Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1
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 2
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

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.

NEW QUESTION 3
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 4
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 5
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
C. For the collector, you should allocate most of the disk space to analytics logs.
D. Analyzer mode is the default operating mode.

Answer: B

Explanation:
When in analyzer mode, FortiAnalyzer supports event management and reporting features.
In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.
Analyzer mode is the default operating mode.
By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:
In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.
In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 6
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 7
Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

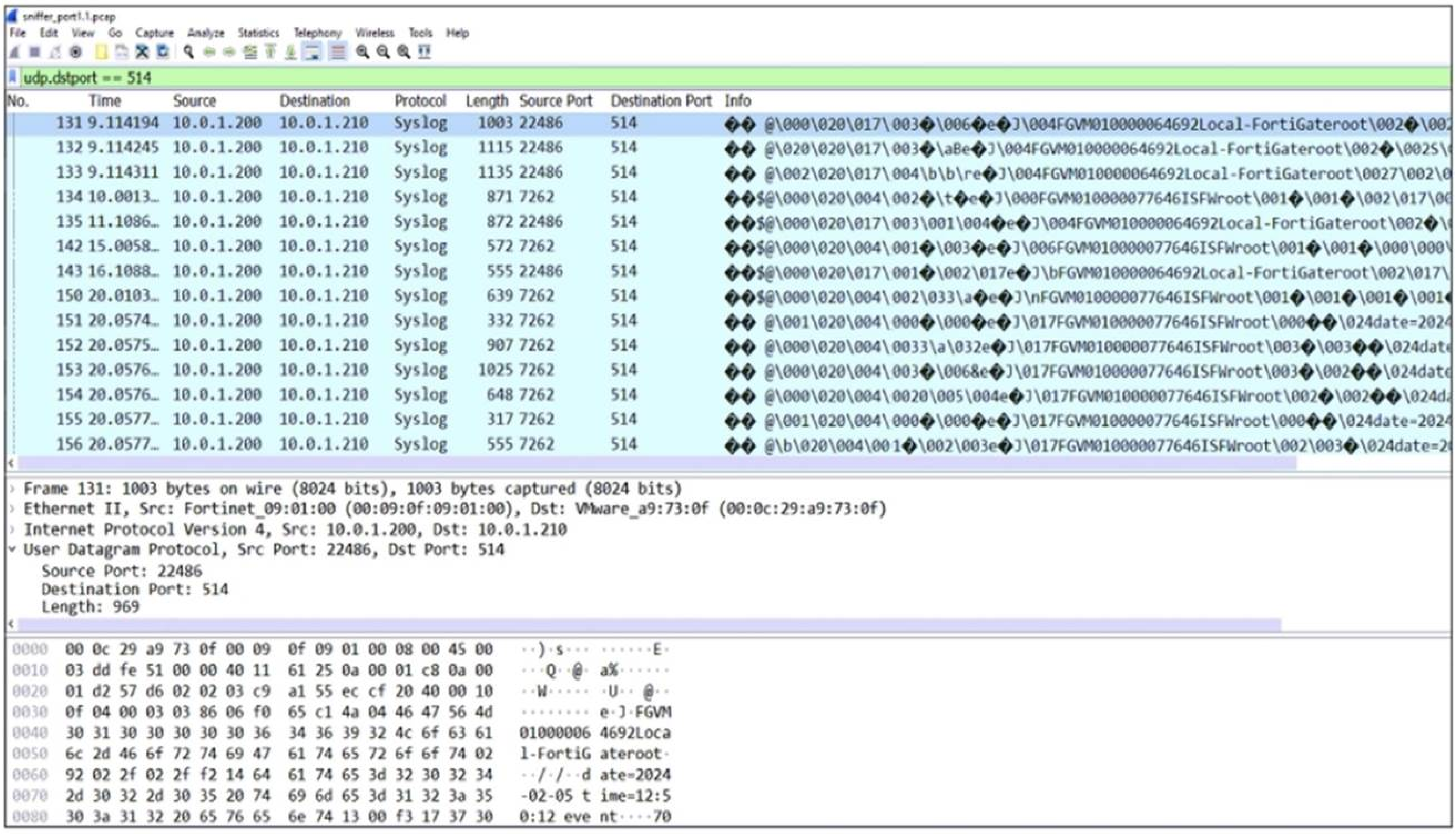
A. Configure trusted hosts.
B. Limit access to specific virtual domains.
C. Fabric connectors to external LDAP servers.
D. Use administrator profiles.

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 8
Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark


sniffer_port1.1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.dstport == 514
No.   Time      Source      Destination  Protocol  Length Source Port  Destination Port  Info
  131 9.114194  10.0.1.200  10.0.1.210   Syslog    1003 22486          514              �� @\000\020\017\003�\006�e�J\004FGVM010000064692Local-FortiGateroot\002�\002
  132 9.114245  10.0.1.200  10.0.1.210   Syslog    1115 22486          514              �� @\020\020\017\003�\aBe�J\004FGVM010000064692Local-FortiGateroot\002�\002S\
  133 9.114311  10.0.1.200  10.0.1.210   Syslog    1135 22486          514              �� @\002\020\017\004\b\b\re�J\004FGVM010000064692Local-FortiGateroot\0027\002\0
  134 10.0013…  10.0.1.200  10.0.1.210   Syslog     871 7262           514              ��$@\000\020\004\002�\t�e�J\000FGVM010000077646ISFWroot\001�\001�\002\017\00
  135 11.1086…  10.0.1.200  10.0.1.210   Syslog     872 22486          514              ��$@\000\020\017\003\001\004�e�J\004FGVM010000064692Local-FortiGateroot\002�\
  142 15.0058…  10.0.1.200  10.0.1.210   Syslog     572 7262           514              ��$@\000\020\004\001�\003�e�J\006FGVM010000077646ISFWroot\001�\001�\000\000\
  143 16.1088…  10.0.1.200  10.0.1.210   Syslog     555 22486          514              ��$@\000\020\017\001�\002\017e�J\bFGVM010000064692Local-FortiGateroot\002\017\
  150 20.0103…  10.0.1.200  10.0.1.210   Syslog     639 7262           514              ��$@\000\020\004\002\033\a�e�J\nFGVM010000077646ISFWroot\001�\001�\001�\001
  151 20.0574…  10.0.1.200  10.0.1.210   Syslog     332 7262           514              �� @\001\020\004\000�\000�e�J\017FGVM010000077646ISFWroot\000��\024date=2024
  152 20.0575…  10.0.1.200  10.0.1.210   Syslog     907 7262           514              �� @\000\020\004\0033\a\032e�J\017FGVM010000077646ISFWroot\003�\003��\024date
  153 20.0576…  10.0.1.200  10.0.1.210   Syslog    1025 7262           514              �� @\000\020\004\003�\006&e�J\017FGVM010000077646ISFWroot\003�\002��\024date
  154 20.0576…  10.0.1.200  10.0.1.210   Syslog     648 7262           514              �� @\000\020\004\0020\005\004e�J\017FGVM010000077646ISFWroot\002�\002��\024da
  155 20.0577…  10.0.1.200  10.0.1.210   Syslog     317 7262           514              �� @\001\020\004\000�\000�e�J\017FGVM010000077646ISFWroot\000��\024date=2024
  156 20.0577…  10.0.1.200  10.0.1.210   Syslog     555 7262           514              �� @\b\020\004\001�\002\003e�J\017FGVM010000077646ISFWroot\002\003�\024date=20

> Frame 131: 1003 bytes on wire (8024 bits), 1003 bytes captured (8024 bits)
> Ethernet II, Src: Fortinet_09:01:00 (00:09:0f:09:01:00), Dst: VMware_a9:73:0f (00:0c:29:a9:73:0f)
> Internet Protocol Version 4, Src: 10.0.1.200, Dst: 10.0.1.210
v User Datagram Protocol, Src Port: 22486, Dst Port: 514
    Source Port: 22486
    Destination Port: 514
    Length: 969

0000  00 0c 29 a9 73 0f 00 09  0f 09 01 00 08 00 45 00   ··)·s··· ······E·
0010  03 dd fe 51 00 00 40 11  61 25 0a 00 01 c8 0a 00   ···Q··@· a%······
0020  01 d2 57 d6 02 02 03 c9  a1 55 ec cf 20 40 00 10   ··W····· ·U·· @··
0030  0f 04 00 03 03 86 06 f0  65 c1 4a 04 46 47 56 4d   ········ e·J·FGVM
0040  30 31 30 30 30 30 30 36  34 36 39 32 4c 6f 63 61   01000006 4692Loca
0050  6c 2d 46 6f 72 74 69 47  61 74 65 72 6f 6f 74 02   l-FortiG ateroot·
0060  92 02 2f 02 2f f2 14 64  61 74 65 3d 32 30 32 34   ··/·/··d ate=2024
0070  2d 30 32 2d 30 35 20 74  69 6d 65 3d 31 32 3a 35   -02-05 t ime=12:5
0080  30 3a 31 32 20 65 76 65  6e 74 13 00 f3 17 37 30   0:12 eve nt····70
```

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.

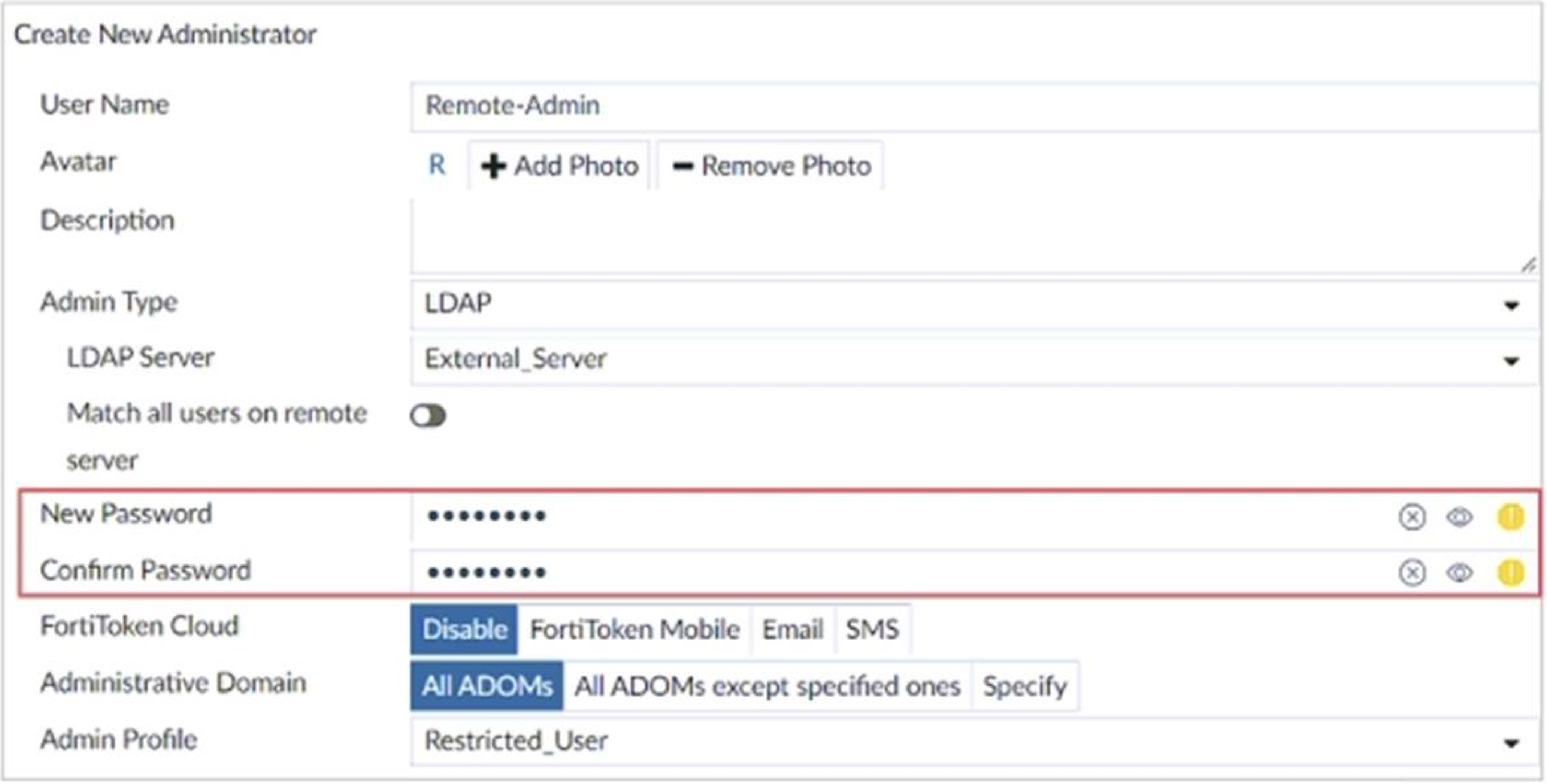
NEW QUESTION 9
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

A. The traffic destination is another 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.

NEW QUESTION 10
Refer to the exhibit.



Create New Administrator

User Name: Remote-Admin

Avatar: R

Description:

Admin Type: LDAP

LDAP Server: External_Server

Match all users on remote server: ○

New Password: ••••••••

Confirm Password: ••••••••

FortiToken Cloud: [✓ Disable] FortiToken Mobile Email SMS

Administrative Domain: [✓ All ADOMs] All ADOMs except specified ones Specify

Admin Profile: Restricted_User

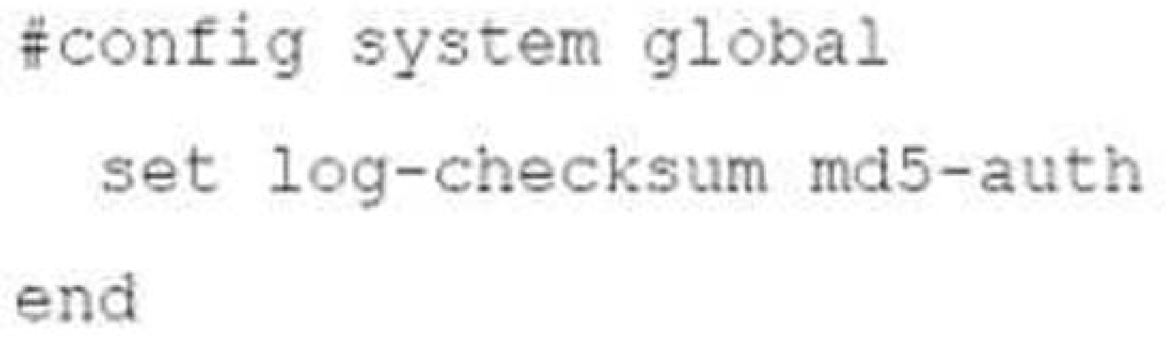
The exhibit shows the creation of a new administrator on FortiAnalyzer. The new account uses the credentials stored on an LDAP server.
Why would an administrator configure a password for this account?

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.

NEW QUESTION 10
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 file
B. To encrypt log transfer between FortiAnalyzer and other device
C. To create the secure channel used by the OFTP proces
D. To verify the integrity of the log files received.

Answer: A

Explanation:
:
The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

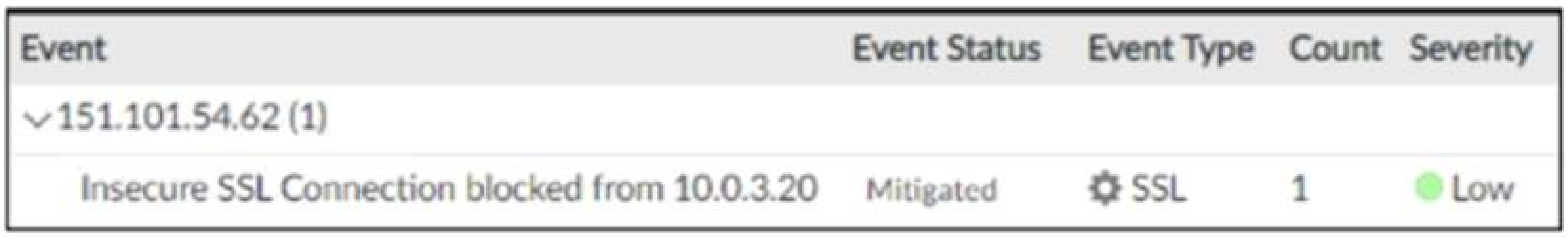
NEW QUESTION 13
Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:
RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION 15
Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
∨151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙ SSL	1	● Low

Which statement is correct regarding the event displayed?

A. An incident was created from this event.
B. The security risk was blocked or dropped.
C. The security event risk is considered open.
D. The risk source is isolated.

Answer: B

Explanation:
The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented.
Events in FortiAnalyzer will be in one of four statuses.
The current status will determine if more actions need to be taken by the security team or not.
The possible statuses are: Unhandled: The security event risk is not mitigated or contained, so it is considered open.
Contained: The risk source is isolated.
Mitigated: The security risk is mitigated by being blocked or dropped.

NEW QUESTION 20
It is a best practice to upload FortiAnalyzer local logs to a remote server.Which two remote servers are supported for the upload? (Choose two.)

A. FTP
B. SFTP
C. UDP
D. TFTP

Answer: AB

Explanation:
When it's considered a best practice to upload FortiAnalyzer local logs to a remote server, the following two remote server protocols are commonly supported: These protocols provide secure and reliable ways to transfer logs and data to remote servers for storage and analysis while maintaining data integrity and confidentiality.

NEW QUESTION 22
......