Vendor: Fortinet

Exam Code: FCP_FAZ_AD-7.4

Exam Name: FCP - FortiAnalyzer 7.4 Administrator

Version: DEMO

QUESTION 1
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.

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

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 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 3
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 files.
B. To encrypt log transfer between FortiAnalyzer and other devices.
C. To create the secure channel used by the OFTP process.
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.

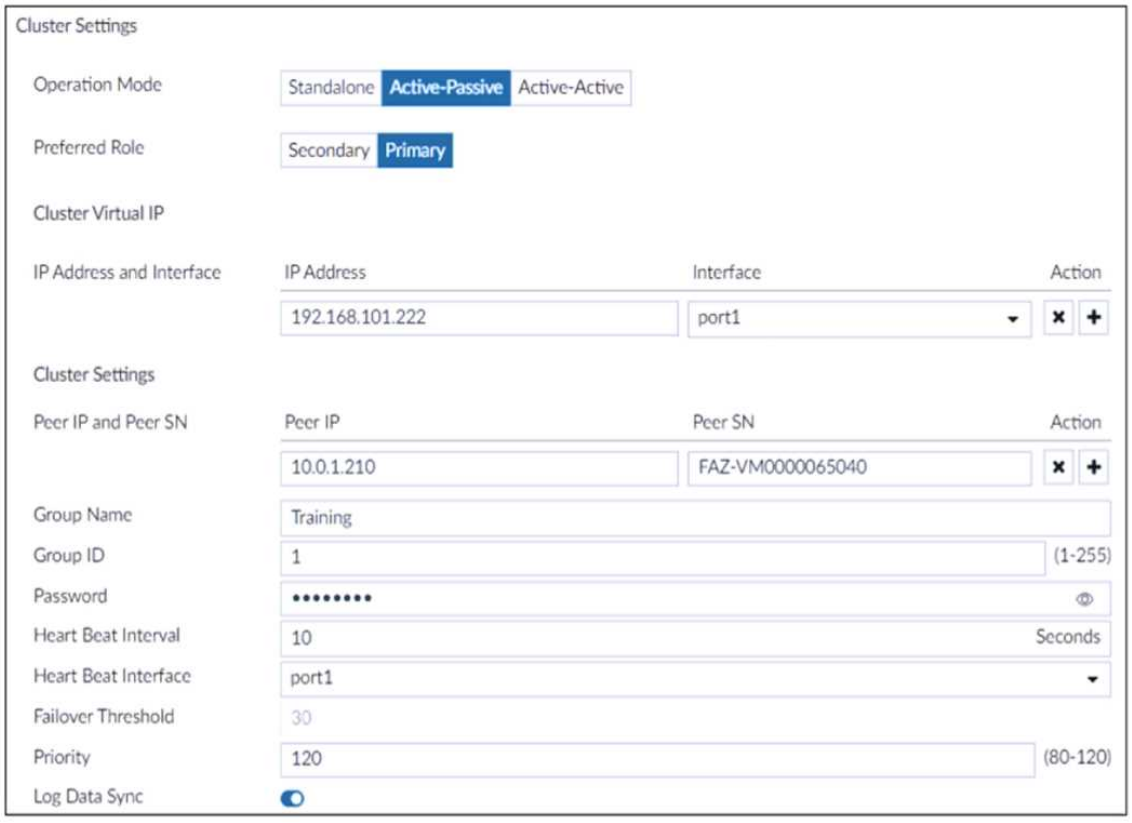
QUESTION 4
Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

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.

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.

QUESTION 5
Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.

FortiAnalyzer HA cluster settings



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.

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

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.

QUESTION 7
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.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14