Free Questions for FCP_FAZ_AD-7.4

Shared by Atkins on 03-10-2024

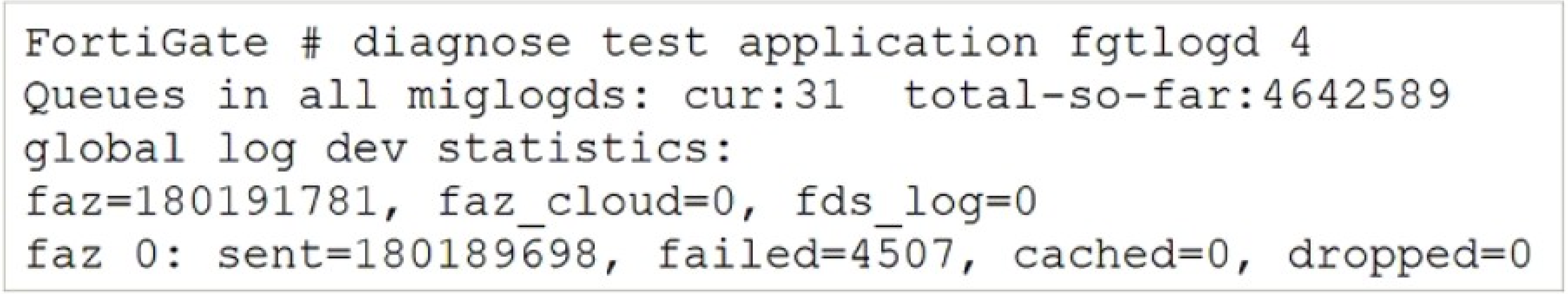
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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.

Question 2

Question Type: **MultipleChoice**

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

Options:

A- RAIDO

B- RAID 5

C- RAID1

D- RAID 6+0

E- RAID 0+0

Answer:

B, C, D

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.

Question 3

Question Type: MultipleChoice

Which statement when you are upgrading the firmware on an HA cluster made up of three FortiAnalyzer devices is true?

Options:

A- You can perform the firmware upgrade using only a console connection.

B- All FortiAnalyzer devices will be upgraded at the same time.

C- Enabling uninterruptible-upgrade prevents normal operations from being interrupted during the upgrade.

D- First, upgrade the secondary devices, and then upgrade the primary device.

Answer:

D

Explanation:

When upgrading firmware on an HA cluster of FortiAnalyzer devices, it is recommended to upgrade the secondary devices first, and then upgrade the primary device to minimize downtime and maintain continuity in log collection and other HA functions. This ensures that the primary device continues to handle operations while the secondary devices are being upgraded, and once the secondary devices are updated, the primary device can be upgraded with minimal service disruption.

Question 4

Question Type: MultipleChoice

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

Options:

A- Configure trusted hosts.

B- Limit access to specific virtual domains.

C- Fabric connectors to external LDAP servers.

D- Use administrator profiles.

Answer:

A, D

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 5

Question Type: MultipleChoice

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.)

Options:

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:

B, D

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 6

Question Type: **MultipleChoice**

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

Options:

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:

A, D

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 7

Question Type: **MultipleChoice**

Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

Options:

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.

20%
DISCOUNT