Question 1

Which two statements are true regarding ADOM modes? (Choose two.)

Options:

A- You can only change ADOM modes through CLI.

B- In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.

C- In an advanced mode ADOM. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.

D- Normal mode is the default ADOM mode.

Answer:

C, D

Question 2

An administrator has configured the following settings:

config system fortiview settings

set resolve-ip enable

end

What is the significance of executing this command?

Options:

A- Use this command only if the source IP addresses are not resolved on FortiGate.

B- It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.

C- You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.

D- It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer:

D

Question 3

Which two statements are true regarding log fetching on FortiAnalyzer? (Choose two.)

Options:

A- A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with the same FortiAnalyzer devices at the other end.

B- Log fetching can be done only on two FortiAnalyzer devices that are running the same firmware version.

C- Log fetching allows the administrator to fetch analytics logs from another FortiAnalyzer for redundancy.

D- Log fetching allows the administrator to run queries and reports against historical data by retrieving archived logs from one FortiAnalyzer device and sending them to another FortiAnalyzer device.

Answer:

B, D

Explanation:

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

FortiAnalyzer_7.0_Study_Guide-Online pag. 168

Question 4

What are offline logs on FortiAnalyzer?

Options:

A- Compressed logs, which are also known as archive logs, are considered to be offline logs.

B- When you restart FortiAnalyzer. all stored logs are considered to be offline logs.

C- Logs that are indexed and stored in the SQL database.

D- Logs that are collected from offline devices after they boot up.

Answer:

A

Explanation:

Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as archive logs and are considered offline so they don't offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy. FortiAnalyzer_7.0_Study_Guide-Online page 140

Question 5

Question Type: **MultipleChoice**

Which two purposes does the auto cache setting on reports serve? (Choose two.)

Options:

A- It automatically updates the hcache when new logs arrive.

B- It provides diagnostics on report generation time.

C- It reduces the log insert lag rate.

D- It reduces report generation time.

Answer:

A, D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

Question 6

Question Type: **MultipleChoice**

For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)

Options:

A- Principal

B- Service provider

C- Identity collector

D- Identity provider

Answer:

B, D

Explanation:

20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available.

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-admin-authentication

In FortiAnalyzer, SAML can be enabled across all Security Fabric devices, enabling smooth movement between devices for the administrator by means of single sign-on (SSO).

FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

FortiAnalyzer_7.0_Study_Guide-Online pag. 48

Question 7

What is the purpose of a predefined template on the FortiAnalyzer?

Options:

A- It can be edited and modified as required

B- It specifies the report layout which contains predefined texts, charts, and macros

C- It specifies report settings which contains time period, device selection, and schedule

D- It contains predefined data to generate mock reports

Explanation:

Reference: https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMGFAZ/
2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number%
20of,create%20and%2For%20build%20reports.&text=A%20template%20populates%20the%20Layout,that%
20is%20to%20be%20created.
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

Answer:

B

To Get Premium Files for NSE5_FAZ-7.2 Visit

https://www.p2pexams.com/products/nse5_faz-7.2

For More Free Questions Visit

https://www.p2pexams.com/fortinet/pdf/nse5-faz-7.2