

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.passapply.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



https://www.passapply.com/nse5_faz-7-0.html 2024 Latest passapply NSE5_FAZ-7.0 PDF and VCE dumps Download

QUESTION 1

Correct Answer: A

correct log correlation.

Which daemon is responsible for enforcing the log file size?
A. sqlplugind
B. logfiled
C. miglogd
D. ofrpd
Correct Answer: B
Disk quota enforcement is performed by different processes:
The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.
FortiAnalyzer_7.0_Study_Guide-Online pag. 121
QUESTION 2
If you upgrade your FortiAnalyzer firmware, what report elements can be affected?
A. Output profiles
B. Report settings
C. Report scheduling
D. Custom datasets
Correct Answer: D
QUESTION 3
Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?
A. To properly correlate logs
B. To use real-time forwarding
C. To resolve host names
D. To improve DNS response times

Study Guide 7.0 page 30: Synchronize the time on FortiAnalyzer and all Registered devices wit han NTP server for

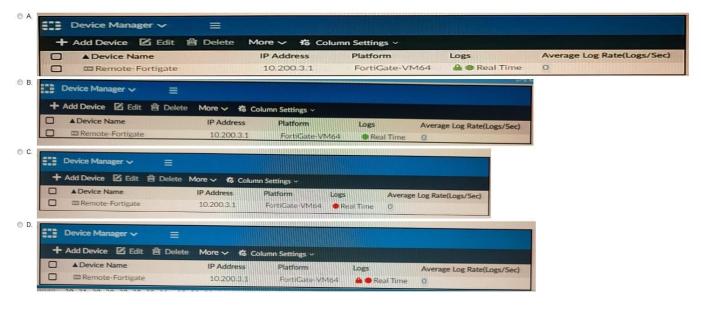


QUESTION 4

Refer to the exhibit.

```
Wireshark - Packet 50 - sniffer_port3.1.pcap
   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): �� @\001\020\020\004\000\001\000�\000�a�7\FGVM010000065036Remote
   Message: 00 @\001\020\020\004
       00 0c 29 c0 81 79 00 0c
                                   29 a8 79 e6 08 00 45 00
                                                                        ) · y ·
       01 4b fb 88 00 00 3f 11
                                   64 b7 0a c8 03 01 0a c8
       01 d2 3d f8 02 02 01
                              37
                                   7c
                                         ec cf 20 40 01 10
37 5c 46 47 56 4d
                                      24 ec
       10 04 00 01 00 f7 00 fe
                                   61 a7
                                                                         a 7\FGVM
       30 31 30 30 30 30 30
                              36
                                   35
                                      30 33 36 52 65 6d 6f
                                                               01000006 5036Remo
       74 65 2d 46 6f 72 74 69
                                   47 61 74 65 72 6f 6f 74
                                                               te-Forti Gateroot
       00 fe f1 14 64 61 74 65
20 30 31 20 74 69 60 65
                                  3d 32 30 32
3d 30 30 3a
                                                               -01 time
       36 20 65 76 65 6e 74 13
                                  00 f1 29 31 36 33 38 33
                                                                          )16383
       34 38 36 33
                    36 39 34 39
                                   32 36 35 35 36 35 20 74
                                                               48636949 265565 t
       7a 3d 22 2d 30 38 30 30
                                                               z="-0800
                                  22 20 6c 6f 67
                                                   69 64 3d
                                                                        " logid=
       22 30 31 30
                    30 30 32 30
                                   30 31 34 22 20 74 79 70
                                                               "0100020 014" typ
       65 3d 22 42 00 52 22 20
                                  73 75 62 10 00 f1 11 73
                                                               e="B-R"
ystem" 1
                                                                        sub
       79 73 74 65 6d 22 20 6c
                                  65
                                     76 65 6c
                                               3d 22 77 61
       72 6e 69 6e 67 22 20 76
                                  64 3d 22 72
                                               6f 6f 74 4b
                                                               rning" v d="rootK
       00 f0 12 64 65 73
                          63
                              3d
                                  22 54 65 73
                                               74 22 20 75
                                                               · · · desc= "Test" u
       73 65 72 3d 22 61 64 6d
                                  69 6e 22 20 61 63 74 69
                                                               ser="adm in"
                                                              on="o n" statu
s="succe ss" msg=
"2 1 ged
       6f 6e 3d 22 6f 00 f0 0a
                                  6e 22 20 73
                                               74 61 74 75
       73 3d 22 73 75 63 63
                                         22 20 6d 73 67 3d
                                      73
       22 32 00 11
                    20 31 00 00
                                  97
                                     00
                                         f0 0e 67 65 64 20
       69 6e 74 6f 20 74 68 65
                                                              into the fw
38348636 "
                                  20 66 77 20 2d 20 31 36
       33 38
             33 34 38 36 33 36
                                  22
```

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



- A. Option A
- B. Option B
- C. Option C



https://www.passapply.com/nse5_faz-7-0.html 2024 Latest passapply NSE5_FAZ-7.0 PDF and VCE dumps Download

D. Option D

Correct Answer: D

QUESTION 5

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

Correct Answer: B

<u>Latest NSE5_FAZ-7.0</u> <u>Dumps</u>

NSE5 FAZ-7.0 PDF Dumps

NSE5 FAZ-7.0 Practice
Test