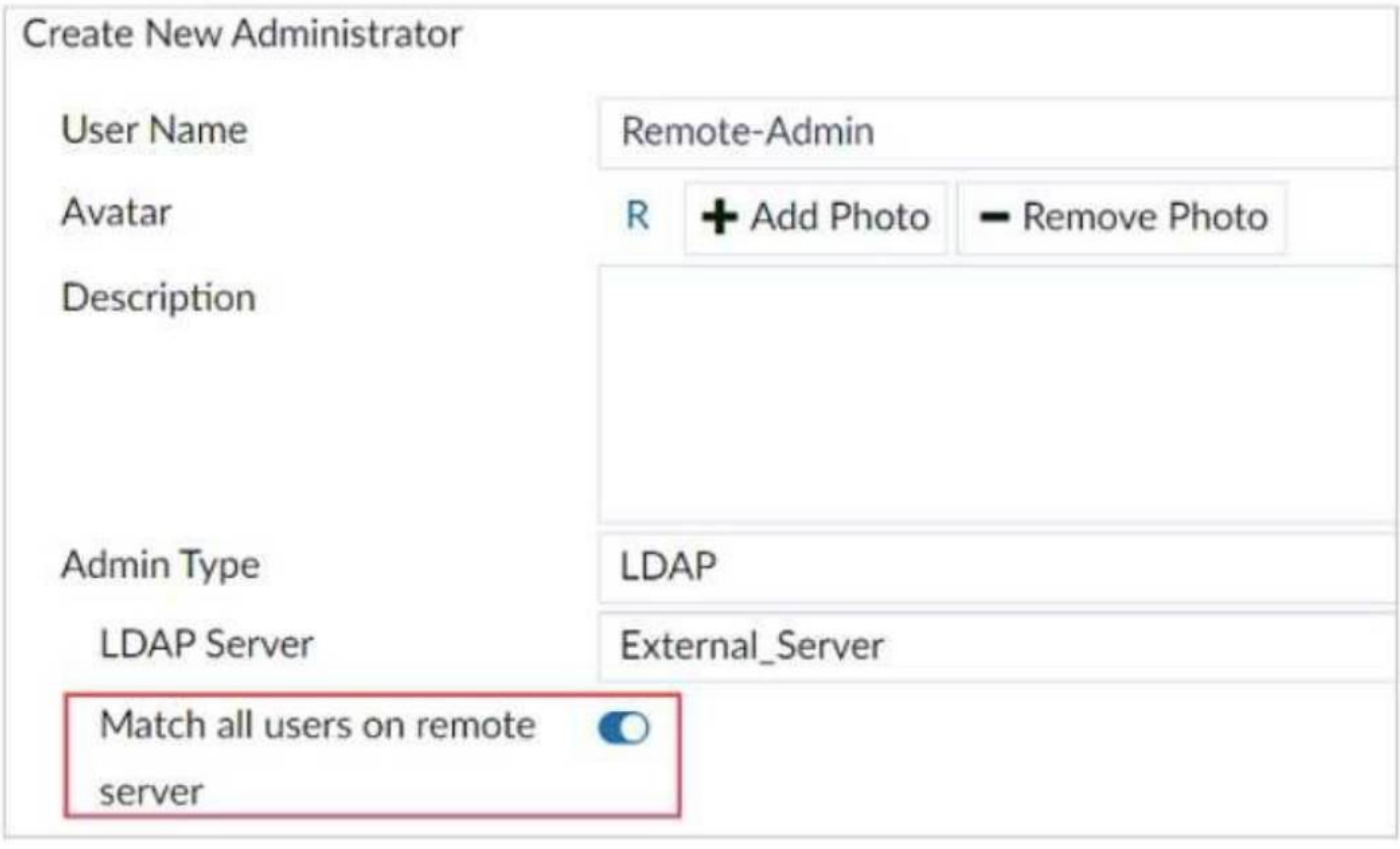
A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.

B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
C. For the collector, you should allocate most of the disk space to analytics logs.
D. Analyzer mode is the default operating mode.

Answer: B

Explanation:
When in analyzer mode, FortiAnalyzer supports event management and reporting features.
In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.
Analyzer mode is the default operating mode.
By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:
In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.
In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 6
Refer to the exhibit.



The exhibit shows the creation of a new administrator on FortiAnalyzer.
What are two effects of enabling the choice Match all users on remote server when configuring a new administrator? (Choose two.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Enabling this option allows any user authenticated by the LDAP server to log in to FortiAnalyzer, effectively creating a wildcard administrator.

NEW QUESTION 7
The connection status of a new device on FortiAnalyzer is listed as Unauthorized. What does that status mean?

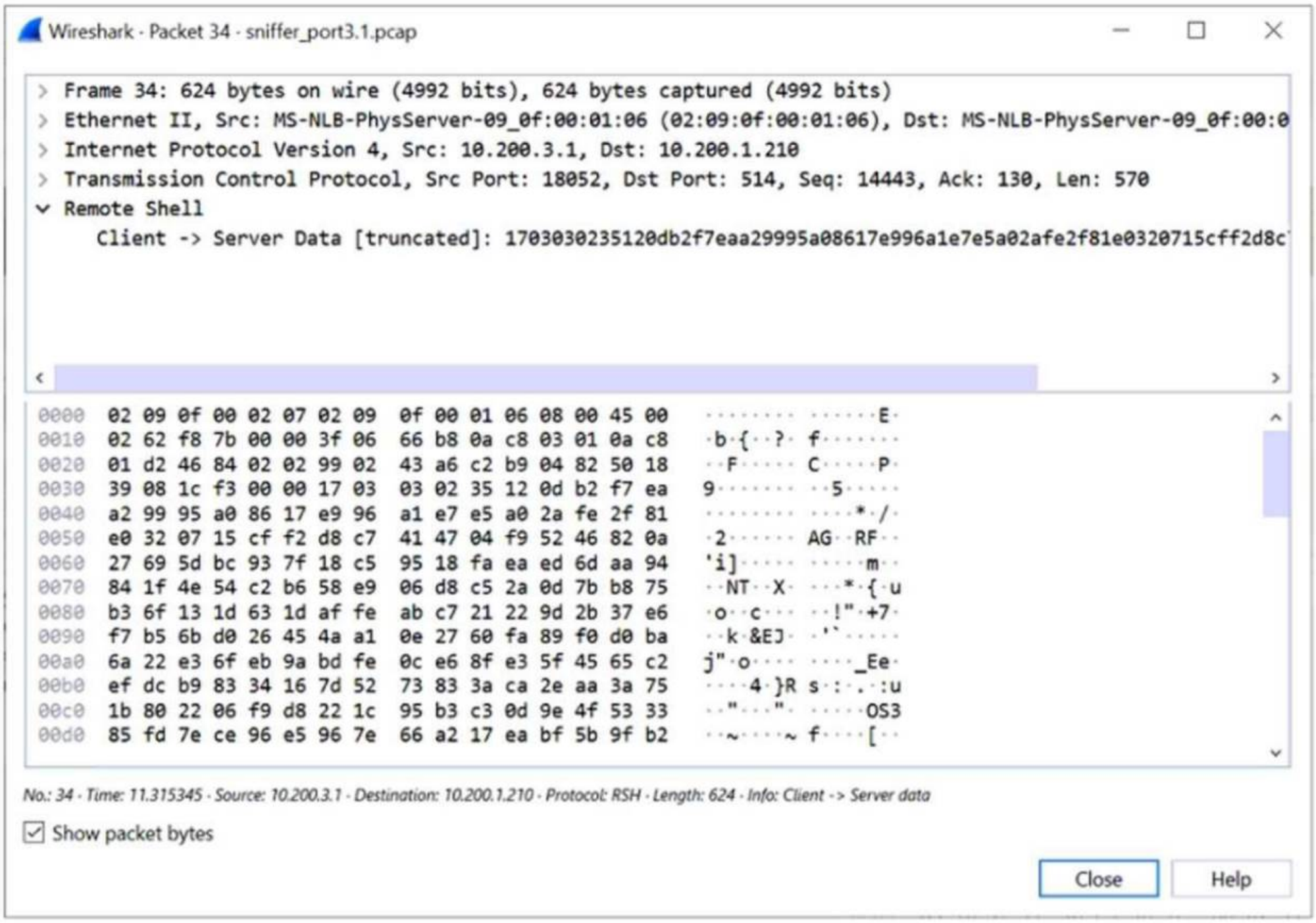
A. It is a device whose registration has not yet been accepted in FortiAnalvzer.
B. It is a device that has not yet been assigned an ADOM.
C. It is a device that is waiting for you to configure a pre-shared key.
D. It is a device that FortiAnalvzer does not support.

Answer: A

Explanation:
The "Unauthorized" status indicates that the device has been discovered or attempted to connect but has not yet been authorized for management by FortiAnalyzer. It requires an administrator to approve or authorize the device before it can be fully managed.

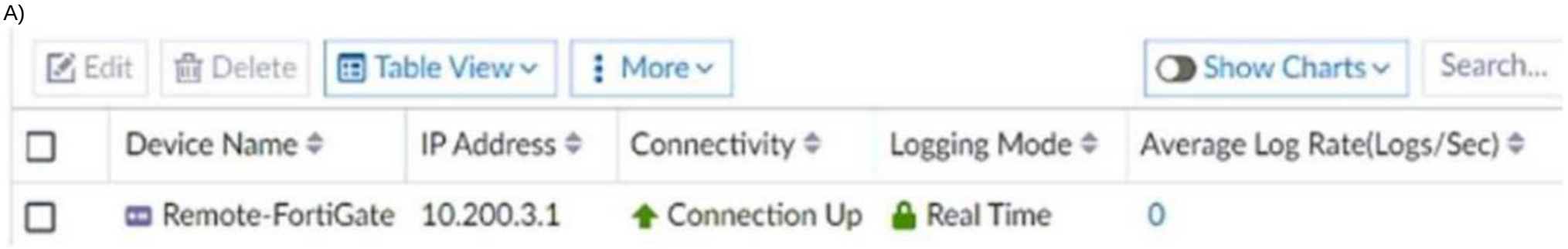
NEW QUESTION 8
Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

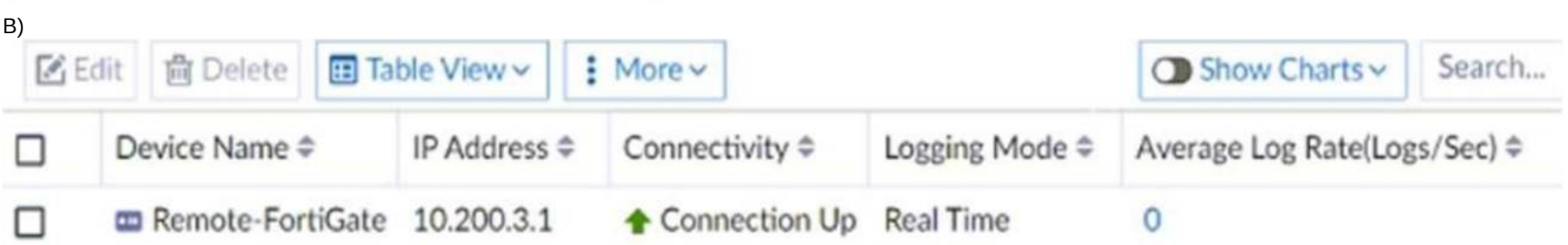


Which image corresponds to the packet capture shown in the exhibit?

A)

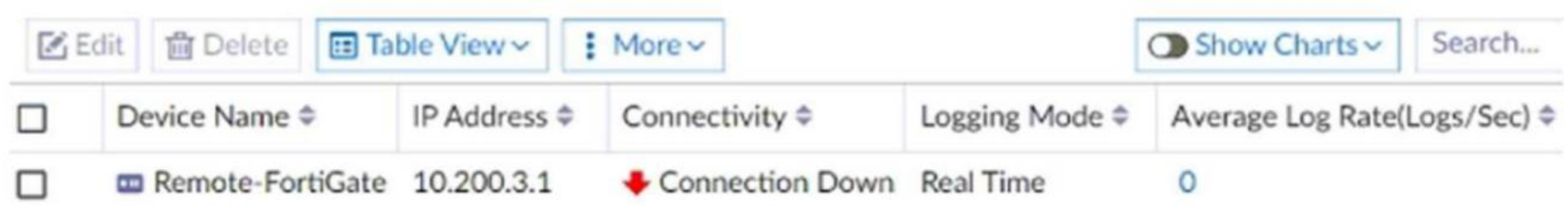


B)



C)

D)



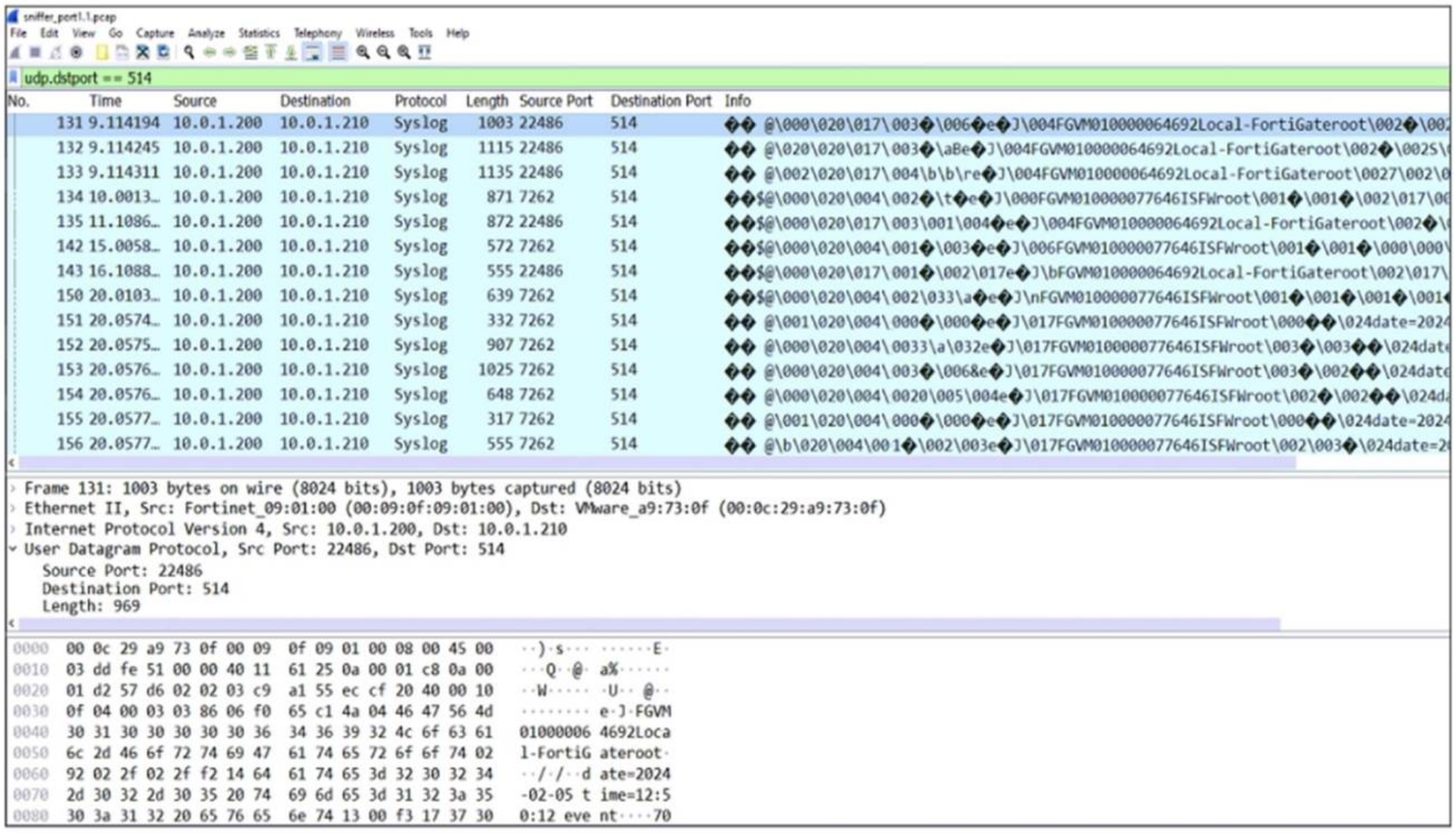
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.

NEW QUESTION 9
Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



The capture displayed was taken on a FortiAnalyzer.
Why is a single IP address shown as the source for all logs received?

A. FortiAnalyzer is using the device MAC addresses to differentiate their logs.
B. The logs belong to devices that are part of a high availability (HA) cluster.
C. FortiAnalyzer is receiving logs from the root FortiGate of a Security Fabric.
D. The device sending logs has two VDOMs in the same ADOM.

Answer: C

Explanation:
In a Fortinet Security Fabric, logs from downstream devices can be sent to FortiAnalyzer through the root FortiGate. This is why all the logs have the same source IP address (the root FortiGate). The root FortiGate aggregates and forwards the logs from all downstream devices, so the source IP in the log capture will appear to be from the root FortiGate itself, even though the logs originate from multiple devices within the fabric.

NEW QUESTION 10
Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

A. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
B. FortiAnalyzer HA active-passive mode can function without VRRP.
C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
D. All devices in a FortiAnalyzer HA cluster must have the same available disk space.

Answer: A

Explanation:
The two correct statements about high availability (HA) on FortiAnalyzer are:
FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
FortiAnalyzer HA synchronizes both logs and certain system configuration settings between the units in the cluster to ensure consistent operation.
All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
In an HA cluster, all devices must be configured to operat` e in the same mode --- either analyzer mode or collector mode---to ensure consistency and proper functionality across the cluster.
The other options, such as VRRP, are not required for HA in FortiAnalyzer, and disk space can vary between nodes but may impact log storage capacity.

NEW QUESTION 10
Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them togethe
B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyze
D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:
This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 15
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 file
B. To encrypt log transfer between FortiAnalyzer and other device
C. To create the secure channel used by the OFTP proces
D. To verify the integrity of the log files received.

Answer: A

Explanation:
:
The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

NEW QUESTION 18
Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:
RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

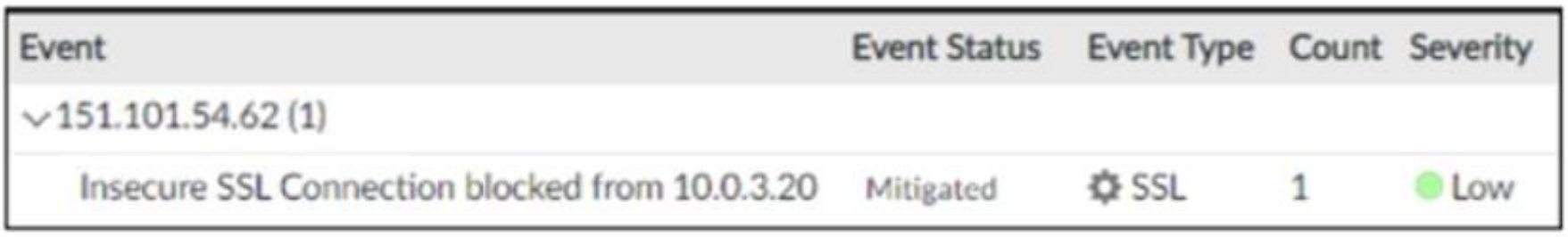
NEW QUESTION 21
What is the recommended method of expanding disk space on a FortiAnalyzer VM?

A. From the VM host manager, add an additional virtual disk and use the #execute lvm extendcommand 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 # executeformat 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:
Adding an Additional Virtual Disk:
From the VM host manager (such as VMware vSphere or Hyper-V), you can add a new virtual disk to the FortiAnalyzer VM.
Extending the Logical Volume:
After adding the new disk, use commands like #execute lvm extend within the FortiAnalyzer to extend the logical volume, making the additional storage available to the VM. This is particularly useful when you need to add more storage without disrupting existing data.
This approach is recommended when you need to ensure the FortiAnalyzer VM can handle more storage without reformatting or affecting existing data.

NEW QUESTION 26
Refer to the exhibit.



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.

Answer: B

Explanation:
The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented.
Events in FortiAnalyzer will be in one of four statuses.
The current status will determine if more actions need to be taken by the security team or not.
The possible statuses are: Unhandled: The security event risk is not mitigated or contained, so it is considered open.
Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped.

NEW QUESTION 31
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)

Answer: AC

Explanation:
FortiAnalyzer acts as a central repository for collecting and storing logs from multiple Fortinet devices. This centralized log management facilitates efficient analysis, search, and correlation of logs from across the network.
FortiAnalyzer provides robust reporting capabilities, allowing users to generate detailed reports based on collected logs and data. These reports can include insights on security events, network performance, and compliance.
Cloud-based management is not a primary feature of FortiAnalyzer, as it is typically an on-premises appliance, although it can integrate with cloud services.
Virtual domains (VDOMs) are a feature of FortiGate devices, allowing them to be partitioned into multiple virtual domains for administrative and policy separation.
FortiAnalyzer itself does not provide VDOMs.

NEW QUESTION 35
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FAZ_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FAZ_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

Money Back Guarantee

FCP_FAZ_AD-7.4 Practice Exam Features:

* FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently

* FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year