

NSE5_FAZ-7.0^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse5_faz-7-0.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

- 😳 365 Days Free Update
- 800,000+ Satisfied Customers





QUESTION 1

An administrator has configured the following settings:

config system fortiview settings set resolve-ip enable end

What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.

B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.

C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.

D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Correct Answer: D

Reference: https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in-FortiAnalyzer/m-p/95351?m=156950

QUESTION 2

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

- A. A FortiGate ADOM
- B. The FortiGate serial number
- C. A pre-shared key
- D. Valid FortiAnalyzer credentials

Correct Answer: D

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration. FortiAnalyzer_7.0_Study_Guide-Online pag. 93

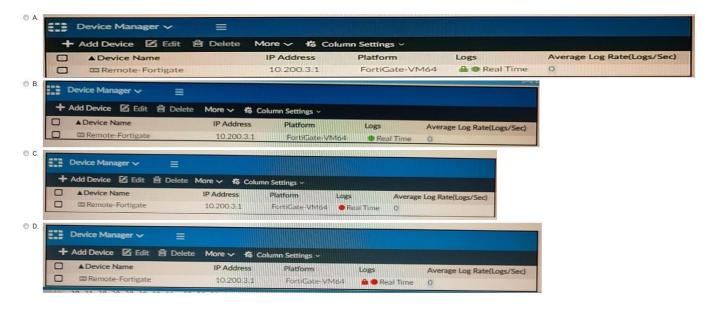
QUESTION 3

Refer to the exhibit.



<pre>> Fram > Ethe > Inte > User </pre>	Wireshark - Packet 50 - sniffer_portl1pcap > Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) > Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79) > Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210 > User Datagram Protocol, Src Port: 15864, Dst Port: 514 [truncated]Syslog message: (unknown):												
0000 0010 0020 0030 0040 0050 0050 0060	00 0c 01 4b 01 d2 10 04 30 31 74 65 00 fe 20 30	fb 88 3d f8 00 01 30 30 2d 46 f1 14	8 00 3 02 1 00 3 30 5 6f 4 64	00 3 02 0 f7 00 30 30 72 74 61 74	f 11 1 37 0 fe 0 36 4 69 4 65	29 a8 79 64 b7 0 7c 24 ec 61 a7 3 35 30 3 47 61 74 3d 32 30 3d 30 36	c8 0 cf 26 5c 46 36 5 65 7 32 31	01 0a 40 01 47 56 65 6d 6f 6f 2d 31	c8 10 4d 6f 74 32	01000006 te-Forti date			
0080 0090 00a0 00b0 00c0 00c0	36 20 34 38 7a 3d 22 30 65 3d 79 73	65 76 36 33 22 20 31 30 22 42 74 65	5 65 3 36 1 30 0 30 2 00 5 6d	6e 74 39 34 38 30 30 32 52 22 22 20	4 13 4 39 0 30 2 30 2 20 0 6c	00 f1 25 32 36 35 22 20 60 30 31 34 73 75 62 65 76 65	31 30 35 36 6f 67 22 20 10 00	5 33 38 5 35 20 7 69 64 9 74 79 9 f1 11	33 74 3d 70 73	6 event 48636949 z="-0800)16383 265565 t "logid= 014" typ sub s		
00e0 00f0 0100 0110 0120 0130 0140 0150	72 6e 00 f0 73 65 6f 6e 73 3d 22 32 69 6e 33 38	12 64 72 3d 3d 22 22 73 00 11 74 6f	65 22 6f 75 20 20	73 63 61 64 00 fe 63 63 31 06 74 68	3 3d 4 6d 9 0a 8 65 9 00 8 65	64 3d 22 22 54 65 69 6e 22 6e 22 20 73 73 22 97 00 f0 20 66 77 22	73 74 20 61 73 74 20 60 0e 67	22 20 63 74 61 74 73 67 65 64	75 69 75 3d 20	rning" v desc= ser="adm on="o s="succe "2 1 into the 38348636	"Test" u in" acti n" statu		

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



- A. Option A
- B. Option B
- C. Option C
- D. Option D
- Correct Answer: D



QUESTION 4

How are logs forwarded when FortiAnalyzer is using aggregation mode?

- A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.
- B. Logs and content files are stored and uploaded at a scheduled time.
- C. Logs are forwarded as they are received.
- D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/ https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes Reference: https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-andlog-aggregation-modes

QUESTION 5

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

- A. Remote logging must be enabled on FortiGate
- B. Log encryption must be enabled
- C. ADOMs must be enabled
- D. FortiGate must be registered with FortiAnalyzer

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit."

https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6- Administration%20Guide.pdf

Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."

NSE5_FAZ-7.0 VCE Dumps NSE5_FAZ-7.0 Study Guide NSE5_FAZ-7.0 Exam

Questions