Fortinet

Exam Questions NSE6_FAZ-7.2

Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

NEW QUESTION 1
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 2
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 3
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 4
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 5

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 6
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 7
An administrator, fortinet, can view logs and perform device management tasks, such as adding and removing registered devices.
However, administrator fortinet is not able to create a mail server that can be used to send alert emails.
What can be the problem?

A. ADOM mode is configured with Advanced mode.
B. fortinet is assigned the Standard_User administrative profile.
C. A trusted host is configured.
D. fortinet is assigned Restricted_User administrative profile.

Answer: B

Explanation:
If the administrator 'fortinet' can view logs and perform device management tasks but cannot create a mail server for alert emails, it is likely due to the administrative profile assigned to them. The Standard_User administrative profile may restrict certain administrative functions, such as creating mail servers. To perform all administrative tasks, including creating mail servers, a higher privilege profile, such as Super_Admin, might be required. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Mail Server' section.

NEW QUESTION 8
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 9
After you have moved a registered logging device out of one ADOM and into a new ADOM, you run the following command: execute sql-local rebuild-adom <new-ADOM-name>
What is the purpose of running this CLI command?

A. To reset the ADOM disk quota enforcement to its default value
B. To migrate the archive logs to the new ADOM
C. To populate the new ADOM with analytical logs for the moved device, so you can run reports
D. To remove the analytics logs of the device from the old database

Answer: C

Explanation:
When you move a registered logging device from one ADOM (Administrative Domain) to another in FortiAnalyzer, it's essential to ensure that the analytical logs for the moved device are available in the new ADOM to maintain continuity in reporting and log analysis. The commandexecute sql-local rebuild-adom < new-ADOM-name>is used specifically for this purpose. Running this command populates the new ADOM with the analytical logs of the moved device, enabling you to generate accurate and comprehensive reports based on the historical data of the device in its new ADOM context. This process ensures that the transition of devices between ADOMs does not lead to a loss of analytical insight or reporting capabilities for the device's traffic and events.

NEW QUESTION 10
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. LDAP servers IP addresses added as trusted hosts
B. One or more remote LDAP servers
C. A local wildcard administrator account
D. An administrator group

Answer: BD

Explanation:
To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate.References:FortiAnalyzer 7.2 Administrator Guide, "Configuring remote authentication for administrators using LDAP" section.

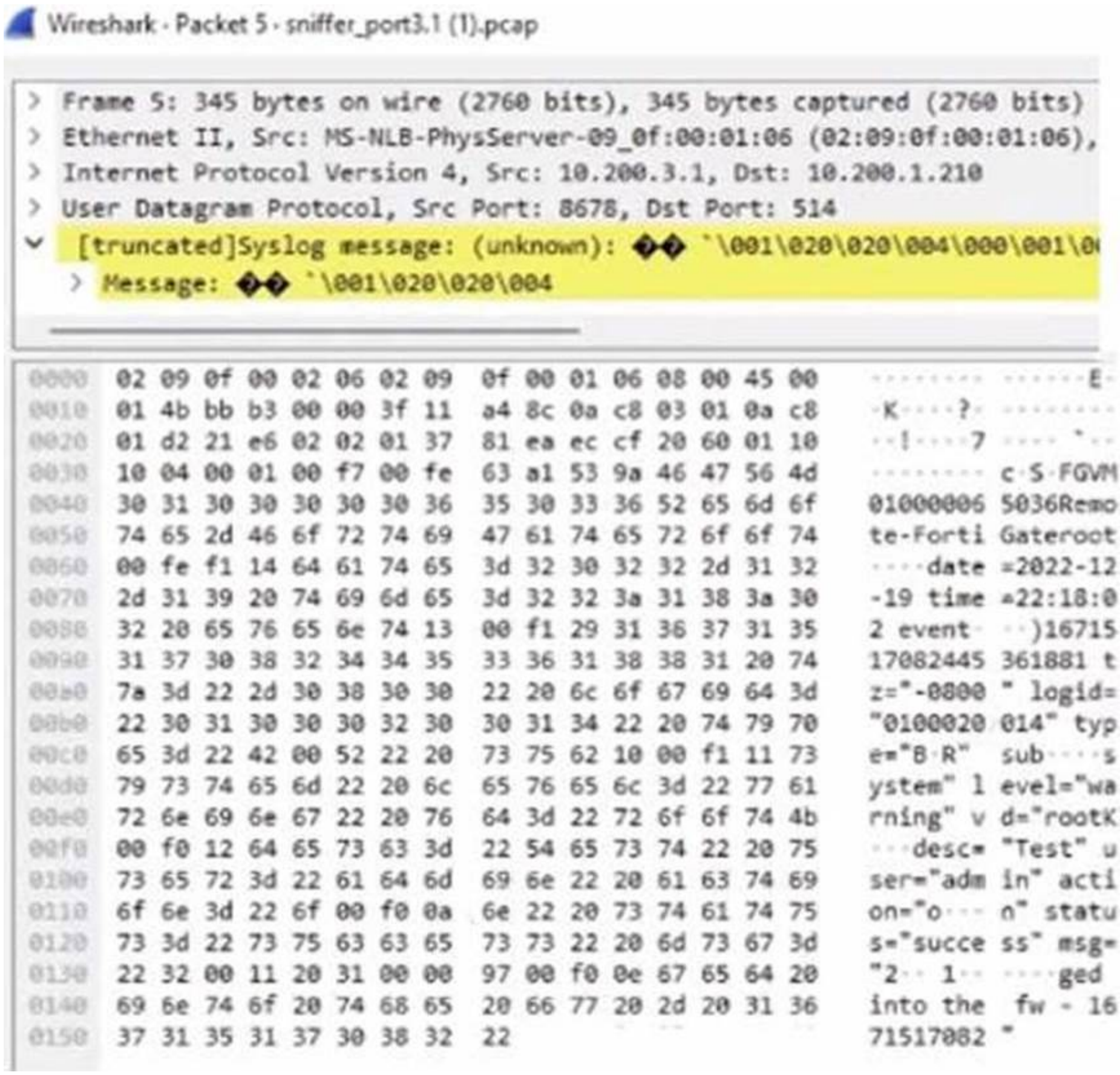
NEW QUESTION 10
Which items must you configure on FortiAnalyzer to send its reports to an external server?

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.

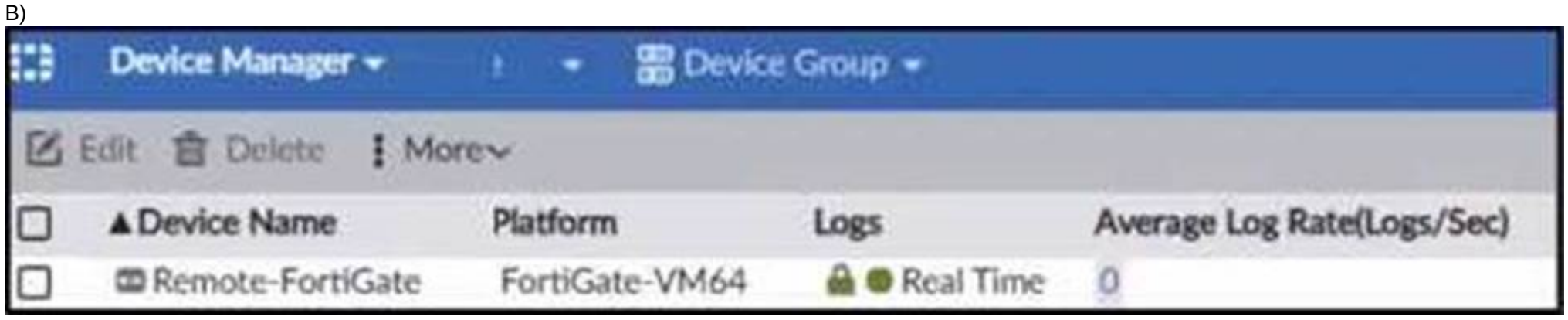
NEW QUESTION 14
Refer to the exhibit.



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 19
.....

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