

Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator



NEW QUESTION 1

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.

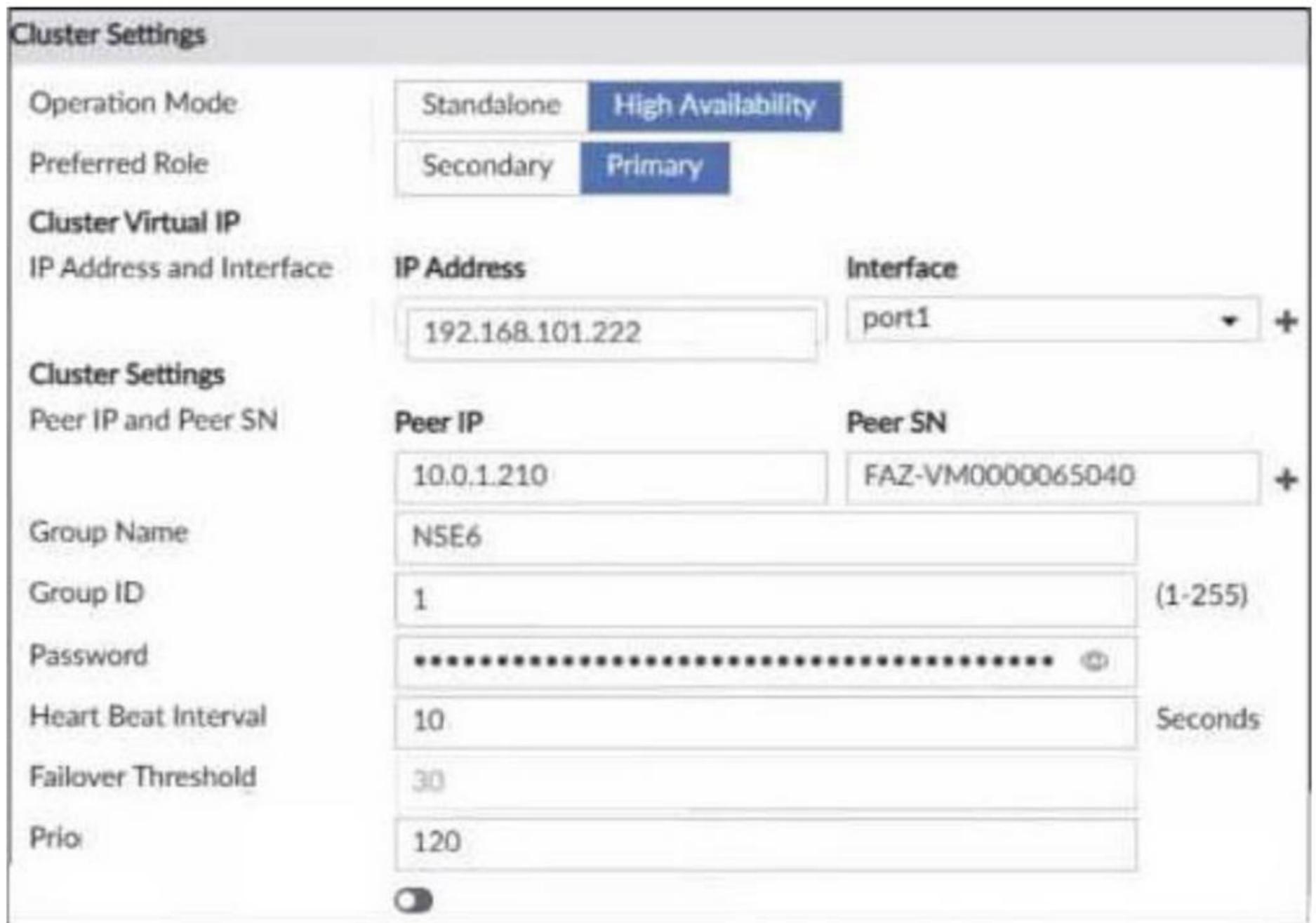
Answer: B

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 2

Refer to the exhibit.



The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?

- A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer will join to the existing HA cluster as the primary.
- D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: A

Explanation:

Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.

Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.

Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.

Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.

Given these points, the correct conclusion from the options provided is:

* C. This FortiAnalyzer will join the existing HA cluster as the primary.

NEW QUESTION 3

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 4

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 5

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 6

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

Answer: C

Explanation:

When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 7

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 8

What are two potential advantages of deploying RAID on FortiAnalyzer? (Choose two.)

- A. It provides redundancy.
- B. It improves performance.
- C. It provides backups.
- D. It reduces system resource usage.

Answer: AB

Explanation:

Here are two potential advantages of deploying RAID on FortiAnalyzer:

RAID configurations can mirror or stripe data across multiple disks. This redundancy helps ensure that even if one disk fails, the data remains accessible and recoverable. This is crucial for FortiAnalyzer as it stores security logs which are critical for analysis and forensic investigations.

Certain RAID configurations, like RAID 0 (striping) can improve read performance by distributing data reads across multiple disks. This can be beneficial for FortiAnalyzer when performing faster searches or retrieving large log sets.

Here's why the other options are not necessarily advantages:

While RAID can improve data availability in case of disk failures, it's not a replacement for proper backups. Backups should be done regularly to a separate location to ensure data recovery in case of catastrophic events like hardware failures or ransomware attacks.

RAID itself doesn't necessarily reduce system resource usage. In fact, some RAID configurations can introduce additional overhead for managing the redundant data.

NEW QUESTION 9

What are two of the key features of FortiAnalyzer? (Choose two.)

- A. Centralized log repository
- B. Cloud-based management
- C. Reports
- D. Virtual domains (VDOMs)

Answer: AC

Explanation:

FortiAnalyzer acts as a central repository for collecting and storing logs from multiple Fortinet devices. This centralized log management facilitates efficient analysis, search, and correlation of logs from across the network.

FortiAnalyzer provides robust reporting capabilities, allowing users to generate detailed reports based on collected logs and data. These reports can include insights on security events, network performance, and compliance.

Cloud-based management is not a primary feature of FortiAnalyzer, as it is typically an on-premises appliance, although it can integrate with cloud services.

Virtual domains (VDOMs) are a feature of FortiGate devices, allowing them to be partitioned into multiple virtual domains for administrative and policy separation. FortiAnalyzer itself does not provide VDOMs.

NEW QUESTION 10

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

Answer: D

Explanation:

The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 10

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here's how this works:

Assign the ADOMs to the Administrator's Account (Option B):

In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 15

.....

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](#)