

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

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

Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.

FortiAnalyzer HA cluster settings

Cluster Settings

Operation Mode

Standalone
Active-Passive
Active-Active

Preferred Role

Secondary
Primary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

Action

192.168.101.222

port1

x
+

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

Action

10.0.1.210

FAZ-VM0000065040

x
+

Group Name

Training

Group ID

1

(1-255)

Password

.....

Heart Beat Interval

10

Seconds

Heart Beat Interface

port1

Failover Threshold

30

Priority

120

(80-120)

Log Data Sync

The administrator wants to join this FortiAnalyzer to an existing HA cluster. What can you conclude from the configuration displayed?

- A. After joining the cluster, this FortiAnalyzer will forward received logs to its peers.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer is configured to route HA traffic through a gateway.
- D. This FortiAnalyzer will join the existing HA cluster as the secondary.

Answer: B

Explanation:

The "Preferred Role" is set to Secondary, which means this FortiAnalyzer is configured to join the cluster as the secondary unit in an Active-Passive HA configuration. Other settings, such as the peer IP and serial number, confirm its setup to communicate with the primary unit.

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

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 7

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

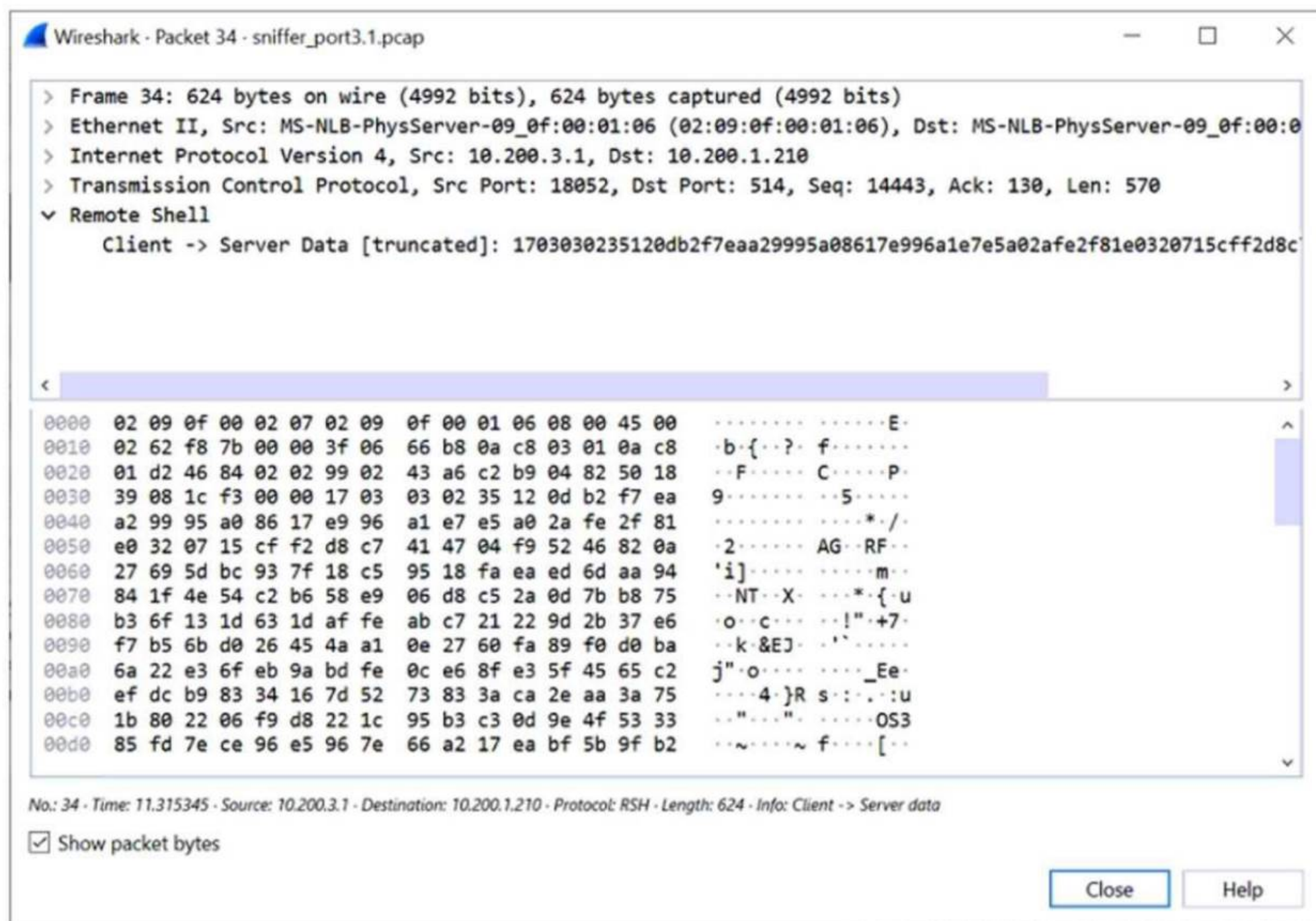
Explanation:

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 8

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



Which image corresponds to the packet capture shown in the exhibit?

A)

					Search...
<input type="checkbox"/>	Device Name ⇅	IP Address ⇅	Connectivity ⇅	Logging Mode ⇅	Average Log Rate(Logs/Sec) ⇅
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↑ Connection Up	🔒 Real Time	0

B)

					Search...
<input type="checkbox"/>	Device Name ⇅	IP Address ⇅	Connectivity ⇅	Logging Mode ⇅	Average Log Rate(Logs/Sec) ⇅
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↑ Connection Up	Real Time	0

C)

					Search...
<input type="checkbox"/>	Device Name ⇅	IP Address ⇅	Connectivity ⇅	Logging Mode ⇅	Average Log Rate(Logs/Sec) ⇅
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↓ Connection Down	🔒 Real Time	0

D)

					Search...
<input type="checkbox"/>	Device Name ⇅	IP Address ⇅	Connectivity ⇅	Logging Mode ⇅	Average Log Rate(Logs/Sec) ⇅
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↓ Connection Down	Real Time	0

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.

NEW QUESTION 9

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

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 operate 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 10

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 14

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 process
- 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 16

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 TB
- B. RAID 10 combines mirroring striping and distributed parity to provide performance and fault tolerance
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 TB
- 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 20

View the exhibit:

Data Policy			
Keep Logs for Analytics	60	Days	
Keep Logs for Archive	365	Days	
Disk Utilization			
Maximum Allowed	1000	MB	
Analytics: Archive	70%	30%	
Alert and Delete When Usage Reaches	90%		

Out of Available: 62.8 GB

☐ Modify

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 21

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 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 30

.....

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