Fortinet

FCP_FAZ_AD-7.4 Exam

FCP - FortiAnalyzer 7.4 Administrator

Questions & Answers
Demo

ExamsLand provides 100% free Fortinet FCP_FAZ_AD-7.4 practice questions and answers in pdf. Instant access.

Page 2

Version: 4.1

Question: 1

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: C, D

Question: 2

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 IPs. 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.

Question: 3

Refer to the exhibit.

ExamsLand provides 100% free Fortinet FCP_FAZ_AD-7.4 practice questions and answers in pdf. Instant access.

Page 3

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	🔵

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. It allows user accounts in the LDAP server to use two-factor authentication.
B. It creates a wildcard administrator using an LDAP server.
C. User Remote-Admin from the LDAP server will be able to log in to FortiAnalyzer at any time.
D. Administrators can log in to FortiAnalyzer using their credentials on the remote LDAP server.

Answer: B, D

Explanation:

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

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 FortiAnalvzer.
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 FortiAnalvzer does not support.

ExamsLand provides 100% free Fortinet FCP_FAZ_AD-7.4 practice questions and answers in pdf. Instant access.
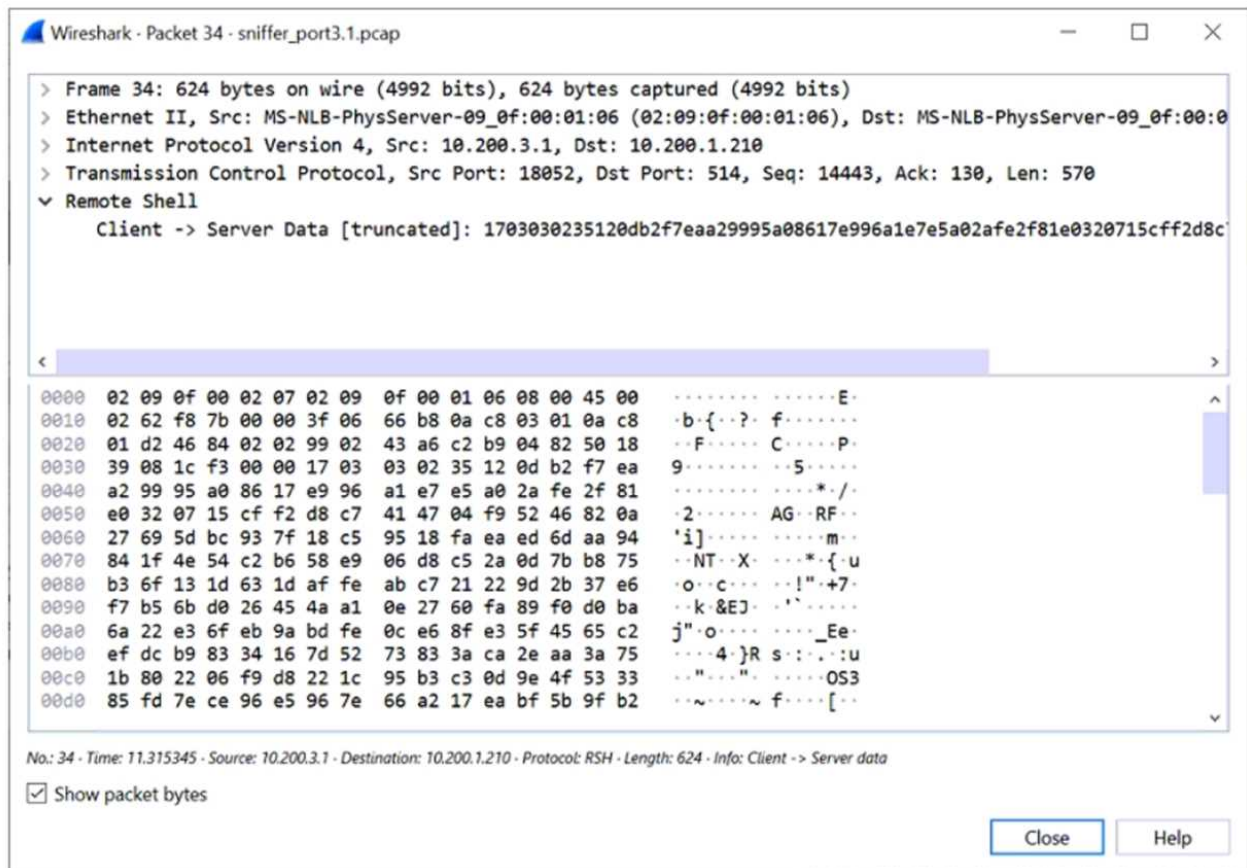
Page 4

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.

Question: 5

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

```
Wireshark · Packet 34 · sniffer_port3.1.pcap                                  —    □    ✕

> Frame 34: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06), Dst: MS-NLB-PhysServer-09_0f:00:0
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> Transmission Control Protocol, Src Port: 18052, Dst Port: 514, Seq: 14443, Ack: 130, Len: 570
∨ Remote Shell
    Client -> Server Data [truncated]: 1703030235120db2f7eaa29995a08617e996a1e7e5a02afe2f81e0320715cff2d8c

<                                                                              >

0000  02 09 0f 00 02 07 02 09  0f 00 01 06 08 00 45 00   ········ ······E·
0010  02 62 f8 7b 00 00 3f 06  66 b8 0a c8 03 01 0a c8   ·b·{··?· f·······
0020  01 d2 46 84 02 02 99 02  43 a6 c2 b9 04 82 50 18   ··F····· C·····P·
0030  39 08 1c f3 00 00 17 03  03 02 35 12 0d b2 f7 ea   9······· ··5·····
0040  a2 99 95 a0 86 17 e9 96  a1 e7 e5 a0 2a fe 2f 81   ········ ····*·/·
0050  e0 32 07 15 cf f2 d8 c7  41 47 04 f9 52 46 82 0a   ·2······ AG··RF··
0060  27 69 5d bc 93 7f 18 c5  95 18 fa ea ed 6d aa 94   'i]····· ····m··
0070  84 1f 4e 54 c2 b6 58 e9  06 d8 c5 2a 0d 7b b8 75   ··NT··X· ···*·{·u
0080  b3 6f 13 1d 63 1d af fe  ab c7 21 22 9d 2b 37 e6   ·o··c··· ··!"·+7·
0090  f7 b5 6b d0 26 45 4a a1  0e 27 60 fa 89 f0 d0 ba   ··k·&EJ· ·'`·····
00a0  6a 22 e3 6f eb 9a bd fe  0c e6 8f e3 5f 45 65 c2   j"·o···· ····_Ee·
00b0  ef dc b9 83 34 16 7d 52  73 83 3a ca 2e aa 3a 75   ····4·}R s·:·.·:u
00c0  1b 80 22 06 f9 d8 22 1c  95 b3 c3 0d 9e 4f 53 33   ··"···"· ·····OS3
00d0  85 fd 7e ce 96 e5 96 7e  66 a2 17 ea bf 5b 9f b2   ··~····~ f····[··

No.: 34 · Time: 11.315345 · Source: 10.200.3.1 · Destination: 10.200.1.210 · Protocol: RSH · Length: 624 · Info: Client -> Server data

☑ Show packet bytes                                                    [ Close ]   [ Help ]
```

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

A)

ExamsLand provides 100% free Fortinet FCP_FAZ_AD-7.4 practice questions and answers in pdf. Instant access.

Page 5

	Device Name ⇕	IP Address ⇕	Connectivity ⇕	Logging Mode ⇕	Average Log Rate(Logs/Sec) ⇕
☐	Remote-FortiGate	10.200.3.1	▲ Connection Up	🔒 Real Time	0

B)

	Device Name ⇕	IP Address ⇕	Connectivity ⇕	Logging Mode ⇕	Average Log Rate(Logs/Sec) ⇕
☐	Remote-FortiGate	10.200.3.1	▲ Connection Up	Real Time	0

C)

	Device Name ⇕	IP Address ⇕	Connectivity ⇕	Logging Mode ⇕	Average Log Rate(Logs/Sec) ⇕
☐	Remote-FortiGate	10.200.3.1	▼ Connection Down	🔒 Real Time	0

D)

	Device Name ⇕	IP Address ⇕	Connectivity ⇕	Logging Mode ⇕	Average Log Rate(Logs/Sec) ⇕
☐	Remote-FortiGate	10.200.3.1	▼ Connection Down	Real Time	0

A. Option A
B. Option B
C. Option C
D. Option D

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.

Thank You For Trying FCP_FAZ_AD-7.4 PDF Demo

To try our FCP_FAZ_AD-7.4 Premium Files visit link below:

https://examsland.com/latest-exam-questions/FCP_FAZ_AD-7.4/

Start Your FCP_FAZ_AD-7.4 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.