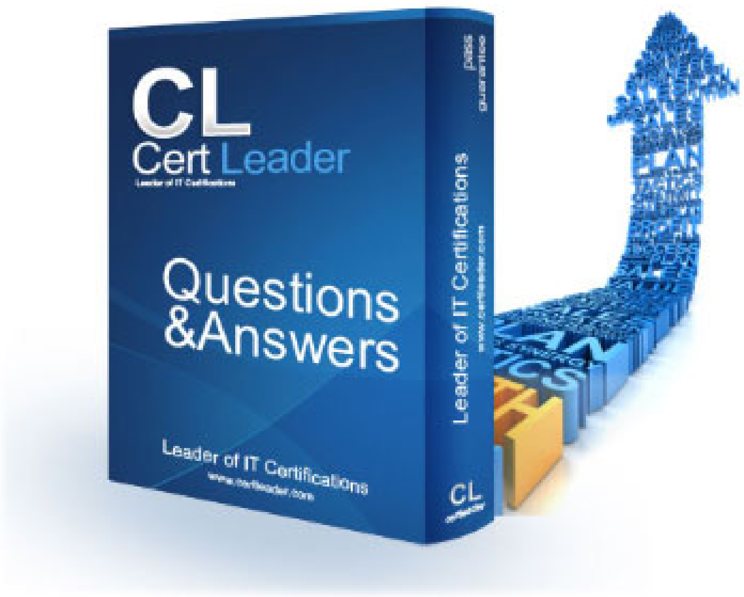
FCP_FAZ_AD-7.4 Dumps

FCP - FortiAnalyzer 7.4 Administrator

https://www.certleader.com/FCP_FAZ_AD-7.4-dumps.html



NEW QUESTION 1
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. Total quota
B. License type
C. RAID level
D. Disk size

Answer: C

Explanation:
RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.
Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.
The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

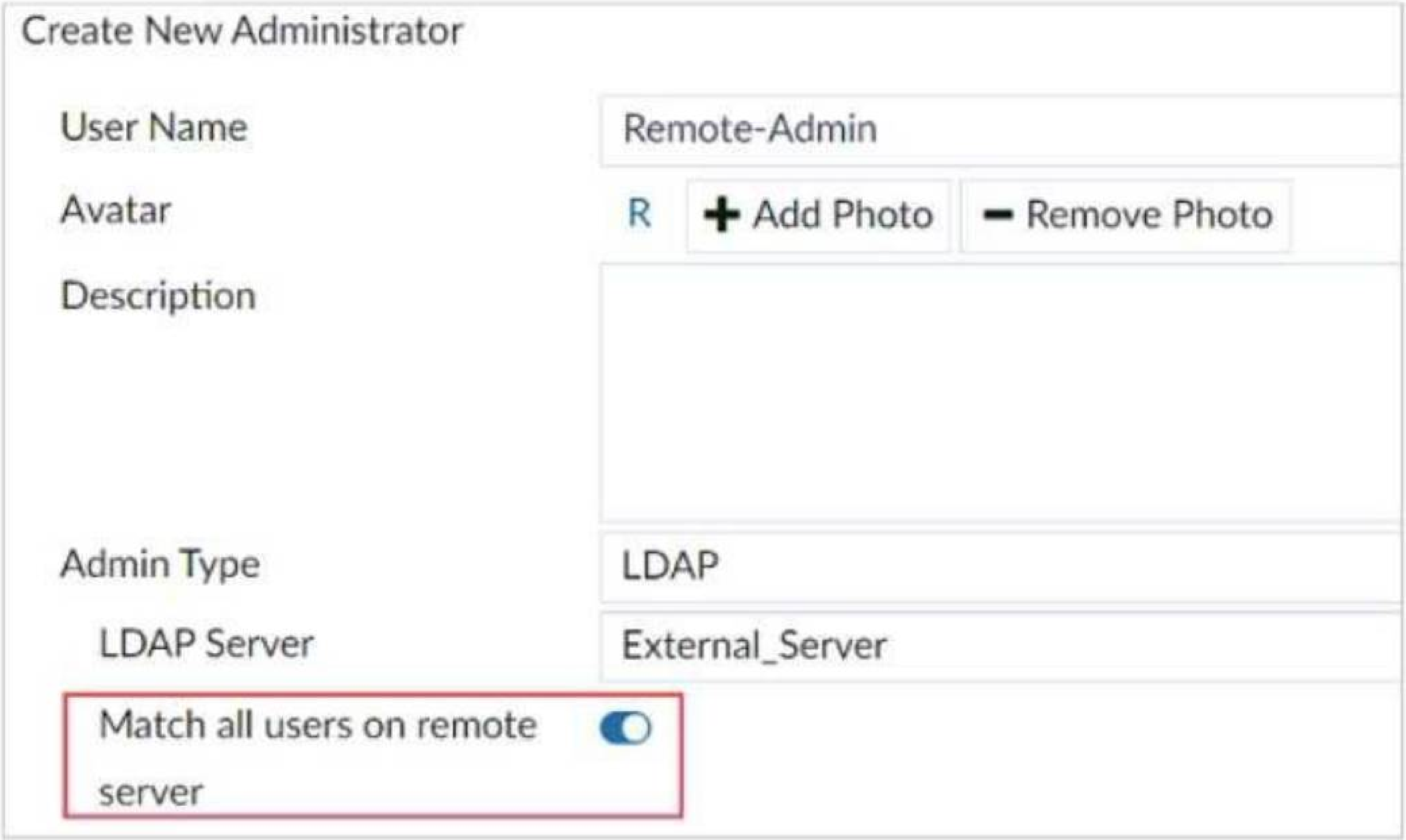
NEW QUESTION 2
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
C. For the collector, you should allocate most of the disk space to analytics logs.
D. Analyzer mode is the default operating mode.

Answer: B

Explanation:
When in analyzer mode, FortiAnalyzer supports event management and reporting features.
In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.
Analyzer mode is the default operating mode.
By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:
In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.
In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 3
Refer to the exhibit.



Create New Administrator

User Name: Remote-Admin
Avatar: R
Description:
Admin Type: LDAP
LDAP Server: External_Server
Match all users on remote server: ●

The exhibit shows the creation of a new administrator on FortiAnalyzer.
What are two effects of enabling the choice Match all users on remote server when configuring a new administrator? (Choose two.)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Enabling this option allows any user authenticated by the LDAP server to log in to FortiAnalyzer, effectively creating a wildcard administrator.

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
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.

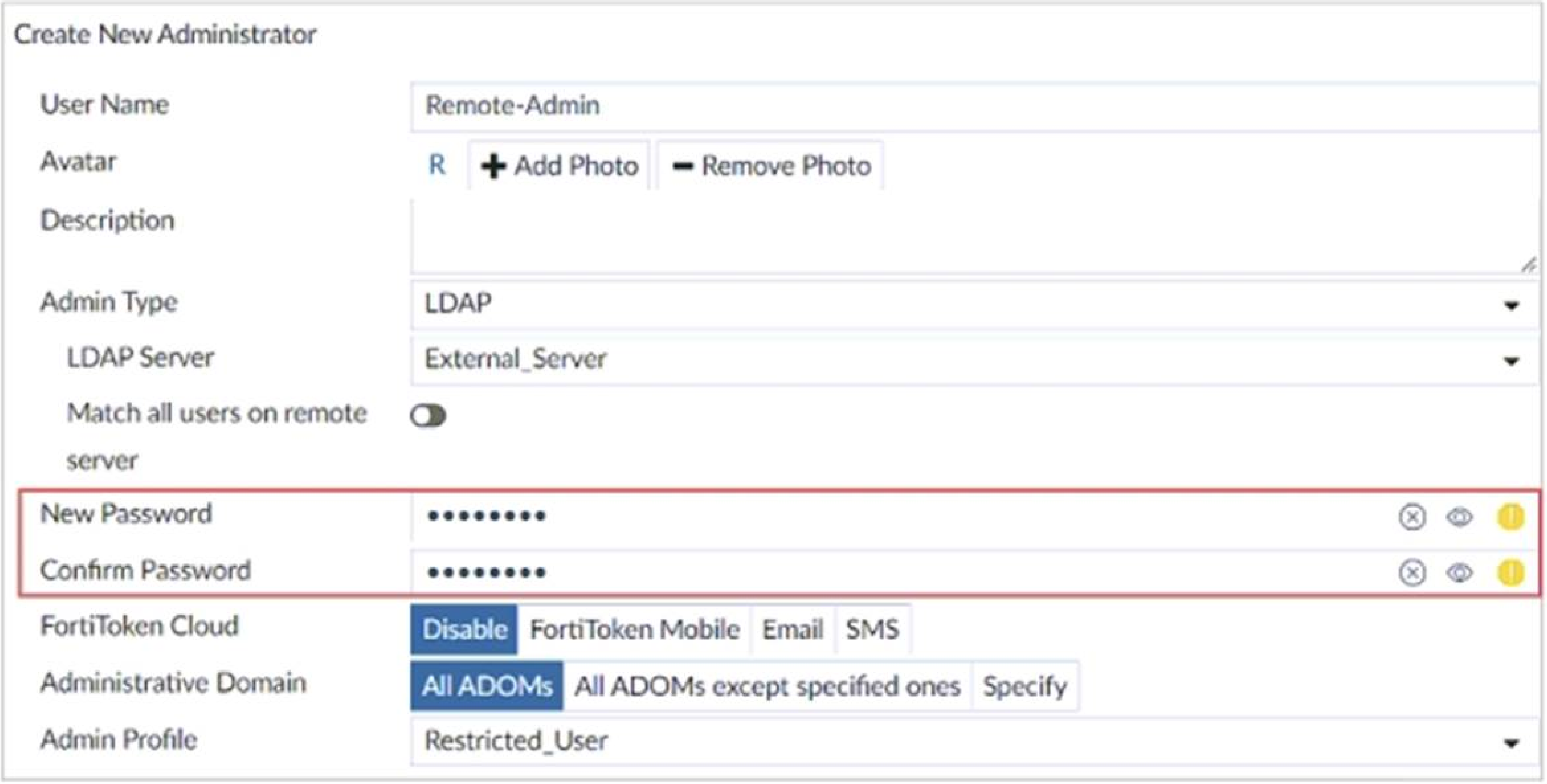
NEW QUESTION 6
Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

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 7
Refer to the exhibit.



Create New Administrator

User Name: Remote-Admin
Avatar: R | + Add Photo | − Remove Photo
Description:
Admin Type: LDAP
LDAP Server: External_Server
Match all users on remote server: ○
New Password: ••••••••
Confirm Password: ••••••••
FortiToken Cloud: Disable | FortiToken Mobile | Email | SMS
Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify
Admin Profile: Restricted_User

The exhibit shows the creation of a new administrator on FortiAnalyzer. The new account uses the credentials stored on an LDAP server.
Why would an administrator configure a password for this account?

A. This password is used if the authentication server becomes unreachable.
B. This password authenticates FortiAnalyzer aqainst the LDAP server.
C. This password is set to comply with FortiAnalvzer password policy
D. This password is required because this is a restricted user.

Answer: A

Explanation:
When using LDAP for authentication, a password can be set locally on FortiAnalyzer as a fallback option in case the LDAP server becomes unreachable. This ensures that the administrator can still log in if there are issues with the LDAP server.

NEW QUESTION 8
You finished registering a FortiGate device. After traffic starts to flow through FortiGate, you notice that only some of the logs expected are being received on FortiAnalyzer.
What could be the reason for the logs not arriving on FortiAnalyzer?

A. This FortiGate is part of an HA cluster but it is the secondary device.
B. This FortiGate model is not fully supported.
C. FortiGate does not have logging configured correctly.
D. FortiGate was added to the wrong ADOM type.

Answer: C

Explanation:
When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 9
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 10
What are two potential advantages of deploying RAID on FortiAnalyzer? (Choose two.)

A. It provides redundancy.
B. It improves performance.
C. It provides backups.
D. It reduces system resource usage.

Answer: AB

Explanation:
Here are two potential advantages of deploying RAID on FortiAnalyzer:
RAID configurations can mirror or stripe data across multiple disks. This redundancy helps ensure
that even if one disk fails, the data remains accessible and recoverable. This is crucial for FortiAnalyzer as it stores security logs which are critical for analysis and forensic investigations.
Certain RAID configurations, like RAID 0 (striping) can improve read performance by distributing data reads across multiple disks. This can be beneficial for FortiAnalyzer when performing faster searches or retrieving large log sets.
Here's why the other options are not necessarily advantages:
While RAID can improve data availability in case of disk failures, it's not a replacement for proper backups. Backups should be done regularly to a separate location to ensure data recovery in case of catastrophic events like hardware failures or ransomware attacks.
RAID itself doesn't necessarily reduce system resource usage. In fact, some RAID configurations can introduce additional overhead for managing the redundant data.

NEW QUESTION 10
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 12
......