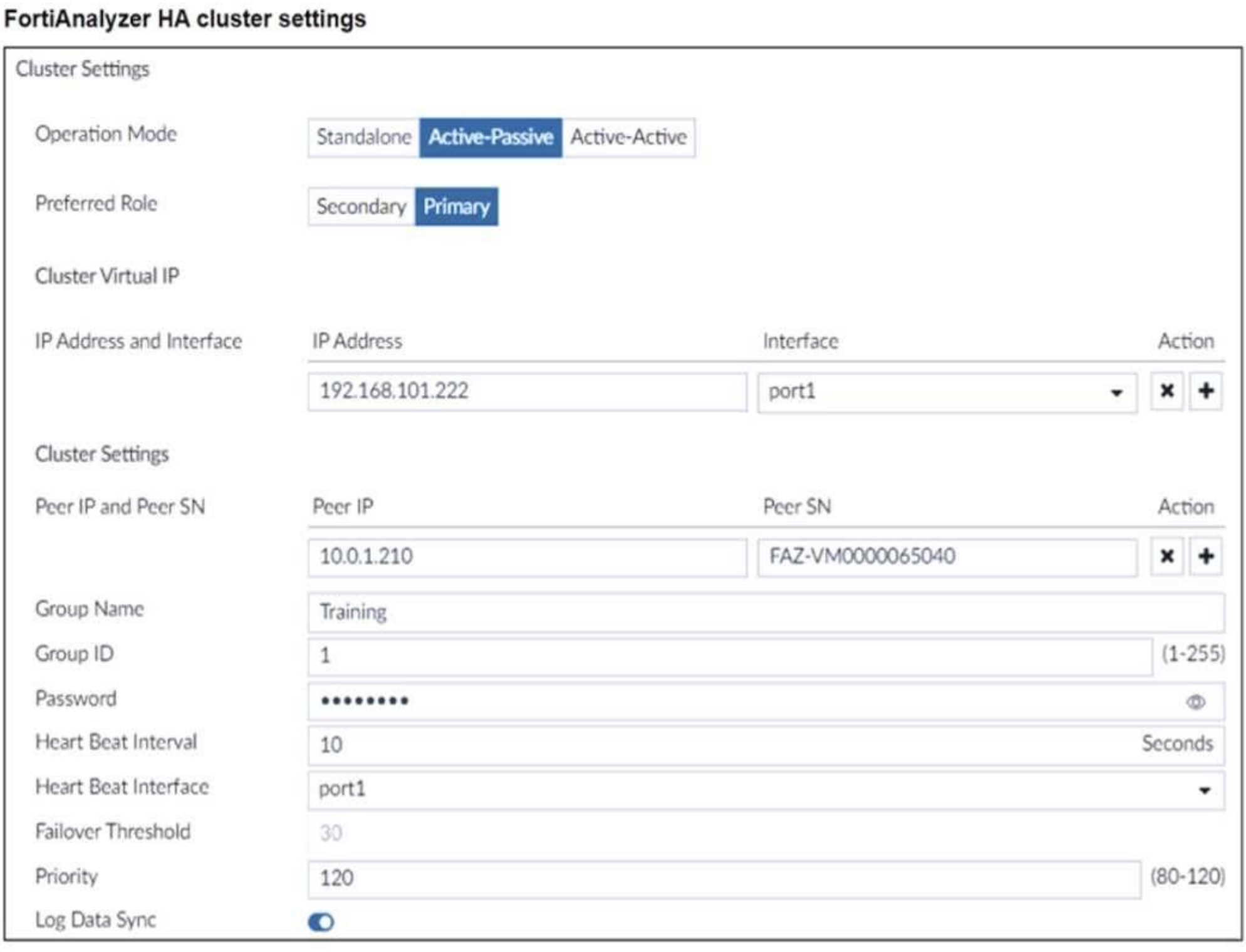
Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1
Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.



The administrator wants to join this FortiAnalyzer to an existing HA cluster. What can you conclude from the configuration displayed?

A. After joining the cluster, this FortiAnalyzer will forward received logs to its peers.
B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
C. This FortiAnalyzer is configured to route HA traffic through a gateway.
D. This FortiAnalyzer will join the existing HA cluster as the secondary.

Answer: B

Explanation:
The "Preferred Role" is set to Secondary, which means this FortiAnalyzer is configured to join the cluster as the secondary unit in an Active-Passive HA configuration. Other settings, such as the peer IP and serial number, confirm its setup to communicate with the primary unit.

NEW QUESTION 2
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.)

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: BD

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.

NEW QUESTION 3
What does the disk status Degraded mean for RAID management?

A. The hard drive is no longer being used by the RAID controller.
B. One or more drives are missing from the FortiAnalyzer unit.
C. The device is writing data to the disk to restore the volume to an optimal state.
D. FortiAnalyzer determined that the parity data in the disk is not valid.

Answer: B

Explanation:
When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

NEW QUESTION 4
Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

A. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
B. FortiAnalyzer HA active-passive mode can function without VRRP.
C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
D. All devices in a FortiAnalyzer HA cluster must have the same available disk space.

Answer: A

Explanation:
The two correct statements about high availability (HA) on FortiAnalyzer are:
FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
FortiAnalyzer HA synchronizes both logs and certain system configuration settings between the units in the cluster to ensure consistent operation.
All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
In an HA cluster, all devices must be configured to operat` e in the same mode --- either analyzer mode or collector mode---to ensure consistency and proper functionality across the cluster.
The other options, such as VRRP, are not required for HA in FortiAnalyzer, and disk space can vary between nodes but may impact log storage capacity.

NEW QUESTION 5
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

A. The traffic destination is another FortiGate in the fabric.
B. The upstream FortiGate is configured to do NAT
C. Log redundancy is configured in the fabric.
D. The downstream device cannot connect to FortiAnalyzer.

Answer: B

Explanation:
When the upstream FortiGate is performing Network Address Translation (NAT), it creates new session entries for traffic passing through it. As a result, it generates its own traffic logs for those sessions, even if the sessions were initiated on a downstream FortiGate.
This is because the upstream FortiGate is altering the source IP address, making it responsible for tracking the session details.

NEW QUESTION 6
An administrator has configured the following settings:

```
#config system global
   set log-checksum md5-auth
end
```

What is the purpose of executing these commands?

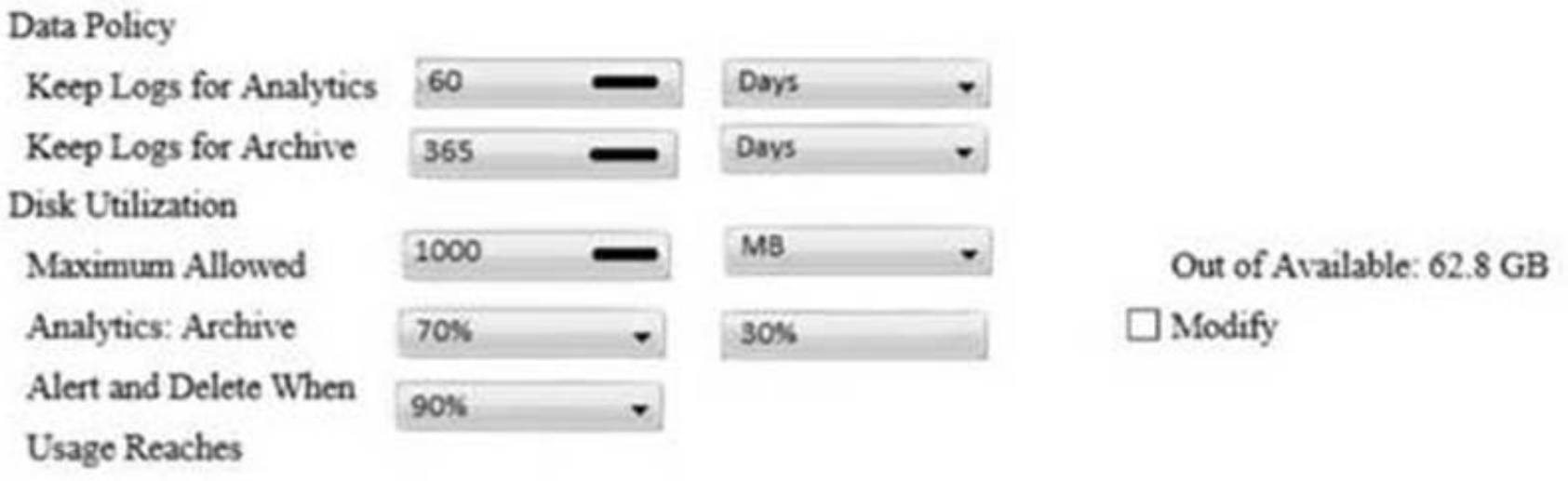
A. To record the hash value and authentication code of log file
B. To encrypt log transfer between FortiAnalyzer and other device
C. To create the secure channel used by the OFTP proces
D. To verify the integrity of the log files received.

Answer: A

Explanation:
:
The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

NEW QUESTION 7

View the exhibit:



What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model
B. The disk quota for all devices in the ADOM
C. The disk quota for each device in the ADOM
D. The disk quota for the ADOM type

Answer: B

Explanation:
The 1000MB maximum for disk utilization refers to the total disk quota allocated for storing logs from all devices within the specific ADOM (Autonomous Domain) you're configuring.

NEW QUESTION 8
Which SQL query is in the correct order to query the database in the FortiAnalyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERl'
B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERl' SELECT devid GROUP BY devid

Answer: C

Explanation:
C is correct because it follows the proper SQL query structure:
SELECT: Specifies the column(s) to retrieve.
FROM: Indicates the table to query (Slog in this case).
WHERE: Adds a condition to filter the results (user = 'USERl').
GROUP BY: Groups the results by the specified column (devid).
A, B, and D are incorrect because they do not follow the correct SQL query order:
A is incorrect because the GROUP BY clause is incorrectly placed before the WHERE clause.
B is incorrect because the WHERE clause is incorrectly placed before the FROM clause.
D is incorrect because the SELECT clause is incorrectly placed after the FROM and WHERE clauses.

NEW QUESTION 9
How do you restrict an administrator's access to a subset of your organization's ADOMs?

A. Set the ADOM mode to Advanced
B. Assign the ADOMs to the administrator's account
C. Configure trusted hosts
D. Assign the default Super_User administrator profile

Answer: B

Explanation:
To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here??s how this works:
Assign the ADOMs to the Administrator's Account (Option B):
In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FAZ_AD-7.4 Practice Exam Features:

* FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently

* FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year