Free Questions for FCP_FAZ_AD-7.4

Shared by Hampton on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which process is responsible for enforcing the log file size?

Options:

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.

Question 2

Question Type: MultipleChoice

What does the disk status Degraded mean for RAID management?

Options:

A- The hard drive is no longer being used by the RAID controller.

B- One or more drives are missing from the FortiAnalyzer unit.

C- The device is writing data to the disk to restore the volume to an optimal state.

D- FortiAnalyzer determined that the parity data in the disk is not valid.

Answer:

B

Explanation:

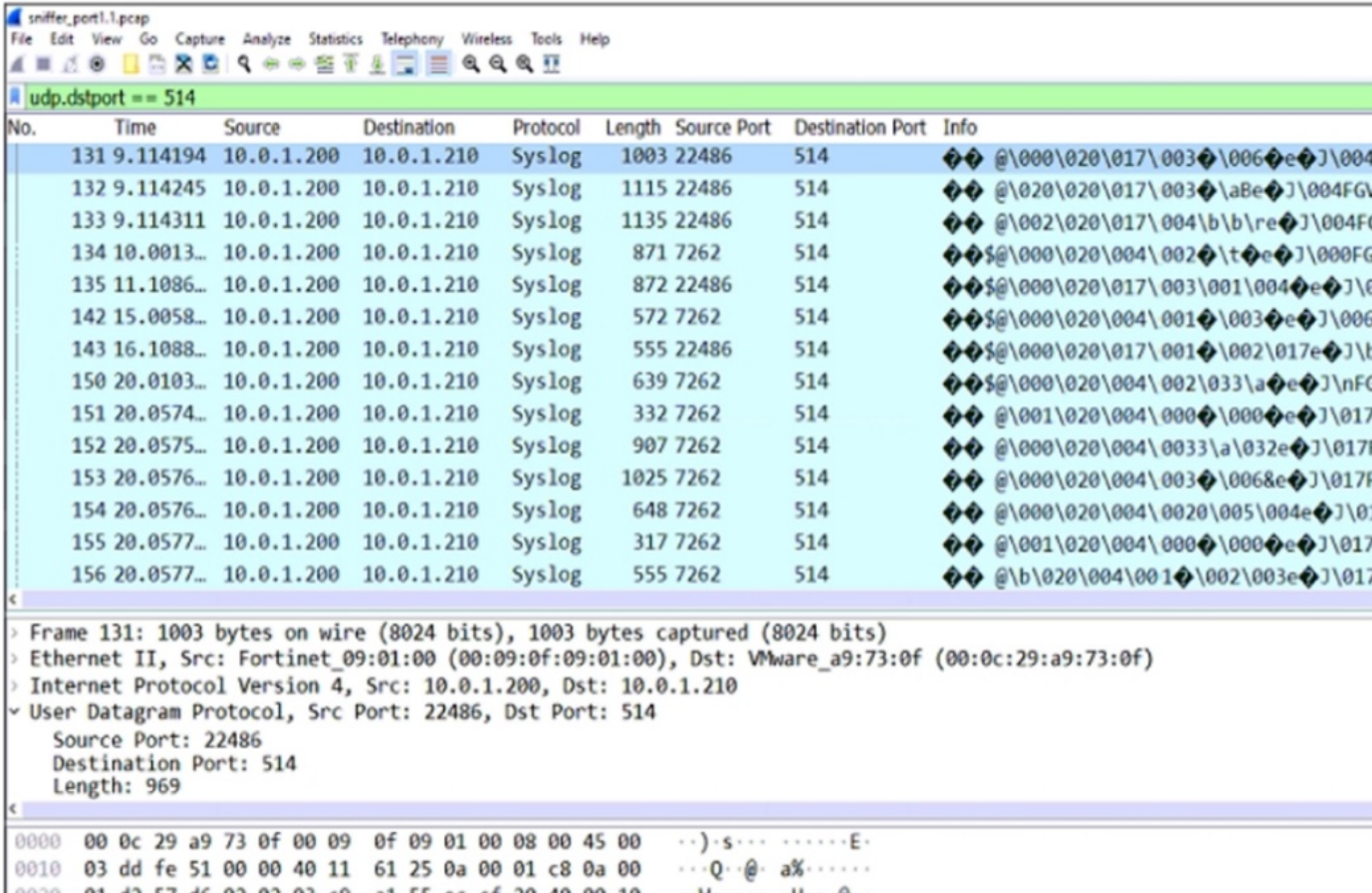
When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

Question 3

Question Type: **MultipleChoice**

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?

Options:

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.

Question 4

Question Type: MultipleChoice

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

Options:

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.

Question 5

Question Type: MultipleChoice

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

Options:

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.

Question 6

Question Type: MultipleChoice

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

Options:

A- The traffic destination is another FortiGate in the fabric.

B- The upstream FortiGate is configured to do NAT

C- Log redundancy is configured in the fabric.

D- The downstream device cannot connect to FortiAnalyzer.

Answer:

B

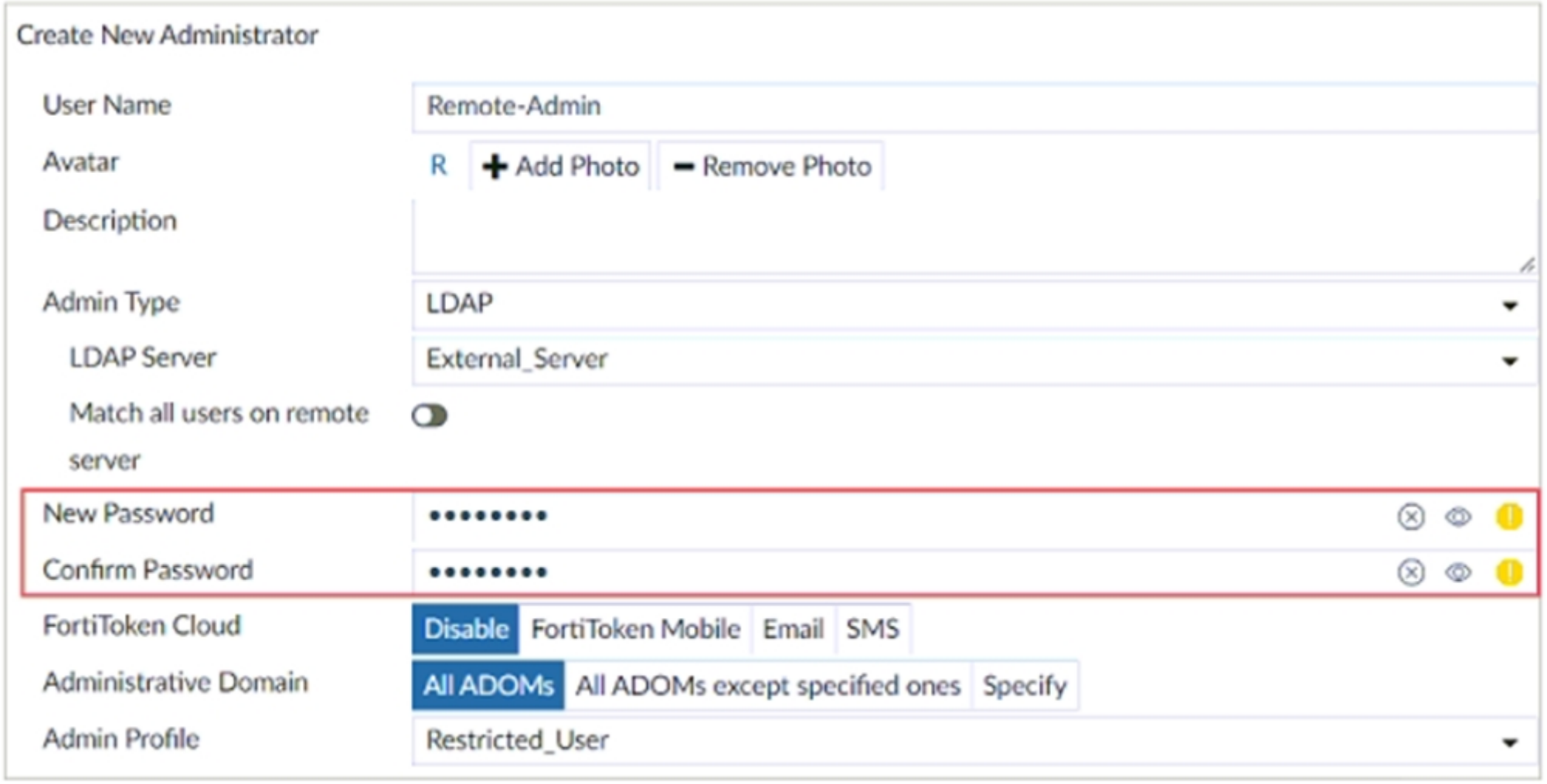
Explanation:

When the upstream FortiGate is performing Network Address Translation (NAT), it creates new session entries for traffic passing through it. As a result, it generates its own traffic logs for those sessions, even if the sessions were initiated on a downstream FortiGate. This is because the upstream FortiGate is altering the source IP address, making it responsible for tracking the session details.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



The exhibit shows the creation of a new administrator on FortiAnalyzer. The new account uses the credentials stored on an LDAP server.

Why would an administrator configure a password for this account?

Options:

A- This password is used if the authentication server becomes unreachable.

B- This password authenticates FortiAnalyzer aqainst the LDAP server.

C- This password is set to comply with FortiAnalvzer password policy

D- This password is required because this is a restricted user.

Answer:

A

Explanation:

When using LDAP for authentication, a password can be set locally on FortiAnalyzer as a fallback option in case the LDAP server becomes unreachable. This ensures that the administrator can still log in if there are issues with the LDAP server.

Question 8

Question Type: MultipleChoice

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

Options:

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.