NSE5_FAZ-7.0$^{\text{Q\&As}}$

Fortinet NSE 5 - FortiAnalyzer 7.0

QUESTION 1

What can the CLI command # diagnose test application oftpd 3 help you to determine?

A. What devices and IP addresses are connecting to FortiAnalyzer

B. What logs, if any, are reaching FortiAnalyzer

C. What ADOMs are enabled and configured

D. What devices are registered and unregistered

Correct Answer: A

Device and ADOM Status Check

diagnose test application oftpd 3 # Devices and IPs are connecting to FortiAnalyzer diagnose test application oftpd 8 # Receiving logs in FortiAnalyzre diagnose dvm adom list # ADOMs are enabled and configured diagnose dvm device list # Devices or VDOMs are currently registed and unregistered

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli- reference/395556/test#test_application

QUESTION 2

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-and-log-aggregation-modes

QUESTION 3

What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.

B. The log file rolls over and is archived.

C. The log file is purged from the database.

D. The log file is overwritten.

Correct Answer: B

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/6d9f8fb5-6cf4-11e9-81a4-00505692583a/FortiAnalyzer-6.0.5-Administration-Guide.pdf

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log- browse

QUESTION 4

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

A. Virtual domains

B. Administrative access profiles

C. Trusted hosts

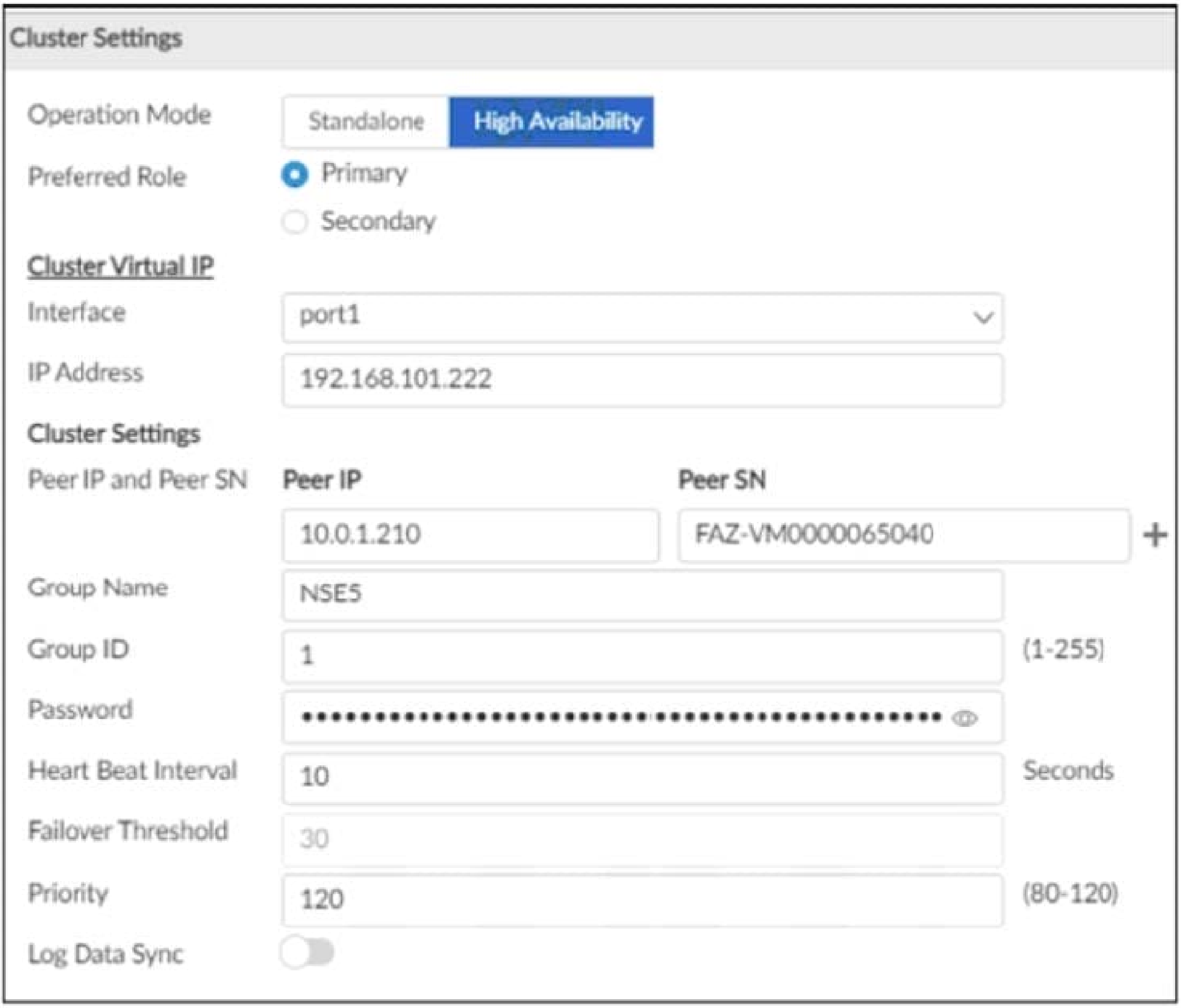
D. Security Fabric

Correct Answer: BC

Reference: https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration- guide/219292/administrator-profiles https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration- guide/581222/trusted-hosts

QUESTION 5

Refer to the exhibit.



Cluster Settings

Operation Mode: Standalone | **High Availability**

Preferred Role: ● Primary ○ Secondary

Cluster Virtual IP

Interface: port1

IP Address: 192.168.101.222

Cluster Settings

Peer IP and Peer SN

Peer IP	Peer SN
10.0.1.210	FAZ-VM0000065040

Group Name: NSE5

Group ID: 1 (1-255)

Password: ••

Heart Beat Interval: 10 Seconds

Failover Threshold: 30

Priority: 120 (80-120)

Log Data Sync

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?

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.

Correct Answer: B

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.