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
You finished registering a FortiGate device. After traffic starts to flow through FortiGate. you notice that only some of the logs expected are being received on FortiAnalyzer.
What could be the reason for the logs not arriving on FortiAnalyzer?

A. FortiGate does not have logging configured correctly.
B. This FortiGate model is not fully supported.
C. This FortiGate is part of an HA cluster but it is the secondary device.
D. FortiGate was added to the wrong ADOM type.

Answer: A

Explanation:
When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 4
Which two statements are true regarding FortiAnalyzer system backups? (Choose two.)

A. Existing reports can be included in the backup files.
B. The system reserves at least 5% to 20% disk space for backup files.
C. Scheduled system backups can be configured only from the CLI.
D. Backup files can be uploaded to SCP and SFTP servers.

Answer: AD

Explanation:
FortiAnalyzer allows for the inclusion of existing reports in the backup files, providing a comprehensive backup of configurations and data. Additionally, the backup files can be configured to be uploaded to SCP and SFTP servers, ensuring secure transfer and offsite storage of backup data. This can be configured both in the GUI and the CLI, providing flexibility in how backups are scheduled and managed.References:FortiAnalyzer 7.4.1 Administration Guide, "Scheduling automatic backups" section.

NEW QUESTION 5
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
:onsole-output
:ountry-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 6
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.

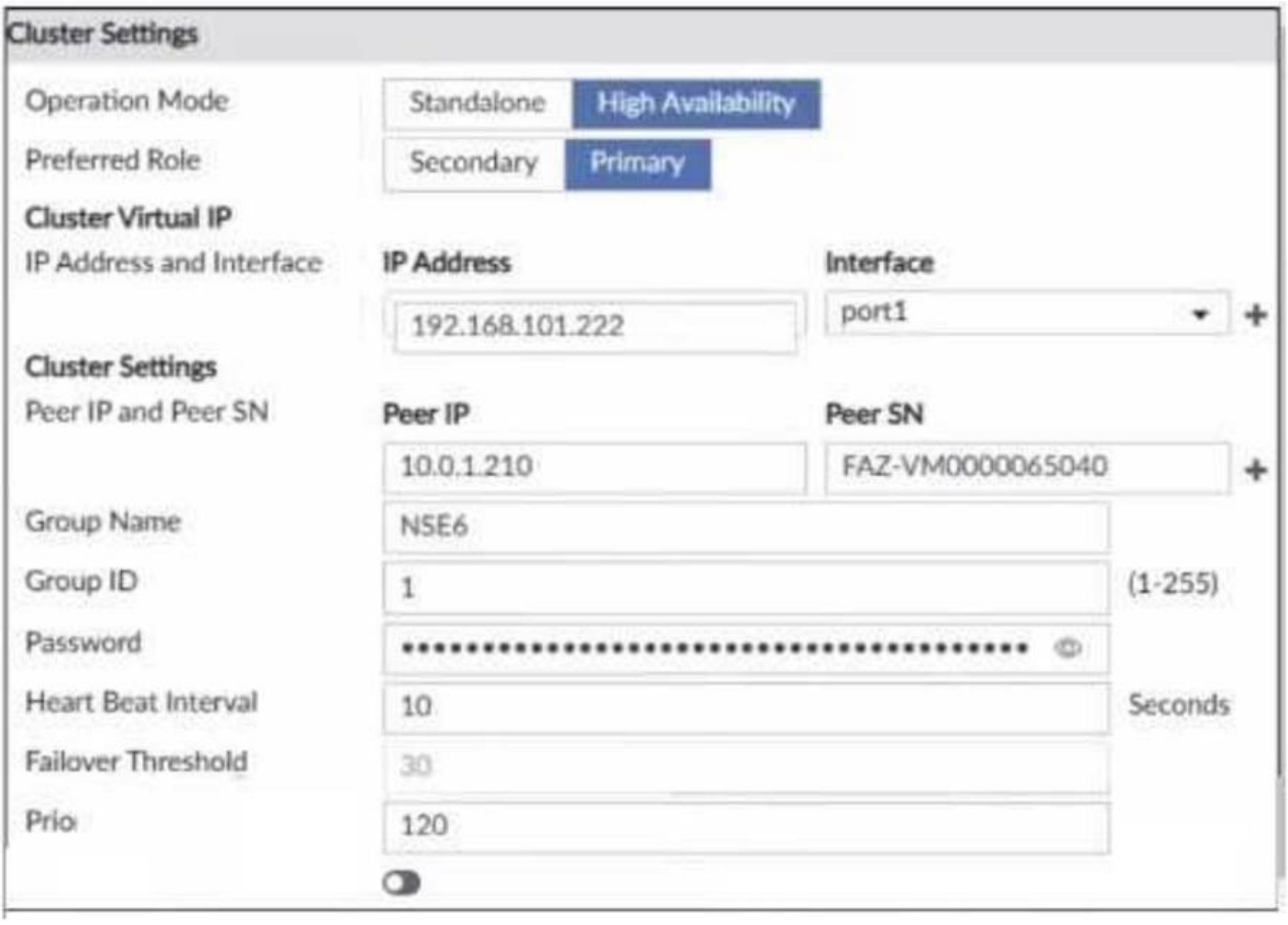
NEW QUESTION 7
Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

A. Use administrator profiles.
B. Configure trusted hosts.
C. Fabric connectors to external LDAP servers.
D. Limit access to specific virtual domains.

Answer: AB

Explanation:
To restrict administrative access on FortiAnalyzer, two effective methods are using administrator profiles and configuring trusted hosts.
Administrator profiles allow for defining the level of access and permissions for different administrators, controlling what each administrator can see and do within the FortiAnalyzer unit. Configuring trusted hosts enhances security by limiting administrative access to specified IP addresses, ensuring that administrators can only connect from approved locations or networks, thus preventing unauthorized access from outside specified subnets or IP addresses. Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Administrators' and 'Trusted hosts' sections.

NEW QUESTION 8
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 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
Which statement is true about using aggregation mode on FortiAnalyzer?

A. Aggregation mode supports log filters.
B. Aggregation mode can work with syslog servers.
C. In aggregation mode, logs and content files are forwarded in real time.
D. Aggregation mode can be configured only on the CLI.

Answer: B

Explanation:
In aggregation mode, FortiAnalyzer stores logs received from devices and forwards them at a specified time each day to avoid duplication. It is specifically designed to work between two FortiAnalyzer units and does not support syslog or CEF servers. Additionally, aggregation mode configurations are limited to CLI commandslog-forwardandlog-forward-service.References:FortiAnalyzer 7.2 Administrator Guide, "Aggregation" and "CLI Commands for Aggregation Mode" sections.

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 13
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.

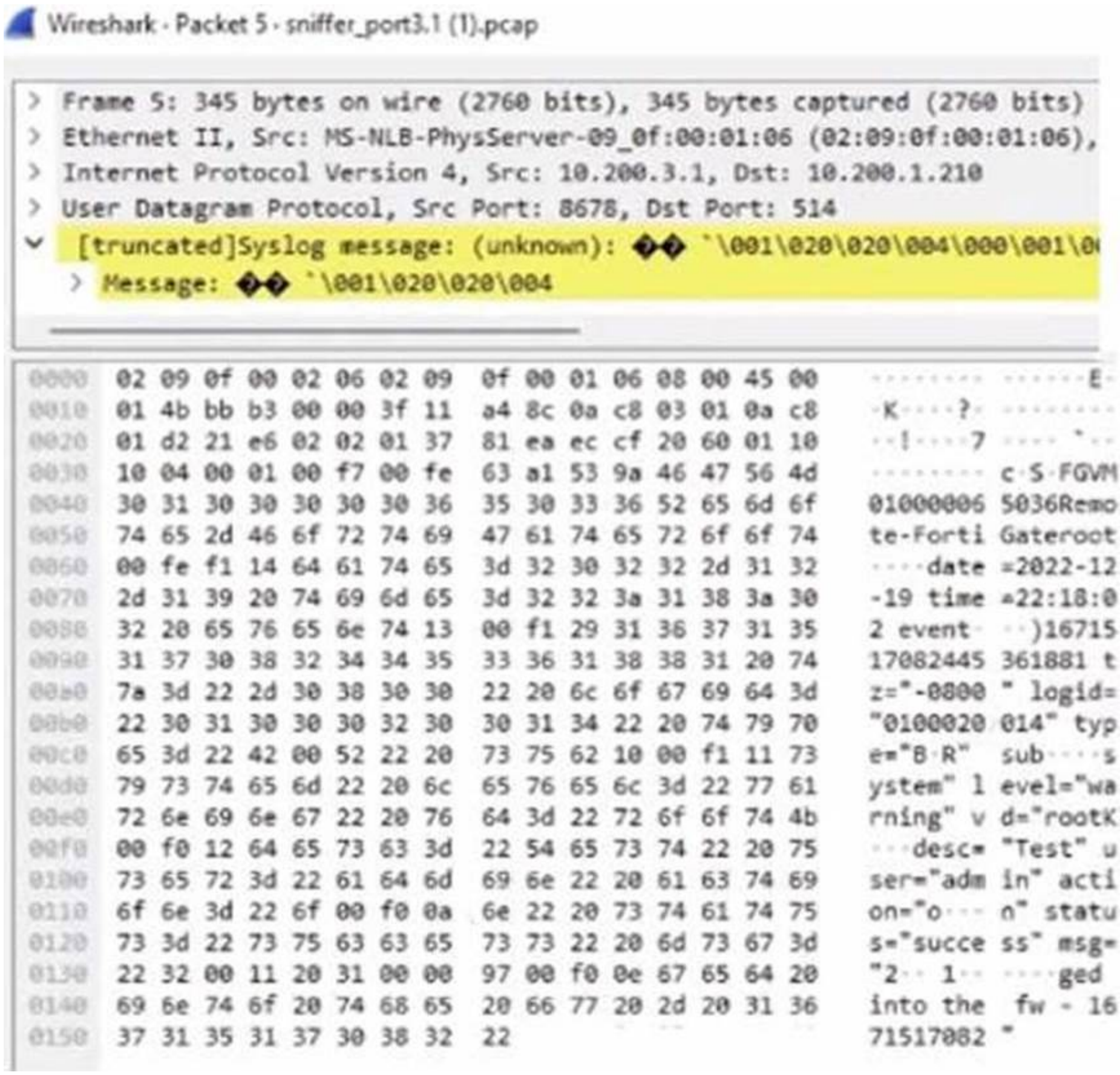
NEW QUESTION 16
Which items must you configure on FortiAnalyzer to send its reports to an external server?

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.

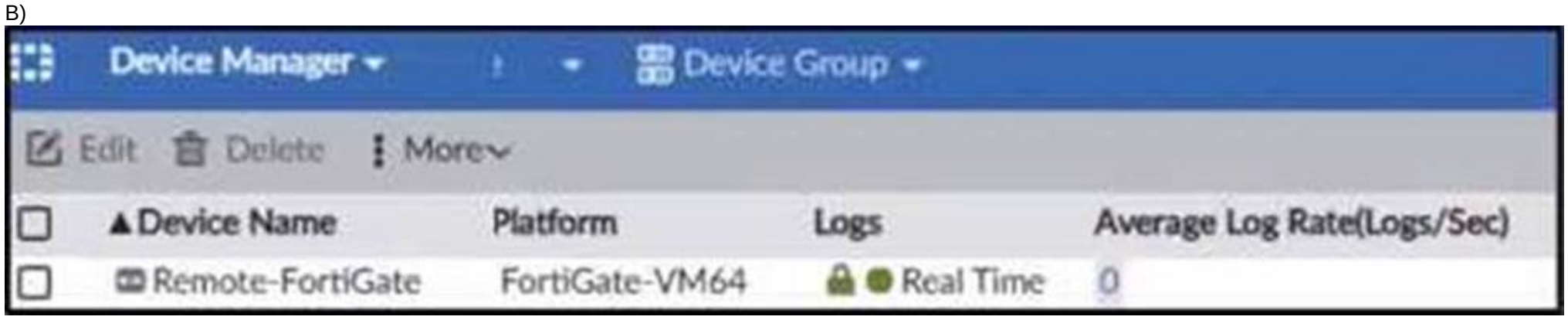
NEW QUESTION 20
Refer to the exhibit.



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 22
.....

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