



**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

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.

**Answer:** C

#### Explanation:

In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

#### NEW QUESTION 3

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 4

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 5

Refer to the exhibit.

```
FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:31 total-so-far:4642589
global log dev statistics:
faz=180191781, faz_cloud=0, fds_log=0
faz 0: sent=180189698, failed=4507, cached=0, dropped=0
```

Based on the output, what can you conclude about the FortiAnalyzer logging status?

- A. The connection between FortiGate and FortiAnalyzer is overloaded.
- B. FortiGate has logs to send, but FortiAnalyzer is unavailable.

- C. FortiGate is configured to send logs in batches.
- D. FortiGate is sending logs again after it performed a reboot.

Answer: B

Explanation:

The output shows that FortiGate has sent a large number of logs (sent=180189698), but some logs have failed to be sent (failed=4507). This suggests that FortiAnalyzer was temporarily unavailable or had an issue receiving logs, leading to the failure count. There are no logs cached or dropped, indicating FortiGate is still attempting to send logs but with some failures.

NEW QUESTION 6

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

FortiAnalyzer HA cluster settings

Cluster Settings

Operation Mode

StandaloneActive-PassiveActive-Active

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address	Interface	Action
192.168.101.222	port1	<div>✕+</div>

Cluster Settings

Peer IP and Peer SN	Peer IP	Peer SN	Action
	10.0.1.210	FAZ-VM0000065040	<div>✕+</div>

Group Name

Training

Group ID

1

(1-255)

Password

.....

👁

Heart Beat Interval

10

Seconds

Heart Beat Interface

port1

▼

Failover Threshold

30

Priority

120

(80-120)

Log Data Sync

🔘

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 7

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

- A. RAID0
- 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 8

Which feature can you configure to add redundancy to FortiAnalyzer?

- A. Primary and secondary DNS
- B. VLAN interfaces
- C. IPv6 administrative access
- D. Link aggregation

**Answer:** D

#### Explanation:

Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable.

Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

#### NEW QUESTION 9

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.

**Answer:** AD

#### 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.

#### NEW QUESTION 10

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

- 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 operate 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.

#### NEW QUESTION 10

Refer to the exhibit.

Create New Administrator

User Name

Remote-Admin

Avatar

R + Add Photo - Remove Photo

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 against the LDAP server.
- C. This password is set to comply with FortiAnalyzer 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 14**

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 tolerance
- 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**

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 17**

Which SQL query is in the correct order to query the database in the FortiAnalyzer?



- A. SELECT devid FROM Slog GROOP BY devid WHERE \* user' =\* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE \*user' =' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user\*' =' USERI' SELECT devid GROUP BY devid

**Answer:** C

**Explanation:**

C is correct because it follows the proper SQL query structure:

SELECT: Specifies the column(s) to retrieve.

FROM: Indicates the table to query (Slog in this case).

WHERE: Adds a condition to filter the results (user = 'USERI').

GROUP BY: Groups the results by the specified column (devid).

A, B, and D are incorrect because they do not follow the correct SQL query order:

A is incorrect because the GROUP BY clause is incorrectly placed before the WHERE clause.

B is incorrect because the WHERE clause is incorrectly placed before the FROM clause.

D is incorrect because the SELECT clause is incorrectly placed after the FROM and WHERE clauses.

**NEW QUESTION 21**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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 First Try
- \* FCP\_FAZ\_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCP\\_FAZ\\_AD-7.4 Practice Test Here](#)**