Free Questions for NSE5_FAZ-7.2

Shared by Harrington on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements are true regarding FortiAnalyzer log forwarding? (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 as well.
C- Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
D- Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.

Answer:

A, C

Explanation:

A) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 148: The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide. (You need to interpret this. 'Real time' and 'aggregation' is about the 'moment' when Fortigate sends the logs. However, no matter the moment, Fortigate will upload logs encrypted or unencrypted based on previous / differente config).

C) FortiAnalyzer_7.0_Study_Guide-Online.pdf page 147: Aggregation: Logs and content files stored and uploaded at scheduled time.

Question 2

Question Type: MultipleChoice

Which statement describes online logs on FortiAnalyzer?

Options:

A- Logs that reached a specific size and were rolled over
B- Logs that can be used to create reports

C- Logs that can be viewed using Log Browse
D- Logs that are saved to disk, compressed, and available in FortiView

Answer:

C

Question 3

Question Type: MultipleChoice

After generating a report, you notice the information you were expecting to see is not included in it. What are two possible reasons for this scenario? (Choose two.)

Options:

A- You enabled auto-cache with extended log filtering.
B- The logfiled service has not indexed all the expected logs.
C- The logs were overwritten by the data retention policy.
D- The time frame selected in the report is wrong.

Answer:

B, C

Question 4

Question Type: MultipleChoice

What are two advantages of setting up fabric ADOM? (Choose two.)

Options:

A- It can be used for fast data processing and log correlation
B- It can be used to facilitate communication between devices in same Security Fabric
C- It can include all Fortinet devices that are part of the same Security Fabric
D- It can include only FortiGate devices that are part of the same Security Fabric

Answer:

A, C

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

Question 5

Question Type: MultipleChoice

What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

Options:

A- FortiAnalyzer distinguishes different devices by their serial number.
B- FortiAnalyzer receives logs from d devices in a duster.
C- FortiAnalyzer receives bgs only from the primary device in the cluster.
D- FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Answer:

A, B

Question 6

Question Type: MultipleChoice

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

Options:

A- First, upgrade the secondary device, and then upgrade the primary device.
B- Both FortiAnalyzer devices will be upgraded at the same time.
C- You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.

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

Answer:

A

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 64: To upgrade FortiAnalyzer HA cluster firmware:

1. Log in to each secondary device.

2. Upgrade the firmware of all secondary devices.

3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.

4. Verify that logs on all secondary devices are synchronized with the primary device.

5. Upgrade the primary device.

https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

Question 7

Question Type: MultipleChoice

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

Options:

A- FortiAnalyzer provides the ability to create custom reports.
B- FortiAnalyzer glows you to schedule reports to run.
C- FortiAnalyzer includes pre-defined reports only.
D- FortiAnalyzer allows reporting for FortiGate devices only.

Answer:

A, B