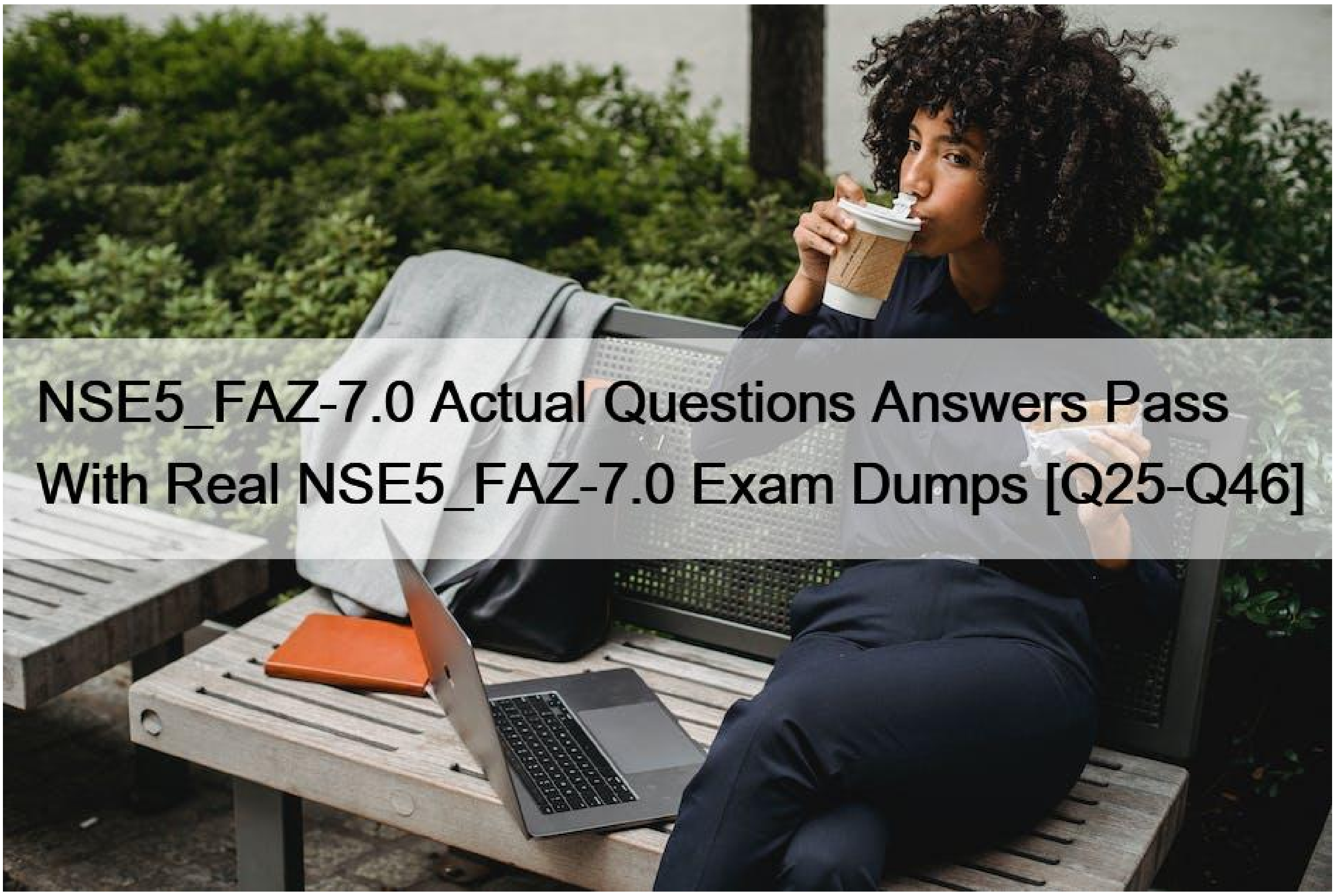
NSE5_FAZ-7.0 Actual Questions Answers Pass With Real NSE5_FAZ-7.0 Exam Dumps [Q25-Q46



NSE5_FAZ-7.0 Actual Questions Answers Pass With Real NSE5_FAZ-7.0 Exam Dumps NSE5_FAZ-7.0 Dumps Prepare Your Exam With 116 Questions

Fortinet NSE5_FAZ-7.0 Exam Syllabus Topics:

TopicDetailsTopic 1- Explain SOC features in FortiAnalyzer- Perform initial configurationTopic 2- Customize and generate reports - Device registration and communicationTopic 3- Configure high availability (HA)- Troubleshoot and manage logsTopic 4- Troubleshoot device communication issues- Configure administrative accessTopic 5- Manage events and event handlers- Manage and troubleshoot reportsTopic 6- Configure administrative domains (ADOMs)- Create and manage playbooksTopic 7 - System configuration- Protect log data- Manage incidents

QUESTION 25

Which two purposes does the auto cache setting on reports serve? (Choose two.)

* It automatically updates the hcache when new logs arrive.

* It provides diagnostics on report generation time.

* It reduces the log insert lag rate.
* It reduces report generation time.
Reference:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

QUESTION 26

By default, what happens when a log file reaches its maximum file size?
* FortiAnalyzer overwrites the log files.
* FortiAnalyzer stops logging.
* FortiAnalyzer rolls the active log by renaming the file.
* FortiAnalyzer forwards logs to syslog.

QUESTION 27

Which two statements are true regarding FortiAnalyzer log forwarding? (Choose two.)
* In aggregation mode, you can forward logs to syslog and CEF servers as well.
* Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
* Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
* Both modes, forwarding and aggregation, support encryption of logs between devices.

QUESTION 28

Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?
* To properly correlate logs
* To use real-time forwarding
* To resolve host names
* To improve DNS response times

QUESTION 29

Which statement is true regarding Macros on FortiAnalyzer?
* Macros are ADOM specific and each ADOM will have unique macros relevant to that ADOM.
* Macros are supported only on the FortiGate ADOM.
* Macros are useful in generating excel log files automatically based on the reports settings.
* Macros are predefined templates for reports and cannot be customized.
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 283: Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

QUESTION 30

An administrator has moved FortiGate A from the root ADOM to ADOM1. However, the administrator is not able to generate reports for FortiGate A in ADOM1.

What should the administrator do to solve this issue?
* Use the execute sql-local rebuild-db command to rebuild all ADOM databases.
* Use the execute sql-local rebuild-adom ADOM1 command to rebuild the ADOM database.

* Use the execute sql-report run ADOM1 command to run a report.
* Use the execute sql-local rebuild-adom root command to rebuild the ADOM database.

QUESTION 31

Which two statements express the advantages of grouping similar reports? (Choose two.)
* Improve report completion time.
* Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
* Reduce the number of hcache tables and improve auto-hcache completion time.
* Provides a better summary of reports.

QUESTION 32

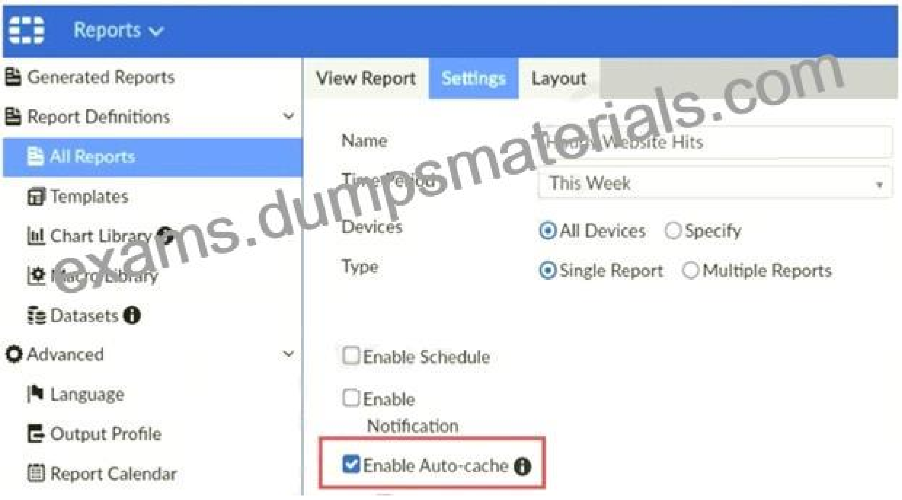
Which two statements are correct regarding the export and import of playbooks? (Choose two.)
* You can export only one playbook at a time.
* You can import a playbook even if there is another one with the same name in the destination.
* Playbooks can be exported and imported only within the same FortiAnaryzer.
* A playbook that was disabled when it was exported, will be disabled when it is imported.
If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.

Playbooks are imported with the same status they had (enabled or disabled) when they were exported.

Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

QUESTION 33

Refer to the exhibit.



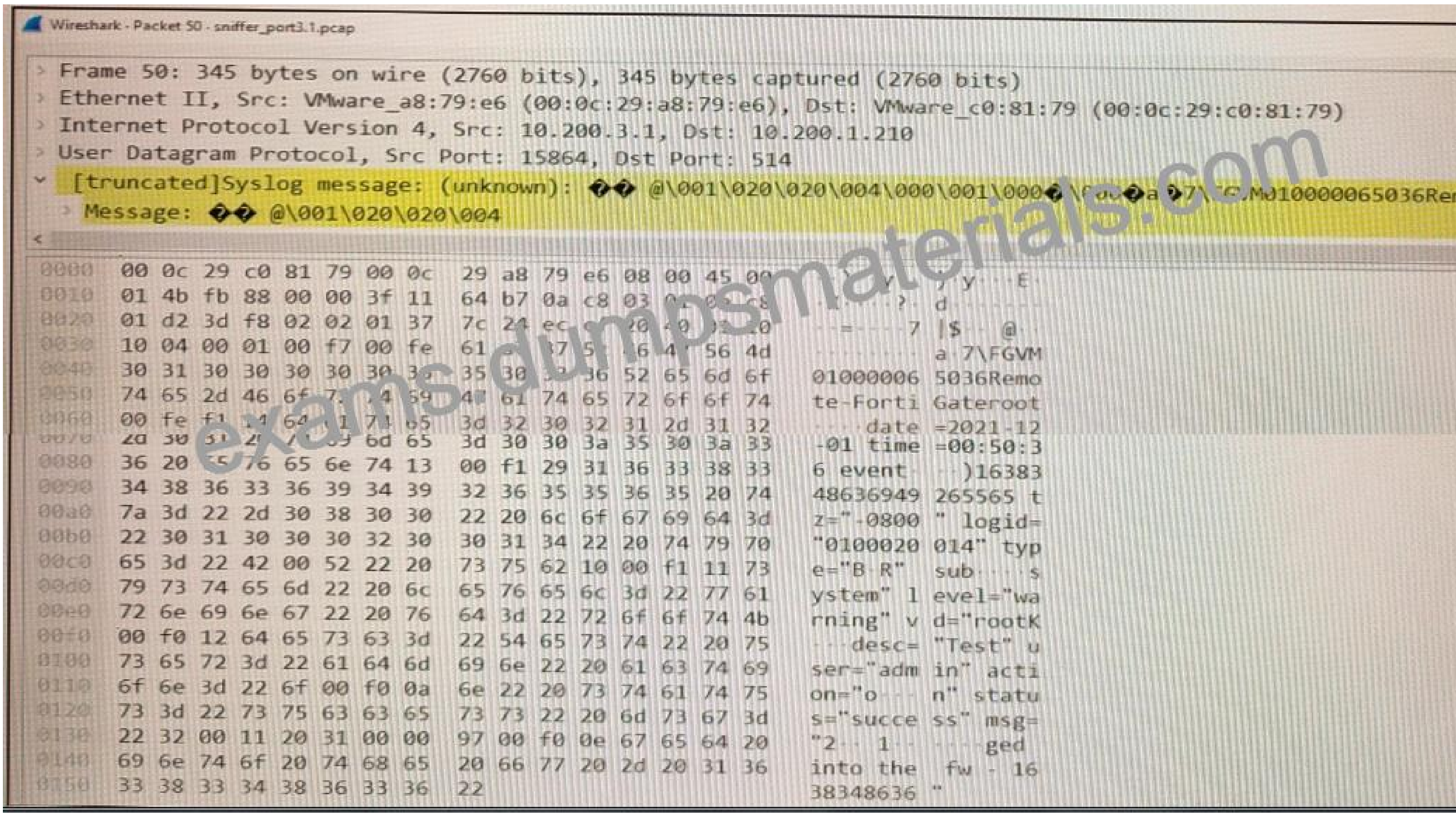
Name: Hourly Website Hits
Time Period: This Week
Devices: ● All Devices ○ Specify
Type: ● Single Report ○ Multiple Reports
□ Enable Schedule
□ Enable Notification
☑ Enable Auto-cache

Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)
* Report size will be optimized to conserve disk space on FortiAnalyzer.
* Reports will be cached in the memory.
* This feature is automatically enabled for scheduled reports.

* Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

QUESTION 34

Refer to the exhibit.

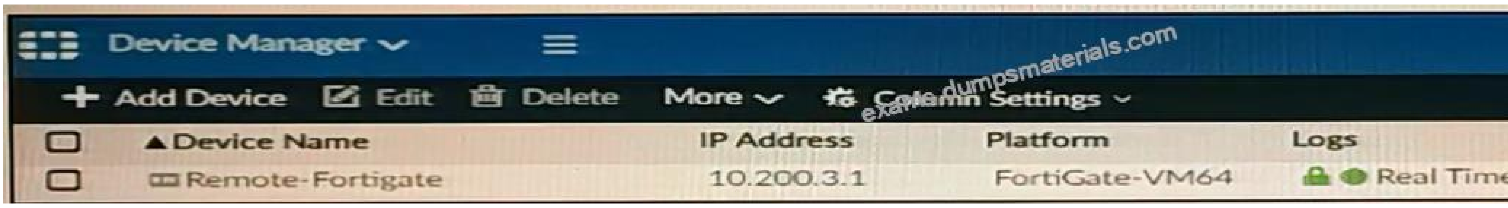


```
> Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 15864, Dst Port: 514
v [truncated]Syslog message: (unknown): �� @\001\020\020\004\000\001\000�\[illegible]�a�7\[illegible]M010000065036Re
  > Message: �� @\001\020\020\004

0000  00 0c 29 c0 81 79 00 0c  29 a8 79 e6 08 00 45 00   ..)..y.. ).y...E.
0010  01 4b fb 88 00 00 3f 11  64 b7 0a c8 03 01 0a c8   .K....?. d.......
0020  01 d2 3d f8 02 02 01 37  7c 24 ec [illegible] 20 40 [illegible] 10   ..=....7 |$.. @..
0030  10 04 00 01 00 f7 00 fe  61 [illegible] 37 5c 46 47 56 4d   ........ a.7\FGVM
0040  30 31 30 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 31 2d 31 32   ....date =2021-12
0070  2d 30 31 20 74 69 6d 65  3d 30 30 3a 35 30 3a 33   -01 time =00:50:3
0080  36 20 65 76 65 6e 74 13  00 f1 29 31 36 33 38 33   6 event. ..)16383
0090  34 38 36 33 36 39 34 39  32 36 35 35 36 35 20 74   48636949 265565 t
00a0  7a 3d 22 2d 30 38 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  33 38 33 34 38 36 33 36  22                        38348636 "
```

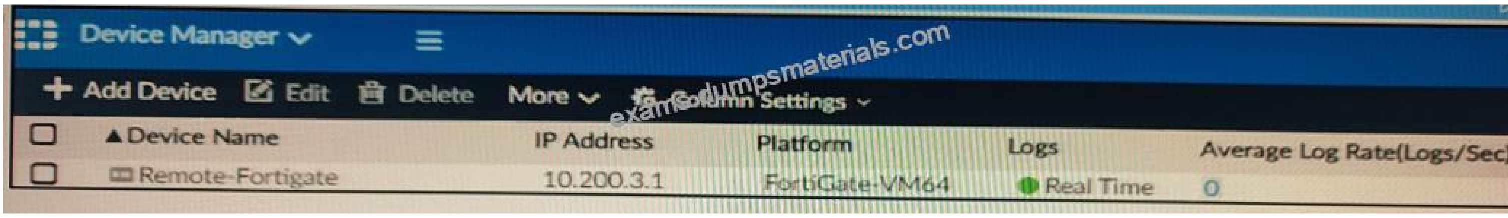
Which image corresponds to the packet capture shown in the exhibit?

A)



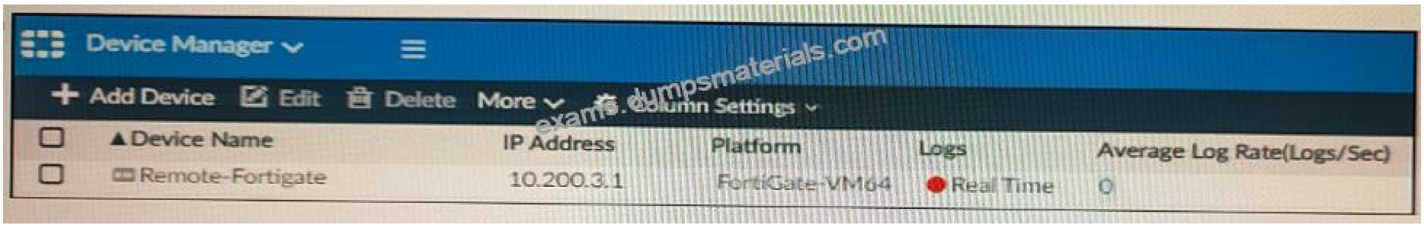
☐	▲Device Name	IP Address	Platform	Logs
☐	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time

B)



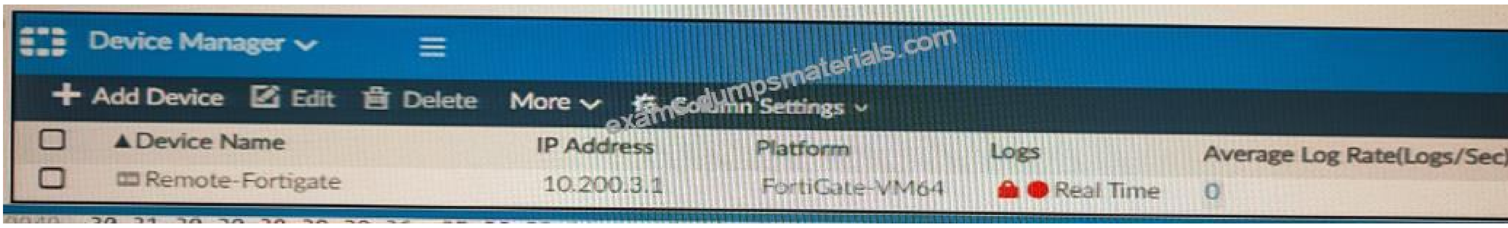
☐	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
☐	Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	0

C)



□	Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	0

D)



□	Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time	0

* Option A
* Option B
* Option C
* Option D

QUESTION 35

Which statements are correct regarding FortiAnalyzer reports? (Choose two)
* FortiAnalyzer provides the ability to create custom reports.
* FortiAnalyzer glows you to schedule reports to run.
* FortiAnalyzer includes pre-defined reports only.
* FortiAnalyzer allows reporting for FortiGate devices only.

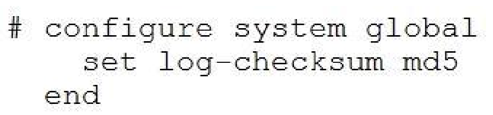
QUESTION 36

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results.

Similarly, which feature you can use for FortiView?
* Export to Report Chart
* Export to PDF
* Export to Chart Builder
* Export to Custom Chart

QUESTION 37

Consider the CLI command:



```
# configure system global
    set log-checksum md5
  end
```

What is the purpose of the command?
* To add a unique tag to each log to prove that it came from this FortiAnalyzer
* To add the MD5 hash value and authentication code
* To add a log file checksum
* To encrypt log communications
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

QUESTION 38

What are two advantages of setting up fabric ADOM? (Choose two.)
* It can be used for fast data processing and log correlation
* It can be used to facilitate communication between devices in same Security Fabric
* It can include all Fortinet devices that are part of the same Security Fabric
* It can include only FortiGate devices that are part of the same Security Fabric
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

QUESTION 39

What purposes does the auto-cache setting on reports serve? (Choose two.)
* To reduce report generation time
* To automatically update the hcache when new logs arrive
* To reduce the log insert lag rate
* To provide diagnostics on report generation time

QUESTION 40

If the primary FortiAnalyzer in an HA cluster fails, how is the new primary elected?
* The configured IP address is checked first.
* The active port number is checked first.
* The firmware version is checked first.
* The configured priority is checked first
In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:

* All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.

* If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.

* If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.

FortiAnalyzer_7.0_Study_Guide-Online page 62

QUESTION 41

Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

* First, upgrade the secondary device, and then upgrade the primary device.

* Both FortiAnalyzer devices will be upgraded at the same time.

* You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.

* You can perform the firmware upgrade using only a console connection.

QUESTION 42

The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.

What can be the reason for this failure?

* FortiAnalyzer is in an HA cluster.

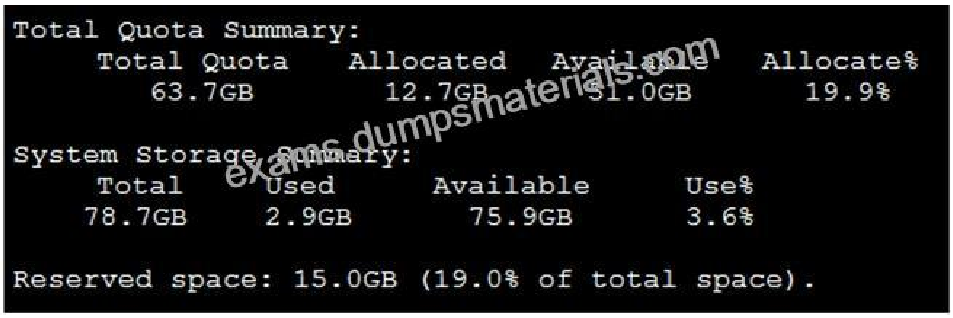
* ADOM mode should be set to advanced, in order to register the FortiClient EMS device.

* ADOMs are not enabled on FortiAnalyzer.

* A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

QUESTION 43

View the exhibit.



```
Total Quota Summary:
     Total Quota    Allocated    Available    Allocate%
        63.7GB        12.7GB       51.0GB        19.9%

System Storage Summary:
     Total      Used       Available      Use%
     78.7GB     2.9GB        75.9GB       3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?

* 3.6% of the system storage is already being used.

* Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files

* The oftpd process has not archived the logs yet

* The logfiled process is just estimating the total quota

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

QUESTION 44

Which two methods are the most common methods to control and restrict administrative access on FortiAnalyzer? (Choose two.)

* Virtual domains

* Administrative access profiles

* Trusted hosts

* Security Fabric
Reference:

https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts

QUESTION 45

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?
* Incidents dashboards
* Threat hunting
* FortiView Monitor
* Outbreak alert services
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

QUESTION 46

Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)
* FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
* FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
* All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
* FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

New NSE5_FAZ-7.0 Dumps - Real Fortinet Exam Questions:
https://www.dumpsmaterials.com/NSE5_FAZ-7.0-real-torrent.html]