Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

NEW QUESTION 1
Which process caches logs on FortiGate when FortiAnalyzer is not readable?

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

Answer: A

Explanation:
The processlogfiledin FortiGate units with an SSD disk is responsible for buffering logs when FortiAnalyzer is unreachable. If the connection to FortiAnalyzer is lost and the memory log buffer is full,logfiledallows logs to be buffered on disk. These logs are then sent to FortiAnalyzer once the connection is restored. This reliable logging mechanism ensures that logs are not lost during periods when FortiAnalyzer is not reachable, thereby maintaining log integrity and continuity.References:FortiOS 7.4.1 Administration Guide, "Log Buffering" and "Reliable Logging" sections.

NEW QUESTION 2
Which command can you use to find the IP addresses of the devices sending logs to FortiAnalyzer?

A. diagnose debug applicationoftpd 8
B. diagnose dvm adorn List
C. diagnose teatapplication miglogd6
D. diagnose bestapplicationoftpd 3

Answer: A

Explanation:
The commanddiagnose debug application oftpd 8is used to obtain detailed debug output for the OFTP (Over the FortiGate Protocol) daemon on FortiAnalyzer. This protocol is responsible for the communication and log transfer between FortiGate devices and FortiAnalyzer. By using this debug level, administrators can find information including the IP addresses of devices that are sending logs to FortiAnalyzer.References:FortiOS 7.4.1 Administration Guide, "Diagnostic commands" section.

NEW QUESTION 3
Which statement is true about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer?

A. Each cluster member sends its logs directly to FortiAnalyzer.
B. You must add the device lo the cluster first, and thenregistersthe cluster with FortiAnalyzer.
C. FortiAnalyzer distinguishes each cluster member by its MAC address.
D. Only the primary device in the cluster communicates with FortiAnalyzer.

Answer: D

Explanation:
In a FortiGate high availability (HA) cluster, only the primary device sends its logs to the FortiAnalyzer. This is to ensure that logs are not duplicated between the primary and secondary devices in the cluster. The configuration of the FortiAnalyzer server on the FortiGate is such that the HA primary device is set as the server that forwards the logs.References:FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

NEW QUESTION 4
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.

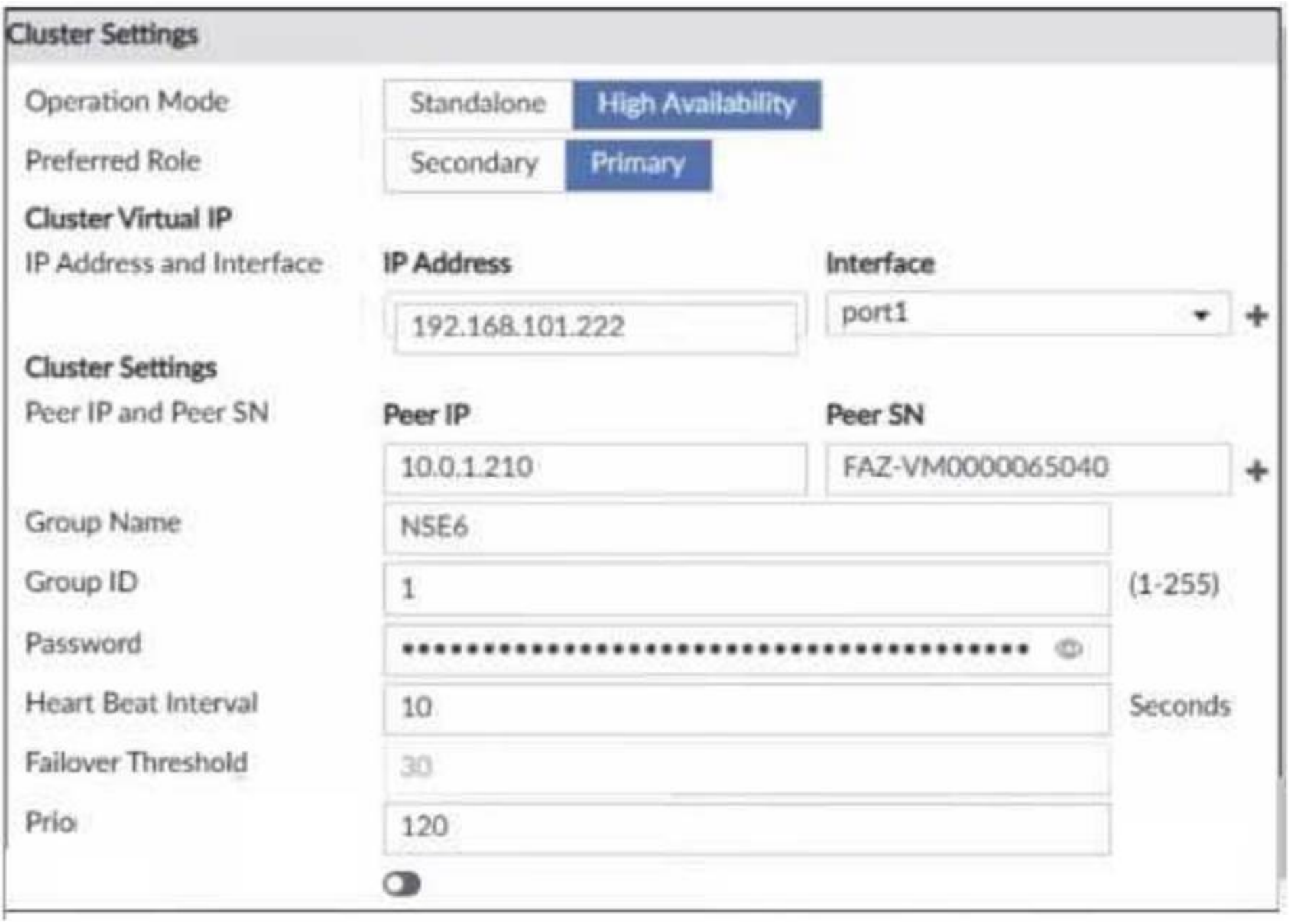
NEW QUESTION 5
Which two of the available registration methods place the device automatically in its assigned ADOM? (Choose two.)

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 6
Refer to the exhibit.



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 7
Which statement is true when you areupgrading the firmware on an HA cluster made up of throe FortiAnalyzer devices?

A. All FortiAnalyzer devices will be upgraded at the same time.
B. Enabling uninterruptible-upgrade prevents normal operations from being interrupted during the upgrade.
C. You can perform thefirmware upgrade using only a console connection.
D. First, upgrade the secondary devices, and then upgrade the primary device.

Answer: D

Explanation:
In an HA cluster, the firmware upgrade process involves upgrading the secondary devices first. This approach ensures that the primary device can continue to handle traffic and maintain the operational stability of the network while the secondary devices are being upgraded. Once the secondary devices have successfully upgraded their firmware and are operational, the primary device can then be upgraded. This method minimizes downtime and maintains network integrity during the upgrade process.
When upgrading firmware in a High Availability (HA) cluster of FortiAnalyzer units, the recommended practice is to first upgrade the secondary devices before upgrading the primary device. This approach ensures that the primary device, which coordinates the cluster's operations, remains functional for as long as possible, minimizing the impact on log collection and analysis. Once the secondary devices are successfully upgraded and operational, the primary device can be upgraded, ensuring a smooth transition and maintaining continuous operation of the cluster.References:FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

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

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

Answer: AC

Explanation:
The amount of reserved disk space required by FortiAnalyzer is influenced by the disk size and the RAID level. The system reserves a portion of the disk space for system use and unexpected quota overflow, with the rest available for device allocation. The RAID level determines the disk size and the reserved disk quota level, with different RAID configurations leading to variations in the reserved space.References:FortiAnalyzer 7.2 Administrator Guide, "Disk Space Allocation" and "RAID Level Impact" sections.

NEW QUESTION 10
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

A. The traffic destination is another FoitiGate in the fabric.
B. Log redundancy is configured in the fabric.
C. The upstream FortiGate is configured to do NAT.
D. The downstream device cannot connect to FortiAnalyzer.

Answer: D

Explanation:
In a Fortinet Security Fabric, an upstream FortiGate may create traffic logs for sessions initiated on downstream FortiGate devices if the downstream device is unable to connect to FortiAnalyzer. This allows for continuity of logging and ensures that session logs are captured and stored even if the downstream device loses its connection to the log management system.References:FortiAnalyzer 7.4.1 Administration Guide, "Fortinet Security Fabric" section.

NEW QUESTION 10
Which feature can you configure to add redundancy to FortiAnalyzer?

A. Primary and secondary DNS
B. VLAN interfaces
C. IPv6 administrative access
D. Link aggregation

Answer: D

Explanation:
Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable.References:The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 15
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Shul down FortiAnalyzer and replace the disk.

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

Answer: B

Explanation:
In systems that support hardware RAID, hot swapping allows for the replacement of a failed disk without shutting down the system. This capability is crucial for maintaining uptime and ensuring data redundancy and availability, especially in critical environments. The RAID controller rebuilds the data on the new disk using redundancy data from the other disks in the array, ensuring no data loss and minimal impact on system performance.
In the context of a FortiAnalyzer unit equipped with hardware RAID support, the optimal approach to addressing a hard disk failure is to perform a hot swap of the disk. Hardware RAID configurations are designed to provide redundancy and fault tolerance, allowing for the replacement of a failed disk without the need to shut down the system. Hot swapping enables the administrator to replace the faulty disk with a new one while the system is still running, and the RAID controller will rebuild the data on the new disk, restoring the RAID array to its fully operational state.References:FortiAnalyzer 7.2 Administrator Guide - "Hardware Maintenance" and "RAID Management" sections.

NEW QUESTION 17
What are analytics logs on FortiAnalyzer?

A. Logs that are compressed and saved to a log file
B. Logs that roll over when the log file reaches a specific size
C. Logs that are indexed and stored in the SQL
D. Logs classified as type Traffic, or type Security

Answer: C

Explanation:
On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.
Reference:
FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

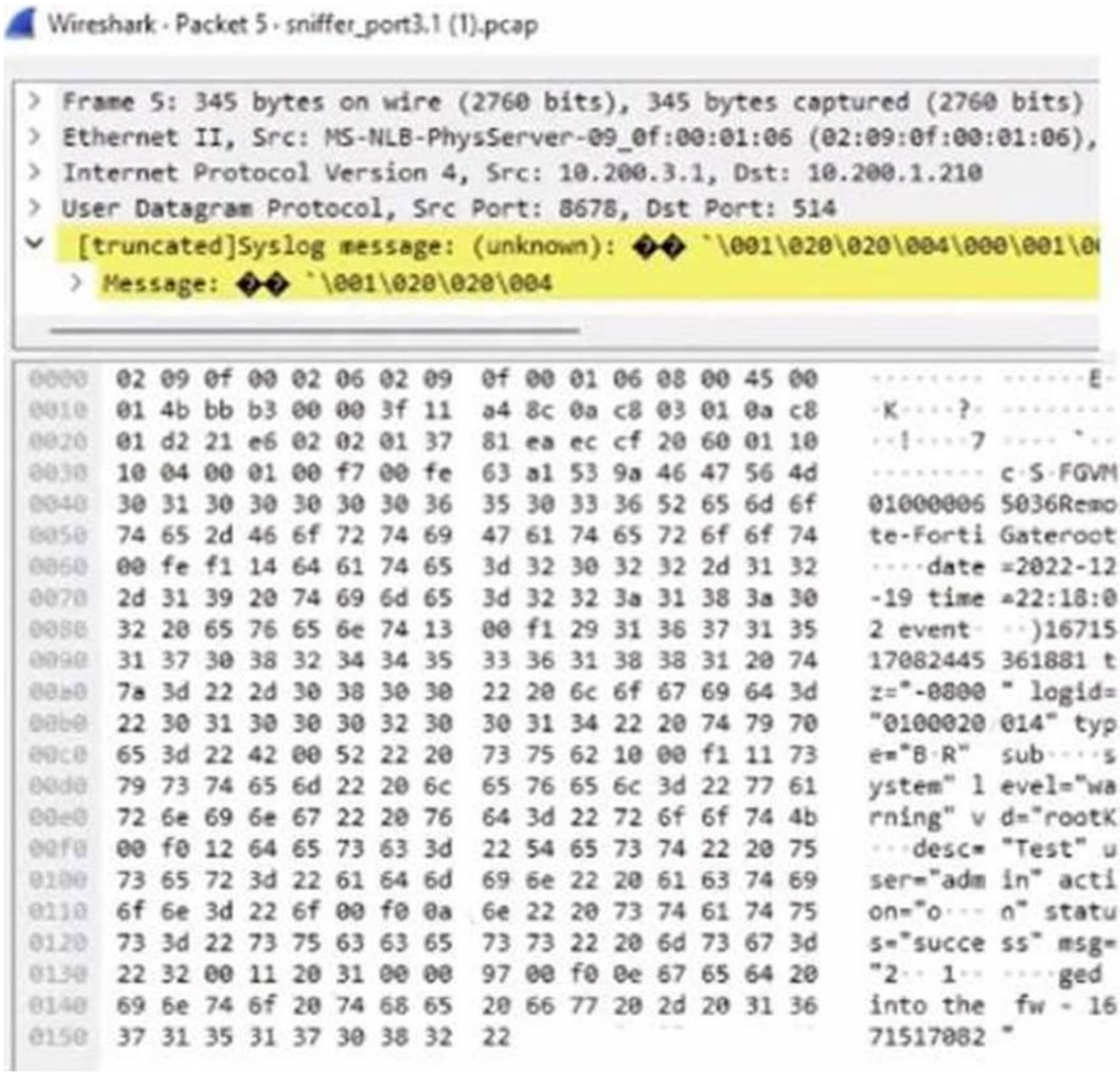
NEW QUESTION 22
Which items must you configure on FortiAnalyzer to send its reports to an external server?

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.

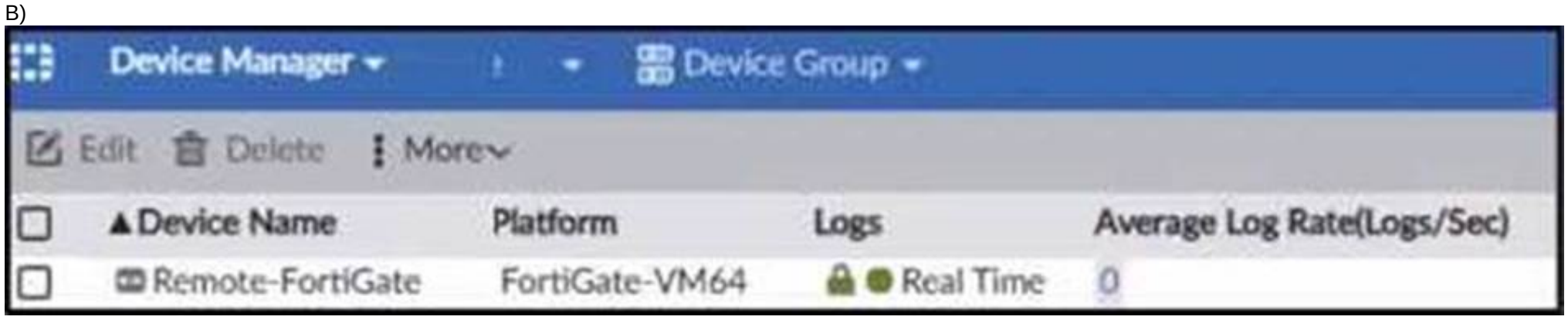
NEW QUESTION 24
Refer to the exhibit.



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

A)

B)



C)

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 28
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE6_FAZ-7.2 Practice Exam Features:

* NSE6_FAZ-7.2 Questions and Answers Updated Frequently

* NSE6_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year