Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1
An administrator has moved a FortiGate device from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be present in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:
When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

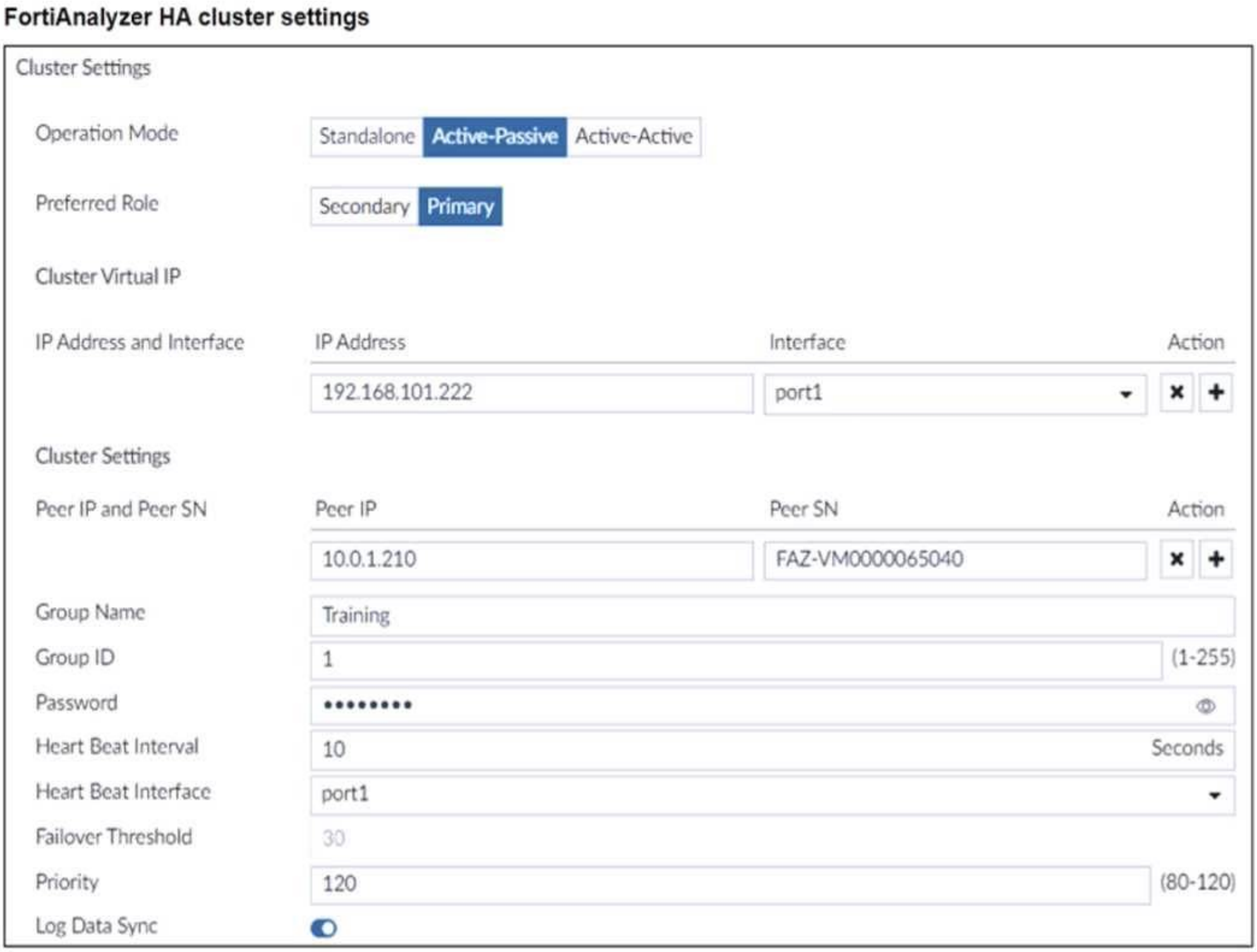
NEW QUESTION 2
Which process is responsible for enforcing the log file size?

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
Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.



The administrator wants to join this FortiAnalyzer to an existing HA cluster. What can you conclude from the configuration displayed?

A. After joining the cluster, this FortiAnalyzer will forward received logs to its peers.
B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
C. This FortiAnalyzer is configured to route HA traffic through a gateway.

D. This FortiAnalyzer will join the existing HA cluster as the secondary.

Answer: B

Explanation:
The "Preferred Role" is set to Secondary, which means this FortiAnalyzer is configured to join the cluster as the secondary unit in an Active-Passive HA configuration. Other settings, such as the peer IP and serial number, confirm its setup to communicate with the primary unit.

NEW QUESTION 4
Which two statements about deleting ADOMs are true? (Choose two.)

A. Logs must be purged or migrated before you can delete an ADOM.
B. ADOMs with registered devices cannot be deleted.
C. Default ADOMs cannot be deleted.
D. The status of the ADOMs must be unlocked.

Answer: B

Explanation:
DOMs with registered devices cannot be deleted.
An ADOM cannot be deleted if it has registered devices. You must first remove or deregister the devices before deleting the ADOM.
The status of the ADOMs must be unlocked.
An ADOM must be in an unlocked state before it can be deleted. If the ADOM is locked, it will not allow deletion.

NEW QUESTION 5
You are trying to initiate an authorization request from FortiGate to FortiAnalyzer, but the Security Fabric window does not open when you click Authorize.
Which two reasons can cause this to happen? (Choose two.)

A. A pre-shared key needs to be established on both sides.
B. The management computer does not have connectivity to the authorization IP address and port combination.
C. The Security Fabric root is unauthorized and needs to be added as a trusted host.
D. The fabric authorization settings on FortiAnalyzer are misconfigured.

Answer: BD

Explanation:
The management computer does not have connectivity to the authorization IP address and port combination.
If there is no network connectivity between the management computer and the FortiAnalyzer on the specific IP address and port used for authorization, the Security Fabric window will not open.
The fabric authorization settings on FortiAnalyzer are misconfigured.
If the fabric authorization settings on FortiAnalyzer are not properly configured, FortiGate will not be able to initiate the authorization request, preventing the Security Fabric window from opening.
The other options are not applicable because:
Pre-shared keys are not required for initial authorization between FortiGate and FortiAnalyzer; they are typically used for establishing VPN tunnels.
The Security Fabric root does not need to be added as a trusted host to open the authorization window. Trusted hosts are more relevant to FortiGate's access control for management interfaces.

NEW QUESTION 6
Which three RAID configurations provide fault tolerance on FortiAnalyzer? (Choose three.)

A. RAIDO
B. RAID 5
C. RAID1
D. RAID 6+0
E. RAID 0+0

Answer: BCD

Explanation:
RAID 1 provides fault tolerance through disk mirroring.
RAID 5 provides fault tolerance by using distributed parity across multiple disks. RAID 6+0 combines striping with double parity, offering enhanced fault tolerance.
RAID 0 and RAID 0+0 do not provide any fault tolerance, as they focus on performance through data striping but offer no redundancy.

NEW QUESTION 7
Which two statements regarding ADOM modes are true? (Choose two.)

A. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advanced mode, the disk quota of the ADOM is flexible.
B. You can change ADOM modes only through the CLI.
C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
D. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 8
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 9
Which statement is true when you are upgrading 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 theupgrade.
C. You can perform the firmware 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.
Reference: FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

NEW QUESTION 10
Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

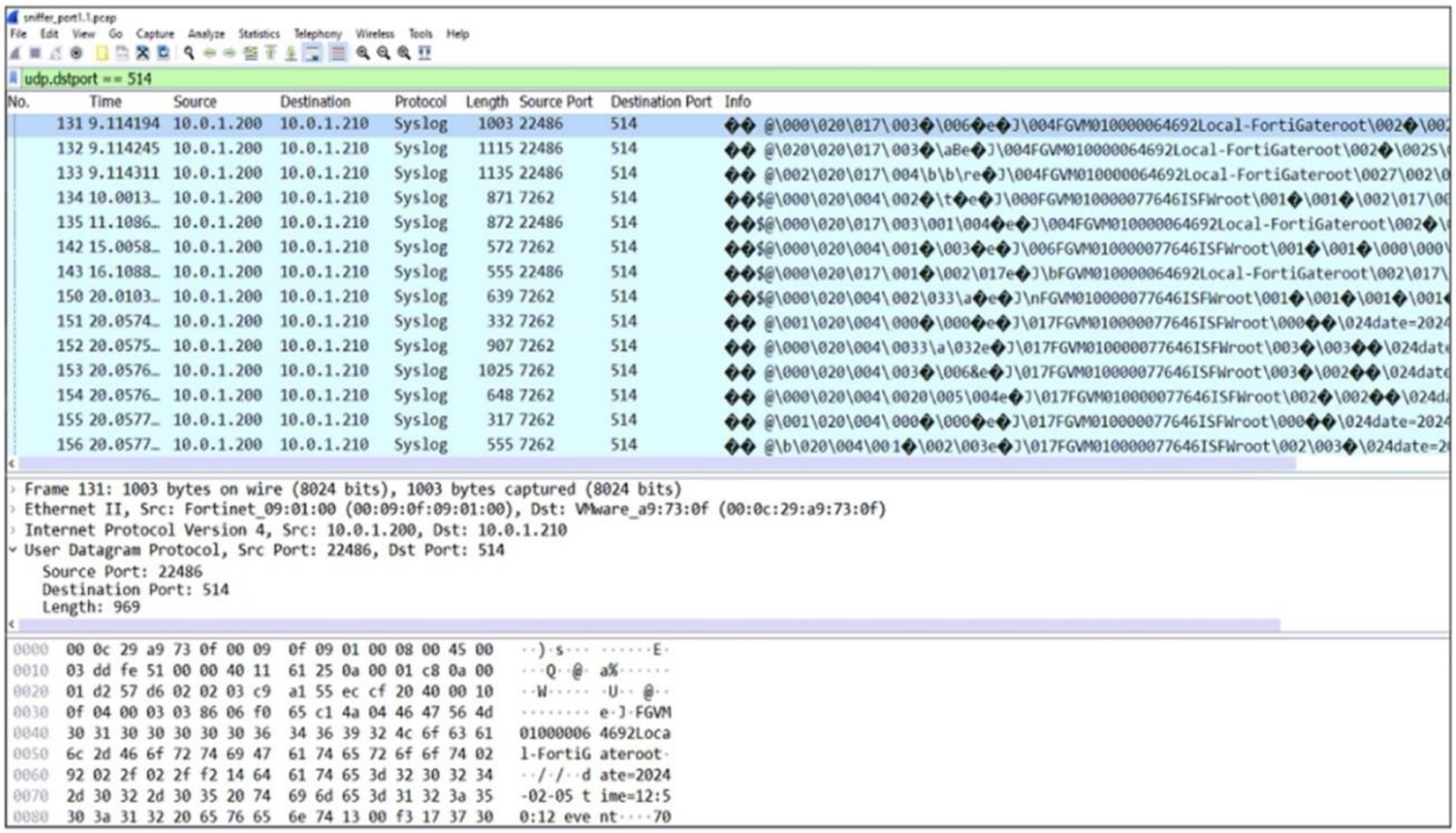
A. Configure trusted hosts.
B. Limit access to specific virtual domains.
C. Fabric connectors to external LDAP servers.
D. Use administrator profiles.

Answer: AD

Explanation:
Configure trusted hosts.
Trusted hosts restrict administrative access to FortiAnalyzer by limiting the IP addresses or subnets from which administrators can log in.
Use administrator profiles.
Administrator profiles define roles and permissions, restricting what specific administrators can access and manage on FortiAnalyzer.
The other options are not applicable because:
Limiting access to specific virtual domains is not applicable to FortiAnalyzer, as virtual domains (VDOMs) are a concept used in FortiGate, not FortiAnalyzer.
Fabric connectors to external LDAP servers are used for authentication purposes but do not directly restrict administrative access based on roles or IP addresses.

NEW QUESTION 10
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 15
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 20
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 21
What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data
B. To provide data separation between ADOMs
C. To separate analytical and archive data
D. To back up your logs

Answer: A

Explanation:
RAID (Redundant Array of Independent Disks) is used in FortiAnalyzer primarily to provide data redundancy and ensure data integrity. Here,s how it relates to each option:
To Introduce Redundancy to Your Log Data (Option A):
The main purpose of employing RAID in FortiAnalyzer is to add redundancy to the storage system. By using RAID configurations (such as RAID 1, RAID 5, or RAID 6), data is replicated across multiple disks, which helps in protecting against disk failures and ensures that log data is not lost if a disk fails. This redundancy enhances the reliability and availability of the log data.

NEW QUESTION 25
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator??s access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

Explanation:
ADOMs constrain other administrators' access privileges to a subset of devices in the device list: ADOMs allow you to partition the FortiAnalyzer's management capabilities by restricting access to certain devices and logs based on the administrator's role. This segmentation helps in managing large deployments with different administrative needs.
Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM: When ADOMs are enabled, the FortiAnalyzer interface segments the Device Manager, FortiView, Event Management, and Reports tabs based on the selected ADOM. This allows administrators to work within their specific ADOM context.
ADOMs are enabled by default: This is incorrect because ADOMs are not enabled by default. They must be manually configured and enabled according to the organization's needs.
All administrators can create ADOMs--not just the admin administrator: This is not correct. Typically, creating and managing ADOMs requires administrative privileges, often restricted to the main admin or specific roles with sufficient permissions.

NEW QUESTION 30
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 32
What FortiGate process caches logs when FortiAnalyzer is not reachable?

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

Answer: D

Explanation:
The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 36
How do you restrict an administrator's access to a subset of your organization's ADOMs?

A. Set the ADOM mode to Advanced
B. Assign the ADOMs to the administrator's account

C. Configure trusted hosts
D. Assign the default Super_User administrator profile

Answer: B

Explanation:
To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here??s how this works:
Assign the ADOMs to the Administrator's Account (Option B):
In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 40
.....

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

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