Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

https://www.2passeasy.com/dumps/NSE5_FAZ-7.2/

NEW QUESTION 1
What is Log Insert Lag Time on FortiAnalyzer?

A. The number of times in the logs where end users experienced slowness while accessing resources.
B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Answer: C

NEW QUESTION 2
Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

A. Mail server
B. Output profile
C. SFTP server
D. Report scheduling

Answer: AB

NEW QUESTION 3
Which two statements express the advantages of grouping similar reports? (Choose two.)

A. Improve report completion time.
B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
C. Reduce the number of hcache tables and improve auto-hcache completion time.
D. Provides a better summary of reports.

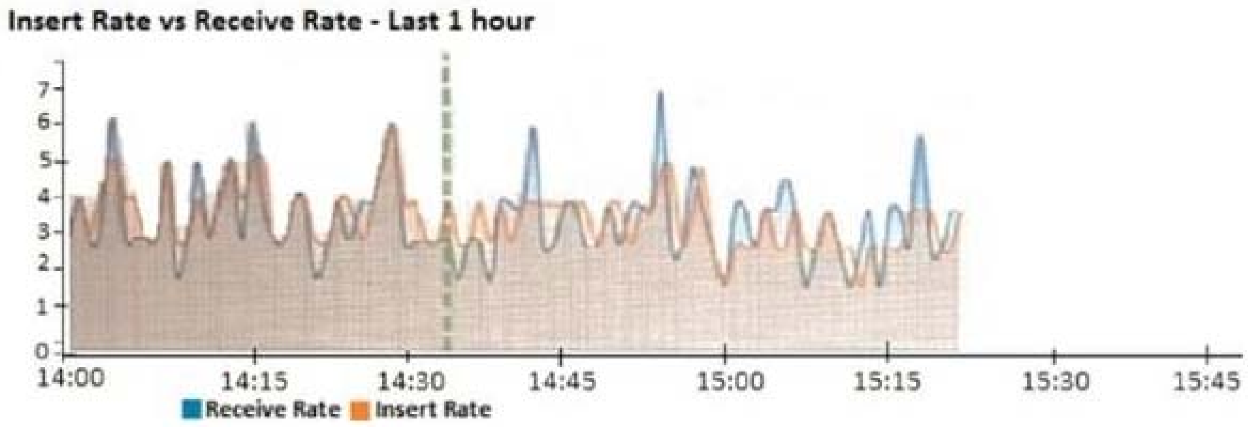
Answer: AC

NEW QUESTION 4
What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

A. FortiAnalyzer distinguishes different devices by their serial number.
B. FortiAnalyzer receives logs from d devices in a duster.
C. FortiAnalyzer receives bgs only from the primary device in the cluster.
D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

Answer: AB

NEW QUESTION 5
View the exhibit.



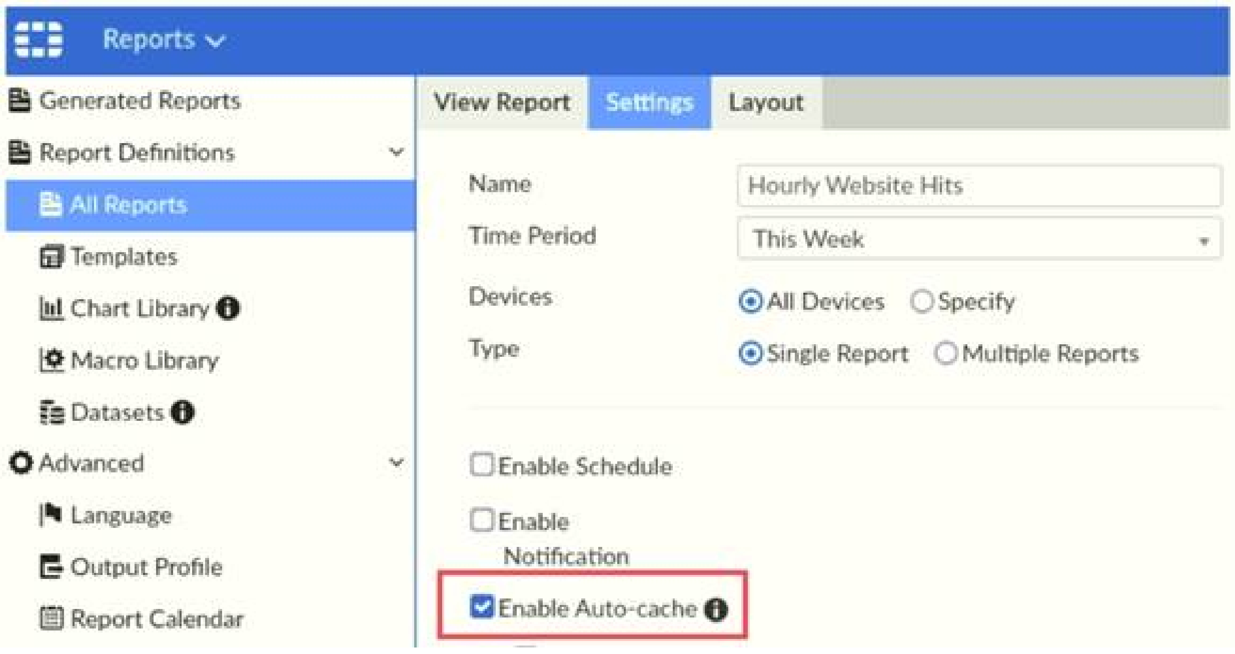
What does the data point at 14:35 tell you?

A. FortiAnalyzer is dropping logs.
B. FortiAnalyzer is indexing logs faster than logs are being received.
C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi

NEW QUESTION 6
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.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.
B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

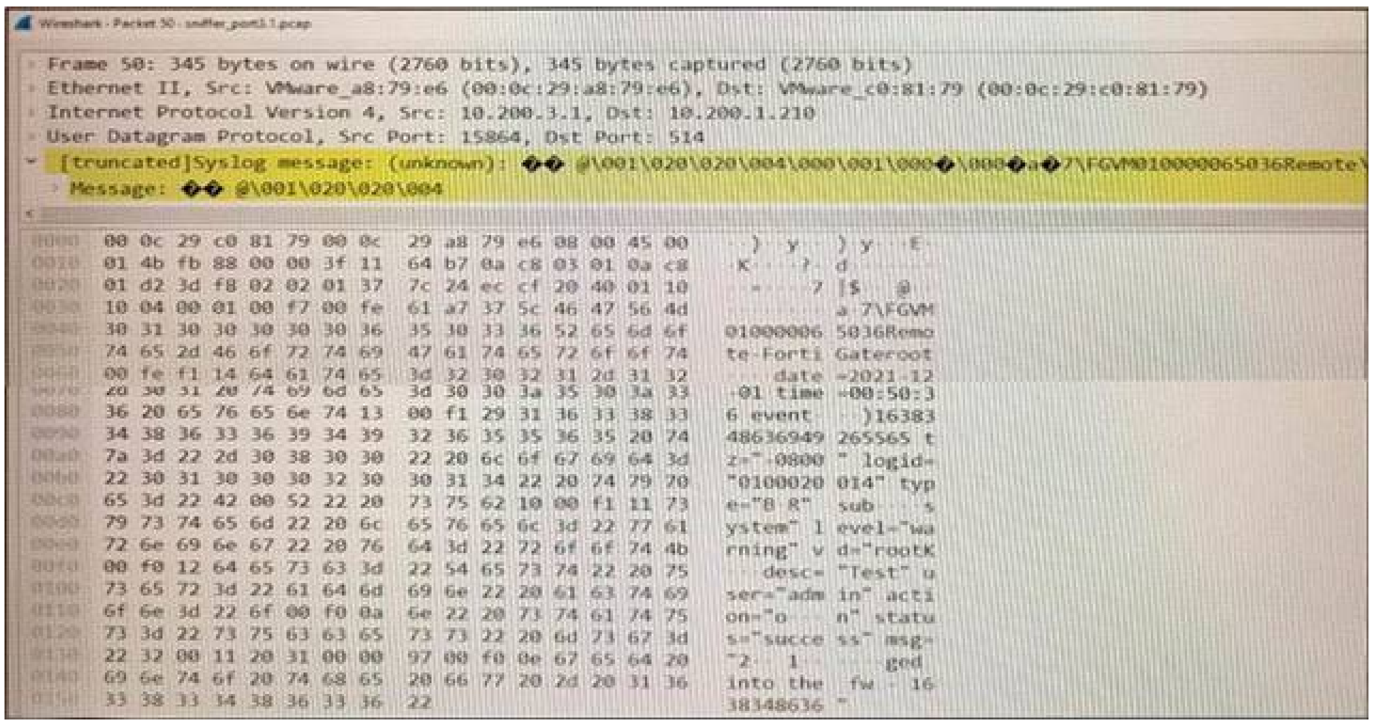
Answer: CD

NEW QUESTION 7
Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)

A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
B. Collector mode is the default operating mode.
C. When in collector mod
D. FortiAnalyzer supports event management and reporting features.
E. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting

Answer: AD

NEW QUESTION 8
Refer to the exhibit.

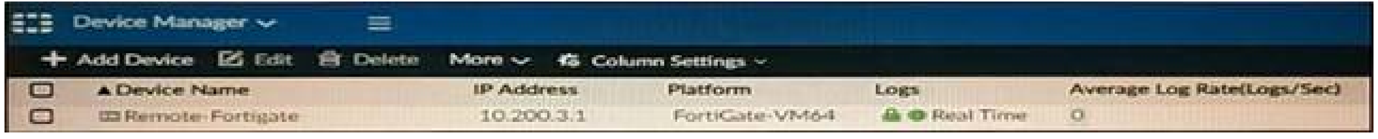


```
> Frame 50: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: VMware_a8:79:e6 (00:0c:29:a8:79:e6), Dst: VMware_c0:81:79 (00:0c:29:c0:81:79)
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 15864, Dst Port: 514
v [truncated]Syslog message: (unknown): �� @\001\020\020\004\000\001\000�\000�a�7\FGVM010000065036Remote\
  > 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 cf 20 40 01 10   ..=....7 |$.. @..
0030  10 04 00 01 00 f7 00 fe  61 a7 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  20 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 "
```

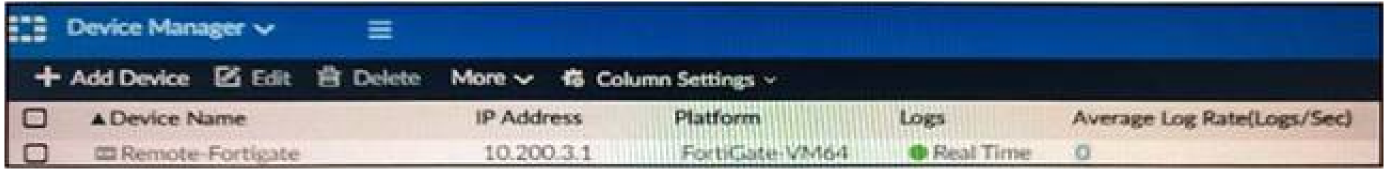
Which image corresponds to the packet capture shown in the exhibit?

A)



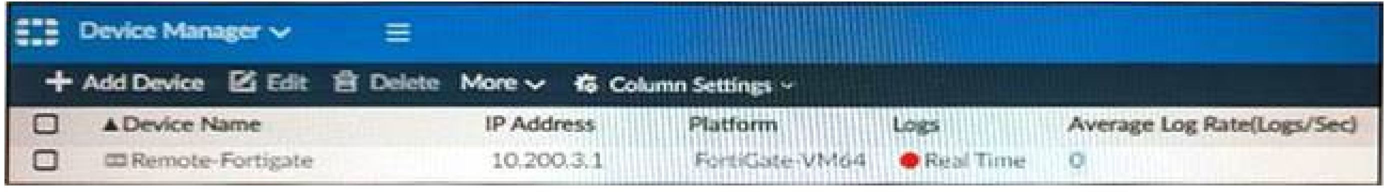
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	🔒 ● Real Time	0

B)



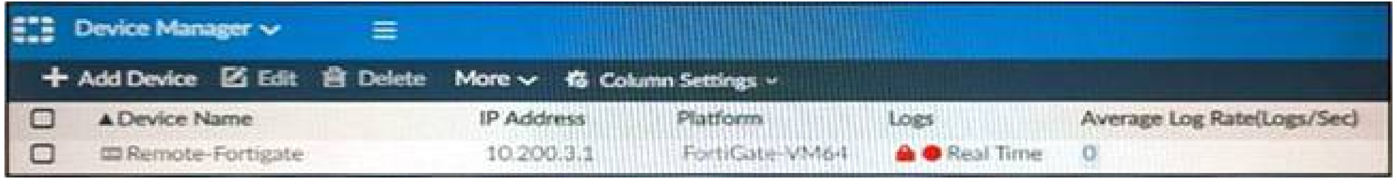
□	▲Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-Fortigate	10.200.3.1	FortiGate-VM64	● Real Time	0

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

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

Answer: D

NEW QUESTION 9
Which statement is true about sending notifications with incident updates?

A. Notifications can be sent only when an incident is updated or deleted.
B. If you use multiple fabric connectors, all connectors must have the same notification settings
C. Notifications can be sent only by email.
D. You can send notifications to multiple external platforms

Answer: A

NEW QUESTION 10
Which FortiAnalyzer feature allows you to retrieve the archived logs matching a specific timeframe from another FortiAnalyzer device?

A. Log upload
B. Indicators of Compromise
C. Log forwarding an aggregation mode
D. Log fetching

Answer: D

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/651442/fetcher-management

NEW QUESTION 10
You’ve moved a registered logging device out of one ADOM and into a new ADOM. What happens when you rebuild the new ADOM database?

A. FortiAnalyzer resets the disk quota of the new ADOM to default.
B. FortiAnalyzer migrates archive logs to the new ADOM.
C. FortiAnalyzer migrates analytics logs to the new ADOM.
D. FortiAnalyzer removes logs from the old ADOM.

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40383

NEW QUESTION 12
You crested a playbook on FortiAnalyzer that uses a FortiOS connector
When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stitch are available in the FortiOS connector?

A. FortiAnalyzer Event Handler
B. Incoming webhook
C. FortiOS Event Log
D. Fabric Connector event

Answer: D

NEW QUESTION 17
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

Answer: AD

Explanation:
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."

NEW QUESTION 18
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards
B. Threat hunting
C. FortiView Monitor
D. Outbreak alert services

Answer: B

NEW QUESTION 20
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

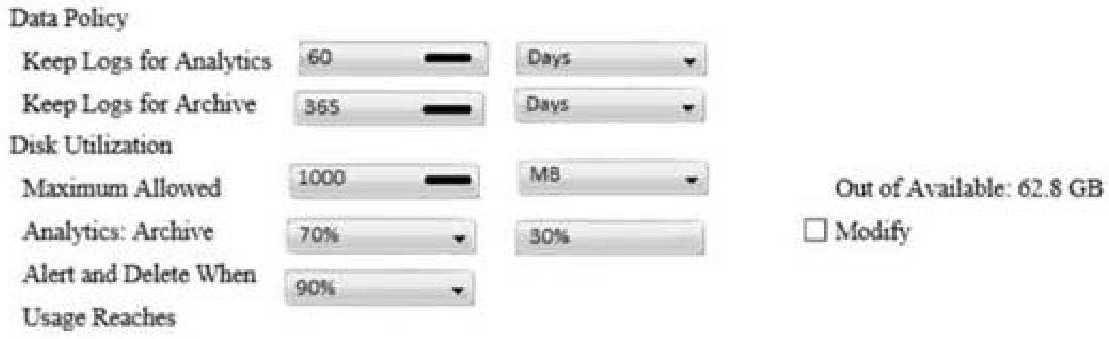
NEW QUESTION 22
How does FortiAnalyzer retrieve specific log data from the database?

A. SQL FROM statement
B. SQL GET statement
C. SQL SELECT statement
D. SQL EXTRACT statement

Answer: A

Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/137bb60e-ff37-11e8-8524-f8bc1258b8

NEW QUESTION 23
View the exhibit:



Data Policy
Keep Logs for Analytics 60 Days
Keep Logs for Archive 365 Days
Disk Utilization
Maximum Allowed 1000 MB Out of Available: 62.8 GB
Analytics: Archive 70% 30% □ Modify
Alert and Delete When Usage Reaches 90%

What does the 1000MB maximum for disk utilization refer to?

A. The disk quota for the FortiAnalyzer model
B. The disk quota for all devices in the ADOM
C. The disk quota for each device in the ADOM
D. The disk quota for the ADOM type

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-pol

NEW QUESTION 26
Which two statements are true regarding fabric connectors? (Choose two.)

A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.
B. Fabric connectors allow to save storage costs and improve redundancy.
C. Storage connector service does not require a separate license to send logs to cloud platform.
D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

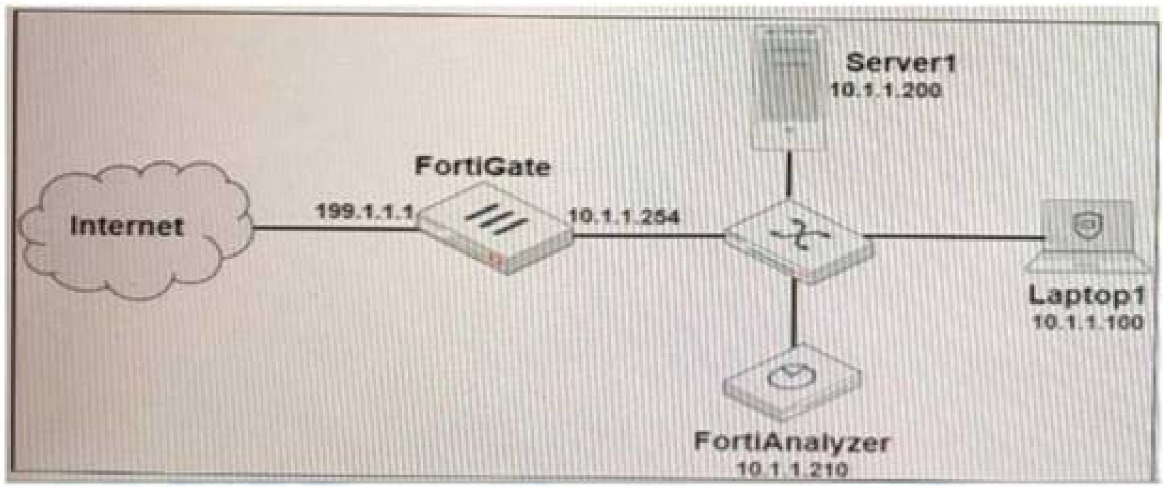
NEW QUESTION 31
What are the operating modes of FortiAnalyzer? (Choose two)

A. Standalone
B. Manager
C. Analyzer

D. Collector

Answer: CD

NEW QUESTION 34
Refer to the exhibit.



Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

A. operation—login & performed_on==BGUI(10.1.1.100)" & userl=admin
B. operation—login & srcip=10.1 -1.100 & dstip==10 1.1.210 & user=admin
C. operation—login & performed1_on=,'GUI(10.1.1.210)" & user!=admin
D. operation—login & dstip=10.1 . 1.2.10 & user1—admin

Answer: C

NEW QUESTION 35
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

NEW QUESTION 39
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.

Answer: D

NEW QUESTION 44
What purposes does the auto-cache setting on reports serve? (Choose two.)

A. To reduce report generation time
B. To automatically update the hcache when new logs arrive
C. To reduce the log insert lag rate
D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 49
Which statement is true when you are upgrading the firmware on an HA cluster made up of two FortiAnalyzer devices?

A. First, upgrade the secondary device, and then upgrade the primary device.
B. Both FortiAnalyzer devices will be upgraded at the same time.
C. You can enable uninterruptible-upgrade so that the normal FortiAnalyzer operations are not interrupted while the cluster firmware upgrades.
D. You can perform the firmware upgrade using only a console connection.

Answer: D

NEW QUESTION 54
What statements are true regarding disk log quota? (Choose two)

A. The FortiAnalyzer stops logging once the disk log quota is met.
B. The FortiAnalyzer automatically sets the disk log quota based on the device.
C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
D. The FortiAnalyzer disk log quota is configurable, but has a minimum o 100mb a maximum based on the reserved system space.

Answer: CD

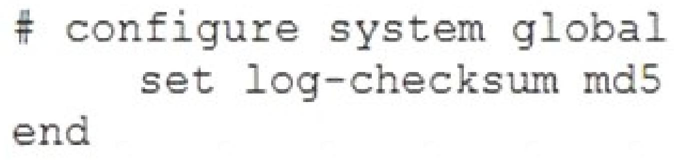
NEW QUESTION 55
How do you restrict an administrator's access to a subset of your organization's ADOMs?

A. Set the ADOM mode to Advanced
B. Assign the ADOMs to the administrator's account
C. Configure trusted hosts
D. Assign the default Super_User administrator profile

Answer: B

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to

NEW QUESTION 56
What is the purpose of the following CLI command?



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

A. To add a log file checksum
B. To add the MD's hash value and authentication code
C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
D. To encrypt log communications

Answer: A

Explanation:
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

NEW QUESTION 59
Which daemon is responsible for enforcing the log file size?

A. sqlplugind
B. logfiled
C. miglogd
D. ofrpd

Answer: B

NEW QUESTION 63
Which tabs do not appear when FortiAnalyzer is operating in Collector mode?

A. FortiView
B. Event Management
C. Device Manger
D. Reporting

Answer: B

NEW QUESTION 67
An administrator has configured the following settings:
config system global
set log-checksum md5-auth end
What is the significance of executing this command?

A. This command records the log file MD5 hash value.
B. This command records passwords in log files and encrypts them.
C. This command encrypts log transfer between FortiAnalyzer and other devices.
D. This command records the log file MD5 hash value and authentication code.

Answer: D

NEW QUESTION 72
Which two purposes does the auto cache setting on reports serve? (Choose two.)

A. It automatically updates the hcache when new logs arrive.

B. It provides diagnostics on report generation time.
C. It reduces the log insert lag rate.
D. It reduces report generation time.

Answer: AD

NEW QUESTION 74
When you perform a system backup, what does the backup configuration contain? (Choose two.)

A. Generated reports
B. Device list
C. Authorized devices logs
D. System information

Answer: BD

Explanation:
https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 79
FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?

A. To upload logs to an SFTP server
B. To prevent log modification during backup
C. To send an identical set of logs to a second logging server
D. To encrypt log communication between devices

Answer: D

NEW QUESTION 80
Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

A. Antivirus logs
B. Web filter logs
C. IPS logs
D. Application control logs

Answer: B

NEW QUESTION 85
Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
B. Must establish an IPsec tunnel ID and pre-shared key.
C. IPsec cannot be enabled if SSL is enabled as well.
D. IPsec is only enabled through the CLI on FortiAnalyzer.

Answer: C

NEW QUESTION 87
What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

A. RADIUS
B. Local
C. LDAP
D. PKI
E. TACACS+

Answer: ACE

NEW QUESTION 92
What are two advantages of setting up fabric ADOM? (Choose two.)

A. It can be used for fast data processing and log correlation
B. It can be used to facilitate communication between devices in same Security Fabric
C. It can include all Fortinet devices that are part of the same Security Fabric
D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a

NEW QUESTION 94
An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be presented in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BD

NEW QUESTION 95
Logs are being deleted from one of your ADOMs earlier that the configured setting for archiving in your data policy. What is the most likely problem?

A. The total disk space is insufficient and you need to add other disk.
B. CPU resources are too high.
C. The ADOM disk quota is set too low based on log rates.
D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

NEW QUESTION 99
What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

A. SFTP, FTP, or SCP server
B. Mail server
C. Output profile
D. Report scheduling

Answer: BC

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

NEW QUESTION 104
By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.
B. FortiAnalyzer stops logging.
C. FortiAnalyzer rolls the active log by renaming the file.
D. FortiAnalyzer forwards logs to syslog.

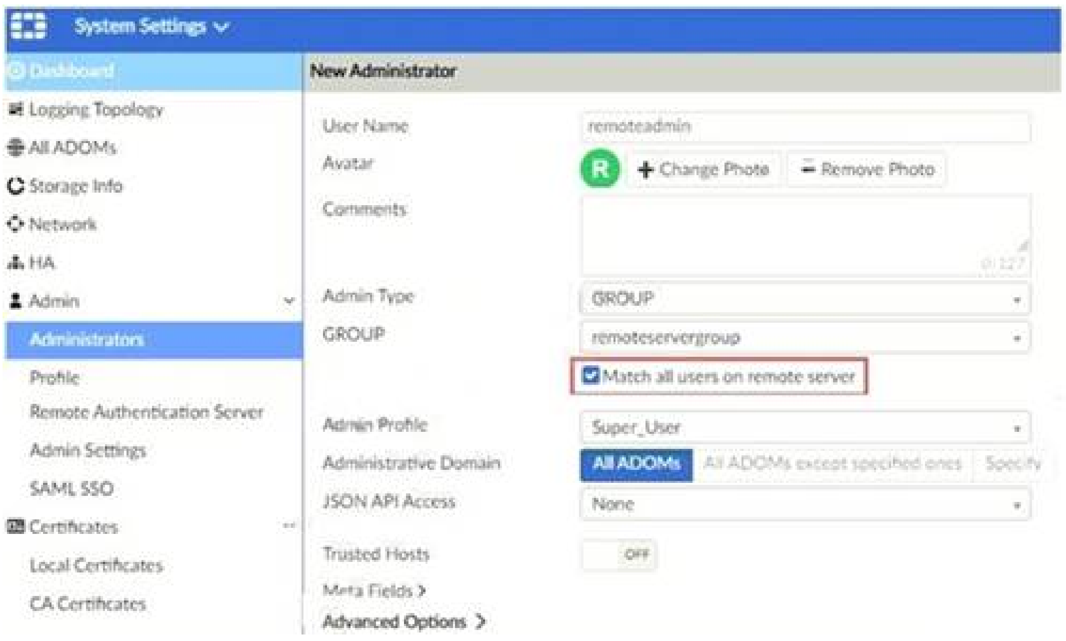
Answer: C

NEW QUESTION 108
Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

A. FROM
B. LIMIT
C. WHERE
D. ORDER BY

Answer: A

NEW QUESTION 111
Refer to the exhibit.



New Administrator

User Name: remoteadmin
Avatar: R
Comments: 0/127
Admin Type: GROUP
GROUP: remoteservergroup
☑ Match all users on remote server
Admin Profile: Super_User
Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify
JSON API Access: None
Trusted Hosts: OFF

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling “Match all users on remote server” when
configuring a new administrator? (Choose two.)

A. It creates a wildcard administrator using LDAP and RADIUS servers.
B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 115
What two things should an administrator do to view Compromised Hosts on FortiAnalyzer? (Choose two.)

A. Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
B. Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer.
C. Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up-to-date.
D. Make sure all endpoints are reachable by FortiAnalyzer.

Answer: BC

NEW QUESTION 117
An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.
What could be the problem?

A. Fortinet is assigned the Standard_ User administrator profile.
B. A trusted host is configured.
C. ADOM mode is configured with Advanced mode.
D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

NEW QUESTION 121
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?

A. Export to Report Chart
B. Export to PDF
C. Export to Chart Builder
D. Export to Custom Chart

Answer: A

NEW QUESTION 126
......