Number: FCP_FAZ_AD-7.4
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: FCP_FAZ_AD-7.4

Exam Name: FCP - FortiAnalyzer 7.4 Administrator

Exam A

QUESTION 1
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.

Correct Answer: A, D
Section:
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.

QUESTION 2
Which two statements regarding FortiAnalyzer log forwarding modes are true? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.
B. In aggregation mode, you can forward logs to syslog and CEF servers.
C. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
D. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

Correct Answer: A, D
Section:
Explanation:
Both modes, forwarding and aggregation, support encryption of logs between devices.
Both forwarding and aggregation modes can use encryption to securely transfer logs between FortiAnalyzer devices.
Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
In aggregation mode, logs are stored and then transferred to another FortiAnalyzer at a scheduled time, rather than in real-time. This mode is typically used when consolidating logs from multiple devices into a central FortiAnalyzer.
The other options are incorrect because:
Forwarding mode sends logs in real-time but not exclusively to other FortiAnalyzer devices; it can also send logs to external systems like syslog servers.
Aggregation mode is primarily for consolidating logs to another FortiAnalyzer and doesn't focus on forwarding logs to syslog or CEF servers.

QUESTION 3
Refer to the exhibit.

FortiAnalyzer partial configuration output

```
FortiAnalyzer1# get system status
Platform Type                    : FAZVM64-KVM
Platform Full Name               : FortiAnalyzer-VM64-KVM
Version                          : v7.4.1-build2308 230831 (GA)
Serial Number                    : FAZ-VM0000065040
BIOS version                     : 04000002
Hostname                         : FortiAnalyzer1
Max Number of Admin Domains      : 5
Admin Domain Configuration       : Enabled
FIPS Mode                        : Disabled
HA Mode                          : Stand Alone
Branch Point                     : 2308
Release Version Information      : GA
Time Zone                        : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                       : Free 43.60GB, Total 58.80GB
File System                      : Ext4
License Status                   : Valid
```

```
FortiAnalyzer3# get system status
Platform Type                    : FAZVM64
Platform Full Name               : FortiAnalyzer-VM64
Version                          : v7.4.1-build2308 230831 (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                     : 2308
Release Version Information      : GA
Time Zone                        : (GMT-8:00) Pacific Time (US & Canada)
Disk Usage                       : Free 53.06GB, Total 79.80GB
File System                      : Ext4
License Status                   : Valid
```

```
FortiAnalyzer2# get system global
adom-mode                        : normal
adom-select                      : enable
adom-status                      : enable
console-output                   : standard
country-flag                     : enable
enc-algorithm                    : high
ha-member-auto-grouping          : enable
hostname                         : FortiAnalyzer2
log-checksum                     : md5
log-forward-cache-size           : 5
log-mode                         : collector
longitude                        : (null)
max-aggregation-tasks            : 0
max-running-reports              : 5
oftp-ssl-protocol                : tlsv1.2
ssl-low-encryption               : disable
ssl-protocol                     : tlsv1.3 tlsv1.2
task-list-size                   : 2000
webservice-proto                 : tlsv1.3 tlsv1.2
```

```
FortiAnalyzer3# get system global
adom-mode                        : normal
adom-select                      : enable
adom-status                      : enable
console-output                   : standard
country-flag                     : enable
enc-algorithm                    : high
ha-member-auto-grouping          : enable
hostname                         : FortiAnalyzer3
log-checksum                     : md5
log-forward-cache-size           : 5
log-mode                         : analyzer
longitude                        : (null)
max-aggregation-tasks            : 0
max-running-reports              : 5
oftp-ssl-protocol                : tlsv1.2
ssl-low-encryption               : disable
ssl-protocol                     : tlsv1.3 tlsv1.2
task-list-size                   : 2000
webservice-proto                 : tlsv1.3 tlsv1.2
```

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

A. FortiAnalyzer1 and FortiAnalyzer3
B. All devices listed can be members.
C. FortiAnalyzer1 and FortiAnalyzer2
D. FortiAnalyzer2 and FortiAnalyzer3

Correct Answer: C
Section:
Explanation:
Based on the partial configuration output, the primary factor for determining which devices can be members of a FortiAnalyzer Fabric is the log-mode setting. Devices with the same log mode can be part of the same FortiAnalyzer Fabric.
FortiAnalyzer1: Log mode is set to collector.
FortiAnalyzer2: Log mode is set to collector.
FortiAnalyzer3: Log mode is set to analyzer.
Devices with the same log mode can be part of the same fabric. Since FortiAnalyzer1 and FortiAnalyzer2 both have their log modes set to collector, they can be members of a FortiAnalyzer Fabric.
Therefore, the correct answer is FortiAnalyzer1 and FortiAnalyzer2.

QUESTION 4
What are offline logs on FortiAnalyzer?

A. Compressed logs, also known as archive logs
B. Logs that are indexed and stored in the SQL database
C. Any logs collected from offline devices after they boot up
D. Real-time logs that are not yet indexed

Correct Answer: C
Section:
Explanation:
These logs are generated when devices that were previously offline come back online and send their log data to the FortiAnalyzer.

QUESTION 5
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. A local wildcard administrator account
B. An administrator group
C. One or more remote LDAP servers
D. LDAP servers IP addresses added as trusted hosts

Correct Answer: A, C
Section:
Explanation:
A wildcard administrator account allows any user from the specified LDAP group to authenticate, and the remote LDAP servers must be configured to validate those user credentials. The combination of these settings enables authentication via LDAP for non-local users.

QUESTION 6
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

Correct Answer: C
Section:
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.

QUESTION 7
Which two parameters are used to calculate the Total Quota value available on FortiAnalyzer? (Choose two.)

A. Used storage
B. Retention policy
C. Reserved space
D. Total system storage

Correct Answer: C, D
Section:
Explanation:
The Total Quota is derived from the total system storage minus any reserved space allocated for system use, such as databases, system files, or reserved space for log retention policies. Used storage and retention policies do not directly impact the calculation of the quota available, though they can influence overall space utilization.

QUESTION 8
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.

Correct Answer: B, D
Section:
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.

QUESTION 9

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

Correct Answer: A
Section:
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.

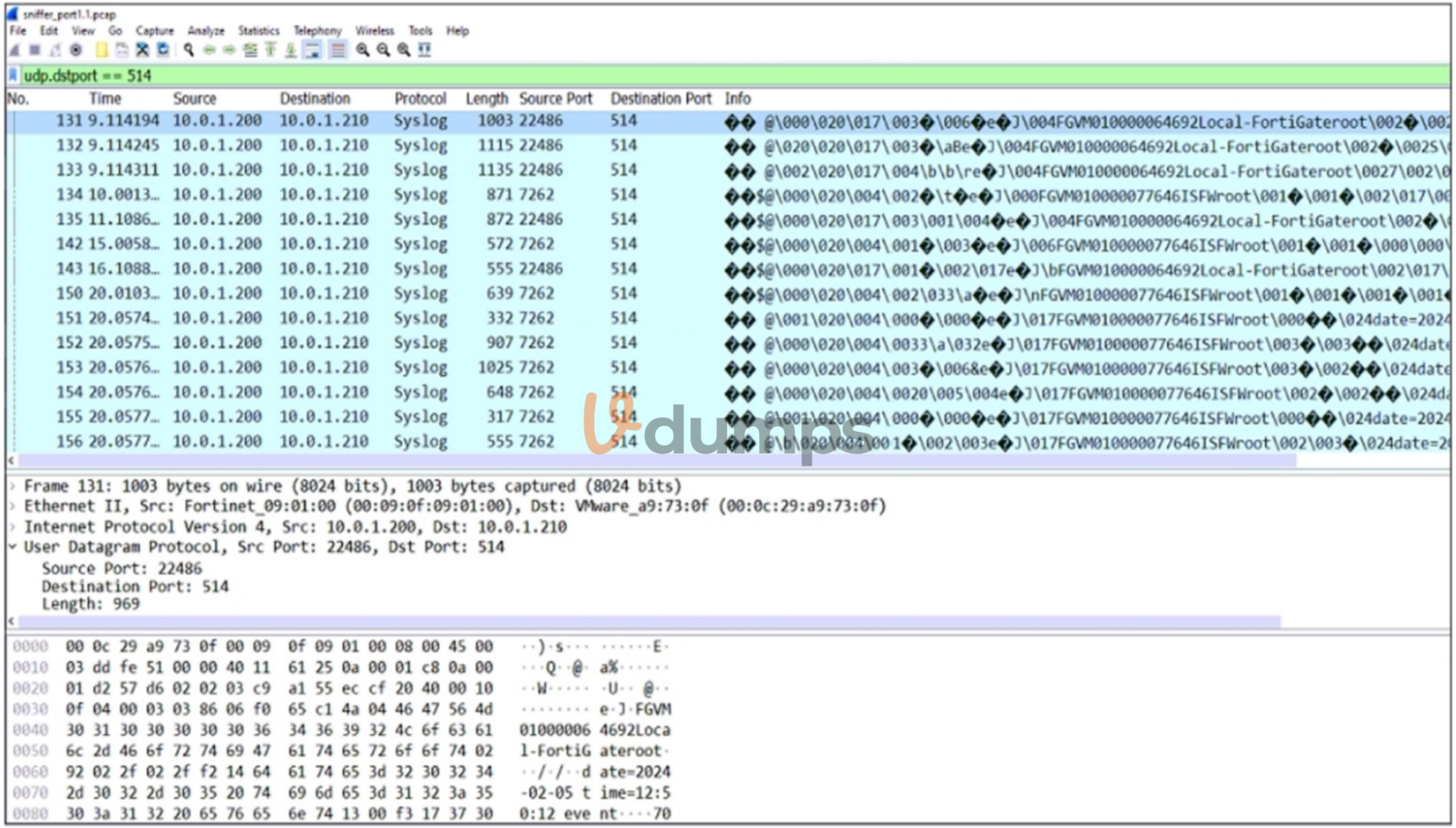
QUESTION 10
Which two statements about deleting ADOMs are true? (Choose two.)

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.

Correct Answer: B
Section:
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 11
Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



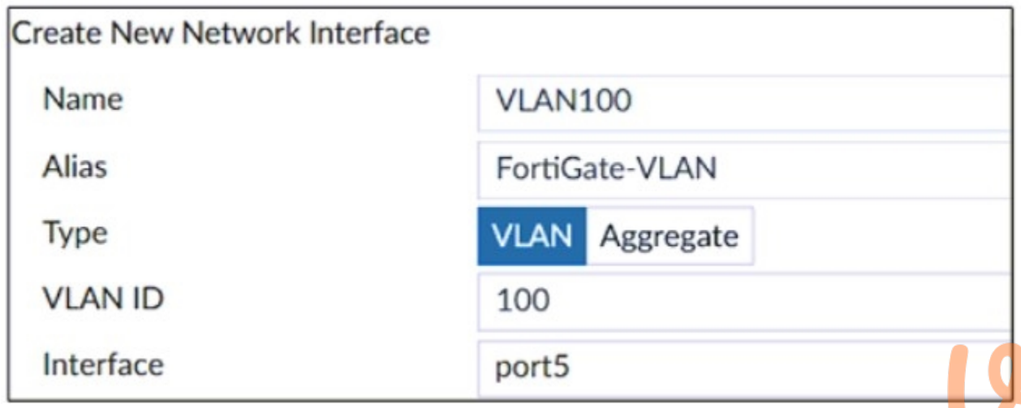
The capture displayed was taken on a FortiAnalyzer.
Why is a single IP address shown as the source for all logs received?

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.

Correct Answer: C
Section:
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 12
Refer to the exhibit.



What is the purpose of configuring FortiAnalyzer with the settings displayed in the image?

A. To increase reliability
B. To expand bandwidth
C. To maximize resiliency
D. To improve security

Correct Answer: D
Section:
Explanation:
The settings displayed in the image show the creation of a VLAN interface on FortiAnalyzer. The VLAN ID is set to 100, and it is associated with port 5.
The purpose of configuring a VLAN interface like this is generally: To improve security.
By creating a VLAN, traffic can be segmented into isolated networks, which helps limit access and enhances security by reducing the broadcast domain and keeping different types of traffic (e.g., management, user, and data traffic) separate.

QUESTION 13
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. A trusted host is configured.
C. fortinet is assigned the default Standard_User administrative profile.

D. fortinet is assigned the default Restricted_User administrative profile.

Correct Answer: C
Section:
Explanation:
The Standard_User profile allows viewing logs and performing some device management tasks but typically does not allow configuring global settings like creating a mail server for alert emails. To create a mail server, the administrator would need to have a profile with higher privileges, such as Super_User or a custom profile with the necessary permissions.

QUESTION 14
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. Logs from registered devices
B. Database snapshot
C. Report information
D. System information

Correct Answer: C, D
Section:
Explanation:
A FortiAnalyzer system backup includes configurations, report settings, and system information, but it does not include logs from registered devices or database snapshots. Logs are stored separately and are not part of the system configuration backup.

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 together.
B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message headers.
C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyzer.
D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Correct Answer: B
Section:
Explanation:
This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

QUESTION 16
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. There is no need to do anything because the disk will self-recover.
B. Run execute format disk to format and restart the FortiAnalyzer device.
C. Perform a hot swap of the disk.
D. Shut down FortiAnalyzer and replace the disk.

Correct Answer: C
Section:
Explanation:
In a RAID configuration, especially when hot-swapping is supported, you can replace a failed disk without shutting down the device. The RAID array will automatically rebuild once the new disk is inserted, minimizing downtime and maintaining data integrity.

QUESTION 17
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.

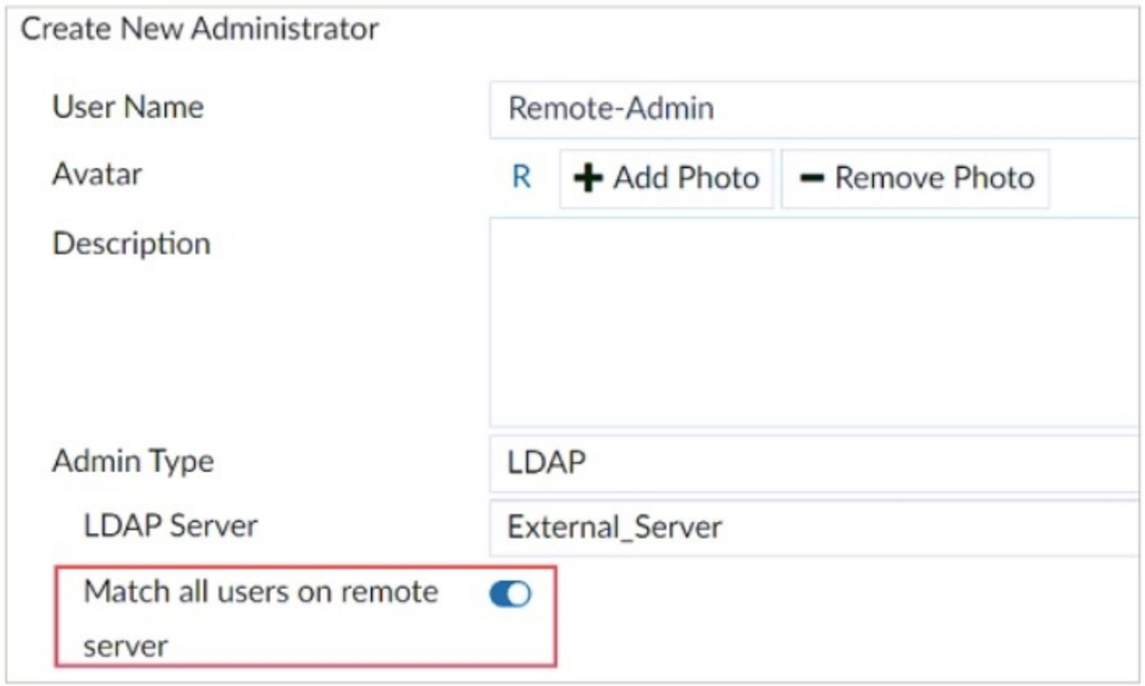
Correct Answer: B
Section:
Explanation:
When the upstream FortiGate is performing Network Address Translation (NAT), it creates new session entries for traffic passing through it. As a result, it generates its own traffic logs for those sessions, even if the sessions were initiated on a downstream FortiGate.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

QUESTION 18
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 was added to the wrong ADOM type.
B. This FortiGate model is not fully supported.
C. FortiGate does not have logging configured correctly.
D. This FortiGate is part of an HA cluster but it is the secondary device.

Correct Answer: C
Section:
Explanation:
This issue can occur if FortiGate is not properly configured to send logs to FortiAnalyzer, such as incorrect logging settings or filters being applied that prevent certain logs from being sent. It's important to verify that logging is enabled on FortiGate and that the correct log settings (such as log severity or log type) are configured for transmission to FortiAnalyzer.

QUESTION 19
Refer to the exhibit.



The exhibit shows the creation of a new administrator on FortiAnalyzer.
What are two effects of enabling the choice Match all users on remote server when configuring a new administrator? (Choose two.)

A. It allows user accounts in the LDAP server to use two-factor authentication.
B. It creates a wildcard administrator using an LDAP server.
C. User Remote-Admin from the LDAP server will be able to log in to FortiAnalyzer at any time.
D. Administrators can log in to FortiAnalyzer using their credentials on the remote LDAP server.

Correct Answer: B, D
Section:
Explanation:
Enabling this option allows any user authenticated by the LDAP server to log in to FortiAnalyzer, effectively creating a wildcard administrator.