



Free Questions for [NSE6_FAZ-7.2](#) by [certsinside](#)

Shared by [Brady](#) on [22-07-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Which two statements are true regarding the log synchronization states for HA on FortiAnalyzer? (Choose two.)

Options:

- A-** Log Data Sync provides real-time log synchronization to all backup devices.
- B-** When Log Data Sync is turned on, the backup device reboots and then rebuilds the log database with the synchronized logs.
- C-** With Initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D-** By default. Log Data Sync is disabled on all backup devices.

Answer:

A, C

Explanation:

For HA on FortiAnalyzer, Log Data Sync ensures real-time log synchronization among all cluster members, including backup devices. This feature is enabled by default. The Initial Logs Sync state is triggered when a new unit is added to an HA cluster, where the primary unit synchronizes its logs with the newly added unit. After the initial synchronization, the secondary unit reboots and rebuilds its log

database with the synchronized logs. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Log synchronization' section.

Question 2

Question Type: MultipleChoice

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

Options:

- A- LDAP servers IP addresses added as trusted hosts
- B- One or more remote LDAP servers
- C- A local wildcard administrator account
- D- An administrator group

Answer:

B, D

Explanation:

To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Configuring remote authentication for administrators using LDAP' section.

Question 3

Question Type: MultipleChoice

Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

Options:

A- Disk size

B- Total quota

C- RAID level

D- License type

Answer:

A, C

Explanation:

The amount of reserved disk space required by FortiAnalyzer is influenced by the disk size and the RAID level. The system reserves a portion of the disk space for system use and unexpected quota overflow, with the rest available for device allocation. The RAID level determines the disk size and the reserved disk quota level, with different RAID configurations leading to variations in the reserved space. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Disk Space Allocation' and 'RAID Level Impact' sections.

Question 4

Question Type: MultipleChoice

Which statement is true about using aggregation mode on FortiAnalyzer?

Options:

- A- Aggregation mode supports log filters.
- B- Aggregation mode can work with syslog servers.
- C- In aggregation mode, logs and content files are forwarded in real time.
- D- Aggregation mode can be configured only on the CLI.

Answer:

B

Explanation:

In aggregation mode, FortiAnalyzer stores logs received from devices and forwards them at a specified time each day to avoid duplication. It is specifically designed to work between two FortiAnalyzer units and does not support syslog or CEF servers. Additionally, aggregation mode configurations are limited to CLI commands log-forward and log-forward-service. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Aggregation' and 'CLI Commands for Aggregation Mode' sections.

Question 5

Question Type: MultipleChoice

Which items must you configure on FortiAnalyzer to send its reports to an external server?

Options:

- A- Report schedule
- B- Mail server
- C- Fabric connector
- D- Output profile

Answer:

D

Explanation:

To send reports from FortiAnalyzer to an external server, you must configure the output profile. This involves specifying the method (FTP, SFTP, or SCP), server IP, username, password, and the directory where the report will be saved. Additionally, you have the option to delete the report after it has been uploaded to the server. Reference: FortiAnalyzer 7.2 Administrator Guide, 'Enable uploading of generated reports to a server' section.

Question 6

Question Type: MultipleChoice

Refer to the exhibit.


```


> Frame 5: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06),
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 8678, Dst Port: 514
▼ [truncated] Syslog message: (unknown): \001\020\020\004\000\001\0
  > Message: \001\020\020\004

```

0000	02 09 0f 00 02 06 02 09 0f 00 01 06 08 00 45 00E.
0010	01 4b bb b3 00 00 3f 11 a4 8c 0a c8 03 01 0a c8	-K....?-.....
0020	01 d2 21 e6 02 02 01 37 81 ea ec cf 20 60 01 10	..!....7`..
0030	10 04 00 01 00 f7 00 fe 63 a1 53 9a 46 47 56 4dc·S·FGVM
0040	30 31 30 30 30 30 36 35 30 33 36 52 65 6d 6f	01000006 5036Remo
0050	74 65 2d 46 6f 72 74 69 47 61 74 65 72 6f 6f 74	te-Forti Gateroot
0060	00 fe f1 14 64 61 74 65 3d 32 30 32 32 2d 31 32	...date =2022-12
0070	2d 31 39 20 74 69 6d 65 3d 32 32 3a 31 38 3a 30	-19 time =22:18:0
0080	32 20 65 76 65 6e 74 13 00 f1 29 31 36 37 31 35	2 event· ..)16715
0090	31 37 30 38 32 34 34 35 33 36 31 38 38 31 20 74	17082445 361881 t
00a0	7a 3d 22 2d 30 30 30 30 22 20 6c 6f 67 69 64 3d	z="-0800 " logid=
00b0	22 30 31 30 30 30 32 30 30 31 34 22 20 74 79 70	"0100020 014" typ
00c0	65 3d 22 42 00 52 22 20 73 75 62 10 00 f1 11 73	e="B·R" sub···s
00d0	79 73 74 65 6d 22 20 6c 65 76 65 6c 3d 22 77 61	ystem" l evel="wa
00e0	72 6e 69 6e 67 22 20 76 64 3d 22 72 6f 6f 74 4b	rning" v d="rootK
00f0	00 f0 12 64 65 73 63 3d 22 54 65 73 74 22 20 75	...desc= "Test" u
0100	73 65 72 3d 22 61 64 6d 69 6e 22 20 61 63 74 69	ser="adm in" acti
0110	6f 6e 3d 22 6f 00 f0 0a 6e 22 20 73 74 61 74 75	on="o·· n" statu
0120	73 3d 22 73 75 63 63 65 73 73 22 20 6d 73 67 3d	s="succe ss" msg=
0130	22 32 00 11 20 31 00 00 97 00 f0 0e 67 65 64 20	"2· 1· ···ged
0140	69 6e 74 6f 20 74 68 65 20 66 77 20 2d 20 31 36	into the fw - 16
0150	37 31 35 31 37 30 38 32 22	71517082 "

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

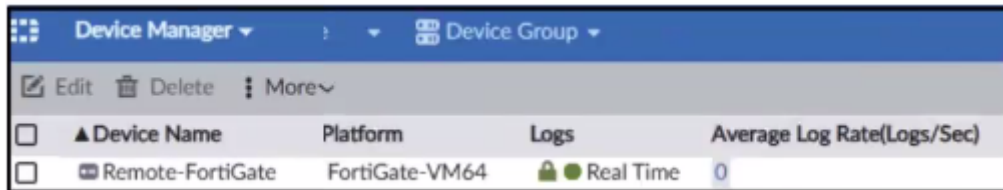
A)



The screenshot shows the FortiGate Device Manager interface. At the top, there are tabs for 'Device Manager' and 'Device Group'. Below the tabs, there are action buttons: 'Edit', 'Delete', and 'More'. A table lists the device details:

<input type="checkbox"/>	▲ Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	FortiGate-VM64	● Real Time	0


B)



The screenshot shows the FortiGate Device Manager interface. At the top, there are tabs for 'Device Manager' and 'Device Group'. Below the tabs, there are action buttons: 'Edit', 'Delete', and 'More'. A table lists the device details:

<input type="checkbox"/>	▲ Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	FortiGate-VM64	● Real Time	0

C)



The screenshot shows the FortiGate Device Manager interface. At the top, there are tabs for 'Device Manager' and 'Device Group'. Below the tabs, there are action buttons: 'Edit', 'Delete', and 'More'. A table lists the device details:

<input type="checkbox"/>	▲ Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	FortiGate-VM64	● Real Time	0

Options:

A- Option A

B- Option B

C- Option C

Answer:

A

Explanation:

The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions 'real-time'. Therefore, Option A is the correct answer because it shows logs with 'Real Time' status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture. Reference: Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

Question 7

Question Type: MultipleChoice

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?

Options:

- A- FortiGate does not have logging configured correctly.
- B- This FortiGate model is not fully supported.
- C- This FortiGate is part of an HA cluster but it is the secondary device.
- D- FortiGate was added to the wrong ADOM type.

Answer:

A

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.

To Get Premium Files for NSE6_FAZ-7.2 Visit

https://www.p2pexams.com/products/nse6_faz-7.2

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse6-faz-7.2>

