Free Questions for NSE5_FAZ-7.2

Shared by Cooke on 23-08-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What statements are true regarding disk log quota? (Choose two)

Options:

A- The FortiAnalyzer stops logging once the disk log quota is met.
B- The FortiAnalyzer automatically sets the disk log quota based on the device.
C- The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D- The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Answer:

C, D

Question 2

Question Type: MultipleChoice

Why must you wait for several minutes before you run a playbook that you just created?

Options:

A- FortiAnalyzer needs that time to parse the new playbook.
B- FortiAnalyzer needs that time to back up the current playbooks.
C- FortiAnalyzer needs that time to ensure there are no other playbooks running.
D- FortiAnalyzer needs that time to debug the new playbook.

Answer:

A

Question 3

Question Type: MultipleChoice

A playbook contains five tasks in total. An administrator runs the playbook and four out of five

tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

Options:

A- Running
B- Failed
C- Upstream_failed
D- Success

Answer:

B

Question 4

Question Type: MultipleChoice

What is the purpose of the following CLI command?

```
# configure system global
     set log-checksum md5
end
```

Options:

A- To add a log file checksum
B- To add the MD's hash value and authentication code
C- To add a unique tag to each log to prove that it came from this FortiAnalyzer
D- To encrypt log communications

Answer:

A

Explanation:

https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

Question 5

Question Type: MultipleChoice

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

Options:

A- Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
B- Must establish an IPsec tunnel ID and pre-shared key.
C- IPsec cannot be enabled if SSL is enabled as well.
D- IPsec is only enabled through the CLI on FortiAnalyzer.

Answer:

B, D

Explanation:

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.

Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

Question 6

Question Type: MultipleChoice

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

Options:

A- The size of newly generated reports is optimized to conserve disk space.
B- FortiAnalyzer local cache is used to store generated reports.
C- When new logs are received, the hard-cache data is updated automatically.

D- The generation time for reports is decreased.

Answer:

C, D

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

Question 8

Question Type: MultipleChoice

When working with FortiAnalyzer reports, what is the purpose of a dataset?

Options:

A- To provide the layout used for reports
B- To define the chart type to be used
C- To retrieve data from the database
D- To set the data included in templates

Answer:

C

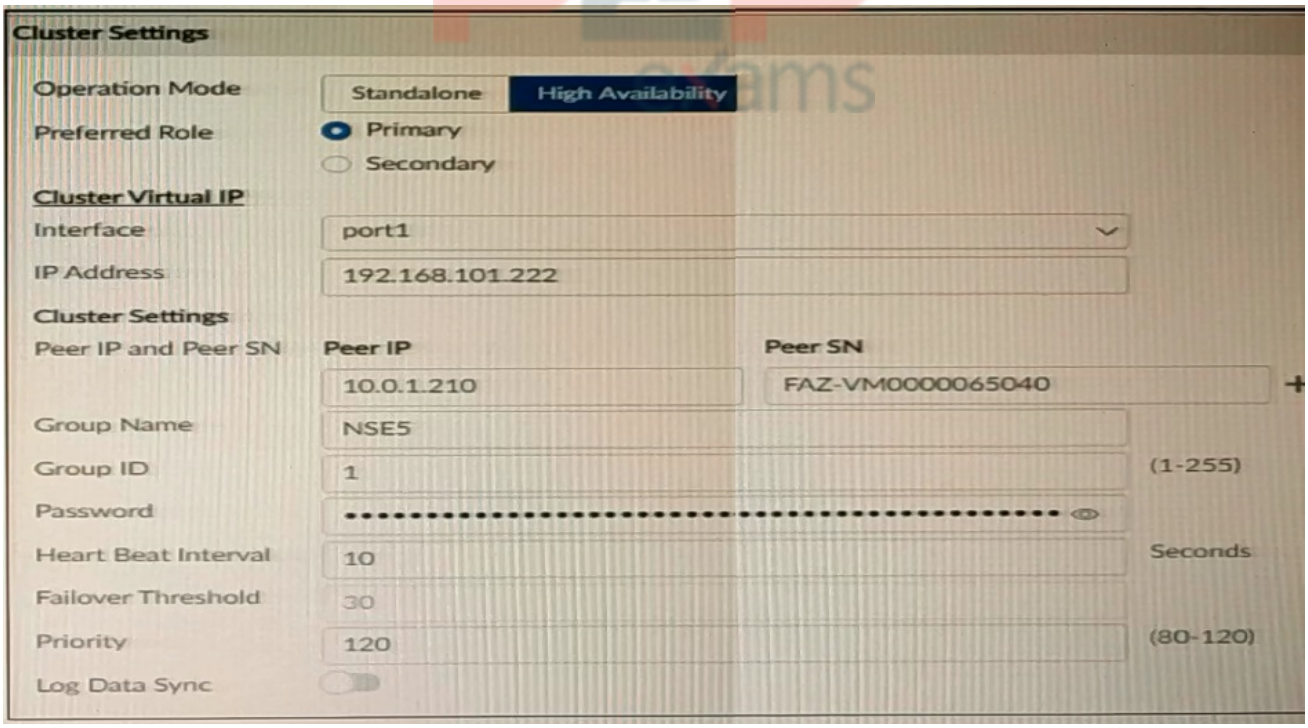
Explanation:

Datasets: Structured Query Language (SQL) SELECT queries that extract specific data from the database

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



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

What can you conclude from the configuration displayed?

Options:

A- This FortiAnalyzer will join to the existing HA cluster as the primary.
B- This FortiAnalyzer is configured to receive logs in its port1.
C- This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
D- After joining to the cluster, this FortiAnalyzer will keep an updated log database.
'If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit.'

(https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104)

Answer:

B

Question 10

Question Type: MultipleChoice

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

Options:

A- Incidents dashboards
B- Threat hunting
C- FortiView Monitor
D- Outbreak alert services

Answer:

B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

Question 11

Question Type: MultipleChoice

Which two statements about log forwarding are true? (Choose two.)

Options:

A- Forwarded logs cannot be filtered to match specific criteria.
B- Logs are forwarded in real-time only.
C- The client retains a local copy of the logs after forwarding.
D- You can use aggregation mode only with another FortiAnalyzer.

Answer:

C, D

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding