



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

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:

ADOMs 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 3

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 4

The connection status of a new device on FortiAnalyzer is listed as Unauthorized. What does that status mean?

- A. It is a device whose registration has not yet been accepted in FortiAnalyzer.
- B. It is a device that has not yet been assigned an ADOM.
- C. It is a device that is waiting for you to configure a pre-shared key.
- D. It is a device that FortiAnalyzer does not support.

Answer: A

Explanation:

The "Unauthorized" status indicates that the device has been discovered or attempted to connect but has not yet been authorized for management by FortiAnalyzer. It requires an administrator to approve or authorize the device before it can be fully managed.

NEW QUESTION 5

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 6

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 together
- 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 FortiAnalyzer
- 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 7

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extendcommand to expand the storage.
- B. From the VM host manager, expand the size of the existing virtual disk.
- C. From the VM host manager, expand the size of the existing virtual disk and use the # executeformat disk command to reformat the disk.
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array.

Answer: A

Explanation:

Adding an Additional Virtual Disk:

From the VM host manager (such as VMware vSphere or Hyper-V), you can add a new virtual disk to the FortiAnalyzer VM.

Extending the Logical Volume:

After adding the new disk, use commands like #execute lvm extend within the FortiAnalyzer to extend the logical volume, making the additional storage available to the VM. This is particularly useful when you need to add more storage without disrupting existing data.

This approach is recommended when you need to ensure the FortiAnalyzer VM can handle more storage without reformatting or affecting existing data.

NEW QUESTION 8

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

Answer: A

Explanation:

RAID (Redundant Array of Independent Disks) is used in FortiAnalyzer primarily to provide data redundancy and ensure data integrity. Here,s how it relates to each option:

To Introduce Redundancy to Your Log Data (Option A):

The main purpose of employing RAID in FortiAnalyzer is to add redundancy to the storage system. By using RAID configurations (such as RAID 1, RAID 5, or RAID 6), data is replicated across multiple disks, which helps in protecting against disk failures and ensures that log data is not lost if a disk fails. This redundancy enhances the reliability and availability of the log data.

NEW QUESTION 9

It is a best practice to upload FortiAnalyzer local logs to a remote server.Which two remote servers are supported for the upload? (Choose two.)

- A. FTP
- B. SFTP
- C. UDP
- D. TFTP

Answer: AB

Explanation:

When it's considered a best practice to upload FortiAnalyzer local logs to a remote server, the following two remote server protocols are commonly supported: These protocols provide secure and reliable ways to transfer logs and data to remote servers for storage and analysis while maintaining data integrity and confidentiality.

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 10

.....

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](#)