

Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator



NEW QUESTION 1

An administrator has moved a FortiGate device from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

- A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
- B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
- C. Logs will be present in both ADOMs immediately after the move.
- D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:

When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

NEW QUESTION 2

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

- A. There is no need to do anything because the disk will self-recover.
- B. Run execute format disk to format and restart the FortiAnalyzer device.
- C. Perform a hot swap of the disk.
- D. Shut down FortiAnalyzer and replace the disk.

Answer: C

Explanation:

In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

NEW QUESTION 3

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 4

Which two statements regarding ADOM modes are true? (Choose two.)

- A. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advanced mode, the disk quota of the ADOM is flexible.
- B. You can change ADOM modes only through the CLI.
- C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- D. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 5

What is the purpose of the FortiAnalyzer command diagnose system print netstat?

- A. It provides network statistics for active connections, including the protocols, IP addresses, and connection states.
- B. It provides the complete routing table, including directly connected routes.
- C. It provides the static DNS table, including the host names and their expiration timers.
- D. It provides NTP server information, including server IP
- E. stratum, poll time, and latency.

Answer: A

Explanation:

The diagnose system print netstat command in FortiAnalyzer provides detailed information on active network connections, similar to the netstat command found in many operating systems.

NEW QUESTION 6
 Refer to the exhibit.

Create New Administrator

User Name	Remote-Admin
Avatar	<div style="display: flex; align-items: center; gap: 10px;"> R <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">+ Add Photo</div> <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">- Remove Photo</div> </div>
Description	
Admin Type	LDAP
LDAP Server	External_Server
Match all users on remote server	<input checked="" type="checkbox"/>

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 7
 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?

- A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer will join to the existing HA cluster as the primary.
- D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: A

Explanation:

Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.

Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.

Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.

Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.

Given these points, the correct conclusion from the options provided is:

* C. This FortiAnalyzer will join the existing HA cluster as the primary.

NEW QUESTION 8

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 9

Which statement is true when you are upgrading the firmware on an HA cluster made up of three FortiAnalyzer devices?

- A. All FortiAnalyzer devices will be upgraded at the same time.
- B. Enabling uninterruptible-upgrade prevents normal operations from being interrupted during the upgrade.
- C. You can perform the firmware upgrade using only a console connection.
- D. First, upgrade the secondary devices, and then upgrade the primary device.

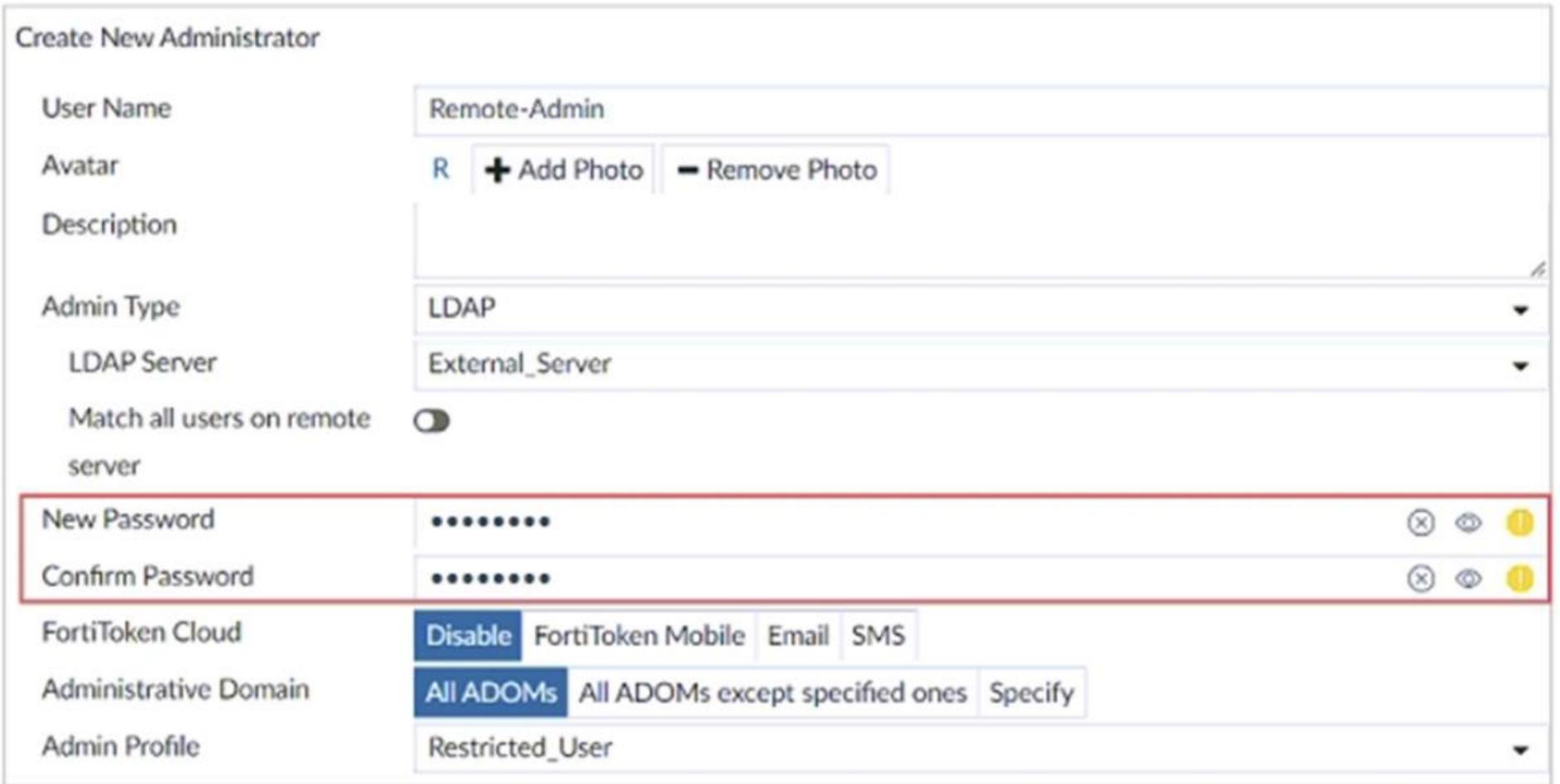
Answer: D

Explanation:

In an HA cluster, the firmware upgrade process involves upgrading the secondary devices first. This approach ensures that the primary device can continue to handle traffic and maintain the operational stability of the network while the secondary devices are being upgraded. Once the secondary devices have successfully upgraded their firmware and are operational, the primary device can then be upgraded. This method minimizes downtime and maintains network integrity during the upgrade process. When upgrading firmware in a High Availability (HA) cluster of FortiAnalyzer units, the recommended practice is to first upgrade the secondary devices before upgrading the primary device. This approach ensures that the primary device, which coordinates the cluster's operations, remains functional for as long as possible, minimizing the impact on log collection and analysis. Once the secondary devices are successfully upgraded and operational, the primary device can be upgraded, ensuring a smooth transition and maintaining continuous operation of the cluster. Reference: FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

NEW QUESTION 10

Refer to the exhibit.



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 against the LDAP server.
- C. This password is set to comply with FortiAnalyzer 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 10

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 11

Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

- A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
- B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
- D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:

RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION 13

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 14

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 17

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' =* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE *user' =' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user* =' USERI' 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 = 'USERI').

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 19

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 21

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

Answer: D

Explanation:

The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 23

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 26

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FAZ_AD-7.4 Practice Test Here](#)