

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 process is responsible for enforcing the log file size?

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

Answer: D

Explanation:

The logfiled process is responsible for enforcing log file size and managing log rotation on FortiAnalyzer. It ensures that log files do not exceed the configured size limits and handles the creation and rotation of new log files when necessary.

NEW QUESTION 3

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 4

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 5

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 6

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

- A. RAID0
- 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 7

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 8

Refer to the exhibit.

Cluster Settings

Operation Mode: Standalone | **High Availability**

Preferred Role: Secondary | **Primary**

Cluster Virtual IP

IP Address and Interface: IP Address: 192.168.101.222 | Interface: port1

Cluster Settings

Peer IP and Peer SN: Peer IP: 10.0.1.210 | Peer SN: FAZ-VM0000065040

Group Name: NSE6

Group ID: 1 (1-255)

Password: [Masked]

Heart Beat Interval: 10 Seconds

Failover Threshold: 30

Priority: 120

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 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

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

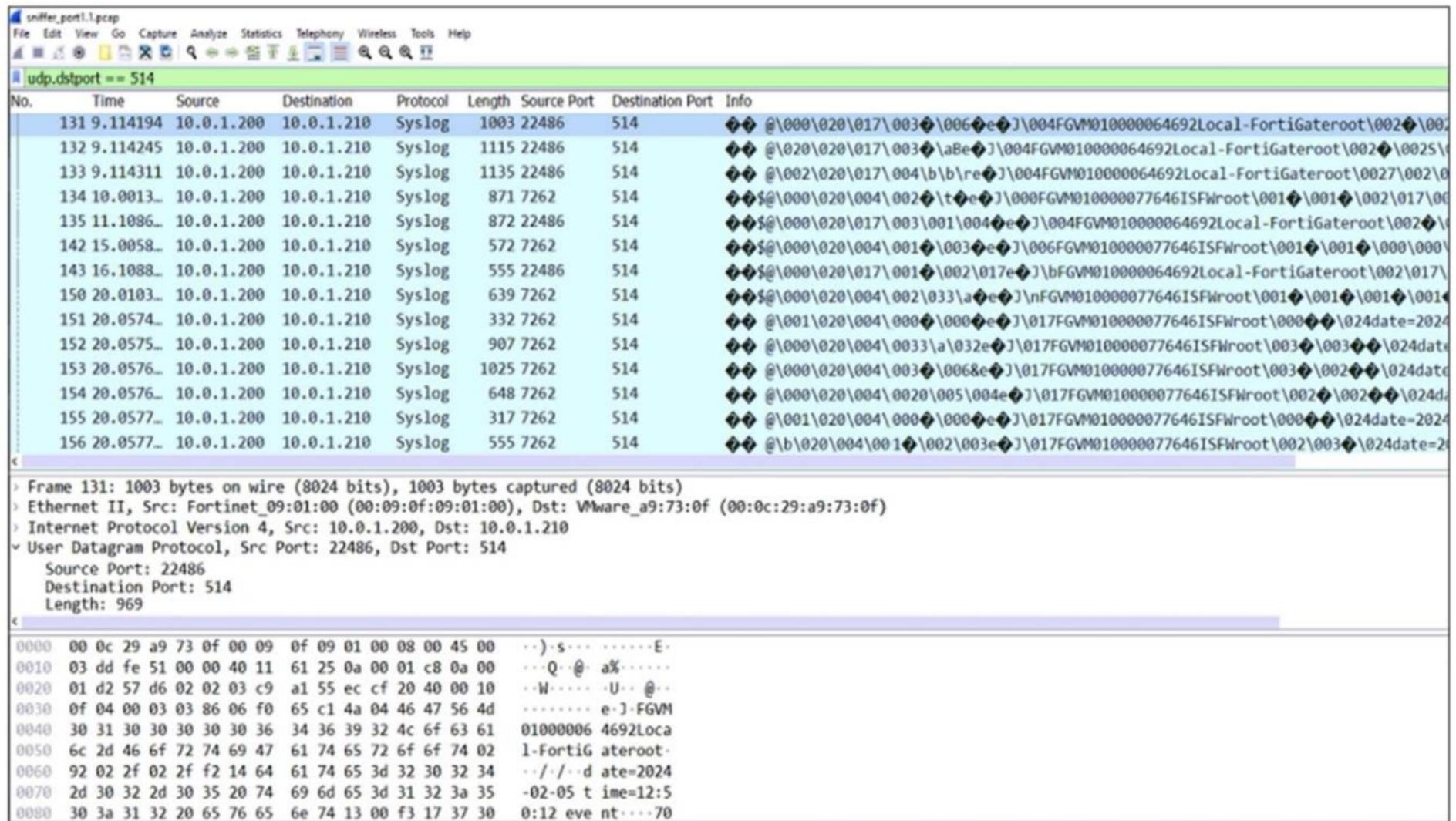
Explanation:

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 10

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



The capture displayed was taken on a FortiAnalyzer. Why is a single IP address shown as the source for all logs received?

- A. FortiAnalyzer is using the device MAC addresses to differentiate their logs.
- B. The logs belong to devices that are part of a high availability (HA) cluster.
- C. FortiAnalyzer is receiving logs from the root FortiGate of a Security Fabric.
- D. The device sending logs has two VDOMs in the same ADOM.

Answer: C

Explanation:

In a Fortinet Security Fabric, logs from downstream devices can be sent to FortiAnalyzer through the root FortiGate. This is why all the logs have the same source IP address (the root FortiGate). The root FortiGate aggregates and forwards the logs from all downstream devices, so the source IP in the log capture will appear to be from the root FortiGate itself, even though the logs originate from multiple devices within the fabric.

NEW QUESTION 12

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 16

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 20

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 22

Refer to the exhibit.

Event	Event Status	Event Type	Count	Severity
<div style="display: flex; align-items: center;"> ▼ 151.101.54.62 (1) </div>				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙️ SSL	1	🟢 Low

Which statement is correct regarding the event displayed?

- A. An incident was created from this event.
- B. The security risk was blocked or dropped.
- C. The security event risk is considered open.
- D. The risk source is isolated.

Answer: B

Explanation:

The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented.

Events in FortiAnalyzer will be in one of four statuses.

The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are: Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

NEW QUESTION 23

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 26

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 29

.....

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](#)