Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

NEW QUESTION 1
Which two statements about deleting ADOMs are true? (Choose two.)

A. Logs must be purged or migrated before you can delete an ADOM.
B. ADOMs with registered devices cannot be deleted.
C. Default ADOMs cannot be deleted.
D. The status of the ADOMs must be unlocked.

Answer: B

Explanation:
DOMs with registered devices cannot be deleted.
An ADOM cannot be deleted if it has registered devices. You must first remove or deregister the devices before deleting the ADOM.
The status of the ADOMs must be unlocked.
An ADOM must be in an unlocked state before it can be deleted. If the ADOM is locked, it will not allow deletion.

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
Which three RAID configurations provide fault tolerance on FortiAnalyzer? (Choose three.)

A. RAIDO
B. RAID 5
C. RAID1
D. RAID 6+0
E. RAID 0+0

Answer: BCD

Explanation:
RAID 1 provides fault tolerance through disk mirroring.
RAID 5 provides fault tolerance by using distributed parity across multiple disks. RAID 6+0 combines striping with double parity, offering enhanced fault tolerance.
RAID 0 and RAID 0+0 do not provide any fault tolerance, as they focus on performance through data striping but offer no redundancy.

NEW QUESTION 4
Which feature can you configure to add redundancy to FortiAnalyzer?

A. Primary and secondary DNS
B. VLAN interfaces
C. IPv6 administrative access
D. Link aggregation

Answer: D

Explanation:
Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable.
Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 5
What are analytics logs on FortiAnalyzer?

A. Logs that are compressed and saved to a log file

B. Logs that roll over when the log file reaches a specific size
C. Logs that are indexed and stored in the SQL
D. Logs classified as type Traffic, or type Security

Answer: C

Explanation:
On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.
Reference: FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

NEW QUESTION 6
Which two statements regarding FortiAnalyzer log forwarding modes are true? (Choose two.)

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.
C. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
D. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

Answer: AD

Explanation:
Both modes, forwarding and aggregation, support encryption of logs between devices.
Both forwarding and aggregation modes can use encryption to securely transfer logs between FortiAnalyzer devices.
Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
In aggregation mode, logs are stored and then transferred to another FortiAnalyzer at a scheduled time, rather than in real-time. This mode is typically used when consolidating logs from multiple devices into a central FortiAnalyzer.
The other options are incorrect because:
Forwarding mode sends logs in real-time but not exclusively to other FortiAnalyzer devices; it can also send logs to external systems like syslog servers.
Aggregation mode is primarily for consolidating logs to another FortiAnalyzer and doesn't focus on forwarding logs to syslog or CEF servers.

NEW QUESTION 7
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 8
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.

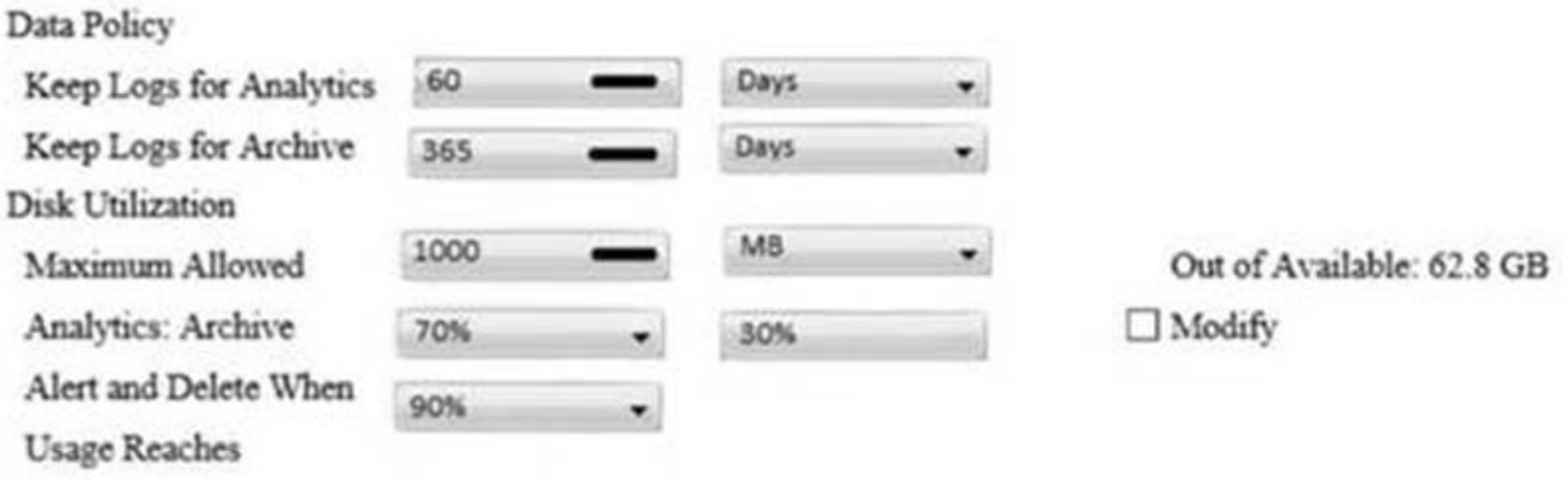
NEW QUESTION 9
Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them togethe
B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyze
D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:
This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 10
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 10
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator??s access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

Explanation:
ADOMs constrain other administrators' access privileges to a subset of devices in the device list: ADOMs allow you to partition the FortiAnalyzer's management capabilities by restricting access to certain devices and logs based on the administrator's role. This segmentation helps in managing large deployments with different administrative needs.
Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM: When ADOMs are enabled, the FortiAnalyzer interface segments the Device Manager, FortiView, Event Management, and Reports tabs based on the selected ADOM. This allows administrators to work within their specific ADOM context.
ADOMs are enabled by default: This is incorrect because ADOMs are not enabled by default. They must be manually configured and enabled according to the organization's needs.
All administrators can create ADOMs--not just the admin administrator: This is not correct. Typically, creating and managing ADOMs requires administrative privileges, often restricted to the main admin or specific roles with sufficient permissions.

NEW QUESTION 15
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 20
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FAZ_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FAZ_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

Money Back Guarantee

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